



用户指南

AWS Systems Manager 自动化运行手册参考



AWS Systems Manager 自动化运行手册参考: 用户指南

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

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

自动化运行手册参考	1
查看运行手册内容	3
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	4
AWSConfigRemediation-EnableAPIGatewayTracing	5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWSSupport-TroubleshootAPIGatewayCustomDomainConfig	8
AWSSupport-TroubleshootAPIGatewayHttpErrors	12
AWS Batch	16
AWSSupport-TroubleshootAWSBatchJob	17
CloudFormation	22
AWS-DeleteCloudFormationStack	22
AWS-EnableCloudFormationSNSNotification	23
AWS-RunCfnLint	25
AWSSupport-TroubleshootCFNCustomResource	27
AWS-UpdateCloudFormationStack	29
CloudFront	30
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	30
AWSConfigRemediation-EnableCloudFrontAccessLogs	31
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	33
AWSConfigRemediation-EnableCloudFrontOriginFailover	35
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	36
CloudTrail	38
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	38
AWS-EnableCloudTrail	40
AWS-EnableCloudTrailCloudWatchLogs	41
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	43
AWS-EnableCloudTrailKmsEncryption	44
AWSConfigRemediation-EnableCloudTrailLogFileValidation	45
AWS-EnableCloudTrailLogFileValidation	47
AWS-QueryCloudTrailLogs	48
CloudWatch	50
AWS-ConfigureCloudWatchOnEC2Instance	50
AWS-EnableCWAlarm	51

AWSSupport-TroubleshootCloudWatchAgent	54
AWSSupport-TroubleshootCloudWatchAlarm	60
Amazon DocumentDB	67
AWS-EnableDocDbClusterBackupRetentionPeriod	67
CodeBuild	69
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK	69
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	71
AWS CodeDeploy	72
AWSSupport-TroubleshootCodeDeploy	72
AWS Config	74
AWSSupport-SetupConfig	74
Connect Customer	77
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	77
AWSSupport-CollectAmazonConnectContactFlowLog	85
AWS Directory Service	90
AWS-CreateDSManagementInstance	90
AWSSupport-TroubleshootADConnectorConnectivity	95
AWSSupport-TroubleshootDirectoryTrust	98
AWS AppSync	101
AWS-EnableAppSyncGraphQLApiLogging	102
Amazon Athena	104
AWS-EnableAthenaWorkGroupEncryptionAtRest	104
DynamoDB	106
AWS-ChangeDDBRWCapacityMode	107
AWS-CreateDynamoDBBackup	109
AWS-DeleteDynamoDbBackup	110
AWSConfigRemediation-DeleteDynamoDbTable	111
AWS-DeleteDynamoDbTableBackups	112
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	113
AWSConfigRemediation-EnablePITRForDynamoDbTable	115
AWS-EnableDynamoDbAutoscaling	116
AWS-RestoreDynamoDBTable	119
AWS Database Migration Service	121
AWSSupport-TroubleshootDMSTableErrors	121
AWSSupport-TroubleshootDMSEndpointConnection	127
Amazon EBS	135

AWSSupport-AnalyzeEBSResourceUsage	136
AWS-ArchiveEBSVolumeSnapshots	142
AWS-AttachEBSVolume	144
AWSSupport-CalculateEBSPerformanceMetrics	145
AWS-CopySnapshot	152
AWS-CreateSnapshot	153
AWS-DeleteSnapshot	154
AWSConfigRemediation-DeleteUnusedEBSVolume	155
AWS-DeregisterAMIs	156
AWS-DetachEBSVolume	158
AWSConfigRemediation-EnableEbsEncryptionByDefault	159
AWS-ExtendEbsVolume	160
AWSSupport-ModifyEBSSnapshotPermission	162
AWSConfigRemediation-ModifyEBSVolumeType	164
Amazon EC2	166
AWS-ASGEnterStandby	168
AWS-ASGExitStandby	169
AWS-CreateImage	170
AWS-DeleteImage	171
AWS-PatchAsgInstance	173
AWS-PatchInstanceWithRollback	175
AWS-QuarantineEC2Instance	177
AWS-ResizeInstance	179
AWS-RestartEC2Instance	180
AWS-SetupJupyter	181
AWS-StartEC2Instance	185
AWS-StopEC2Instance	185
AWS-TerminateEC2Instance	186
AWS-UpdateLinuxAmi	187
AWS-UpdateWindowsAmi	191
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	194
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	196
AWSEC2-CloneInstanceAndUpgradeSQLServer	197
AWSEC2-CloneInstanceAndUpgradeWindows	201
AWSEC2-PatchLoadBalancerInstance	204
AWSEC2-SQLServerDBRestore	206

AWSSupport-ActivateWindowsWithAmazonLicense	211
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	213
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	217
AWSSupport-CheckXenToNitroMigrationRequirements	222
AWSSupport-CloneXenEC2InstanceAndMigrateToNitro	225
AWSSupport-CollectSAPHANALogs	232
AWSSupport-ConfigureEC2Metadata	238
AWSSupport-ContainEC2Instance	241
AWSSupport-CopyEC2Instance	251
AWSPremiumSupport-DiagnoseDiskUsageOnLinux	255
AWSSupport-EnableWindowsEC2SerialConsole	259
AWSPremiumSupport-ExtendVolumesOnWindows	266
AWSSupport-ExecuteEC2Rescue	270
AWSSupport-ListEC2Resources	273
AWSSupport-ManageRDPSettings	275
AWSSupport-ManageWindowsService	277
AWSSupport-MigrateEC2ClassicToVPC	279
AWSSupport-MigrateXenToNitroLinux	285
AWSSupport-ResetAccess	295
AWSSupport-ResetLinuxUserPassword	298
AWSSupport-RunEC2RescueForWindowsTool	304
AWSPremiumSupport-ResizeNitroInstance	307
AWSSupport-ShareEncryptedAMIOrEBSSnapshot	313
AWSSupport-RestoreEC2InstanceFromSnapshot	318
AWSSupport-SendLogBundleToS3Bucket	322
AWSSupport-StartEC2RescueWorkflow	323
AWSSupport-TroubleshootActiveDirectoryReplication	333
AWSPremiumSupport-TroubleshootEC2DiskUsage	338
AWSSupport-TroubleshootEC2InstanceConnect	343
AWSSupport-TroubleshootLinuxMGNDRAgentLogs	348
AWSSupport-TroubleshootRDP	351
AWSSupport-TroubleshootSSH	357
AWSSupport-TroubleshootSUSERegistration	360
AWSSupport-TroubleshootWindowsPerformance	362
AWSSupport-TroubleshootWindowsUpdate	369
AWSSupport-UpgradeWindowsAWSDrivers	375

Amazon ECS	379
AWSSupport-CollectECSInstanceLogs	379
AWS-InstallAmazonECSAgent	381
AWS-ECSRunTask	383
AWSSupport-TroubleshootECSContainerInstance	386
AWSSupport-TroubleshootECSTaskFailedToStart	388
AWS-UpdateAmazonECSAgent	392
Amazon EFS	394
AWSSupport-CheckAndMountEFS	394
Amazon EKS	397
AWS-CreateEKSClusterWithFargateProfile	398
AWS-CreateEKSClusterWithNodegroup	401
AWS-DeleteEKSCluster	404
AWS-MigrateToNewEKSSelfManagedNodeGroup	407
AWSPremiumSupport-TroubleshootEKSCluster	413
AWSSupport-TroubleshootEKSWorkerNode	416
AWS-UpdateEKSCluster	418
AWS-UpdateEKSMangedNodeGroup	420
AWS-UpdateEKSSelfManagedLinuxNodeGroups	424
AWSSupport-CollectEKSLinuxNodeStatistics	427
AWSSupport-CollectEKSInstanceLogs	433
AWSSupport-SetupK8sApiProxyForEKS	436
AWSSupport-TroubleshootEbsCsiDriversForEks	446
AWSSupport-TroubleshootEKSSALBControllerIssues	455
AWSSupport-TroubleshootEKSDNSFailure	466
Elastic Beanstalk	470
AWSSupport-CollectElasticBeanstalkLogs	471
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	473
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	475
AWSSupport-TroubleshootElasticBeanstalk	476
Elastic Load Balancing	479
AWSConfigRemediation-DropInvalidHeadersForALB	480
AWS-EnableCLBAccessLogs	481
AWS-EnableCLBConnectionDraining	483
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	484
AWSConfigRemediation-EnableELBDeletionProtection	485

AWSConfigRemediation-EnableLoggingForALBAndCLB	487
AWSSupport-TroubleshootCLBConnectivity	488
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	491
AWS-UpdateALBDesyncMitigationMode	493
AWS-UpdateCLBDesyncMitigationMode	494
AWSSupport-TroubleshootELBHealthChecks	496
Amazon EMR	500
AWSSupport-AnalyzeEMRLogs	501
AWSSupport-DiagnoseEMRLogsWithAthena	506
亚马逊 OpenSearch 服务	514
AWSConfigRemediation-DeleteOpenSearchDomain	514
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	515
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	517
AWSSupport-TroubleshootOpenSearchRedYellowCluster	518
AWSSupport-TroubleshootOpenSearchHighCPU	524
EventBridge	530
AWS-AddOpsItemDedupStringToEventBridgeRule	530
AWS-DisableEventBridgeRule	532
AWS Glue	533
AWSSupport-TroubleshootGlueConnection	533
Amazon FSx	544
AWSSupport-ValidateFSxWindowsADConfig	545
GuardDuty	558
AWSConfigRemediation-CreateGuardDutyDetector	559
IAM	560
AWSSupport-TroubleshootIAMAccessDeniedEvents	560
AWS-AttachIAMToInstance	566
AWS-DeleteIAMInlinePolicy	569
AWSConfigRemediation-DeleteIAMRole	570
AWSConfigRemediation-DeleteIAMUser	571
AWSConfigRemediation-DeleteUnusedIAMGroup	574
AWSConfigRemediation-DeleteUnusedIAMPolicy	575
AWSConfigRemediation-DetachIAMPolicy	576
AWSConfigRemediation-EnableAccountAccessAnalyzer	578
AWSSupport-GrantPermissionsToIAMUser	579
AWSConfigRemediation-RemoveUserPolicies	584

AWSConfigRemediation-ReplaceIAMInlinePolicy	585
AWSConfigRemediation-RevokeUnusedIAMUserCredentials	587
AWSConfigRemediation-SetIAMPasswordPolicy	589
AWSSupport-ContainIAMPrincipal	592
AWSSupport-TroubleshootSAMLIssues	604
事件检测和响应	609
AWSPremiumSupport-OnboardWorkloadToIDR	610
Amazon Kinesis Data Streams	616
AWS-EnableKinesisStreamEncryption	617
AWS KMS	618
AWSConfigRemediation-CancelKeyDeletion	619
AWSConfigRemediation-EnableKeyRotation	620
Lambda	621
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	621
AWSConfigRemediation-DeleteLambdaFunction	623
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	624
AWSConfigRemediation-MoveLambdaToVPC	625
AWSSupport-RemediateLambdaS3Event	627
AWSSupport-TroubleshootLambdaInternetAccess	629
AWSSupport-TroubleshootLambdaS3Event	633
Amazon Managed Workflows for Apache Airflow	634
AWSSupport-TroubleshootMWAAEnvironmentCreation	634
Neptune	641
AWS-EnableNeptuneDbAuditLogsToCloudWatch	641
AWS-EnableNeptuneDbBackupRetentionPeriod	642
AWS-EnableNeptuneClusterDeletionProtection	644
Amazon RDS	646
AWS-CreateEncryptedRdsSnapshot	647
AWS-CreateRdsSnapshot	649
AWSConfigRemediation-DeleteRDSCluster	650
AWSConfigRemediation-DeleteRDSClusterSnapshot	652
AWSConfigRemediation-DeleteRDSInstance	653
AWSConfigRemediation-DeleteRDSInstanceSnapshot	655
AWSConfigRemediation-DisablePublicAccessToRDSInstance	656
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	657
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	659

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	660
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance	662
AWSConfigRemediation-EnableMultiAZOnRDSInstance	663
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	665
AWSConfigRemediation-EnableRDSClusterDeletionProtection	667
AWSConfigRemediation-EnableRDSInstanceBackup	668
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	670
AWSConfigRemediation-ModifyRDSInstancePortNumber	672
AWSSupport-ModifyRDSSnapshotPermission	673
AWSPremiumSupport-PostgreSQLWorkloadReview	675
AWS-RebootRdsInstance	690
AWSSupport-ShareRDSSnapshot	691
AWS-StartRdsInstance	694
AWS-StartStopAuroraCluster	695
AWS-StopRdsInstance	697
AWSSupport-TroubleshootConnectivityToRDS	698
AWSSupport-TroubleshootRDSIAMAuthentication	700
AWSSupport-ValidateRdsNetworkConfiguration	707
Amazon Redshift	712
AWSConfigRemediation-DeleteRedshiftCluster	713
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	714
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	716
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	717
AWSConfigRemediation-EnableRedshiftClusterEncryption	719
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	720
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	721
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	723
AWSConfigRemediation-ModifyRedshiftClusterNodeType	724
Amazon S3	726
AWS-ArchiveS3BucketToIntelligentTiering	727
AWS-ConfigureS3BucketLogging	729
AWS-ConfigureS3BucketVersioning	731
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	732
AWSConfigRemediation-ConfigureS3PublicAccessBlock	734
AWS-CreateS3PolicyToExpireMultipartUploads	736
AWS-DisableS3BucketPublicReadWrite	738

AWS-EnableS3BucketEncryption	739
AWS-EnableS3BucketKeys	740
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	742
AWSConfigRemediation-RestrictBucketSSLRequestsOnly	743
AWSSupport-TroubleshootS3PublicRead	744
AWSSupport-ConfigureS3ReplicationSameAndCrossAccount	750
AWSSupport-EmptyS3Bucket	767
AWSSupport-TroubleshootS3EventNotifications	774
AWSSupport-ContainS3Resource	781
Amazon SES	789
AWSSupport-AnalyzeSESMessagesSendingStatus	789
AWSSupport-DeploySESSendingLogsToCloudWatchLogs	792
SageMaker AI	798
AWS-DisableSageMakerNotebookRootAccess	798
AWSSupport-RequestSageMakerLimitIncrease	800
Secrets Manager	804
AWSConfigRemediation-DeleteSecret	804
AWSConfigRemediation-RotateSecret	805
Security Hub CSPM	807
AWSConfigRemediation-EnableSecurityHub	807
AWS Shield	808
AWSPremiumSupport-DDoSResiliencyAssessment	809
Amazon SNS	817
AWS-EnableSNSTopicDeliveryStatusLogging	817
AWSConfigRemediation-EncryptSNSTopic	819
AWS-PublishSNSNotification	821
Amazon SQS	822
AWS-EnableSQSEncryption	822
Step Functions	824
AWS-EnableStepFunctionsStateMachineLogging	824
Systems Manager	826
AWS-BulkDeleteAssociation	827
AWS-BulkEditOpsItems	828
AWS-BulkResolveOpsItems	831
AWS-ConfigureMaintenanceWindows	833
AWS-CreateManagedLinuxInstance	835

AWS-CreateManagedWindowsInstance	837
AWSConfigRemediation-EnableCWLoggingForSessionManager	840
AWS-ExportOpsDataToS3	841
AWS-ExportPatchReportToS3	843
AWS-SetupInventory	844
AWS-SetupManagedInstance	848
AWS-SetupManagedRoleOnEC2Instance	850
AWSSupport-TroubleshootManagedInstance	851
AWSSupport-TroubleshootPatchManagerLinux	853
AWSSupport-TroubleshootSessionManager	857
Third-party	861
AWS-CreateJiraIssue	862
AWS-CreateServiceNowIncident	864
AWS-RunPacker	866
Amazon VPC	868
AWS-CloseSecurityGroup	869
AWSSupport-ConfigureDNSQueryLogging	870
AWSSupport-ConfigureTrafficMirroring	873
AWSSupport-ConnectivityTroubleshooter	876
AWSSupport-TroubleshootVPN	879
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	884
AWSConfigRemediation-DeleteUnusedENI	886
AWSConfigRemediation-DeleteUnusedSecurityGroup	887
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	888
AWSConfigRemediation-DeleteVPCFlowLog	889
AWSConfigRemediation-DetachAndDeleteInternetGateway	891
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	892
AWS-DisableIncomingSSHOnPort22	894
AWS-DisablePublicAccessForSecurityGroup	895
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	897
AWSSupport-EnableVPCFlowLogs	898
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	904
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	906
AWS-ReleaseElasticIP	908
AWS-RemoveNetworkACLUnrestrictedSSHRDP	909
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	910

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	911
AWSSupport-SetupIPMonitoringFromVPC	913
AWSSupport-TerminateIPMonitoringFromVPC	920
AWS WAF	923
AWS-AddWAFRegionalRuleToRuleGroup	924
AWS-AddWAFRegionalRuleToWebAcl	926
AWSConfigRemediation-EnableWAFCClassicLogging	928
AWSConfigRemediation-EnableWAFCClassicRegionalLogging	930
AWSConfigRemediation-EnableWAFV2Logging	931
Amazon WorkSpaces	933
AWS-CreateWorkSpace	933
AWSSupport-RecoverWorkSpace	936
X-Ray	940
AWSConfigRemediation-UpdateXRayKMSKey	940
.....	cmxlii

Systems Manager 自动化运行手册参考

为了帮助您快速入门，AWS Systems Manager 提供了预定义的运行手册。这些运行手册由 Amazon Web Services 和 AWS 支持 AWS Config、维护。《运行手册参考》描述了 Systems Manager 提供的每个预定义运行手册支持、和。AWS Config

Important

如果您运行使用 AWS Identity and Access Management (IAM) 服务角色调用其他服务的自动化工作流程，请注意必须使用权限将该服务角色配置为调用这些服务。该要求适用于所有 AWS 自动化运行手册（AWS-* 运行手册），例如 AWS-ConfigureS3BucketLogging、AWS-CreateDynamoDBBackup 和 AWS-RestartEC2Instance 运行手册等。此要求也适用于您创建的任何自定义 Automation 运行手册，这些运行手册通过调用其他 AWS 服务的操作来调用其他服务。例如，如果您使用 `aws:executeAwsApi`、`aws:createStack` 或 `aws:copyImage` 操作，则您必须配置具有权限的服务角色来调用这些服务。您可以通过向角色添加 IAM 内联策略来启用对其他 AWS 服务的权限。有关更多信息，请参阅[添加 Automation 内联策略以调用其他 AWS 服务](#)。

本参考资料包括描述由 AWS、AWS 支持和拥有的每个 Systems Manager 运行手册的主题。AWS Config 运行手册由相关 AWS 服务人员整理。每个页面都提供了使用运行手册时可以指定的必需参数和可选参数的说明。每个页面还列出了运行手册中的步骤和自动化的输出（如有）。

本参考不包括需要批准的运行手册的单独页面，例如 AWS-CreateManagedLinuxInstanceWithApproval 或 AWS-StopEC2InstanceWithApproval 运行手册。任何包含 WithApproval 的运行手册名称均表示运行手册包含 `aws:approve` 操作。此操作会临时暂停自动化执行，直至指定主体批准或拒绝操作。在达到所需批准数后，自动化执行将恢复。

有关运行自动化的信息，请参阅[运行简单自动化](#)。有关在多个目标上运行自动化的信息，请参阅[运行使用目标和速率控制的自动化](#)。

主题

- [查看运行手册内容](#)
- [API Gateway](#)
- [AWS Batch](#)
- [CloudFormation](#)

- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Connect Customer](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [AWS Database Migration Service](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)
- [亚马逊 OpenSearch 服务](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [事件检测和响应](#)
- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)

- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [Amazon SES](#)
- [SageMaker AI](#)
- [Secrets Manager](#)
- [Security Hub CSPM](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [Step Functions](#)
- [Systems Manager](#)
- [Third-party](#)
- [Amazon VPC](#)
- [AWS WAF](#)
- [Amazon WorkSpaces](#)
- [X-Ray](#)

查看运行手册内容

您可以在 Systems Manager 控制台查看运行手册的内容。

查看运行手册内容

1. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
2. 在导航窗格中，选择 文档。

–或者–

如果首先打开 AWS Systems Manager 主页，请选择菜单图标



以打开导航窗格，然后在导航窗格中选择“文档”。

3. 在类别部分，选择自动化文档。
4. 选择运行手册，然后选择查看详细信息。
5. 选择内容选项卡。

API Gateway

AWS Systems Manager 自动化为 Amazon API Gateway 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-DeleteAPIGatewayStage](#)
- [AWSConfigRemediation-EnableAPIGatewayTracing](#)
- [AWSConfigRemediation-UpdateAPIGatewayMethodCaching](#)
- [AWSSupport-TroubleshootAPIGatewayCustomDomainConfig](#)
- [AWSSupport-TroubleshootAPIGatewayHttpErrors](#)

AWSConfigRemediation-DeleteAPIGatewayStage

描述

AWSConfigRemediation-DeleteAPIGatewayStage运行手册删除了亚马逊 API Gateway (API Gateway) 阶段。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- StageArn

类型：字符串

描述：(必需) 要删除的 API 网关的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- apigateway:GET
- apigateway:DELETE

文档步骤

- aws:executeScript - 删除 StageArn 参数中指定的 API Gateway 阶段。

AWSConfigRemediation-EnableAPIGatewayTracing

描述

该AWSConfigRemediation-EnableAPIGatewayTracing运行手册支持在亚马逊 API Gateway (API Gateway) 阶段进行跟踪。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- StageArn

类型：字符串

描述：(必需) 要启用跟踪的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- config:GetResourceConfigHistory
- apigateway:GET
- apigateway:PATCH

文档步骤

- aws:executeScript- 对 StageArn 参数中指定的 API Gateway 阶段启用跟踪。

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

描述

AWSConfigRemediation-UpdateAPIGatewayMethodCaching 运行手册将更新 Amazon API Gateway 阶段资源的缓存方法设置。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- CachingAuthorizedMethods

类型：StringList

描述：(必需) 授权启用缓存的方法。该列表必须是 DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT 的某种组合。对选定方法启用缓存，对非选定方法禁用缓存。对所有选定 ANY 的方法启用缓存，对所有选定 NONE 的方法禁用缓存。

- StageArn

类型：字符串

描述：(必需) REST API 的 API Gateway 阶段 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- apigateway:PATCH
- apigateway:GET

文档步骤

- aws:executeScript - 接受阶段资源 ID 作为输入，使用 UpdateStage API 操作更新 API Gateway 阶段的缓存方法设置，并验证更新。

AWSSupport-TroubleshootAPIGatewayCustomDomainConfig

描述

该操作AWSSupport-TroubleshootAPIGatewayCustomDomainConfig手册可帮助您识别 Amazon API Gateway 中的自定义域名配置存在的问题。运行手册分析了以下配置步骤：

- 在 API Gateway 中创建了一个自定义域名。
- 自定义域名和相关 API 之间存在映射。
- 自定义域名存在一个 DNS 记录，该记录指向了正确的目标。

Important

本运行手册不支持对 API Gateway 自定义域名的 mTLS 问题进行故障排除。

Important

本运行手册仅支持对可公开解析的自定义域名进行故障排除。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- apigateway:GET
- route53:ListResourceRecordSets

示例 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "route53:ListResourceRecordSets"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

启动运行手册的 IAM 用户或角色需要执行以下操作：

- iam:ListRoles

- iam:PassRole
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeDocument
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:StartAutomationExecution

说明

按照这些步骤对自动化进行配置：

1. [AWSsupport-TroubleshootAPIGatewayCustomDomainConfig](#)在 Systems Manager 的“文档”下导航至。

2. 选择 Execute automation (执行自动化) 。

3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DomainName (必填)：

为您的 Amazon API Gateway API 创建的自定义域名。

- Apild (必填)：

您的 API Gateway 的 API ID。

- DNSServerIp (可选)：

用于解析自定义域名和 API Gateway 域名的 DNS 服务器的 IPv4 地址。如果未指定值，则将使用 AWS DNS 服务器 (169.254.169.253)。

- HostedZoneId (可选)：

在 Amazon Route 53 中创建自定义域名的 DNS 记录的公共托管区域 ID。如果 Route 53 未用于 DNS，则该值不是必需的。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **CheckAPIExists:**

检查是否存在亚马逊 API Gateway API。

- **GetDomainName:**

获取在 Amazon API Gateway 中配置的自定义域名的详细信息。

- **GetMappings:**

检索为自定义域名配置的所有 Amazon API Gateway API 映射，并验证指定的 API ID 是否具有具有正确阶段和路径配置的有效映射。

- **CheckDNSRecordExists:**

检查自定义域名 DNS 并返回关联的记录。

- **ValidateDNSResults:**

比较自定义域名的 DNS 详细信息（A 或 CNAME 记录），确保记录指向正确的 Amazon API Gateway 分配域名。

- **Results:**

格式化 Systems Manager 自动化的总体输出，将自定义域配置分析结果的结构化摘要返回到 Systems Manager 控制台。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-TroubleshootAPIGatewayHttpErrors

描述

该AWSSupport-TroubleshootAPIGatewayHttpErrors运行手册通过解析访问 and/or 执行日志和分析错误，通过 re: Post 文章和文档提供补救步骤，从而帮助解决调用已部署的 Amazon API Gateway REST API 时出现的 5XX/4XX 错误。AWS

Important

本运行手册有以下限制：

- 必须启用日志记录。请参阅[使用 CloudWatch API Gateway 控制台设置亚马逊 API 日志](#)。
- 错误发生之前必须已启用日志。日志捕获和分析不能追溯性地完成。
- 涵盖的错误：500、502、503、504、401、403、429。
- 仅支持 REST APIs 。 WebSocket 而且 HTTP (v2) 未包含在本运行手册中。

Important

使用此运行手册可能会因您的 REST API 捕获的 Amazon CloudWatch 日志以及分析中使用的 CloudWatch 日志见解而向您的 AWS 账户收取额外费用。有关可能产生的费用的更多详细信息，请参阅 [Amazon CloudWatch 定价](#)。如果该aws:deletestack步骤失败，请前往 CloudFormation 控制台手动删除堆栈。此运行手册创建的堆栈名称以 AWSSupport-TroubleshootAPIGatewayHttpErrors 开头。有关删除 CloudFormation 堆栈的信息，请参阅《AWS CloudFormation 用户指南》中的[删除堆栈](#)。

如何工作？

运行手册执行以下验证和分析步骤：

- 验证指定的 REST API 是否存在并且您是否具有必要的权限。
- 验证 API 中是否存在指定的阶段。
- 验证 API 中是否存在指定的资源路径。
- 验证资源是否存在指定的 HTTP 方法。
- 根据指定参数和时间范围分析 CloudWatch 日志，以识别错误并提供补救建议。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- apigateway:GET
- logs:CreateLogGroup
- logs:CreateLogStream
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:PutLogEvents
- logs:StartQuery
- logs:GetQueryResults

示例 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
```

```

        "logs:PutLogEvents",
        "logs:StartQuery",
        "logs:GetQueryResults"
    ],
    "Resource": "*"
}
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootAPIGatewayHttpErrors](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，SSM Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - RestApild (必填)：
 - 描述：(必填) 需要进行故障排除的 API 的 API ID。必须是 10 个字符的字母数字字符串。
 - 类型：String
 - 允许的模式：`^[a-zA-Z0-9]{10}$`
 - StageName (必填)：
 - 描述：(必填) 已部署阶段的名称。必须是 1-128 个字符，包含字母、数字、下划线或连字符。
 - 类型：String
 - 允许的模式：`^[a-zA-Z0-9_\\-]{1,128}$`
 - ResourcePath (可选)：
 - 描述：(可选) 为其配置方法的资源路径。示例：`/`、`/store/items`、`/resource`。

- 默认值：/
- HttpMethod（可选）：
 - 描述：（可选）配置资源路径的方法。
 - 类型：String
 - 允许的值：[ANY, DELETE, HEAD, OPTIONS, GET, POST, PUT, PATCH]
 - 默认值：GET
- StartTime（可选）：
 - 描述：（可选）查询 CloudWatch 日志的开始日期和时间。格式：采用 yyyy-MM-ddTHH:mm:ss UTC 时区。如果未指定，则默认为当前时间前 3 天。
 - 类型：String
 - 允许的模式：`^$|^([0-9]{4})-([01-9]|1[0-2])-([01-9]|[1-2][0-9]|3[0-1])T([0-3]|01[0-9]):([0-5][0-9]):([0-5][0-9])$`
 - 默认值：""
- EndTime（可选）：
 - 描述：（可选）查询 CloudWatch 日志的结束日期和时间。格式：采用 yyyy-MM-ddTHH:mm:ss UTC 时区。如果未指定，则默认为当前时间。
 - 类型：String
 - 允许的模式：`^$|^([0-9]{4})-([01-9]|1[0-2])-([01-9]|[1-2][0-9]|3[0-1])T([0-3]|01[0-9]):([0-5][0-9]):([0-5][0-9])$`
 - 默认值：""
- AccessLogs（可选）：
 - 描述：（可选）是否应分析访问日志。
 - 类型：Boolean
 - 允许的值：[true, false]
 - 默认值：false
- RequestId（可选）：
 - 描述：（可选）观察到错误的请求的请求 ID。必须是有效的 UUID 格式。
 - 类型：String
 - 允许的模式：`^$|^([0-9a-f]{8})-([0-9a-f]{4})-([0-9a-f]{4})-([0-9a-f]{4})-([0-9a-f]{12})$`
 - 默认值：""

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- CheckApiExists:

验证所提供的 REST API 是否存在，并且您是否具有访问该应用程序的必要权限。

- CheckStageExists:

验证所提供的阶段名称是否存在于给定的 API 中，并检索访问日志组信息。

- CheckResourceExists:

验证所提供的资源路径是否存在于 API 中，并检索资源 ID。

- CheckMethodExists:

验证指定资源是否存在所提供的 HTTP 方法。

- AnalyseLogs:

使用提供的参数搜索日志，并根据发现的任何错误返回建议。此步骤将分析执行和访问日志（如果启用），以识别 4XX 和 5XX 错误，并提供具体的补救指导。

7. 完成后，请查看“输出”部分，了解执行的详细结果，包括错误分析和补救建议。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWS Batch

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Batch 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-TroubleshootAWSBatchJob](#)

AWSupport-TroubleshootAWSBatchJob

描述

AWSupport-TroubleshootAWSBatchJob运行手册可帮助您解决导致 AWS Batch 任务无法从状态升级RUNNABLE到STARTING状态的问题。

如何工作？

此运行手册执行以下检查：

- 如果计算环境处于INVALID或DISABLED状态。
- 如果计算环境的Max vCPU参数足够大，足以容纳作业队列中的任务量。
- 如果任务需要的 vCPU 或内存资源超过计算环境的实例类型所能提供的数量。
- 如果作业应在 GPU-based 实例上运行，但计算环境未配置为使用 GPU-based 实例。
- 如果计算环境的 Auto Scaling 组无法启动实例。
- 如果启动的实例可以加入底层的亚马逊弹性容器服务 (Amazon ECS) Service 集群；如果没有，则运行[AWSupport-TroubleshootECSContainerInstance](#)手册。
- 如果有任何权限问题阻碍了运行作业所需的特定操作。

Important

- 此 Runbook 必须与处于RUNNABLE状态的任务在同一个 AWS 区域启动。
- 可以为在亚马逊 ECS AWS Fargate 或亚马逊弹性计算云 (Amazon EC2) 实例上安排的 AWS Batch 任务启动本运行手册。如果在亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 上为 AWS Batch 任务启动自动化，则启动将停止。
- 如果实例可用于运行任务，但无法注册 Amazon ECS 集群，则此运行手册将启动AWSupport-TroubleshootECSContainerInstance自动化运行手册以尝试确定原因。有关更多信息，请参阅[AWSupport-TroubleshootECSContainerInstance](#)运行手册。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- JobId

类型：字符串

描述：(必填) 处于RUNNABLE状态的 AWS Batch Job 的 ID。

允许的模式：`^[a-f0-9]{8}(-[a-f0-9]{4}){3}-[a-f0-9]{12}(:[0-9]+)?(#[0-9]+)?$`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeScalingActivities
- batch:DescribeComputeEnvironments
- batch:DescribeJobs
- batch:DescribeJobQueues
- batch:ListJobs
- cloudtrail:LookupEvents
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceAttribute

- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetRequestHistory`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecs:DescribeClusters`
- `ecs:DescribeContainerInstances`
- `ecs:ListContainerInstances`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

说明

1. 在 AWS Systems Manager 控制台 [AWS Support-TroubleshootAWSBatchJob](#) 中导航到。
2. 选择 Execute automation (执行自动化)

3. 要输入参数，请输入内容：

- AutomationAssumeRole (可选)：

AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 允许 Systems Manager Automation 代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- JobId (必填)：

处于RUNNABLE状态的 AWS Batch Job 的 ID。

Input parameters

AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. Choose an option ▼	JobId (Required) The ID of the AWS Batch Job that is stuck in RUNNABLE status. b9[REDACTED]e32

4. 选择执行。

5. 请注意，自动化已启动。

6. 文档将执行以下步骤：

- PreflightPermissionChecks:

对初始 user/role 人执行预检 IAM 权限检查。如果缺少任何权限，则此步骤将提供全局输出部分中缺少的 API 操作。

- ProceedOnlyIfUserHasPermission:

根据您是否有权执行运行手册的所有必要操作进行分支。

- AWSBatchJobEvaluation:

对 AWS Batch Job 执行检查，验证其存在且处于RUNNABLE状态。

- ProceedOnlyIfBatchJobExistsAndIsInRunnableState:

根据任务是否存在以及是否处于RUNNABLE状态进行分支。

- BatchComputeEnvironmentEvaluation:

对 AWS Batch 计算环境进行检查。

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

根据计算环境检查是否成功进行分支。

- UnderlyingInfraEvaluation:

根据底层 Auto Scaling 组或 Spot 队列请求执行检查。

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

根据是否有未加入 Amazon ECS 集群的实例进行分支。

- EcsAutomationRunner:

为未加入集群的实例运行 Amazon ECS 自动化。

- ExecutionResults:

根据之前的步骤生成输出。

7. 完成后，将提供评估报告 HTML 文件的 URI：

运行手册成功执行后该报告的 S3 控制台链接和 Amazon S3 URI

▼ Outputs

```
ExecutionResults.message
#####
EXECUTION RESULT SUMMARY
#####
Here is the summary of the execution of this runbook:

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html

[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

#####
RUNBOOK EXECUTION LOGS
#####

+++++
STEP:PreflightPermissionChecks
+++++
[INFO]: The IAM Identity used to execute the runbook has all required permissions, proceeding further for next steps in execution.

+++++
STEP:AWSBatchJobEvaluation
+++++
[INFO]: Job with ID "411-XXXXXXXXXXXX-606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

+++++
STEP:BatchComputeEnvironmentEvaluation
+++++

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html

[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.
```

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

CloudFormation

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS CloudFormation有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-DeleteCloudFormationStack](#)
- [AWS-EnableCloudFormationSNSNotification](#)
- [AWS-RunCfnLint](#)
- [AWSSupport-TroubleshootCFNCustomResource](#)
- [AWS-UpdateCloudFormationStack](#)

AWS-DeleteCloudFormationStack

描述

删除 CloudFormation 堆栈。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- StackNameOrId

类型：字符串

描述：(必填) 要删除的 CloudFormation 堆栈的名称或唯一 ID

AWS-EnableCloudFormationSNSNotification

描述

AWS-EnableCloudFormationSNSNotification运行手册为您指定的 () 堆栈启用亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 通知。AWS CloudFormation CloudFormation

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- StackArn

类型：字符串

描述：(必填) 您要为其启用 Amazon SNS 通知的 CloudFormation 堆栈的 ARN 或名称。

- NotificationArn

类型：字符串

描述：(必填) 您要与堆栈关联的 Amazon SNS 主题的 ARN。CloudFormation

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm : GetAutomationExecution
- ssm : StartAutomationExecution
- 云层 : DescribeStacks
- 云层 : UpdateStack
- kms:Decrypt
- kms: GenerateDataKey
- sns:Publish
- sqs: GetQueueAttributes

文档步骤

- CheckCfnSnsLimits (aws:executeScript)-验证尚未与您指定的堆栈关联的 Amazon SNS 主题的最大数量。CloudFormation
- EnableCfnSnsNotification (aws:executeAwsApi)-为堆栈启用 Amazon SNS 通知。CloudFormation
- VerificationCfnSnsNotification (aws:executeScript)-验证是否已为堆栈启用 Amazon SNS 通知。CloudFormation

输出

CheckCfnSnsLimits。 NotificationArnList -接收堆栈 ARNs 的 Amazon SNS 通知的 CloudFormation 人员名单。

VerificationCfnSnsNotification。 VerifySnsTopicsResponse -来自 API 操作的响应，确认已为堆栈启用 Amazon SNS 通知。 CloudFormation

AWS-RunCfnLint

描述

本运行手册使用 [AWS CloudFormation Linter](#) (cfn-python-lint) 根据资源规范验证 YAML 和 JSON 模板。 CloudFormation AWS-RunCfnLint 运行手册执行其他检查，例如确保为资源属性输入了有效的值。如果验证失败，RunCfnLintAgainstTemplate 步骤将失败，并且在错误消息中提供 linter 工具的输出。此运行手册使用 cfn-lint v0.24.4。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ConfigureRuleFlag

类型：字符串

描述：(可选) 要传递给 `--configure-rule` 参数的规则的配置选项。

示例：E2001:strict=false,E3012:strict=false。

- FormatFlag

类型：字符串

描述：(可选) 传递给 `--format` 参数以指定输出格式的值。

有效值：Default | quiet | parseable | json

默认：Default

- IgnoreChecksFlag

类型：字符串

描述：(可选) IDs 要传递给 `--ignore-checks` 参数的规则。不会检查这些规则。

示例：E1001,E1003,W7001

- IncludeChecksFlag

类型：字符串

描述：(可选) IDs 要传递给 `--include-checks` 参数的规则。将检查这些规则。

示例：E1001,E1003,W7001

- InfoFlag

类型：字符串

描述：(可选) `--info` 参数的选项。包括启用有关模板处理的其他日志记录信息的选项。

默认：false

- TemplateFileName

类型：字符串

描述：S3 存储桶中的模板文件的名称或键。

- 模板3 BucketName

类型：字符串

描述：包含 Packer 模板的 S3 存储桶的名称。

- RegionsFlag

类型：字符串

描述：(可选) 要传递给 `for --regions` 参数的值，用于对照指定测试模板 AWS 区域。

示例：us-east-1,us-west-1

文档步骤

RunCfnLintAgainstTemplate — 针对指定的 CloudFormation 模板运行该 `cfn-python-lint` 工具。

输出

RunCfnLintAgainstTemplate.output — 工具中的标准输出。 `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

描述

AWSSupport-TroubleshootCFNCustomResource 运行手册可帮助诊断 AWS CloudFormation 堆栈在创建、更新或删除自定义资源时失败的原因。运行手册将检查用于自定义资源的服务令牌以及返回的错误消息。在查看自定义资源的详细信息之后，运行手册的输出会解释该自定义资源的堆栈行为和故障排除步骤。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- StackName

类型：字符串

描述：(必填) 自定义资源失败的 CloudFormation 堆栈的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:ListStackResources
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:DescribeVpcEndpoints
- ec2:DescribeSubnets
- logs:FilterLogEvents

文档步骤

- validateCloudFormationStack-验证 CloudFormation 堆栈是否存在于同一个 AWS 账户 和 AWS 区域中。

- `checkCustomResource`-分析 CloudFormation 堆栈，检查失败的自定义资源，并输出有关如何对失败的自定义资源进行故障排除的信息。

AWS-UpdateCloudFormationStack

描述

使用存储在 Amazon S3 存储桶中的 CloudFormation 模板更新 AWS CloudFormation 堆栈。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `LambdaAssumeRole`

类型：字符串

说明：(必需) Lambda 担任角色的 ARN

- `StackNameOrId`

类型：字符串

描述：(必填) 待更新的 CloudFormation 堆栈的名称或唯一 ID

- TemplateUrl

类型：字符串

描述：(必填) 包含更新 CloudFormation 模板的 S3 存储桶位置 (例如 `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager 自动化为 Amazon CloudFront 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-EnableCloudFrontDefaultRootObject](#)
- [AWSConfigRemediation-EnableCloudFrontAccessLogs](#)
- [AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity](#)
- [AWSConfigRemediation-EnableCloudFrontOriginFailover](#)
- [AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS](#)

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

描述

AWSConfigRemediation-EnableCloudFrontDefaultRootObject 运行手册为您指定的 Amazon CloudFront (CloudFront) 分配配置默认根对象。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- CloudFrontDistributionId

类型：字符串

描述：(必填) 要为其配置默认根对象的 CloudFront 分配的 ID。

- DefaultRootObject

类型：字符串

描述：(必填) 当查看者请求指 CloudFront 向您的根 URL 时，您要返回的对象。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- cloudfront:GetDistributionConfig
- cloudfront:UpdateDistribution

文档步骤

- aws:executeScript-配置您在CloudFrontDistributionId参数中指定的 CloudFront 分配的默认根对象。

AWSConfigRemediation-EnableCloudFrontAccessLogs

描述

AWSConfigRemediation-EnableCloudFrontAccessLogs运行手册为您指定的 Amazon CloudFront (CloudFront) 分配启用访问日志。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- BucketName

类型：字符串

描述：(必需) 您希望将访问日志存储到的 Amazon Simple Storage Service (Amazon S3) 桶的名称。不支持 af-south-1、ap-east-1、eu-south-1 和 me-south-1 AWS 区域 的存储桶。

- CloudFrontId

类型：字符串

描述：(必填) 您要启用访问登录功能的 CloudFront 分配的 ID。

- IncludeCookies

类型：布尔值

有效值：true | false

描述：(必需) 如果您想在访问日志中包含 Cookie , 请将此参数设置为。true

- Prefix

类型：字符串

描述：(可选) 您 CloudFront 要作为分配访问日志filenames前缀的可选字符串，例如myprefix/。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:UpdateDistribution
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:PutBucketAcl

Note

该 s3:GetBucketLocation API 只能用于同一账户中的 S3 存储桶。您不能将其用于跨账户 S3 存储桶。

文档步骤

- aws:executeScript-为CloudFrontDistributionId参数中指定的 CloudFront 分配启用访问日志记录。

AWSConfigRemediation- EnableCloudFrontOriginAccessIdentity

描述

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity运行手册为您指定的 Amazon CloudFront (CloudFront) 分配启用源访问身份。此自动化会为亚马逊简单存储服务 (Amazon S3) Simple Service 的所有来源分配相同的 CloudFront 源站访问身份，而没有您指定的分配的 CloudFront 源访问身份。此自动化不会向原始访问身份授予读取权限，以访问您的 CloudFront Amazon S3 存储桶中的对象。您必须更新 Amazon S3 存储桶权限才能允许访问。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- CloudFrontDistributionId

类型：字符串

描述：(必填) 您要启用源故障转移的 CloudFront 分配的 ID。

- OriginAccessIdentityId

类型：字符串

描述：(必填) 要与 CloudFront 源关联的源访问身份的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

文档步骤

- `aws:executeScript`-为您在`CloudFrontDistributionId`参数中指定的 CloudFront 分配启用源访问身份，并验证是否分配了源访问身份。

AWSConfigRemediation-EnableCloudFrontOriginFailover

描述

AWSConfigRemediation-EnableCloudFrontOriginFailover运行手册为您指定的 Amazon CloudFront (CloudFront) 分配启用源故障转移。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- CloudFrontDistributionId

类型：字符串

描述：(必填) 您要启用源故障转移的 CloudFront 分配的 ID。

- OriginGroupId

类型：字符串

说明：(必需) 源组的 ID。

- PrimaryOriginId

类型：字符串

描述：(必需) 源组中主源 ID。

- SecondaryOriginId

类型：字符串

描述：(必需) 源组中的辅助源 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- cloudfront:GetDistributionConfig
- cloudfront:UpdateDistribution

文档步骤

- aws:executeScript-为CloudFrontDistributionId参数中指定的 CloudFront分配启用源故障转移，并验证是否已启用故障转移。

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

描述

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS运行手册为您指定的 Amazon CloudFront (CloudFront) 发行版启用查看者协议策略。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- CloudFrontDistributionId

类型：字符串

描述：(必填) 您要启用查看器协议策略的 CloudFront 分发的 ID。

- ViewerProtocolPolicy

类型：字符串

有效值：仅限 https , redirect-to-https

描述：(必需) 查看器可用于访问指定的来源中的文件的协议。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `cloudfront:GetDistribution`

文档步骤

- `aws:executeScript`-为您在`CloudFrontDistributionId`参数中指定的 CloudFront 分配启用查看者协议策略，并验证策略是否已分配。

CloudTrail

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS CloudTrail有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWSConfigRemediation-CreateCloudTrailMultiRegionTrail](#)
- [AWS-EnableCloudTrail](#)
- [AWS-EnableCloudTrailCloudWatchLogs](#)
- [AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS](#)
- [AWS-EnableCloudTrailKmsEncryption](#)
- [AWSConfigRemediation-EnableCloudTrailLogFileValidation](#)
- [AWS-EnableCloudTrailLogFileValidation](#)
- [AWS-QueryCloudTrailLogs](#)

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

描述

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`运行手册创建了一个 AWS CloudTrail (CloudTrail) 跟踪，该跟踪 AWS 区域 将多个日志文件传输到您选择的亚马逊简单存储服务 (Amazon S3) Service 存储桶。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- BucketName

类型：字符串

描述：(必需) 要将日志上传到的 Amazon S3 存储桶的名称。

- KeyPrefix

类型：字符串

描述：(可选) 位于您为日志文件传输指定的存储桶的名称之后的 Amazon S3 键前缀。

- TrailName

类型：字符串

描述：(必填) 要创建的 CloudTrail 跟踪的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`
- `cloudtrail:GetTrail`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:PutBucketLogging`
- `s3:ListBucket`

文档步骤

- `aws:executeAwsApi`-接受跟踪名称和 Amazon S3 存储桶名称作为输入并创建 CloudTrail 跟踪。
- `aws:executeAwsApi` - 对创建的跟踪启用日志记录，并开始将日志传输到您指定的 Amazon S3 存储桶。
- `aws:assertAwsResourceProperty`-验证 CloudTrail 跟踪是否已创建。

AWS-EnableCloudTrail

描述

创建 AWS CloudTrail 跟踪并配置对 S3 存储桶的日志记录。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3 BucketName

类型：字符串

说明：(必需) 为发布日志文件指定的 S3 存储桶的名称。

 Note

S3 存储桶必须存在，并且存储桶策略必须授予对其进行写入的 CloudTrail 权限。有关信息，请参阅 [Amazon S3 存储桶政策 CloudTrail](#)。

- TrailName

类型：字符串

说明：(必需) 新跟踪的名称。

AWS-EnableCloudTrailCloudWatchLogs

描述

本运行手册更新了一个或多个 AWS CloudTrail 跟踪的配置，以将事件发送到 Amazon Lo CloudWatch gs 日志组。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CloudWatchLogsLogGroupArn

类型：字符串

描述：(必填) 将要传送 CloudWatch 日志的日志组的 CloudTrail ARN。

- CloudWatchLogsRoleArn

类型：字符串

描述：(必填) 假设 IAM 角色 CloudWatch 日志的 ARN 写入指定的日志组。

- TrailNames

类型：StringList

描述：(必填) 以逗号分隔的列表，列出要将事件发送到 CloudWatch logs 的 CloudTrail 跟踪的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudtrail:UpdateTrail
- iam:PassRole

文档步骤

- `aws:executeScript`-更新指定的 CloudTrail 跟踪以将事件传送到指定的 CloudWatch 日志日志组。

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

描述

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS运行手册使用您指定的 AWS CloudTrail (CloudTrail) 客户托管密钥加密 AWS Key Management Service (AWS KMS) 跟踪。本运行手册应仅用作基准，以确保您的 CloudTrail跟踪按照建议的最低安全最佳实践进行加密。我们建议使用不同的 KMS 密钥加密多个跟踪。CloudTrail 摘要文件未加密。如果您之前已将跟踪的 `EnableLogFileValidation` 参数设置为 `true`，请参阅《AWS CloudTrail 用户指南》中“[CloudTrail 预防性安全最佳实践](#)”主题的“使用 AWS KMS 托管密钥的服务器端加密”部分，了解更多信息。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `KMSKey`我是

类型：字符串

描述：(必需) 您要用于加密您在 `TrailName` 参数中指定的跟踪的客户托管密钥的 ARN、密钥 ID 或密钥别名。

- TrailName

类型：字符串

描述：(必需) 要升级加密的跟踪的 ARN 或名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

文档步骤

- aws:executeAwsApi - 对您在 TrailName 参数中指定的跟踪启用加密。
- aws:executeAwsApi - 收集 KMSKeyId 参数中指定的客户托管密钥的 ARN。
- aws:assertAwsResourceProperty - 验证是否已在 CloudTrail 跟踪中启用加密。

AWS-EnableCloudTrailKmsEncryption

描述

本运行手册更新了一个或多个 AWS CloudTrail 跟踪的配置以使用 AWS Key Management Service (AWS KMS) 加密。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- KMSKey我是

类型：字符串

描述：(必填) 您要用于加密您在TrailName参数中指定的跟踪的客户托管密钥的密钥 ID。该值可以是以“alias/”为前缀的别名、别名的完全指定的 ARN 或密钥的完全指定的 ARN。

- TrailNames

类型：StringList

描述：(必填) 要更新以加密的跟踪列表，以逗号分隔。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudtrail:UpdateTrail
- kms:DescribeKey
- kms:ListKeys

文档步骤

- aws:executeScript-对您在TrailName参数中指定的轨迹启用 AWS KMS 加密。

AWSConfigRemediation-EnableCloudTrailLogFileValidation

描述

AWSConfigRemediation-EnableCloudTrailLogFileValidation运行手册可为您的 AWS CloudTrail 跟踪启用日志文件验证。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- TrailName

类型：字符串

描述：(必需) 要为其启用日志验证的跟踪的 Amazon 资源名称 (ARN) 的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

文档步骤

- `aws:executeAwsApi` - 为您在 `TrailName` 参数中指定的 AWS CloudTrail 跟踪启用日志验证。
- `aws:assertAwsResourceProperty` - 验证您的跟踪是否启用了日志验证。

AWS-EnableCloudTrailLogFileValidation

描述

AWS-EnableCloudTrailLogFileValidation 运行手册为您指定的 AWS CloudTrail 跟踪启用日志文件验证。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `TrailNames`

类型：StringList

描述：(必填) 要为其启用日志验证的 CloudTrail 跟踪名称的逗号分隔列表。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

文档步骤

- aws:executeScript-为您在TrailNames参数中指定的 AWS CloudTrail 跟踪启用日志验证。

AWS-QueryCloudTrailLogs

描述

AWS-QueryCloudTrailLogs运行手册从你选择的亚马逊简单存储服务 (Amazon S3) Simple S3 存储桶中创建一个 Amazon Athena 表，其中包含 () 日志。AWS CloudTrail CloudTrail创建表后，此自动化将运行您指定的 SQL 查询，然后删除该表。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- Query

类型：字符串

描述：(必需) 要运行的 SQL 查询。

- SourceBucketPath

类型：字符串

描述：(必填) 包含您要查询的 CloudTrail 日志文件的 Amazon S3 存储桶的名称。

- TableName

类型：字符串

描述：(可选) 自动化创建的 Athena 表的名称。

默认：cloudtrail_logs

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StartQueryExecution
- glue:CreateTable
- glue>DeleteTable
- glue:GetDatabase
- glue:GetPartitions
- glue:GetTable
- s3:AbortMultipartUpload
- s3:CreateBucket
- s3:GetBucketLocation
- s3:GetObject
- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts

- `s3:PutObject`

文档步骤

- `aws:executeAwsApi` - 创建 Athena 表。
- `aws:executeAwsApi` - 运行您在 Query 参数中指定的查询字符串。
- `aws:executeScript` - 轮询并等待查询完成。
- `aws:executeAwsApi` - 获取查询结果。
- `aws:executeAwsApi` - 删除此自动化创建的表。

CloudWatch

AWS Systems Manager 自动化为 Amazon CloudWatch 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-ConfigureCloudWatchOnEC2Instance](#)
- [AWS-EnableCWAAlarm](#)
- [AWSSupport-TroubleshootCloudWatchAgent](#)
- [AWSSupport-TroubleshootCloudWatchAlarm](#)

AWS-ConfigureCloudWatchOnEC2Instance

描述

启用或禁用 Amazon 对托管实例的 CloudWatch 详细监控。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 您要启用 CloudWatch 监控功能的 Amazon EC2 实例的 ID。

- properties

类型：字符串

说明：(可选) 不支持此参数。此处列出它是为了实现向后兼容性。

- 状态

有效值：启用 | 禁用

说明：(可选) 指定启用还是禁用 CloudWatch。

默认：Enabled

文档步骤

configureCloudWatch -在 Amazon EC2 实例 CloudWatch 上使用给定状态进行配置。

输出

此自动化没有输出。

AWS-EnableCWAlarm

描述

AWS-EnableCWAlarm运行手册会为你 AWS 账户 中还没有警报的 AWS 资源创建 Amazon CloudWatch (CloudWatch) 警报。CloudWatch 为以下 AWS 资源创建警报：

- 亚马逊弹性计算云 (Amazon EC2) 实例
- Amazon Elastic Block Store (Amazon EBS) 卷
- Amazon Simple Storage Service (Amazon S3) 存储桶
- 亚马逊关系数据库服务 (Amazon RDS) 集群

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ComparisonOperator

类型：字符串

有效值：GreaterThanOrEqualToThreshold GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshol | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

描述：(必填) 比较指定统计量和阈值时使用的算术运算。

- MetricName

类型：字符串

描述：(必填) 与警报关联的指标的名称。

- 周期

类型：整数

有效值：10 | 30 | 60 | 60 的倍数

描述：(必填) 应用统计数据的周期 (以秒为单位)。

- 资源 ARNs

类型：StringList

描述：(必填) 要为其创建 CloudWatch 警报 ARNs 的资源列表，以逗号分隔

- Statistic

类型：字符串

有效值：平均值 | 最大值 | 最小值 | SampleCount | 总和

描述：(必填) 与警报关联的指标的统计信息。

- Threshold

类型：整数

描述：(必填) 要与指定统计数据进行比较的值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudwatch:PutMetricAlarm

文档步骤

- aws:executeScript-根据运行手册参数中指定的值为您在参数中指定的资源创建 CloudWatch 警报。ResourceARNs

输出

启用CWAlarm。FailedResources：未 ARNs 为其创建 CloudWatch 警报的资源映射列表以及失败原因。

启用CWAlarm。SuccessfulResources：已成功创建 CloudWatch 警 ARNs 报的资源列表。

AWSSupport-TroubleshootCloudWatchAgent

描述

该AWSSupport-TroubleshootCloudWatchAgent运行手册可自动对您的亚马逊弹性计算云 (Amazon EC2) 实例上的亚马逊 CloudWatch 代理进行故障排除。运行手册通过一系列基本和 (可选) 扩展检查来执行此故障排除。

基本检查包括以下内容：

- 查看 AWS Identity and Access Management (IAM) 实例配置文件
- 验证是否已将必要的亚马逊 CloudWatch 代理 IAM 权限附加到亚马逊 EC2 实例

仅当提供的 Amazon EC2 实例 ID 是 Systems Manager 托管实例时，才会执行扩展检查。这些扩展检查包括以下内容：

- 检查实例上的 Amazon CloudWatch 代理的状态
- 分析 Amazon A CloudWatch gent 的日志，了解常见问题和相关的故障排除步骤
- 将相关日志和配置文件压缩到亚马逊 EC2 实例上，然后选择将其上传到您选择的亚马逊简单存储服务 (Amazon S3) 存储桶
- 在实例和所需终端节点之间执行连接检查

Important

当RunVpcReachabilityAnalyzer参数设置为true，此运行手册将确定是否需要调用子运行手册。AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2子运行手册使用VPC Reachability Analyzer，它会产生相关费用。有关定价的更多信息，请参阅 [Amazon VPC 定价](#) 文档。

Important

本运行手册仅检查您的 IAM 实例配置文件角色是否具有必要的权限。如果您改为依赖 `.aws/credentials` 文件中定义的凭据，则该 `verifyIamPermissions` 步骤的结果可能不准确。

如何工作？

运行手册执行以下步骤：

- `getInstanceProfile`：验证所提供的 Amazon EC2 实例是否附加了 IAM 实例配置文件。
- `verifyIamPermissions`：检查与该实例关联的实例配置文件以确定是否应用了必要的 IAM 权限。
- `getInstanceInformation`：检查实例是否有活动的 Systems Manager 代理，并获取该实例的操作系统类型。
- `getAgentStatus`：检查实例上的 Amazon CloudWatch 代理的状态（扩展检查）。
- `analyzeLogs/analyzeLogsWindows`：根据操作系统类型分析并输出亚马逊 CloudWatch 代理日志的结果。
- `CollectLogs/collectLogsWindows`：根据操作系统类型捆绑并输出相关的 Amazon A CloudWatch gent 疑难解答文件。
- `checkEndpointReachability/checkEndpointReachabilityWindows`：根据操作系统类型检查实例是否可以到达所需的终端节点。
- `analyzeAwsEndpointReachabilityFromEC2`：调用子自动化运行手册以检查所选实例与所需端点的可访问性（如果已启用）。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2: DescribeInstances
- 我是 : GetInstanceProfile
- 我是 : GetRole
- 我是 : ListAttachedRolePolicies
- 我是 : ListRolePolicies
- 我是 : GetRolePolicy
- 我是 : GetPolicy
- 我是 : GetPolicyVersion
- 我是 : SimulatePrincipalPolicy
- ssm : DescribeInstanceInformation
- ssm : SendCommand
- ssm : GetCommandInvocation
- ssm : DescribeInstanceAssociationsStatus
- ssm : StartAutomationExecution

策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:SimulatePrincipalPolicy",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
```

```

        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
}
]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootCloudWatchAgent](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作的 IAM 角色的 ARN。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - InstanceId (必填)：
 - 描述：(必填) 您要对其进行亚马逊 CloudWatch 代理故障排除的 Amazon EC2 实例的 ID。
 - 类型：AWS::EC2::Instance::Id
 - 允许模式：`^i-[0-9a-f]{8,17}$`
 - S3UploadBucket (可选)：
 - 描述：(可选) 用于上传收集的 Amazon A CloudWatch gent 日志的 Amazon S3 存储桶的名称。Amazon EC2 实例配置文件必须具有正确的权限才能将文件上传到此存储桶。这还要求目标 Amazon EC2 实例是 Systems Manager 托管实例。
 - 类型：AWS::S3::Bucket::Name
 - 允许模式：`^$|^[a-z0-9][a-z0-9.-]{1,61}[a-z0-9]$`
 - 默认值：""
 - S3BucketOwnerAccountId (可选)：
 - 描述：(可选) 拥有您要上传亚马逊 CloudWatch 代理日志的 Amazon S3 存储桶的 AWS 账号。如果您不修改此参数，则运行手册将使用运行自动化的用户或角色的 AWS 账户 ID。
 - 类型：String
 - 允许模式：`^\{\{ global:ACCOUNT_ID \}\}$|^[0-9]{12}$`

- 默认值：{{ global:ACCOUNT_ID }}
- 检查EC2终端节点（可选）：
 - 描述：（可选）指定您的代理配置true是否使用选项append_dimensions将 Amazon EC2 指标维度附加到代理收集的指标中。使用append_dimensions时，Amazon A CloudWatch agent 需要连接到 Amazon EC2 API 终端节点，因此将通过扩展检查执行额外的连接测试。
 - 类型：String
 - 允许的值：[true, false]
 - 默认值：false
- RunVpcReachabilityAnalyzer（可选）：
 - 描述：（可选）如果网络问题是由扩展检查确定的，或者指定的true实例 ID 不是托管实例，则指定运行AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2子自动化。
 - 类型：Boolean
 - 默认值：false
- RetainVpcReachabilityAnalysis（可选）：
 - 描述：（可选）仅在RunVpcReachabilityAnalyzer是时才相关true。指定true保留由 VPC Reachability Analyzer 创建的网络洞察路径和相关分析。默认情况下，这些资源将在成功分析后删除。
 - 类型：Boolean
 - 默认值：false

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- getInstanceProfile:

验证所提供的 Amazon EC2 实例是否附加了 IAM 实例配置文件。

- branchOnInstanceProfileStatus:

如果实例配置文件已附加到实例，则分支自动化以检查必要的实例配置文件权限。

- verifyIamPermissions:

检查与该实例关联的实例配置文件，以确定是否应用了必要的 IAM 权限。

- getInstanceInformation:

检查实例是否有活动的 Systems Manager 代理，并获取该实例的操作系统类型。

- `branchOnManaged`实例：

分支自动化以执行扩展检查实例是否处于托管状态。

- `getAgentStatus`:

检查实例上的 Amazon CloudWatch 代理的状态。

- `branchOnInstanceOsType`:

根据操作系统将自动化分支为运行特定的日志 `collection/analysis` 命令。

- `analyze analyzeLogsWindows Logs/`:

根据操作系统类型分析并输出 Amazon A CloudWatch gent 日志的结果。

- 收集日志/ `collectLogsWindows`:

根据操作系统类型捆绑并输出相关的 Amazon A CloudWatch gent 疑难解答文件。

- `checkEndpointReachability/checkEndpointReachabilityWindows`：

根据操作系统类型检查实例是否可以到达所需的终端节点。

- `branchOnRunVpcReachabilityAnalyzer`:

如果启用并检测到网络问题，则将自动化分支到运行 VPC 可访问性分析。

- 生成端点：

根据扩展检查失败和的值生成要检查的端点 `CheckEC2Endpoint`。

- `analyzeAwsEndpointReachabilityFromEC2`:

调用自动化运行手册 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`，检查所选实例与所需端点的可访问性。

- 输出结果：

输出自动化执行步骤的结果。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-TroubleshootCloudWatchAlarm

描述

该AWSSupport-TroubleshootCloudWatchAlarm运行手册有助于识别和解决配置错误或有问题的Amazon CloudWatch (CloudWatch) 警报的问题。它利用公开 AWS APIs 和已知的警报评估逻辑来检测监控指标中延迟或丢失的数据点，这可能导致警报操作错过或延迟。本运行手册提供了一种结构化的方法来调查和解决 Amazon CloudWatch (CloudWatch) 警报相关的问题。

如何工作？

运行手册AWSSupport-TroubleshootCloudWatchAlarm执行以下步骤：

- 验证 Amazon CloudWatch (CloudWatch) 警报详情和AlarmTriggerTimestamp参数值，以检查其是否在 2,592,000 秒 (30 天) 以内。
- 检查警报是基于指标还是公制数学，还是异常探测器警报。
- 检查警报是否处于数据不足状态。
- 检查警报中使用的指标是否与ListMetrics值匹配。
- 验证指标在给定时间戳是否缺少数据点。
- 获取给定时间戳的最新历史记录。
- 检查警报是否由于延迟或错过指标而未触发。
- 检查警报的启用操作是否已 was/were 送达。
- 生成包含所有诊断结果的故障排除报告。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmHistory
- cloudwatch:DescribeAnomalyDetectors
- cloudwatch:GetMetricData
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootCloudWatchAlarm](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 类型：String
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定任何角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - CloudWatchMetricAlarmName (必填)：
 - 类型：String
 - 描述：(必填) 要进行故障排除的 Amazon CloudWatch (CloudWatch) 指标警报的名称。
 - 允许的模式：`^[a-zA-Z0-9.:;,\_\&() ]{1,255}$`
 - AlarmTriggerTimestamp (必填)：
 - 类型：String
 - 描述：(必填) 警报问题发生时的 UTC 时间戳。这些信息对于解决问题和了解问题发生的背景至关重要。时间戳值应为从今天起的最近 30 天内的时间，格式YYYY-MM-DDTHH:mm:ssZ为。
示例：2024-10-29T09:04:00Z
 - 允许的模式：`^((\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2}))Z$`
4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- **VerifyRunbookInputs**

验证 Amazon CloudWatch (CloudWatch) 警报详情和AlarmTriggerTimestamp参数值，以检查其是否在 2,592,000 秒 (30 天) 以内。

- **UpdateSSMDocumentInputChecksVariable**

使用VerifyRunbookInputs步骤SSMDocumentInputChecks中的SSMDocumentInputChecks值更新变量。

- **BranchOnAlarmIsVerified**

分支于 Runbook 的输入验证AlarmTriggerTimestamp和CloudWatchAlarmName.

- **CheckMetricAlarmType**

检查警报是基于指标还是公制数学，还是异常探测器警报。

- **CheckAlarmInInsufficientDataState**

检查警报是否处于数据不足状态。

- **UpdateInsufficientDataChecksVariable**

使用CheckAlarmInInsufficientDataState步骤InsufficientDataChecks中的InsufficientDataChecks值更新变量。

- **BranchOnAlarmHasInsufficientData**

在 ste CheckAlarmInInsufficientDataState p 中的AlarmHasInsufficientData值上进行分支，默认步骤为CheckMetricMismatch。

- **CheckMetricMismatch**

检查警报中使用的指标是否与ListMetrics值匹配。

- **UpdateMetricMismatchChecksVariable**

使用CheckMetricMismatch步骤MetricMismatchChecks中的MetricMismatchChecks值更新变量。

- **BranchOnMetricsMatched**

在 ste CheckMetricMismatch p 中的MetricsMatched值上进行分支，默认步骤为CheckMissingDatapoint。

- **CheckMissingDatapoint**

验证指标在给定时间戳是否缺少数据点。

- **UpdateMetricMissingDatapointsChecksVariable**

使用CheckMissingDatapoint步骤MetricMissingDatapointsChecks中的MetricMissingDatapointsChecks值更新变量。

- **BranchOnMetricMissingDatapoint**

在 ste CheckMissingDatapoint p 中的MetricMissingDatapoint值上进行分支，默认步骤为GetAlarmHistoryDetails。

- **GetAlarmHistoryDetails**

获取给定时间戳的最新历史记录。

- **UpdateAlarmHistoryChecksVariable**

使用GetAlarmHistoryDetails步骤AlarmHistoryChecks中的AlarmHistoryChecks值更新变量。

- **BranchOnAlarmHistoryFound**

在 ste GetAlarmHistoryDetails p 中的AlarmHistoryFound值上进行分支，默认步骤为CheckDelayedMetric。

- **CheckDelayedMetric**

检查警报是否由于延迟或错过指标而未触发。

- **UpdateDelayedMetricChecksVariable**

使用CheckDelayedMetric步骤DelayedMetricChecks中的DelayedMetricChecks值更新变量。

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

分支位于CheckDelayedMetric步骤中的MetricDelayed和DatapointsMeetThreshold值，默认步骤为GenerateReport。

- **CheckActionDelivered**

检查警报的启用操作是否已 was/were 送达。

- **UpdateActionDeliveredChecksVariable**

使用CheckActionDelivered步骤ActionDeliveredChecks的输出ActionDeliveredChecks更新变量。

- **GenerateReport**

编译前面步骤的输出并输出报告。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果：

- GenerateReport. 报告

有关所提供的 Amazon CloudWatch (CloudWatch) 指标警报的报告。

```
-----
|                                     AWS CloudWatch Alarm Troubleshooting Results
|
-----
|      Alarm Name                    -      Demo-Alarm
|
|      Timestamp                    -
2025-03-04T06:31:00Z
|
-----
|      # No Issue(s) Found
|
-----
```

```
=====
1. Validating SSM Document input parameters:
=====
```

```
# [PASSED]: Found a metric alarm with name Demo-Alarm
=====
```

```
=====
2. Checking alarm's data state:
=====
```

```
# [PASSED]: The alarm is not in INSUFFICIENT_DATA state, alarm's
state is: ALARM
=====
```

```
=====
3. Checking if the alarm experienced metric mismatches:
=====
```

```
# [PASSED]: Metric matches with the configured metric for Alarm.
```

```
=====
4. Checking if the alarm's metric(s) experienced missing
datapoint(s):
=====

# [PASSED]: Metric has datapoints

=====

5. Retrieving alarm's history for timestamp 2025-03-04T06:31:00Z:
=====

# [PASSED]: Found most recent alarm history item for the provided
timestamp: '2025-03-04T06:31:00Z'

=====

6. Checking if the alarm experienced metric delays or the alarm's
datapoint(s) did not meet the configured threshold:
=====

# [PASSED]: CloudWatch alarm did not experience any delayed metric

=====

7. Checking if the alarm has actions enabled and if action(s) were
delivered:
=====

# [PASSED]: Successfully executed action arn:aws:sns:us-
east-1:12345678910:Demo_Alarms_Topic

-----

# All the checks have passed for CloudWatch alarm, Demo-Alarm, the
alarm's configuration is correct.
```

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

Amazon DocumentDB

AWS Systems Manager Automation 为亚马逊 DocumentDB 提供了预定义的运行手册 (兼容 MongoDB)。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

AWS-EnableDocDbClusterBackupRetentionPeriod

描述

AWS-EnableDocDbClusterBackupRetentionPeriod运行手册为您指定的 Amazon DocumentDB 集群启用了备份保留期。此功能可设置保留自动备份的总天数。要修改集群，集群必须处于可用状态，引擎类型为docdb。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBClusterResourceId

类型：字符串

描述：(必填) 您要为其启用备份保留期的 Amazon DocumentDB 集群的资源 ID。

- BackupRetentionPeriod

类型：整数

描述：(必填) 保留自动备份的天数。必须是 7-35 天的值。

- PreferredBackupWindow

类型：字符串

描述：(可选) 以世界协调时间 (UTC) 为单位的每日时间范围，格式为 hh24:mm-hh24:mm，例如 07:14-07:44。该值必须至少为 30 分钟，并且不能与首选维护时段冲突。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- docdb:DescribeDBClusters
- docdb:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- GetDocDbClusterIdentifier (aws:executeAwsApi)-使用提供的资源 ID 返回亚马逊文档数据库集群标识符。
- VerifyDocDbEngine (aws:assertAwsResourceProperty)-验证 Amazon DocumentDB 引擎类型docdb是为了防止无意中更改其他 Amazon RDS 引擎类型。

- `VerifyDocDbStatus (aws:waitAwsResourceProperty)`-验证 Amazon DocumentDB 集群的状态为。available
- `ModifyDocDbRetentionPeriod (aws:executeAwsApi)`-使用为指定的 Amazon DocumentDB 集群提供的值设置保留期。
- `VerifyDocDbBackupsEnabled (aws:executeScript)`-验证 Amazon DocumentDB 集群的保留期以及首选备份窗口 (如果已指定) 是否成功设置。

输出

`ModifyDocDbRetentionPeriod`。 `ModifyDbClusterResponse` -来自 `ModifyDBCluster` API 操作的响应。

`VerifyDocDbBackupsEnabled`。 `VerifyDbClusterBackupsEnabledResponse` -确认成功修改 Amazon DocumentDB 集群的`VerifyDocDbBackupsEnabled`步骤的输出。

CodeBuild

AWS Systems Manager 自动化为用户提供了预定义的运行手册。 AWS CodeBuild有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK](#)
- [AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject](#)

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

描述

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK`运行手册使用您指定的 AWS CodeBuild (CodeBuild) 客户托管密钥对 AWS Key Management Service (AWS KMS) 项目的构建工件进行加密。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- KMSKey我是

类型：字符串

描述：(必填) 您要用于加密您在参数中指定的 CodeBuild 项目的 AWS KMS 客户托管密钥的 Amazon 资源名称 (ARN)。ProjectId

- ProjectId

类型：字符串

描述：(必填) 要加密其构建工件的 CodeBuild 项目的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- codebuild:BatchGetProjects
- codebuild:UpdateProject
- config:GetResourceConfigHistory

文档步骤

- `aws:executeAwsApi`-从 CodeBuild 项目 ID 中收集项目名称。
- `aws:executeAwsApi`-对您在 `ProjectId` 参数中指定的 CodeBuild 项目启用加密。
- `aws:assertAwsResourceProperty`-验证是否已在 CodeBuild 项目上启用加密。

输出

UpdateLambdaConfig。UpdateFunctionConfigurationResponse -来自 UpdateFunctionConfiguration API 调用的响应。

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

描述

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject运行手册会从您指定的 AWS CodeBuild (CodeBuild) 项目中删除AWS_ACCESS_KEY_ID和AWS_SECRET_ACCESS_KEY环境变量。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- ResourceId

类型：字符串

描述：(必填) 要删除其访问密钥环境变量的 CodeBuild 项目的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- codebuild:BatchGetProjects
- codebuild:UpdateProject

文档步骤

- aws:executeScript-删除ResourceId参数中指定的 CodeBuild 项目的访问密钥环境变量。

AWS CodeDeploy

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS CodeDeploy有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-TroubleshootCodeDeploy](#)

AWSSupport-TroubleshootCodeDeploy

描述

该AWSSupport-TroubleshootCodeDeploy运行手册有助于诊断亚马逊弹性计算云 (Amazon EC2) 实例的 AWS CodeDeploy 部署失败的原因。运行手册将输出相关步骤，以帮助解决问题或进一步排查问题。还提供了的最佳 CodeDeploy 实践，以帮助避免将来出现类似的问题。

此运行手册可帮助您解决以下问题：

- CodeDeploy 代理未安装或未在 Amazon EC2 实例上运行
- Amazon EC2 实例没有附加 AWS Identity and Access Management (IAM) 实例配置文件
- 附加到亚马逊实例的 IAM EC2 实例配置文件不具备所需的亚马逊简单存储服务 (Amazon S3) Service 权限
- 缺少存储在 Amazon S3 中的修订版本，或者使用的 Amazon S3 存储桶与亚马逊 EC2 实例不同的存储桶中 AWS 区域
- 应用程序规范 (AppSpec) 文件问题
- “文件已存在于某个位置”错误
- CodeDeploy 托管生命周期事件挂钩失败
- 客户托管生命周期事件钩子失败
- 部署期间的横向缩减事件

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DeploymentId

类型：字符串

描述：(必需)失败的部署的 ID。

- InstanceId

类型：字符串

描述：(必填)部署失败的 Amazon EC2 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- codedeploy:GetDeployment
- codedeploy:GetDeploymentTarget
- ec2:DescribeInstances

文档步骤

- aws:executeAwsApi - 验证为 DeploymentId 和 InstanceId 参数提供的值。
- aws:executeScript - 从 Amazon EC2 实例收集信息，例如实例状态和 IAM 实例配置文件详情。
- aws:executeScript - 查看指定的部署，并返回有关部署失败原因的分析。

AWS Config

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Config 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-SetupConfig](#)

AWSSupport-SetupConfig

描述

该AWSSupport-SetupConfig运行手册创建了一个 AWS Identity and Access Management (IAM) 服务相关角色 AWS Config、由其提供支持的配置记录器和一个带有亚马逊简单存储服务 (Amazon S3) Simple Service 存储桶的交付渠道，用于 AWS Config 发送配置快照和配置历史记录文件。如果您

为AggregatorAccountId和AggregatorAccountRegion参数指定值，则运行手册还会为数据聚合创建授权，以便从多个和多个 AWS 账户 中收集 AWS Config 配置和合规性数据。AWS 区域要详细了解如何汇总来自多个账户和区域的数据，请参阅AWS Config 《开发者指南》中的[多账户多区域数据聚合](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AggregatorAccountId

类型：字符串

描述：(可选) 将向 AWS 账户 其中添加聚合器以聚合来自多个账户的 AWS Config 配置和合规性数据的 ID 以及 AWS 区域。聚合器还使用此账户对源账户进行授权。

- AggregatorAccountRegion

类型：字符串

描述：(可选) 将添加聚合器以聚合来自多个账户和地区的 AWS Config 配置和合规性数据的区域。

- IncludeGlobalResourcesRegion

类型：字符串

默认：us-east-1

描述：(必需) 为避免在每个区域中记录全球资源数据，请指定一个区域来记录全球资源数据。

- 分区

类型：字符串

默认：aws

描述：(必需) 要从中收集 AWS Config 配置和合规性数据的分区。

- S3 BucketName

类型：字符串

默认：aws-config-delivery-channel

描述：(可选) 要应用于为交付渠道创建的 Amazon S3 存储桶的名称。账户 ID 会附加到该名称的末尾。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:DescribeConfigurationRecorders
- config:DescribeDeliveryChannels
- config:PutAggregationAuthorization
- config:PutConfigurationRecorder
- config:PutDeliveryChannel
- config:StartConfigurationRecorder
- iam:CreateServiceLinkedRole
- iam:PassRole
- s3:CreateBucket
- s3:ListAllMyBuckets
- s3:PutBucketPolicy

文档步骤

- `aws:executeScript` - 创建一个 AWS Config 的服务相关 IAM 角色 (如果尚不存在)。
- `aws:executeScript` - 创建一个配置记录器 (如果尚不存在)。
- `aws:executeScript` - 创建一个将由交付渠道使用的 Amazon S3 存储桶 (如果尚不存在)。
- `aws:executeScript` - 使用运行手册创建的资源创建一个交付渠道。
- `aws:executeAwsApi` - 停止或启动配置记录器。
- `aws:executeScript` - 如果您为 `AggregatorAccountId` 和 `AggregatorAccountRegion` 参数指定了值，则会为多账户和多区域数据聚合配置授权。

Connect Customer

AWS Systems Manager 自动化为 Connect 客户提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#)
- [AWSSupport-CollectAmazonConnectContactFlowLog](#)

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

描述

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows` 可帮助您将电话号码与 Connect 客户实例中的联系人流程相关联。通过在输入逗号分隔值 (CSV) 文件中提供电话号码和联系人流的映射，运行手册可在 14.5 分钟内将尽可能多的电话号码与联系人流程关联起来。运行手册会生成一个 CSV 文件，其中包含它无法在时限内关联的所有电话号码和联系人流对，以便您可以在下次运行时输入它们。

如何工作？

该运行手册 `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` 可帮助您使用存储在亚马逊简单存储服务 (Amazon S3) 存储桶中的映射数据的 CSV 文件将电话号码与 Connect Customer 实例中的联系人流程关联起来。输入 CSV 文件应与以下格式对齐，`PhoneNumber` 值 [E.164](#) 采用格式。

输入 CSV 文件的示例

```
PhoneNumber,ContactFlowName
+1800555xxxx,ContactFlowA
+1800555yyyy,ContactFlowB
+1800555zzzz,ContactFlowC
```

自动化 runbook 还会在DestinationFileBucket和DestinationFilePath中指定的目标位置创建以下文件。

- **automation:EXECUTION_ID/ResourceIdList.csv**：一个临时文件，其中包含 AssociatePhoneNumberContactFlow API 所需的PhoneNumberId和ContactFlowId对。
- **automation:EXECUTION_ID/ErrorResourceList.csv**：包含由于错误而无法处理的电话号码和联系流对的文件，例如ResourceNotFoundException格式为PhoneNumber,ContactFlowName,ErrorMessage。
- **automation:EXECUTION_ID/NonProcessedResourceList.csv**：包含未处理的电话号码和联系流程对的文件。运行手册尝试在 14.5 分钟（AWS Lambda 功能超时 15 分钟-缓冲 30 秒）内处理尽可能多的电话号码和联系人流。如果由于时间限制而无法处理某些电话号码/联系人流，则运行手册会将其包含在 CSV 文件中，用作下一次运行手册执行的输入。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

```
{
  "Statement": [
    {
      "Action": [
```

```

        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:PutObject",
        "s3:PutObjectAcl"
    ],
    "Resource": [
        "arn:aws:s3:::YOUR-BUCKET/*",
        "arn:aws:s3:::YOUR-BUCKET"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation>DeleteStack",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:TagResource",
        "connect:AssociatePhoneNumberContactFlow",
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs>DeleteLogGroup",
        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "connect:DescribeInstance",
        "connect:ListPhoneNumbers",
        "connect:ListContactFlows",

```



```

        "ds:DescribeDirectories"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": [
          "ssm.amazonaws.com",
          "lambda.amazonaws.com"
        ]
      }
    },
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

如果提供LambdaRoleArn参数，则该角色需要执行以下操作才能成功使用运行手册。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": "arn:aws:logs:us-east-1:111122223333:*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:us-east-1:111122223333:*",
      "Effect": "Allow"
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:logs:us-east-1:111122223333:*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "connect:AssociatePhoneNumberContactFlow"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:PutObject",
      "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/DESTINATION_FILE_PATH*",
    "Effect": "Allow"
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSsupport-AssociatePhoneNumbersToConnectContactFlows](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ConnectInstanceId (必填)

您的 Connect 客户实例的 ID。

- SourceFileBucket (必填)

存储包含电话号码和联系流程对的 CSV 文件的 Amazon S3 存储桶。

- SourceFilePath (必填)

包含电话号码和联系流程对的 CSV 文件的 Amazon S3 对象密钥。例如 path/to/input.csv。

- DestinationFileBucket (必填)

Amazon S3 存储桶，自动化将在其中放置中间文件和结果报告。

- DestinationFilePath (可选)

存储中间文件和结果报告DestinationFileBucket的 Amazon S3 对象路径。例如，如果您指定path/to/files/，则文件存储在下s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/。

- S3BucketOwnerAccount (可选)

拥有您要上传联系流日志的 Amazon S3 存储桶的 AWS 账号。如果您未指定此参数，则运行手册将使用运行自动化的用户或角色的 AWS 账户 ID。

- S3BucketOwnerRoleArn (可选)

有权获取 Amazon S3 存储桶和账户封禁公开访问设置、存储桶加密配置、存储桶 ACL、存储桶策略状态以及向存储桶上传对象的 IAM 角色的 ARN。如果未指定此参数，则运行手册将使用AutomationAssumeRole (如果已指定) 或用户启动此 runbook (如果AutomationAssumeRole未指定)。请参阅运行手册描述中的“所需权限”部分。

- LambdaRoleArn (可选)

允许 AWS Lambda 函数访问所需 AWS 服务和资源的 IAM 角色的 ARN。如果未指定任何角色，则此自动化将在您的账户中为 Lambda 创建一个 IAM 角色。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- CheckConnectInstanceExistence

检查中提供的 Connect Customer 实例ConnectInstanceId是否存在。

- CheckS3BucketPublicStatus

检查中指定的 Amazon S3 存储桶是否DestinationFileBucket允许匿名或公开读取或写入权限。SourceFileBucket

- CheckSourceFileExistenceAndSize

检查中指定的源 CSV 文件SourceFilePath是否存在，以及文件大小是否超过 25 MiB 的限制。

- GenerateResourceIdMap

下载在中指定的源 CSV 文件，SourceFilePathPhoneNumberIdContactFlowId并为每个资源标识和。完成后，它会将包含、PhoneNumberPhoneNumberIdContactFlowName、和的 CSV 文件上传ContactFlowId到中DestinationFileBucket指定的目标 Amazon S3 存储桶。如果PhoneNumberId无法识别某个数字，则该字段在 CSV 文件中将为空。

- AssociatePhoneNumbersToContactFlows

使用 AWS CloudFormation 堆栈在您的账户中创建 AWS Lambda 函数。该 AWS Lambda 函数将每个号码与SourceFileBucket和中指定的源 CSV 文件中列出的联系人流相关。SourceFilePath，AWS CloudFormation 堆栈会调用该函数。在超时（15 分钟）之前，该 AWS Lambda 功能将尽可能多的电话号码映射到联系人流。由于错误而无法处理的电话号码和联系流程列表已上传[automation:EXECUTION_ID]/ErrorResourceList.csv。由于超过了单次执行中可以处理的最大电话号码数而无法处理的电话号码将被上传到中[automation:EXECUTION_ID]/NonProcessedResourceList.csv。如果此步骤失败，它将进入该DescribeCloudFormationErrorFromStackEvents步骤以显示 AWS CloudFormation 堆栈事件失败的原因。

- WaitForPhoneNumberContactFlowAssociationCompletion

等待，直到创建了将电话号码映射到联系人流的 AWS Lambda 函数并且 AWS CloudFormation 堆栈完成调用。

- GenerateReport

生成报告，其中包含映射到联系流的电话号码、由于错误而无法处理的电话号码，以及由于超出单次执行中可以处理的最大电话号码数而无法处理的电话号码。该报告还会显示[automation:EXECUTION_ID]/ErrorResourceList.csv或[automation:EXECUTION_ID]/NonProcessedResourceList.csv的位置（如适用）（亚马逊 S3 URI 和 Amazon S3 控制台 URL）。

- DeleteCloudFormationStack

删除 AWS CloudFormation 堆栈，包括用于映射的 Lambda 函数。

- **DescribeCloudFormationErrorFromStackEvent**

描述AssociatePhoneNumbersToContactFlows步骤 AWS CloudFormation 堆栈中的错误。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- **GenerateReport.OutputPayload**

电话号码和联系流关联的输出。该报告包含以下信息：

- 输入 CSV 文件中列出的电话号码和联系流对的数量
- 在输入 CSV 文件中指定的与联系人流关联的电话号码数量
- 由于错误而无法与联系人流关联的电话号码数量
- 由于时间限制而未与联系流关联的电话号码数量
- CSV 文件的位置 (Amazon S3 URI 和 Amazon S3 控制台 URL)，该文件包含由于错误而无法关联的电话号码和联系流对
- CSV 文件的位置 (Amazon S3 URI 和 Amazon S3 控制台 URL)，该文件包含由于时间限制而未关联的电话号码和联系流对
- **DescribeCloudFormationErrorFromStackEvents.Events**

在AssociatePhoneNumbersToContactFlows步骤失败时显示 AWS CloudFormation 堆栈事件的输出。

使用少量电话号码和联系人流执行的输出

```

▼ Outputs

DescribeCloudFormationErrorFromStackEvents.Events
No output available yet because the step is not successfully executed

GenerateReport.OutputPayload
{"Payload": "
=====
Amazon Connect Phone Number Mapping Result
=====
* Phone number and Contact Flow pairs listed in the provided input: 7
* Phone numbers associated with Contact Flow processed: 7
* Phone numbers that could not be associated with Contact Flow due to an error: 0
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 0

"}

```

执行输出包含大量电话号码和联系人流以及由于错误或时间限制而未关联的电话号码

▼ Outputs

DescribeCloudFormationErrorFromStackEvents.Events

No output available yet because the step is not successfully executed

GenerateReport.OutputPayload

("Payload":

=====

Amazon Connect Phone Number Mapping Result

=====

- * Phone number and Contact Flow pairs listed in the provided input: 1634
- * Phone numbers associated with Contact Flow processed: 1153
- * Phone numbers that could not be associated with Contact Flow due to an error: 8
- * Phone numbers that weren't associated with Contact Flow due to the time constraint: 473

=====

Error list file location

=====

- * S3 URI: s3://[REDACTED]/ErrorResourceList.csv
- * S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[REDACTED]/ErrorResourceList.csv

INFO: The above file contains the list of phone numbers and Contact Flows that could not be associated due to an error. You can look into the error detail in order to address the issue.

=====

Unprocessed list file location

=====

- * S3 URI: s3://[REDACTED]/NonProcessedResourceList.csv
- * S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[REDACTED]/NonProcessedResourceList.csv

INFO: The above file contains the list of phone numbers and Contact Flows that weren't associated due to the time constraint (15 minutes). You can execute this runbook again by specifying the file as an input \"SourceFileLocation\" so that you can process them.

")

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流登录页面](#)

AWSSupport-CollectAmazonConnectContactFlowLog

描述

AWSSupport-CollectAmazonConnectContactFlowLog 自动化运行手册用于收集特定联系人 ID 的 Connect 客户联系流日志。通过提供您的 Connect 客户实例 ID 和联系人 ID，运行手册会从亚马逊 CloudWatch 日志组中搜索联系人流日志，然后将其上传到请求参数中指定的亚马逊简单存储服务 (Amazon S3) 存储桶。运行手册生成的输出提供了 Amazon S3 控制台 URL 和 AWS CLI 命令供您下载日志。

如何工作？

AWSSupport-CollectAmazonConnectContactFlowLog 自动化运行手册有助于收集存储在已配置 CloudWatch 日志组中的特定联系人 ID 的 Connect Customer 联系流日志，并将其上传到指定的 Amazon S3 存储桶。为了帮助保护从 Connect Customer 联系流程中收集的日志的安全，自动化功能会评估 Amazon S3 存储桶配置，以确定该存储桶是否授予公共权限 read 或 write 访问权限，并且归 S3BucketOwnerAccountId 参数中指定的 AWS 账户所有。如果您的 Amazon S3 存储桶使用带有 AWS Key Management Service 密钥的服务器端加密 AWS Identity and Access Management (SSE-

KMS)，请确保运行此自动化的用户或 (IAM) 角色拥有 AWS KMS 密钥的 `kms:GenerateDataKey` 权限。有关您的 Connect Customer 实例生成的日志的更多信息，请参阅[存储在 Amazon CloudWatch 日志组中的流日志](#)。

Important

CloudWatch Logs Insights 查询会根据查询的数据量收取费用。免费套餐客户仅在超出服务限额时才会被收取使用费用。有关更多信息，请参阅[Amazon CloudWatch 定价](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "connect:DescribeInstance",
            "connect:DescribeContact",
            "ds:DescribeDirectories"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "logs:StartQuery",
            "logs:GetQueryResults"

            "Resource": "*",
            "Effect": "Allow"
        ]
    }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-CollectAmazonConnectContactFlowLog](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ConnectInstanceId (必填)：

您的 Connect 客户实例的 ID。

- **ContactId (必填) :**

您要为其收集联系流日志的联系人 ID。

- **S3BucketName (必填) :**

您想要上传联系流日志的账户中的 Amazon S3 存储桶名称。确保存储桶策略不会向不需要访问所收集日志的各方授予不必要的 read/write 权限。

- **S3ObjectPrefix (可选) :**

Amazon S3 存储桶中用于上传的联系流日志的 Amazon S3 对象路径。例如，如果您指定 `CollectedLogs`，则日志将上传为 `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`。如果您未指定此参数，则使用 Systems Manager 自动化执行 ID，例如：`s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`。注意：如果您为指定一个值 `S3ObjectPrefix` 并使用相同的 `[ContactId]` 运行此自动化，则联络流日志将被覆盖。

- **S3BucketOwnerAccount (可选) :**

拥有您要上传联系流日志的 Amazon S3 存储桶的 AWS 账号。如果您未指定此参数，则运行手册将使用运行自动化的用户或角色的 AWS 账户 ID。

- **S3BucketOwnerRoleArn (可选) :**

有权获取 Amazon S3 存储桶和账户的 IAM 角色的 ARN 封禁公开访问设置、存储桶加密配置、存储桶 ACL、存储桶策略状态以及将对象上传到存储桶。如果未指定此参数，则运行手册将使用 `AutomationAssumeRole` (如果已指定) 或用户启动此 runbook (如果 `AutomationAssumeRole` 未指定)。请参阅 Runbook 描述中的“所需权限”部分。

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. SSMAutomationRole	ConnectInstanceId (Required) The ID of your Amazon Connect instance. fedcba98-7654-3210-fedc-ba9876543210
ContactId (Required) The ID of the contact that you want to collect Contact Flow Log for. 01234567-89ab-cdef-0123-456789abcdef	S3BucketName (Required) The Amazon S3 bucket name in your account where you want to upload Contact Flow Log. Make sure that bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs. saw-example-bucket
S3ObjectPrefix (Optional) The Amazon S3 object path in the Amazon S3 bucket for an uploaded the Contact Flow Log. For example, if you specify 'CollectedLogs', the log will be uploaded as 's3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId]_[AWSAccountId].gz'. If you do not specify this parameter, the SSM Automation execution ID is used, example: 's3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog_[ContactId]_[AWSAccountId].gz'. Note: If you specify a value for 'S3ObjectPrefix' and you run this automation using the same [ContactId], the Contact Flow Log will be overwritten. String	S3BucketOwnerAccount (Optional) The AWS Account Number that owns the Amazon S3 bucket where you want to upload the Contact Flow Log. If you do not specify this parameter, the runbooks uses the AWS account ID of the user or role in which the Automation runs. String
S3BucketOwnerRoleArn (Optional) The ARN of the IAM role with permissions to get the Amazon S3 bucket and account block public access settings, bucket encryption configuration, the bucket ACLs, the bucket policy status, and upload objects to the bucket. If this parameter is not specified, the runbook uses the 'AutomationAssumeRole' (if specified) or user that starts this runbook (if 'AutomationAssumeRole' is not specified). Please see the required permissions section in the runbook description.	

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- CheckConnectInstanceExistence

检查中提供的 Connect Customer 实例ConnectInstanceId是否为ACTIVE。

- CheckS3BucketPublicStatus

检查中指定的 Amazon S3 存储桶是否S3BucketName允许匿名或公开读取或写入访问权限。

- GenerateLogSearchTimeRange

基于 DescribeContact API LastUpdateTimestamp 返回的InitiationTimestamp和EndTime为StartQuery步骤生成StartTime和。StartTime将在一个小时之前InitiationTimestamp，EndTime将是一个小时之后LastUpdateTimestamp。

- StartQuery

启动与ContactId中提供的 Connect Customer 实例关联的 Log CloudWatch s 日志组中提供的内容的查询日志ConnectInstanceId。查询在运行 60 分钟后超时。如果您的查询超时，请缩短搜索的时间范围。您可以在 CloudWatch 控制台中查看当前正在进行的查询以及最近的查询历史记录。有关更多信息，请参阅[查看正在运行的查询或查询历史记录](#)。

- WaitForQueryCompletion

等待提供的 CloudWatch 日志查询日志ContactId完成。请注意，查询将在运行 60 分钟后超时。如果您的查询超时，请缩短搜索的时间范围。您可以在 Connect Customer 控制台中查看当前正在进行的查询以及最近的查询历史记录。有关更多信息，请参阅[查看正在运行的查询或查询历史记录](#)。

- UploadContactFlowLog

获取查询结果并将联系流日志上传到中指定的 Amazon S3 存储桶。S3BucketName

- GenerateReport

返回上传联系流日志的 Amazon S3 控制台 URL 以及可用于下载日志文件的示例 AWS CLI 命令。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- GenerateReport.OutputPayload

输出告诉您运行手册已成功检索到指定联系人的联系流日志。此报告还包含 Amazon S3 控制台 URL 和示例 AWS CLI 命令，以便您可以下载日志文件。

▼ Outputs

GenerateReport.OutputPayload

```
{ "Payload": "
```

```
=====
Amazon Connect Contact Flow Log Collector Result
=====
```

Successfully retrieved Contact Flow log for the contact '01234567-89ab-cdef-0123-456789abcdef'.

You can access the log file from the S3 Console URL below:

- S3 Console URL for the Contact Flow Log file

https://s3.console.aws.amazon.com/s3/object/saw-example-bucket?region=us-west-2&prefix=01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz

Alternatively, you can download the log file by using the AWS CLI command below:

```
aws s3 cp s3://saw-example-bucket/01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz . --region us-west-2
```

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflow 登录页面](#)

AWS Directory Service

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Directory Service 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CreateDSManagementInstance](#)
- [AWSSupport-TroubleshootADConnectorConnectivity](#)
- [AWSSupport-TroubleshootDirectoryTrust](#)

AWS-CreateDSManagementInstance

描述

AWS-CreateDSManagementInstance运行手册创建了一个亚马逊弹性计算云 (Amazon EC2) Windows 实例，你可以用它来管理你的目录。AWS Directory Service 该管理实例不能用于管理 AD Connector 目录。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AmiID

类型：字符串

默认：{{ ssm:/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-Base }}

描述：(可选AMI) Amazon Machine Image() 用于启动实例的 ID。默认情况下，该实例将使用最新的微软 Windows Server 2019 Base AMI 启动。

- DirectoryId

类型：字符串

描述：(必填) 您的目录的 Directory Service 目录 ID。

- **IamInstanceProfileName**

类型：字符串

描述：(可选) IAM 实例配置文件名称。默认情况下，如果不存在名为 Amazon 的实例配置文件 `SSMDirectoryServiceInstanceProfileRole`，则 `SSMDirectoryServiceInstanceProfileRole` 将创建名为 Amazon 的实例配置文件。

默认：亚马逊 `SSMDirectoryServiceInstanceProfileRole`

- **InstanceType**

类型：字符串

默认：t3.medium

允许的值：

- t2.nano
- t2.micro
- t2.small
- t2.medium
- t2.large
- t2.xlarge
- t2.2xlarge
- t3.nano
- t3.micro
- t3.small
- t3.medium
- t3.large
- t3.xlarge
- t3.2xlarge

描述：(可选) 要启动的实例类型。默认为 t3.medium。

- **KeyName**

类型：字符串

描述：(可选) 启动实例时使用的密钥对。Windows 不支持 ED25519 密钥对。默认情况下，实例启动时不使用 key pair (NoKeyPair)。

默认：NoKeyPair

- RemoteAccessCidr

类型：字符串

描述：(可选) 使用开放的 RDP 端口 (端口范围 3389) 创建安全组，由 CIDR IPs 指定 (默认值为 0.0.0.0/0)。如果安全组已存在，则不会对其进行修改，也不会更改规则。

默认：0.0.0.0/0

- SecurityGroupName

类型：字符串

描述：(可选) 安全组名称。默认情况下，如果不存在名为 Amazon 的安全组 SSMDirectoryServiceSecurityGroup，则SSMDirectoryServiceSecurityGroup 将创建一个名为 Amazon 的安全组。

默认：亚马逊 SSMDirectory ServiceSecurityGroup

- 标签

类型：MapList

描述：(可选) 要应用于由自动化创建的资源的关键值对。

默认值： [{"Key":"Description","Value":"Created by AWS Systems Manager Automation"}, {"Key":"Created By","Value":"AWS Systems Manager Automation"}]

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ds:DescribeDirectories
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup

- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam>DeleteInstanceProfile`
- `iam>DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam>ListInstanceProfiles`
- `iam>ListInstanceProfilesForRole`
- `iam:PassRole`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:TagInstanceProfile`
- `iam:TagRole`
- `ssm:CreateDocument`
- `ssm>DeleteDocument`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

文档步骤

- `aws:executeAwsApi` - 收集有关您在 `DirectoryId` 参数中指定的类别的详细信息。
- `aws:executeAwsApi` - 获取启动目录所在的虚拟私有云 (VPC) 的 CIDR 块。
- `aws:executeAwsApi` - 使用您在 `SecurityGroupName` 参数中指定的值创建一个安全组。
- `aws:executeAwsApi` - 为新创建的安全组创建一个入站规则，允许来自您在 `RemoteAccessCidr` 参数中指定的 CIDR 的 RDP 流量。
- `aws:executeAwsApi` - 使用您在 `IamInstanceProfileName` 参数中指定的值创建一个 IAM 角色和实例配置文件。
- `aws:executeAwsApi` - 根据您在运行手册参数中指定的值启动一个 Amazon EC2 实例。
- `aws:executeAwsApi` - 创建 AWS Systems Manager 文档以将新启动的实例加入您的目录。
- `aws:runCommand` - 将新实例加入您的目录。
- `aws:runCommand` - 在新实例上安装远程服务器管理工具。

AWSsupport-TroubleshootADConnectorConnectivity

描述

AWSsupport-TroubleshootADConnectorConnectivity 运行手册将验证 AD Connector 的以下先决条件：

- 检查与 AD Connector 关联的安全组和网络访问控制列表 (ACL) 规则是否允许所需的流量。
- 检查 AWS Systems Manager AWS Security Token Service、和 Amazon CloudWatch 接口 VPC 终端节点是否与 AD Connector 位于同一个虚拟私有云 (VPC) 中。

成功完成先决条件检查后，运行手册将启动两个与您的 AD Connector 位于相同子网中的亚马逊弹性计算云 (Amazon EC2) Linux t2.micro 实例。然后使用 `netcat` 和 `nslookup` 实用程序执行网络连接测试。

[运行此自动化 \(控制台 \)](#)

Important

使用此运行手册可能会 AWS 账户 对您的亚马逊 EC2实例、Amazon Elastic Block Store 卷和 Amazon Machine Image (AMI) 在自动化期间创建。有关更多信息，请参阅 [Amazon Elastic Compute Cloud 定价](#)和 [Amazon Elastic Block Store 定价](#)。

如果该aws:deletestack步骤失败，请转到 AWS CloudFormation 控制台手动删除堆栈。此运行手册创建的堆栈名称以 AWSSupport-TroubleshootADConnectorConnectivity 开头。有关删除 CloudFormation 堆栈的信息，请参阅《AWS CloudFormation 用户指南》中的[删除堆栈](#)。

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DirectoryId

类型：字符串

描述：(必需) 要排除连接问题的 AD Connector 目录的 ID。

- Ec2 InstanceProfile

类型：字符串

最多 128 个字符

描述：(必需) 要分配给为执行连接测试而启动的实例的实例配置文件的名称。您指定的实例配置文件必须附加 AmazonSSManagedInstanceCore 策略或等效的权限。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:DescribeImages
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeVpcEndpoints
- ec2:CreateTags
- ec2:RunInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:ListStackResources
- cloudformation>DeleteStack
- ds:DescribeDirectories
- ssm:SendCommand
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:DescribeInstanceInformation

- iam:PassRole

文档步骤

- aws:assertAwsResourceProperty - 确认 DirectoryId 参数中指定的目录是 AD Connector。
- aws:executeAwsApi - 收集有关 AD Connector 的信息。
- aws:executeAwsApi - 收集与 AD Connector 关联的安全组的相关信息。
- aws:executeAwsApi - 收集与 AD Connector 子网关联的网络 ACL 规则的相关信息。
- aws:executeScript - 评价 AD Connector 安全组规则，以验证是否允许所需的出站流量。
- aws:executeScript - 评价 AD Connector 网络 ACL 规则，以验证是否允许所需的出站和入站网络流量。
- aws:executeScript-检查 AWS Systems Manager、AWS Security Token Service 和 Amazon CloudWatch 接口终端节点是否与 AD Connector 位于同一 VPC 中。
- aws:executeScript - 编译在先前步骤执行的检查的输出。
- aws:branch - 根据先前步骤的输出对自动化进行分支。如果安全组和网络缺少所需的出站和入站规则，则自动化将在此处停止 ACLs。
- aws:createStack-创建 CloudFormation 堆栈以启动 Amazon EC2 实例以执行连接测试。
- aws:executeAwsApi-收集新启动的 IDs Amazon EC2 实例。
- aws:waitForAwsResourceProperty-等待第一个新启动的 Amazon EC2 实例报告为由 AWS Systems Manager 管理。
- aws:waitForAwsResourceProperty-等待第二个新启动的 Amazon EC2 实例报告为由 AWS Systems Manager 管理。
- aws:runCommand-从第一个 Amazon EC2 实例对本地 DNS 服务器 IP 地址执行网络连接测试。
- aws:runCommand-从第二个 Amazon EC2 实例对本地 DNS 服务器 IP 地址执行网络连接测试。
- aws:changeInstanceState-停止用于连接测试的 Amazon EC2 实例。
- aws:deleteStack-删除 CloudFormation 堆栈。
- aws:executeScript-输出有关在自动化无法删除 CloudFormation 堆栈时如何手动删除堆栈的说明。

AWSsupport-TroubleshootDirectoryTrust

描述

该AWSsupport-TroubleshootDirectoryTrust运行手册诊断了与 Microsoft Active Directory 之间的信任创建问题。自动化可确保目录类型支持信任，然后检查相关的安全组规则、网络访问控制列表（网络 ACLs）和路由表中是否存在潜在的连接问题。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DirectoryId

类型：字符串

允许的模式：`^d-[a-z0-9]{10}$`

描述：（必填）AWS Managed Microsoft AD 要进行故障排除的 ID。

- RemoteDomainCidrs

类型：StringList

允许的模式：`^((([0-9]{1,3}([0-9]{1,3}([0-9]{1,3}([0-9]{1,3})))|25[0-5]))\.){3}([0-9]{1,3}([0-9]{1,3}([0-9]{1,3}([0-9]{1,3})))|25[0-5])(\v(3[0-2]([1-9]([1-9]([1-9]([1-9]([0-9]{1,3}([0-9]{1,3}([0-9]{1,3}([0-9]{1,3})))|25[0-5])))))))$`

说明：（必需）您尝试与之建立信任关系的远程域的 CIDR。CIDRs 您可以使用逗号分隔的值添加多个值。例如，172.31.48.0/20、192.168.1.10/32。

- RemoteDomainName

类型：字符串

说明：(必需) 将与之建立信任关系的远程域的完全限定域名。

- RequiredTrafficACL

类型：字符串

描述：(必填) 的默认端口要求 AWS Managed Microsoft AD。在大多数情况下，不应修改默认值。

默认值：{"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123,123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- RequiredTrafficSG

类型：字符串

描述：(必填) 的默认端口要求 AWS Managed Microsoft AD。在大多数情况下，不应修改默认值。

默认值：{"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123,123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- TrustId

类型：字符串

说明：(可选) 要排查问题的信任关系的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ds:DescribeConditionalForwarders
- ds:DescribeDirectories
- ds:DescribeTrusts
- ds:ListIpRoutes
- ec2:DescribeNetworkAcls
- ec2:DescribeSecurityGroups

- `ec2:DescribeSubnets`

文档步骤

- `aws:assertAwsResourceProperty` - 确认目录类型为 AWS Managed Microsoft AD。
- `aws:executeAwsApi`-获取有关信息 AWS Managed Microsoft AD。
- `aws:branch` - 在为 `TrustId` 输入参数提供了值时对自动化进行分支。
- `aws:executeAwsApi` - 获取有关信任关系的信息。
- `aws:executeAwsApi` - 获取 `RemoteDomainName` 的条件转发服务器 DNS IP 地址。
- `aws:executeAwsApi` - 获取有关已添加到 AWS Managed Microsoft AD 的 IP 路由的信息。
- `aws:executeAwsApi`-获取 CIDRs AWS Managed Microsoft AD 子网的。
- `aws:executeAwsApi` - 获取有关与 AWS Managed Microsoft AD 关联的安全组的信息。
- `aws:executeAwsApi`-获取 ACLs 与关联的网络的相关信息 AWS Managed Microsoft AD。
- `aws:executeScript` - 确认 `RemoteDomainCidrs` 为有效值。确认 AWS Managed Microsoft AD 有条件转发器 `RemoteDomainCidrs`，AWS Managed Microsoft AD 如果 `RemoteDomainCidrs` 是非 RFC 1918 IP 地址，则已将必需的 IP 路由添加到中。
- `aws:executeScript` - 评估安全组规则。
- `aws:executeScript`-评估网络 ACLs。

输出

`evalDirectorySecurityGroup.Output`-评估与关联的安全组规则是否 AWS Managed Microsoft AD 允许创建信任所需的流量得出的结果。

`evalAclEntries.output`-评估 ACLs 与关联的网络是否 AWS Managed Microsoft AD 允许创建信任所需的流量所得出的结果。

`evaluateRemoteDomaincidr.Output`-评估 `RemoteDomainCidrs` 它们是否为有效值的结果。确认 AWS Managed Microsoft AD 有条件转发器 `RemoteDomainCidrs`，AWS Managed Microsoft AD 如果 `RemoteDomainCidrs` 是非 RFC 1918 IP 地址，则已将必需的 IP 路由添加到中。

AWS AppSync

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS AppSync 有关运行手册的更多信息，请参阅 [使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWS-EnableAppSyncGraphQLApiLogging](#)

AWS-EnableAppSyncGraphQLApiLogging

描述

AWS-EnableAppSyncGraphQLApiLogging运行手册为您指定的 GraphQL AP AWS AppSync I 启用字段级日志和请求级日志记录。即使已经启用了日志记录，运行手册也会将更改应用于指定的 GraphQL API。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- Apild

类型：字符串

描述：(必填) 您要为其启用日志记录功能的 API 的 ID。

- FieldLogLevel

类型：字符串

有效值：错误 | 全部

描述：(必填) 字段记录级别。

- CloudWatchLogsRoleArn

类型：字符串

描述：(必填) AWS AppSync 假设发布到 Amazon CloudWatch Logs 的服务角色的 ARN。

- ExcludeVerboseContent

类型：布尔值

默认值：False

描述：(可选) 设置True为可排除诸如标题、上下文和已评估的映射模板之类的信息，而不考虑日志级别。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- appsync:GetGraphQLApi
- appsync:UpdateGraphQLApi
- iam:PassRole

文档步骤

- aws: executeAwsApi -收集与主要身份验证类型相关的身份验证类型和配置信息。
- aws: branch-基于身份验证类型的分支。
- aws: executeAwsApi -根据为运行手册的 AWS AppSync 输入参数指定的值更新 GraphQL API 的日志配置。

输出

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse:`
来UpdateGraphQLApi电的回应。
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse:`
来UpdateGraphQLApi电的回应。
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse:`
来UpdateGraphQLApi电的回应。
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse:`
来UpdateGraphQLApi电的回应。

Amazon Athena

AWS Systems Manager 自动化为 Amazon Athena 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

AWS-EnableAthenaWorkGroupEncryptionAtRest

描述

AWS-EnableAthenaWorkGroupEncryptionAtRest运行手册为您指定的 Amazon Athena 工作组启用静态加密。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- WorkGroup

类型：字符串

描述：(必填) 要为其启用静态加密的工作组。

- EncryptionOption

类型：字符串

有效值：SSE_S3 | SSE_KMS | CSE_KMS

描述：(必填) 指定使用哪个加密选项。您可以选择使用 Amazon S3 托管密钥 (SSE_S3) 进行服务器端加密，使用托管密钥进行服务器端加密 (SSE_KMS)，或者使用 AWS KMS 托管密钥进行客户端加密 (CSE_KMS)。AWS KMS

- KmsKeyId

类型：字符串

描述：(可选) 如果您使用的是 AWS KMS 加密选项，请指定要使用的密钥 ARN、密钥 ID 或密钥别名。

- EnableMinimumEncryptionConfiguration

类型：布尔值

默认值：True

描述：(可选) 对写入 Amazon S3 的查询和计算结果对工作组实施最低级别的加密。启用后，工作组用户只能在提交查询时将加密设置为管理员设置的最低级别或更高的级别。此设置不适用于启用 Spark 的工作组。

- EnforceWorkGroupConfiguration

类型：布尔值

默认值：True

描述：(可选) 如果设置为True，则工作组的设置将覆盖客户端设置。如果设置为False，则使用客户端设置。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- athena:GetWorkGroup
- athena:UpdateWorkGroup

文档步骤

- aws: branch-基于参数中指定的加密选项的分支。EncryptionOption
- aws: executeAwsApi -此步骤使用指定的加密设置更新 Athena 工作组。
- aws: executeAwsApi -使用指定的加密设置更新 Athena 工作组。
- aws: assertAwsResource 属性-验证是否已启用工作组的加密。

DynamoDB

AWS Systems Manager 自动化为亚马逊 DynamoDB 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-ChangeDDBRWCapacityMode](#)
- [AWS-CreateDynamoDBBackup](#)
- [AWS-DeleteDynamoDbBackup](#)
- [AWSConfigRemediation-DeleteDynamoDbTable](#)
- [AWS-DeleteDynamoDbTableBackups](#)
- [AWSConfigRemediation-EnableEncryptionOnDynamoDbTable](#)

- [AWSConfigRemediation-EnablePITRForDynamoDbTable](#)
- [AWS-EnableDynamoDbAutoscaling](#)
- [AWS-RestoreDynamoDBTable](#)

AWS-ChangeDDBRWCapacityMode

描述

AWS-ChangeDDBRWCapacityMode运行手册将一个或多个 Amazon DynamoDB (DynamoDB) 表的读/写容量模式更改为按需模式或预配置模式。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CapacityMode

类型：字符串

有效值：已配置 | 按请求付费

描述：(必填) 所需的读/写容量模式。从按需 (pay-per-request) 切换到预配置容量时，必须设置初始预配置容量值。初始预配置容量值是根据过去 30 分钟内表和全局二级索引消耗的读取和写入容量估算得出的。

- ReadCapacityUnits

类型：整数

默认：0

描述：(可选) 在 DynamoDB 返回限制异常之前，每秒消耗的最大强一致性读取次数。

- TableNames

类型：字符串

描述：(必填) 用逗号分隔的 DynamoDB 表名称列表，用于更改... 的读/写容量模式

- WriteCapacityUnits

类型：整数

默认：0

描述：(可选) DynamoDB 返回限制异常之前每秒消耗的最大写入次数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- dynamodb:DescribeTable
- dynamodb:UpdateTable

文档步骤

- aws:executeScript-更改参数中指定的 DynamoDB 表的读/写容量模式。TableNames

输出

更改DDBRWCapacity模式。 SuccessesTables -成功更改容量模式的 DynamoDB 表名称列表

更改DDBRWCapacity模式。 FailedTables -更改容量模式失败的 DynamoDB 表名称映射列表以及失败原因。

AWS-CreateDynamoDBBackup

描述

创建 Amazon DynamoDB 表的备份。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BackupName

类型：字符串

说明：(必需) 要创建的备份的名称。

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- TableName

类型：字符串

说明：(必需) DynamoDB 表的名称。

AWS-DeleteDynamoDbBackup

描述

删除 Amazon DynamoDB 表的备份。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BackupArn

类型：字符串

说明：(必需) 要删除的 DynamoDB 表备份的 ARN。

AWSConfigRemediation-DeleteDynamoDbTable

描述

AWSConfigRemediation-DeleteDynamoDbTable运行手册会删除您指定的 Amazon DynamoDB (DynamoDB) 表。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- TableName

类型：字符串

说明：(必需) 要删除的 DynamoDB 表的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- dynamodb:DeleteTable
- dynamodb:DescribeTable

文档步骤

- aws:executeScript - 删除 TableName 参数中指定的 DynamoDB 表。
- aws:executeScript - 验证 DynamoDB 表已被删除。

AWS-DeleteDynamoDbTableBackups

描述

根据保留天数或计数删除 DynamoDB 表的备份。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- RetentionCount

类型：字符串

默认值：10

说明：(可选) 要为表保留的备份数。如果存在超过指定数量的备份，则删除超过该数量的最旧备份。RetentionCount 或者 RetentionDays 可以使用，但不能两者兼而有之。

- RetentionDays

类型：字符串

说明：(可选) 保留表备份的天数。将删除超过指定天数的备份。RetentionCount 或者 RetentionDays 可以使用，但不能两者兼而有之。

- TableName

类型：字符串

说明：(必需) DynamoDB 表的名称。

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

描述

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable运行手册使用您为参数指定的 () 客户托管密钥对亚马逊 DynamoDB (DynamoDB) 表进行 AWS Key Management Service 加密。AWS KMSKMSKeyId

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- KMSKey我是

类型：字符串

描述：(必需) 您要用于加密您在 TableName 参数中指定的 DynamoDB 表的客户托管密钥的 ARN。

- TableName

类型：字符串

说明：(必需) 您要加密的 DynamoDB 表的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- dynamodb:DescribeTable
- dynamodb:UpdateTable

文档步骤

- aws:executeAwsApi - 加密您在 TableName 参数中指定的 DynamoDB 表。
- aws:waitForAwsResourceProperty - 验证 DynamoDB 表 SSESpecification 的 Enabled 属性是否设置为 true。
- aws:assertAwsResourceProperty - 验证 DynamoDB 表是否使用 KMSKeyId 参数中指定的客户托管密钥进行加密。

AWSConfigRemediation-EnablePITRForDynamoDbTable

描述

AWSConfigRemediation-EnablePITRForDynamoDbTable运行手册允许在您指定的亚马逊 DynamoDB 表上进行 point-in-time恢复 (PITR)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- TableName

类型：字符串

描述：(必填) 要启用恢复的 DynamoDB 表的 point-in-time名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `dynamodb:DescribeContinuousBackups`
- `dynamodb:UpdateContinuousBackups`

文档步骤

- `aws:executeAwsApi`-在参数中指定的 DynamoDB 表上启用 point-in-time 恢复。TableName
- `aws:assertAwsResourceProperty`-确认已在 DynamoDB 表上启用 point-in-time 恢复。

AWS-EnableDynamoDbAutoscaling

描述

AWS-EnableDynamoDbAutoscaling 运行手册为你指定的预配置容量 Amazon DynamoDB 表启用了 Application Auto Scaling。Application Auto Scaling 会根据流量模式动态调整预配置的吞吐容量。有关更多信息，请参阅 Amazon DynamoDB [开发者指南中的使用 DynamoDB 自动扩展自动管理吞吐容量](#)。

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- TableName

类型：字符串

描述：(必填) 要在其上启用 Application Auto Scaling 的 DynamoDB 表的名称。

- MinReadCapacity

类型：整数

描述：(必填) DynamoDB 表的最小预配置吞吐量读取容量单位数。

- MaxReadCapacity

类型：整数

描述：(必填) DynamoDB 表的最大预配置吞吐量读取容量单位数。

- TargetReadCapacityUtilization

类型：整数

描述：(必填) 所需的目标读取容量利用率。目标利用率是某个时间点消耗的预配置吞吐量的百分比。您可以将 auto scaling 目标利用率值设置在 20% 到 90% 之间。

- ReadScaleOutCooldown

类型：整数

描述：(必填) 等待上一次读取容量扩展活动生效所需的时间 (以秒为单位)。

- ReadScaleInCooldown

类型：整数

描述：(必填) 读取容量缩减活动完成后，在另一个缩减活动开始之前的时间 (以秒为单位)。

- MinWriteCapacity

类型：整数

描述：(必填) DynamoDB 表的最小预配置吞吐量写入单位数。

- MaxWriteCapacity

类型：整数

描述：(必填) DynamoDB 表的最大预配置吞吐量写入单位数。

- TargetWriteCapacityUtilization

类型：整数

描述：(必填) 所需的目标写入容量利用率。目标利用率是某个时间点消耗的预配置吞吐量的百分比。您可以将 auto scaling 目标利用率值设置在 20% 到 90% 之间。

- WriteScaleOutCooldown

类型：整数

描述：(必填) 等待上一次写入容量扩展活动生效所需的时间 (以秒为单位)。

- WriteScaleInCooldown

类型：整数

描述：(必填) 写入容量缩减活动完成后，另一个缩减活动开始之前的时间 (以秒为单位)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- application-autoscaling:DescribeScalableTargets
- application-autoscaling:DescribeScalingPolicies
- application-autoscaling:PutScalingPolicy
- application-autoscaling:RegisterScalableTarget
- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi)-在您指定的 DynamoDB 表上配置 Application Auto Scaling。
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep)-休眠以避免 API 限制。
- PutScalingPolicyWrite (aws:executeAwsApi)-配置 DynamoDB 表的目标写入容量利用率。
- PutScalingPolicyWriteDelay (aws:sleep)-休眠以避免 API 限制。
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi)-为 DynamoDB 表配置最小和最大读取容量单位。
- RegisterAppAutoscalingTargetReadDelay (aws:sleep)-休眠以避免 API 限制。

- PutScalingPolicyRead (aws:executeAwsApi)-配置 DynamoDB 表的目标读取容量利用率。
- VerifyDynamoDbAutoscalingEnabled (aws:executeScript)-根据您指定的值验证 DynamoDB 表是否启用了 Application Auto Scaling。

输出

- RegisterAppAutoscalingTargetWrite. 响应
- PutScalingPolicyWrite. 响应
- RegisterAppAutoscalingTargetRead. 响应
- PutScalingPolicyRead. 响应
- VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse

AWS-RestoreDynamoDBTable

描述

AWS-RestoreDynamoDBTable运行手册恢复您使用恢复 (PITR) 指定的 point-in-time亚马逊 DynamoDB 表。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EnablePointInTimeRecoverAsNeeded

类型：布尔值

默认：True

描述：(可选) 确定自动化是否根据需要开启恢复以恢复表。 point-in-time

- GlobalSecondaryIndexOverride

类型：字符串

描述：(可选) 新的全局二级索引，用于替换新表的现有二级索引。

- LocalSecondaryIndexOverride

类型：字符串

描述：(可选) 新的本地二级索引，用于替换新表的现有二级索引。

- RestoreDateTime

类型：字符串

描述：(必填) 在 point-in-time过去 35 天内您要将表恢复到的恢复状态。采用以下格式的指定日期和时间：DD/MM/YYYY HH:MM:SS

- SourceTableArn

类型：字符串

说明：(必需) 要复原的表的 ARN。

- SseSpecificationOverride

类型：字符串

描述：(可选) 用于新表的服务器端加密设置。

- TargetTableName

类型：字符串

描述：(必需) 要恢复的表的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- dynamodb:BatchWriteItem
- dynamodb>DeleteItem
- dynamodb:DescribeTable
- dynamodb:GetItem
- dynamodb:PutItem
- dynamodb:Query
- dynamodb:RestoreTableToPointInTime
- dynamodb:Scan
- dynamodb:UpdateItem

文档步骤

- `aws:executeScript`-使用恢复功能恢复您在参数中指定的 DynamoDB 表。TargetTableName point-in-time

AWS Database Migration Service

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Database Migration Service 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-TroubleshootDMSTableErrors](#)
- [AWSSupport-TroubleshootDMSEndpointConnection](#)

AWSSupport-TroubleshootDMSTableErrors

描述

AWS Systems Manager AWSSupport-TroubleshootDMSTableErrors 自动化运行手册可帮助您自动执行数据库迁移任务或无服务器复制 Table errors 中的故障排除过程。AWS Database Migration Service 当数据库迁移任务或 AWS DMS 服务中创建的无服务器复制无法将表从源端点（源数据库）迁移到目标端点（目标数据库）时，就会发生这些错误。本运行手册分析 CloudWatch 日志中的签名错误消息，特别关注传统数据库迁移任务的任务日志和无服务器复制的无服务器日志。它还针对 AWS DMS 迁移 Table error 过程中遇到的常见错误消息提供了有针对性的建议和补救步骤。

如何工作？

运行手册执行以下步骤：

- 获取有关所提供的 ARN AWS DMS N 的信息，该 ARN 可以是数据库迁移任务，也可以是无服务器复制。
- 通过检查 DescribeReplicationTasks API（用于数据库迁移任务）和 DescribeReplications API（用于无服务器复制）响应中的 FreshStartDate 值，验证所提供的 AWS DMS 资源是否至少启动过一次。如果资源尚未启动，则自动化会引发错误。
- 如果资源已启动，则自动化会使用 TableStatistics 信息检查处于 TableError 状态的表。如果未发现任何错误，则在显示一条确认在指定的数据库迁移任务或无服务器复制中未发现表错误的消息后，自动化将结束工作流程。
- 如果找到带有 TableError 状态的表，则自动化会检查是否为指定 AWS DMS 资源启用了 CloudWatch 日志记录。如果未启用日志记录，则自动化会在显示一条表明未启用日志记录的消息后结束工作流程。

注意：预计将启用 CloudWatch 日志记录，因为自动化依赖于这些日志来分析和识别表处于 TableError 状态的问题。

- 如果启用了日志记录，则自动化会分析 CloudWatch 日志，并为每个处于 TableError 状态的表生成报告。该报告包括常见错误消息的建议，并提供相关的错误日志，以帮助识别和解决阻碍表从 AWS DMS 源端点成功迁移到 AWS DMS 目标端点的问题。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DMSArn

类型：字符串

描述：(必填) 数据库迁移任务或无服务器复制的 ARN

允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:(task|replication-config):[a-zA-Z0-9-]+$`

- StartTimeRange

类型：字符串

描述：(可选) 此参数定义给定数据库迁移任务或无服务器复制的 CloudWatch 日志分析时间范围的起点。如果提供，则仅收集和分析从该特定时间起生成的日志。请注意，如果startDate和之间的时间范围太长，endDate则工作流程可能会超时。该值应以 ISO 6081 日期时间格式提供。

允许的模式：`^$|^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\(\d{3})Z$`

- EndTimeRange

类型：字符串

描述：(可选) 此参数设置给定数据库迁移任务或无服务器复制的 CloudWatch 日志分析的时间范围的结束时间。如果提供，则仅收集和分析在此特定时间之前生成的日志。请注意，如果startDate和之间的时间范围太长，endDate则工作流程可能会超时。该值应以 ISO 6081 日期时间格式提供。

允许的模式：`^$|^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3})Z$`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `dms:DescribeReplicationTasks`
- `dms:DescribeReplications`
- `dms:DescribeEndpoints`
- `dms:DescribeReplicationConfigs`
- `dms:DescribeTableStatistics`
- `dms:DescribeReplicationTableStatistics`
- `logs:FilterLogEvents`

自动化承担角色的 IAM policy 示例

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeReplicationConfigs",
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationTableStatistics",
        "dms:DescribeTableStatistics",
        "logs:FilterLogEvents",
        "dms:DescribeReplicationTasks",
        "dms:DescribeReplications"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootDMSTableErrors](#) 在 Systems Manager 的“文档”下导航至。

2. 选择 Execute automation (执行自动化) 。

3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DMSArn

存在表错误的数据库迁移任务或无服务器复制的 ARN。

- StartTimeRange

(可选) ISO 6081 日期时间格式，定义了分析给定数据库迁移任务或无服务器复制 CloudWatch 日志的时间范围的开始时间。

- EndTimeRange

(可选) ISO 6081 日期时间格式，定义了分析给定数据库迁移任务或无服务器复制 CloudWatch 日志的时间范围的结束时间。

4. 从页面底部选择“执行”按钮。

5. 自动化启动。

6. 文档将执行以下步骤：

- 验证 DMSInput TypeAndGatherDetails

验证给定的 AR AWS DMS N 输入并收集后续步骤所需的数据库迁移任务或无服务器复制的基本细节。

- branchOnTable错误

根据上述步骤中发现的表格错误数量对工作流程进行分支。如果计数大于 0，则继续执行-branchOnCWLoggingStatus 步骤。否则，请继续执行-outputNoTableErrors 步骤。

- outputNoTable 错误

输出一条消息，说明在给定的数据库迁移任务或无服务器复制中未发现表错误。

- Branch CWLogging On 状态

根据上述步骤中发现的 CloudWatch 日志状态对工作流程进行分支。如果已启用，则继续执行-gatherTableDetails 步骤。否则，请继续执行-outputNoCWLoggingEnabled 步骤。

- OutputNo CWLogging 已启用

输出一条消息，说明在给定的数据库迁移任务或无服务器复制中未启用 CloudWatch 日志记录。

- gatherTableDetails

收集失败表FullLoadEndTime的时间戳并计算时间范围值以分析日志。 CloudWatch

- analyzeCloudWatch 日志

根据签名错误消息分析在 CloudWatch 日志组中找到的日志，并将报告返回给用户。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果。

- 未找到表错误的输出

如果在提供的数据库迁移任务或无服务器复制中未发现表错误，则自动化会显示相同的输出。

- 输出为“未启用 CloudWatch 登录”

如果在提供的数据库迁移任务或无服务器复制中未启用 CloudWatch 日志记录，则自动化会显示同样的输出并提供启用日志记录的步骤。

- 日志分析报告

输出一份报告，该报告可识别所提供的数据库迁移任务或无服务器复制中Table error处于状态的表，区分错误类型，列出遇到的错误消息，并为每个已识别的表提供有针对性的修复步骤和建议。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflow 登录页面](#)

AWSSupport-TroubleshootDMSEndpointConnection

描述

该AWSSupport-TroubleshootDMSEndpointConnection运行手册有助于诊断和解决 AWS Database Migration Service 复制实例和 AWS DMS 终端节点之间的连接问题。自动化使用 [Reachability Analyzer](#) 检查来测试网络连接，并分析网络配置，以识别可能阻碍成功迁移的潜在连接问题。AWS DMS

Important

在运行本运行手册之前，您必须已使用 AWS DMS 控制台或 API 测试了 AWS DMS 复制实例和终端节点之间的连接。如果您尚未测试连接，请先进行测试，否则可能需要重新运行此运行手册。AWS DMS 复制实例和终端节点都必须处于可用状态，才能进行准确的连接测试。

Important

该运行手册创建和调用 AWS Lambda 函数，这将产生 Lambda 费用。每次 Reachability Analyzer 分析运行也会产生费用。有关定价详情，请参阅网络分析选项卡下的 [Amazon VPC 定价](#) 页面和 [AWS Lambda 定价](#)。

如何工作？

该运行手册通过以下阶段对 AWS DMS 连接进行系统分析：

第 1 阶段：资源验证和先决条件

- 端点验证：验证 AWS DMS 端点是否存在，检索其配置（服务器名称、端口、引擎类型），并确认支持数据库引擎进行故障排除。
- 连接测试状态：使用 AWS DMS DescribeConnections API 检索复制实例和终端节点之间的当前连接测试状态，包括先前测试尝试中的任何失败消息。
- 复制实例分析：收集网络配置详细信息，包括 Amazon VPC ID IDs、子网 IDs、安全组，并识别复制实例的关联弹性网络接口 (ENI)。

第 2 阶段：DNS 解析和网络路径发现

- 基于 Amazon VPC 的 DNS 解析：在与复制实例相同的亚马逊 VPC 内创建一个临时 Lambda 函数，以便在亚马逊 VPC 环境中将终端节点主机名解析为其 IP 地址，从而确保精确的私有 DNS 解析。
- 目标识别：根据终端节点是在同一 Amazon VPC（使用 ENI）还是外部（使用已解析的 IP 地址）内，确定 Reachability Analyzer 的相应目标。
- IPv6 兼容性检查：验证已解析的地址是否是 IPv4，因为 Reachability Analyzer 不支持地址。IPv6

第 3 阶段：全面的网络路径分析

- Reachability Analyzer Execution：创建从复制实例 ENI 到目标（端点 ENI 或 IP 地址）的网络洞察路径，并执行全面分析以测试指定端口上的 TCP 连接。
- 多层网络分析：检查完整的网络路径，包括路由表、安全组、网络、Internet 网关 ACLs、NAT 网关、Amazon VPC 对等连接和传输网关，以确定连接障碍。
- 详细解释生成：对于失败的连接，提供了每个阻塞流量的网络组件的具体说明，包括确切的规则号、CIDR 块、端口范围和协议限制。

第 4 阶段：报告生成和资源清理

- 综合报告：生成一份详细的报告，其中包含连接测试摘要、网络路径分析结果和具体的故障说明以及补救指南。
- 资源管理：自动清理创建的资源（Lambda 函数、IAM 角色、网络洞察路径），除非 PersistReachabilityAnalyzerResults 将参数设置为保留分析结果以供进一步调查。
- 错误处理：为各种故障场景提供特定的错误报告，包括不支持的数据库引擎、资源缺失、DNS 解析失败和权限问题。

该运行手册支持对多个数据库引擎的连接进行故障排除，包括亚马逊 Aurora、亚马逊文档数据库、亚马逊 DynamoDB、亚马逊 Neptune、亚马逊 Redshift、亚马逊 S3、Azure SQL 数据库、MySQL、Oracle、PostgreSQL DB2、SQL Server 等。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- dms:DescribeEndpoints
- dms:DescribeReplicationInstances
- dms:DescribeConnections
- iam:GetRole
- iam:PassRole
- iam:SimulatePrincipalPolicy
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction
- lambda:ListTags
- lambda:TagResource
- lambda:UntagResource
- lambda:UpdateFunctionCode

可选的 IAM 权限

仅当您不提供LambdaRoleArn参数并希望自动化为您创建 Lambda 执行角色时，才需要在中拥有以下权限：AutomationAssumeRole

- iam:CreateRole
- iam>DeleteRole
- iam:AttachRolePolicy

- iam:DetachRolePolicy
- iam:TagRole
- iam:UntagRole

Important

除了上述操作外，还AutomationAssumeRole应将[亚马逊 VPCReachabilityAnalyzerFullAccessPolicy](#)作为 [附加的托管策略](#)，以便成功执行 [Reachability Analyzer](#) 测试。

策略示例：

```
{
  "Version": "2012-10-17"      ,
  "Statement": [
    {
      "Sid": "AllowDMSTroubleshootingActions",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
        "dms:DescribeConnections",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
      ]
    }
  ]
}
```

```

        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowDMSLambdaInvocation",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": "arn:*:lambda:*:*:function:AWSSupport-
TroubleshootDMSEndpointConnection-*"
    },
    {
        "Sid": "AllowPassRoleToDMSLambda",
        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:*:iam:*:*:role/AWSSupport-
TroubleshootDMSEndpointConnection-*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": "lambda.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AllowRolePolicyManagement",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:DetachRolePolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:ResourceTag/AWSSupport-
TroubleshootDMSEndpointConnection": "true"
            }
        }
    }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootDMSEndpointConnection](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，SSM Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - DmsEndpointArn (必填)
 - 描述：(必填) 终端节点的亚马逊资源名称 (ARN)。AWS Database Migration Service
 - 类型：String
 - 允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+\:\d{12}:endpoint:[A-Z0-9]{1,48}$`
 - DmsReplicationInstanceArn (必填)
 - 描述：(必填) AWS Database Migration Service 复制实例的 Amazon 资源名称 (ARN)。
 - 类型：String
 - 允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+\:\d{12}:rep:[A-Z0-9]+$`
 - PersistReachabilityAnalyzerResults (可选)
 - 描述：(可选) 指示是否应保留网络洞察分析执行结果的标志。
 - 类型：Boolean
 - 允许的值：`[true, false]`
 - 默认值：`false`
 - LambdaRoleArn (可选)

- 描述：(可选) 允许该 AWS Lambda 函数访问所需 AWS 服务和资源的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定任何角色，则此 Systems Manager Automation 将在您的账户中为 Lambda 创建一个 IAM 角色。
- 类型：AWS::IAM::Role::Arn
- 默认值：""
- 确认 (必填)
 - 描述：(必填) 输入 yes 以确认本运行手册将在您的账户中创建 Lambda 函数，如果 LambdaRoleArn 未提供，则将创建 IAM 角色。
 - 类型：String
 - 允许的模式：^[Yy][Ee][Ss]\$

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- DescribeEndpointAndCheckEngine:

检索 AWS DMS 端点配置并验证是否支持数据库引擎类型进行故障排除。从端点配置中提取服务器名称、端口和引擎类型。

- BranchOnEndpointAndCheckEngineErrors:

根据端点验证中的任何错误对自动化进行分支。如果发现错误，自动化将继续生成错误报告；否则，它会继续进行连接测试。

- GetTestConnectionStatus:

使用 DescribeConnections API 检索 AWS DMS 终端节点的连接状态和错误消息。此步骤检查是否已执行连接测试并捕获任何失败消息。

- BranchOnTestConnectionStatusErrors:

根据连接测试状态错误对自动化进行分支。如果检测到错误，则自动化会生成错误报告；否则，它会继续进行复制实例分析。

- DescribeReplicationInstance:

检索 AWS DMS 复制实例的网络配置详细信息，包括 Amazon VPC ID、子网 IDs、安全组 IDs，并识别相关的弹性网络接口 (ENI)。

- ValidateResourcePermissions:

验证执行角色是否具有清理将在自动化过程中创建的资源的必要权限。

- 创建 DNSResolver Lambda :

创建一个 AWS CloudFormation 堆栈，其中包含 Lambda 函数，该函数部署在与复制实例相同的 Amazon VPC 中。此函数用于在 Amazon VPC 环境中将 DNS 名称解析为私有 IP 地址。

- DescribeCloudFormationErrorFromStackEvents:

如果 CloudFormation 堆栈创建失败，则此步骤描述堆栈事件中的错误，以提供详细的故障信息以进行故障排除。

- 获取 DNSResolverLambdaName :

从 CloudFormation 堆栈输出中检索 DNS 解析器 Lambda 函数的名称，以便在后续步骤中使用。

- ResolveDmsEndpoint:

在亚马逊 VPC 内调用 Lambda 函数将 AWS DMS 终端节点主机名解析为其 IP 地址。这可确保精确的私有 DNS 解析并验证 IPv4 兼容性。

- BranchOnResolveDmsEndpointErrors:

根据 DNS 解析错误对自动化进行分支。如果端点无法解析或无法解析到 IPv6 地址，则自动化会生成错误报告。

- GetReachabilityAnalyzerTarget:

根据亚马逊 VPC 配置和终端节点位置为 Reachability Analyzer 确定合适的目标。确定是使用 ENI (对于相同的亚马逊 VPC 终端节点) 还是 IP 地址 (对于外部终端节点) 作为目标。

- GenerateErrors:

在前面的步骤中出现故障时，创建全面的错误报告。这包括有关端点验证错误、连接测试失败或 DNS 解析问题的详细信息以及特定的补救指南。

- GenerateReport:

创建一份全面的故障排除报告，其中包含连接状态、使用 Reachability Analyzer 的网络路径分析结果、连接障碍的详细说明以及建议的解决措施。

- CheckStackExists:

检查 CloudFormation 堆栈是否已成功创建，是否需要在清理期间删除。无论自动化成功与否，此步骤均可确保适当的资源管理。

- 删除 DNSResolver Lambda :

删除包含 DNS 解析器 Lambda 函数和相关资源的 CloudFormation 堆栈

(`PersistReachabilityAnalyzerResults` 除非设置 `true` 为)，确保自动化完成后没有剩余资源。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- `GetTestConnectionStatus`. `status`

AWS DMS 复制实例和端点之间的当前连接测试状态（例如，成功、失败、正在测试）。

- `DescribeCloudFormationErrorFromStackEvents`. 活动

如果 CloudFormation 堆栈创建失败，则此输出将包含堆栈创建过程中的详细错误事件，以帮助诊断基础架构部署问题。

- `GenerateReport`. 报告

一份全面的故障排除报告，其中包含连接分析结果、Reachability Analyzer 调查结果、网络路径分析、确定的特定连接障碍以及详细的补救建议，以及相关文档的链接。AWS

- `GenerateErrors`. 报告

如果在自动化过程中出现错误，则此输出将提供详细的错误报告，包括具体的失败原因、受影响的资源以及在重试自动化之前解决问题的指导。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

Amazon EBS

AWS Systems Manager Automation 为 Amazon Elastic Block Store 提供有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSsupport-AnalyzeEBSResourceUsage](#)

- [AWS-ArchiveEBSVolumeSnapshots](#)
- [AWS-AttachEBSVolume](#)
- [AWSSupport-CalculateEBSPerformanceMetrics](#)
- [AWS-CopySnapshot](#)
- [AWS-CreateSnapshot](#)
- [AWS-DeleteSnapshot](#)
- [AWSConfigRemediation-DeleteUnusedEBSVolume](#)
- [AWS-DeregisterAMIs](#)
- [AWS-DetachEBSVolume](#)
- [AWSConfigRemediation-EnableEbsEncryptionByDefault](#)
- [AWS-ExtendEbsVolume](#)
- [AWSSupport-ModifyEBSSnapshotPermission](#)
- [AWSConfigRemediation-ModifyEBSVolumeType](#)

AWSsupport -AnalyzeEBSResourceUsage

描述

AWSsupport -AnalyzeEBSResourceUsage 自动化运行手册用于分析亚马逊 Elastic Block Store (Amazon EBS) 上的资源使用情况。它会分析卷使用情况并识别给定 AWS 区域中废弃的卷、图像和快照。

如何工作？

运行手册执行以下四项任务：

1. 验证亚马逊简单存储服务 (Amazon S3) 存储桶是否存在，或者创建一个新的亚马逊 S3 存储桶。
2. 收集所有处于可用状态的 Amazon EBS 卷。
3. 收集源卷已被删除的所有 Amazon EBS 快照。
4. 收集所有未被任何未终止的亚马逊弹性计算云 (Amazon EC2) 实例使用的亚马逊机器映像 (AMI)。

运行手册生成 CSV 报告并将其存储在用户提供的 Amazon S3 存储桶中。所提供的存储桶应按照最后概述 AWS 的安全最佳实践进行保护。如果账户中不存在用户提供的 Amazon S3 存储桶，则运行手册

会创建一个名称格式的新 Amazon S3 存储桶<User-provided-name>-awssupport-YYYY-MM-DD，使用自定义 AWS Key Management Service (AWS KMS) 密钥加密，启用对象版本控制，禁止公开访问，并且需要请求才能使用。SSL/TLS

如果您想指定自己的 Amazon S3 存储桶，请确保按照以下最佳实践对其进行配置：

- 阻止公众访问存储桶 (设置IsPublic为False)。
- 打开 Amazon S3 访问日志记录。
- [仅允许向您的存储桶发出 SSL 请求](#)。
- 开启对象版本控制。
- 使用 AWS Key Management Service (AWS KMS) 密钥加密您的存储桶。

Important

使用此运行手册可能会因创建 Amazon S3 存储桶和对象而对您的账户产生额外费用。有关可能产生的费用的更多详细信息，请参阅 [Amazon S3 定价](#)。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3BucketName

类型：AWS::S3::Bucket::Name

描述：(必填) 您账户中用于上传报告的 Amazon S3 存储桶。确保存储桶策略不会向不需要访问所收集日志的各方授予不必要的 read/write 权限。如果账户中不存在指定的存储桶，则自动化会在以名称格式启动自动化的区域中创建一个新的存储桶<User-provided-name>-awssupport-YYYY-MM-DD，并使用自定义 AWS KMS 密钥进行加密。

允许的模式：`$|^(?!((([0-9]{1,3}[.]){3}[0-9]{1,3}$))^(?!xn-)(?!.*-s3alias)))[a-z0-9][-a-z0-9]{1,61}[a-z0-9]$`

- CustomerManagedKmsKeyArn

类型：字符串

描述：(可选) 自定义 AWS KMS 密钥 Amazon 资源名称 (ARN)，用于加密新的 Amazon S3 存储桶，如果账户中不存在指定的存储桶，则将创建该存储桶。如果在未指定自定义 AWS KMS 密钥 ARN 的情况下尝试创建存储桶，则自动化将失败。

允许的模式：`(^$|^arn:aws:kms:[-a-z0-9]:[0-9]:key/[-a-z0-9]*$)`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeSnapshots
- ec2:DescribeVolumes
- kms:Decrypt
- kms:GenerateDataKey
- s3:CreateBucket
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:ListBucket

- s3:ListAllMyBuckets
- s3:PutObject
- s3:PutBucketLogging
- s3:PutBucketPolicy
- s3:PutBucketPublicAccessBlock
- s3:PutBucketTagging
- s3:PutBucketVersioning
- s3:PutEncryptionConfiguration
- ssm:DescribeAutomationExecutions

具有运行此运行手册所需的最低 IAM 权限的策略示例：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "KMSGeneratePermissions",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Sid": "S3ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket2/"
    ]
}, {
    "Sid": "S3CreatePermissions",
    "Effect": "Allow",
    "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketLogging",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
    ],
    "Resource": "*"
}]
}

```

说明

按照这些步骤对自动化进行配置：

1. 导航到 AWS Systems Manager 控制台 [AWSSupport-AnalyzeEBSResourceUsage](#) 中的。
2. 要输入参数，请输入以下内容：

- AutomationAssumeRole（可选）：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3BucketName（必填）：

您账户中用于将报告上传到的 Amazon S3 存储桶。

- CustomerManagedKmsKeyArn (可选) :

自定义 AWS KMS 密钥 Amazon 资源名称 (ARN)，用于加密在账户中不存在指定的存储桶时创建的新 Amazon S3 存储桶。

Input parameters

S3BucketName
(Optional) The Amazon Simple Storage Service (S3) bucket in your account to upload the report to. Please make sure the bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs. If the bucket specified does not exist in the account, then automation will create a new bucket in region where automation is executed with name format **<User-provided-name>-awssupport-YYYY-MM-DD***, encrypted with custom Key Management Service (KMS) key

Enter the name of an existing S3 Bucket

S3 Bucket
test-bucket-1
Example: s3-bucket-name

AutomationAssumeRole
(Optional) The ARN of the role that allows Automation to perform the actions on your behalf. If role is not specified, Systems Manager Automation uses the permission of the user that runs this document.

Select an existing IAM Role

admin-my
arn:aws:iam:::role/

CustomerManagedKmsKeyArn
(Optional) The custom KMS key ARN for encrypting the new Amazon Simple Storage Service (S3) bucket that will be created in case the bucket specified does not exist in the account. Automation will fail if bucket creation is attempted without specifying custom KMS key ARN

arn:aws:kms:eu-central-1:::key/:-4216-a498-460a2132ca4c

3. 选择执行。
4. 自动化启动。
5. 自动化运行手册执行以下步骤：

- 检查并发性：

确保该地区只有一个启动该运行手册。如果 runbook 发现另一个正在执行的执行，则会返回错误并结束。

- 验证 OrCreate s3Bucket：

验证 Amazon S3 存储桶是否存在。否则，它会在以名称格式启动自动化的区域创建一个新的 Amazon S3 存储桶<User-provided-name>-awssupport-YYYY-MM-DD，并使用自定义 AWS KMS 密钥进行加密。

- 收集AmiDetails：

搜索任何 Amazon EC2 实例未使用的 AMI，生成名称格式的报告<region>-images.csv，然后将其上传到 Amazon S3 存储桶。

- 收集VolumeDetails：

验证 Amazon EBS 卷是否处于可用状态，生成名称格式的报告<region>-volume.csv，然后将其上传到 Amazon S3 存储桶中。

- 收集SnapshotDetails：

查找已删除的 Amazon EBS 卷的 Amazon EBS 快照，生成名称格式的报告<region>-snapshot.csv，然后将其上传到 Amazon S3 存储桶。

6. 完成后，查看“输出”部分以了解执行的详细结果。

▼ Outputs	
gatherVolumeDetails.gatherVolumeDetailsOutput No volume found in available state in region eu-central-1	verifyOrCreateS3bucket.createdNewBucket true
gatherAmiDetails.gatherAmiDetailsOutput File eu-central-1-image.csv have been uploaded to bucket aws-support-ssm-[REDACTED]1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those AMI.	
gatherSnapshotDetails.gatherSnapshotDetailsOutput File eu-central-1-snapshot.csv have been uploaded to bucket aws-support-ssm-[REDACTED]1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those snapshots.	

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWS-ArchiveEBSVolumeSnapshots

描述

AWS-ArchiveEBSVolumeSnapshots 运行手册通过指定您应用于快照的标签，帮助您归档 Amazon Elastic Block Store (Amazon EBS) 卷的快照。或者，如果您的快照未加标签，您可以提供卷的 ID。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 说明

类型：字符串

描述：(可选) 对 Amazon EBS 快照的说明。

- DryRun

类型：字符串

有效值：是 | 否

描述：(必需) 在未实际发出请求的情况下检查您是否拥有该操作所需的权限，并提供错误响应。

- RetentionCount

类型：字符串

描述：(可选) 要归档的快照数量。如果您为 RetentionDays 参数指定了一个值，则不要为此参数指定值。

- RetentionDays

类型：字符串

描述：(可选) 要归档的前几天快照的数量。如果您为 RetentionCount 参数指定了一个值，则不要为此参数指定值。

- SnapshotWithTag

类型：字符串

有效值：是 | 否

描述：(必需) 指定要归档的快照是否已添加标签。

- TagKey

类型：字符串

描述：(可选) 分配给要归档快照的标签的键。

- TagValue

类型：字符串

描述：(可选) 分配给要归档快照的标签的值。

- VolumeId

类型：字符串

描述：(可选) 要归档快照的卷 ID。如果快照未添加标签，请使用此参数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

文档步骤

aws:executeScript - 使用您用 TagKey 和 TagValue 参数指定的标签或参数 VolumeId 对快照进行归档。

AWS-AttachEBSVolume

描述

将 Amazon Elastic Block Store (Amazon EBS) 卷挂载到 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 设备

类型：字符串

描述：(必填) 设备名称 (例如，/dev/sdh 或 xvdh)。

- InstanceId

类型：字符串

描述：(必需) 要附加卷的实例的 ID。

- VolumeId

类型：字符串

描述：(必需) Amazon EBS 卷的 ID。该卷与实例必须位于同一可用区。

AWSSupport-CalculateEBSPerformanceMetrics

描述

该AWSSupport-CalculateEBSPerformanceMetrics运行手册通过计算性能指标并将其发布到控制面板来帮助诊断 Amazon EBS 性能问题。CloudWatch 控制面板显示目标亚马逊 EBS

卷或连接到目标亚马逊弹性计算云 (Amazon EC2) 实例的所有卷的估计平均 IOPS 和吞吐量。对于 Amazon EC2 实例，它还会显示实例的平均 IOPS 和吞吐量。运行手册输出指向新创建的仪表板的链接，该 CloudWatch 仪表板显示了相关的计算 CloudWatch 指标。CloudWatch 控制面板是在您的账户中创建的，名称为:AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>。

如何工作？

运行手册执行以下步骤：

- 确保指定的时间戳有效。
- 验证资源 ID (亚马逊 EBS 卷或亚马逊 EC2 实例) 是否有效。
- 当您提供 Amazon EC2 作为资源 ID 时，它会 CloudWatch 创建一个控制面板，其中包含该 Amazon EC2 实例的实际 IOPS/Throughput 总数和附加到 Amazon EC2 实例的所有亚马逊 EBS 卷的估计 IOPS/Throughput 平均值图表。
- 当您提供 Amazon EBS 卷作为资源 ID 时，它会 CloudWatch 创建一个包含该交易量的估计 IOPS/Throughput 平均值图表的控制面板。
- 生成 CloudWatch 控制面板后，如果估计平均 IOPS 或估计平均吞吐量分别超过最大 IOPS 或最大吞吐量，则连接到 Amazon EC2 实例的一个或多个卷可能会出现微爆发。

Note

对于可突发卷 (gp2、sc2 和 st1)，在获得突发平衡之前，IOPS/throughput 应考虑最大值。在完全利用突发平衡 (即突发平衡变为零) 之后，请考虑基线 IOPS/throughput 指标。

Important

创建 CloudWatch 控制面板可能会导致您的账户产生额外费用。有关更多信息，请参阅 [Amazon CloudWatch 定价指南](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeVolumes
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- cloudwatch:PutDashboard

政策示例

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
      "Resource": "arn:aws:cloudwatch::111122223333:dashboard/*-EBS-Performance-*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceTypes"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-CalculateEBSPerformanceMetrics](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 资源 ID (必填)：

亚马逊 EC2 实例或亚马逊 EBS 卷的 ID。

- 开始时间 (必填)：

查看数据的开始时间 CloudWatch。时间必须采用格式yyyy-mm-ddThh:mm:ss和 UTC。

- 结束时间 (必填)：

查看数据的结束时间 CloudWatch。时间必须采用格式yyyy-mm-ddThh:mm:ss和 UTC。

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. 	ResourceId (Required) The ID of the EC2 instance or EBS Volume.
StartTime (Required) The start time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddThh:mm:ss' and in UTC. 	EndTime (Required) The end time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddThh:mm:ss' and in UTC.

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- CheckResourceIdAndTimeStamps:

检查结束时间是否比开始时间大于至少一分钟，以及所提供的资源是否存在。

- CreateCloudWatchDashboard:

计算 Amazon EBS 绩效并根据您的资源 ID 显示图表。如果您为参数“资源 ID”提供了 Amazon EBS 卷 ID，则本运行手册将创建一个 CloudWatch 控制面板，其中包含估算的平均 IOPS 和估算的 Amazon EBS 卷平均吞吐量。如果您为参数“资源 ID”提供了 Amazon EC2 实例 ID，则本运行手册将创建一个 CloudWatch 控制面板，其中包含亚马逊 EC2 实例的平均总 IOPS 和平均总吞吐量，以及附加到 Amazon EC2 实例的所有 Amazon EBS 卷的估计平均 IOPS 和估计的平均吞吐量。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

```
▼ Outputs

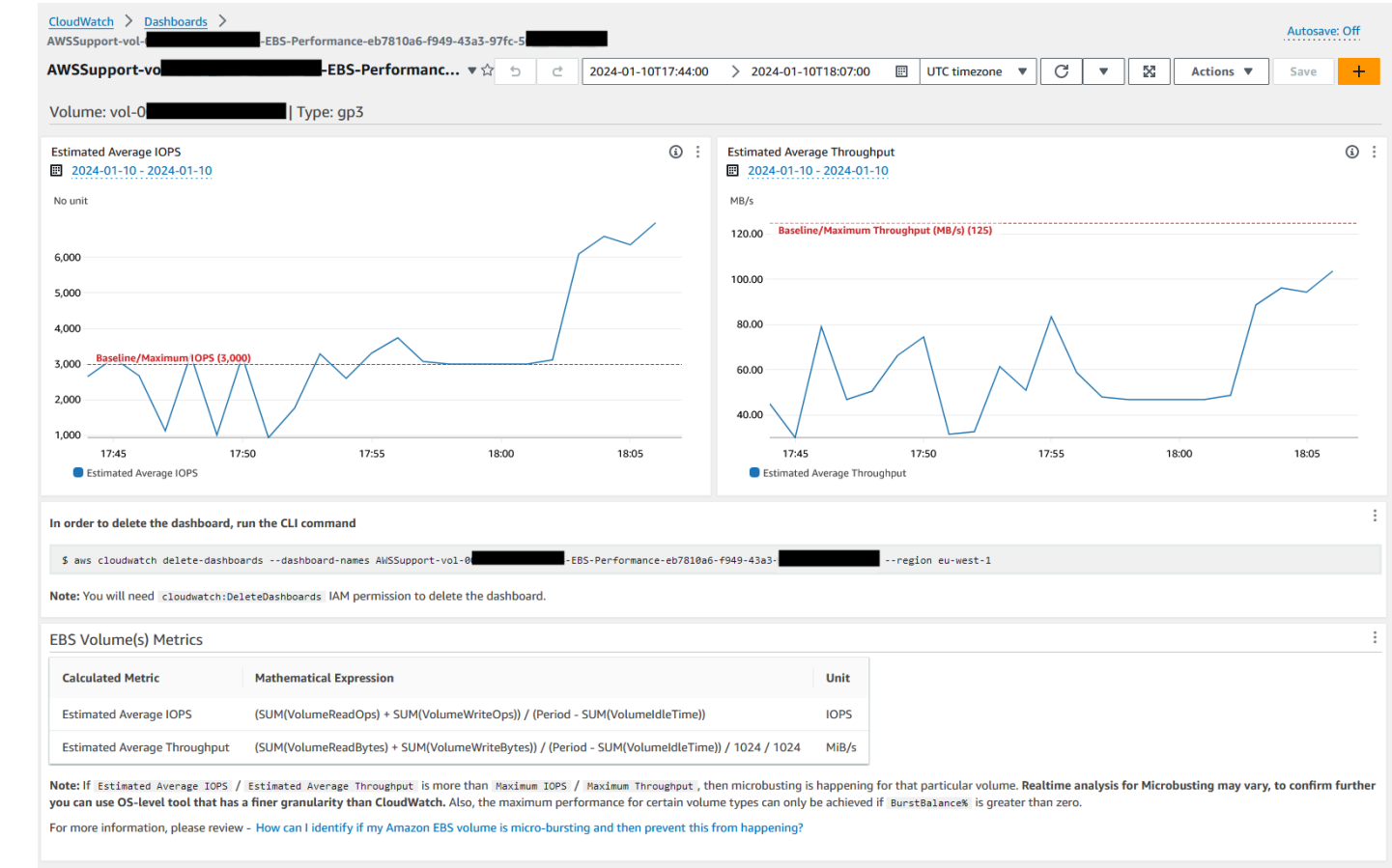
CreateCloudWatchDashboard.CloudWatchDashboardLink
https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=AWSsupport-i-██████████EBS-Performance-443096c1-df23-44ba-96dd-2d005b5ae971

CreateCloudWatchDashboard.CloudWatchDashboardMessage
Open the CloudWatch Dashboard URL in your browser to see the performance metrics for the target resource 'i-██████████'.
You can delete the CloudWatch Dashboard from the CloudWatch console.
```

作为 Amazon EC2 实例的资源 ID 的示例 CloudWatch 控制面板



资源 ID 为 Amazon EBS 卷 ID 的示例 CloudWatch 控制面板



参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

AWS 服务文档

- [如何识别我的 Amazon EBS 交易量是否处于微爆状态，然后防止这种情况发生？](#)
- [CloudWatch 如何使用查看 EC2 实例的 Amazon EBS 综合性能指标？](#)

AWS-CopySnapshot

描述

复制 Amazon Elastic Block Store (Amazon EBS) 卷的时间点快照。您可以在同一区域内复制快照，AWS 区域 也可以将快照从一个区域复制到另一个区域。加密 Amazon EBS 快照的副本保持加密状态。未加密快照的副本保持未加密状态。要复制从另一个账户共享的加密快照，您必须拥有对用于加密快照的 KMS 密钥的权限。通过复制其他快照创建的快照具有一个不应用于任何用途的任意卷 ID。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 说明

类型：字符串

描述：(可选) 对 Amazon EBS 快照的说明。

- SnapshotId

类型：字符串

描述：(必需) 要复制的 Amazon EBS 快照的 ID。

- SourceRegion

类型：字符串

描述：(必需) 源快照当前所在的区域。

文档步骤

copySnapshot - 复制 Amazon EBS 卷的快照。

输出

copy Snapshot.SnapshotId -新快照的 ID。

AWS-CreateSnapshot

描述

创建 Amazon EBS 卷的快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 说明

类型：字符串

描述：(可选) 对快照的说明

- Volumeld

类型：字符串

描述：(必需) 卷的 ID。

AWS-DeleteSnapshot

描述

删除 Amazon EBS 卷快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- SnapshotId

类型：字符串

描述：(必需) EBS 快照的 ID。

AWSConfigRemediation-DeleteUnusedEBSVolume

描述

AWSConfigRemediation-DeleteUnusedEBSVolume 运行手册将删除未使用的 Amazon Elastic Block Store (Amazon EBS) 卷。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- CreateSnapshot

类型：布尔值

描述：(可选) 如果设置为 true , 则自动化会在 Amazon EBS 卷删除之前创建该卷的快照。

- Volumeld

类型：字符串

描述：(必需) 要删除的 Amazon EBS 卷的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateSnapshot
- ec2:DeleteVolume
- ec2:DescribeSnapshots
- ec2:DescribeVolumes

文档步骤

- aws:executeScript - 验证您在 VolumeId 参数中指定的 Amazon EBS 卷未在用，并根据您为 CreateSnapshot 参数选择的值创建一个快照。
- aws:branch - 根据您为 CreateSnapshot 参数选择的值进行分支。
- aws:waitForAwsResourceProperty - 等待快照完成。
- aws:executeAwsApi - 在快照创建失败时删除快照。
- aws:executeAwsApi - 删除您在 VolumeId 参数中指定的 Amazon EBS 卷。
- aws:executeScript - 验证 Amazon EBS 卷已被删除。

AWS-DeregisterAMIs

描述

AWS-DeregisterAMIs 运行手册使用指定已应用于 AMIs 的标签来帮助您取消注册 Amazon Machine Images (AMIs)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DryRun

类型：字符串

有效值：是 | 否

描述：(必需) 在未实际发出请求的情况下检查您是否拥有该操作所需的权限，并提供错误响应。

- RetainNumber

类型：字符串

描述：(可选) 要保留的 AMIs 的数量。如果您为 Age 参数指定了一个值，则不要为此参数指定值。

- 天数

类型：字符串

描述：(可选) 要保留的前几天的 AMIs 数量。如果您为 RetainNumber 参数指定了一个值，则不要为此参数指定值。

- TagKey

类型：字符串

描述：(必需) 分配给要取消注册 AMIs 的标签的键。

- TagValue

类型：字符串

描述：(必需) 分配给要取消注册 AMIs 的标签的值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DeregisterImage
- ec2:DescribeImages

文档步骤

- aws:executeAwsApi - 验证您为运行手册输入参数指定的值。
- aws:executeAwsApi - 使用您用 TagKey 和 TagValue 参数指定的标签来取消 AMIs 的注册。

AWS-DetachEBSVolume

描述

将 Amazon EBS 卷与 Amazon Elastic Compute Cloud (Amazon EC2) 实例分离。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaAssumeRole

类型：字符串

描述：(可选) Lambda担任的角色的 ARN。

- Volumeld

类型：字符串

描述：(必需) EBS 卷的 ID。卷和实例必须位于同一可用区内

AWSConfigRemediation-EnableEbsEncryptionByDefault

描述

该AWSConfigRemediation-EnableEbsEncryptionByDefault运行手册支持对运行自动化的所有新的亚马逊弹性区块存储 (Amazon EBS) 卷进行 AWS 账户 加密。AWS 区域 在运行自动化之前创建的卷不会被加密。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:EnableEbsEncryptionByDefault
- ec2:GetEbsEncryptionByDefault
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文档步骤

- aws:executeAwsApi - 在当前账户和区域，启用默认 Amazon EBS 加密设置。
- aws:assertAwsResourceProperty - 验证是否已启用默认 Amazon EBS 加密设置。

AWS-ExtendEbsVolume

描述

AWS-ExtendEbsVolume 运行手册将增加 Amazon EBS 卷的大小并扩展文件系统。此自动化支持 xfs 和 ext4 文件系统。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DriveLetter

类型：字符串

描述：(可选) 要扩展其文件系统的驱动器的盘符。Windows 实例需要此参数。

- InstanceId

类型：字符串

描述：(可选) 要扩展的 Amazon EBS 卷所附加到的 Amazon EC2 实例的 ID。

- KeepSnapshot

类型：布尔值

默认：True

描述：(可选) 确定是否保留在增加 Amazon EBS 卷大小之前创建的快照。

- MountPoint

类型：字符串

描述：(可选) 要扩展其文件系统的驱动器的装载点。Linux 实例需要此参数。

- SizeGib

类型：字符串

描述：(必需) 要将 Amazon EBS 卷修改成的大小，以 GiB 为单位。

- VolumeId

类型：字符串

描述：(必需) 要扩展的 EBS 卷 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateSnapshot
- ec2:CreateTags
- ec2>DeleteSnapshot
- ec2:DescribeVolumes
- ec2:ModifyVolume
- ssm:DescribeInstanceInformation
- ssm:GetCommandInvocation
- ssm:SendCommand

文档步骤

- aws:executeScript - 将卷的大小增加到您在 VolumeId 参数中指定的值并扩展文件系统。

AWSsupport-ModifyEBSSnapshotPermission

描述

AWSsupport-ModifyEBSSnapshotPermission 运行手册可帮助修改多个 Amazon Elastic Block Store (Amazon EBS) 快照的权限。使用此运行手册，您可以制作快照 Public 或 Private 并将其与其他 AWS 账户分享。使用默认 KMS 密钥加密的快照无法与使用此运行手册的其他账户分享。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AccountIds

类型：StringList

默认：无

描述：(可选) 要与之共享快照的账户的 ID。如果您为 Private 参数值输入 No，则此参数为必选项。

- AccountPermissionOperation

类型：字符串

有效值：添加 | 移除

默认：无

描述：(可选) 要执行的操作类型。

- 专属

类型：字符串

有效值：是 | 否

描述：(必需) 如果要与特定账户共享快照，则为该值输入 No。

- SnapshotIds

类型：StringList

描述：(必需) 要修改其权限的 Amazon EBS 快照的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSnapshots
- ec2:ModifySnapshotAttribute

文档步骤

1. aws:executeScript - 验证 SnapshotIds 参数中提供的快照的 ID。验证 ID 后，脚本会检查加密快照并输出列表（若找到）。
2. aws:branch- 根据为 Private 参数输入的值对自动化进行分支。
3. aws:executeScript- 修改指定快照的权限，以便与指定账户共享快照。
4. aws:executeScript- 修改快照的权限，将其从改 Public 为 Private。

输出

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Result

MakePrivate.Result

MakePrivate.Commands

AWSConfigRemediation-ModifyEBSVolumeType

描述

AWSConfigRemediation-ModifyEBSVolumeType 运行手册将修改 Amazon Elastic Block Store (Amazon EBS) 卷的卷类型。修改卷类型后，该卷将进入 optimizing 状态。有关监控卷修改进度的信息，请参阅 Amazon EC2 用户指南中的[监控卷修改进度](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- EbsVolumeld

类型：字符串

描述：(必需) 要修改的 Amazon EBS 卷的 ID。

- EbsVolumeType

类型：字符串

有效值：标准 | io1 | io2 | gp2 | gp3 | sc1 | st1

描述：要将 Amazon EBS 卷更改成的卷类型。有关亚马逊 EBS 卷类型的信息，请参阅[亚马逊 EC2 用户指南中的亚马逊 EBS 卷类型](#)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeVolumes
- ec2:ModifyVolume

文档步骤

- `aws:waitForAwsResourceProperty` - 验证卷的状态是否为 `available` 或 `in-use`。
- `aws:executeAwsApi` - 修改在您 `EbsVolumeId` 参数中指定的 Amazon EBS 卷。
- `aws:waitForAwsResourceProperty` - 验证卷的类型是否已更改为您在 `EbsVolumeType` 参数中指定的值。

Amazon EC2

AWS Systems Manager Automation 为 Amazon 弹性计算云提供了预定义的运行手册。Amazon Elastic Block Store 的运行手册位于《运行手册参考》[Amazon EBS](#) 部分。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatedImage](#)
- [AWS-DeleteImage](#)
- [AWS-PatchAsgInstance](#)
- [AWS-PatchInstanceWithRollback](#)
- [AWS-QuarantineEC2Instance](#)
- [AWS-ResizeInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)
- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-PatchLoadBalancerInstance](#)

- [AWSEC2-SQLServerDBRestore](#)
- [AWSSupport-ActivateWindowsWithAmazonLicense](#)
- [AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSSupport-CheckXenToNitroMigrationRequirements](#)
- [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#)
- [AWSSupport-CollectSAPHANALogs](#)
- [AWSSupport-ConfigureEC2Metadata](#)
- [AWSSupport-ContainEC2Instance](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSPremiumSupport-ExtendVolumesOnWindows](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)
- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSSupport-RunEC2RescueForWindowsTool](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-ShareEncryptedAMIOrEBSSnapshot](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSSupport-TroubleshootActiveDirectoryReplication](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)

- [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

AWS-ASGEnterStandby

描述

在 Auto Scaling 组中更改亚马逊弹性计算云 (Amazon EC2) 实例的待机状态。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 您要在 Auto Scaling 组中更改其备用状态的 Amazon EC2 实例的 ID。

- LambdaRoleArn

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

AWS-ASGExitStandby

描述

在 Auto Scaling 组中更改亚马逊弹性计算云 (Amazon EC2) 实例的待机状态。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 要在 Auto Scaling 组中更改其备用状态的 EC2 实例的 ID。

- LambdaRoleArn

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

AWS-CreateImage

描述

co从 Amazon Elastic Compute Cloud (Amazon EC2) 实例创建新 Amazon Machine Image (AMI)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) EC2 实例的 ID。

- NoReboot

类型：布尔值

说明：(可选) 创建映像前，不要重启实例。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateImage",
        "ec2:DescribeImages"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS-DeleteImage

描述

删除 Amazon Machine Image (AMI) 和所有关联的快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ImageId

类型：字符串

说明：(必需) AMI 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteSnapshot",
      "Resource": "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeImages",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DeregisterImage",
      "Resource": "*"
    }
  ]
}
```

```
}  
]  
}
```

AWS-PatchAsgInstance

描述

修补自动扩缩组中的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

[运行此自动化 \(控制台\)](#)

Important

该运行手册在执行期间将AutoPatchInstanceInASG标签应用于目标实例。此标签可防止运行手册在同一个实例上同时执行两次——它不是补丁合规性指标。如果修补步骤失败，则Completed即使运行手册执行状态报告，标签值仍可能设置为Failed。要验证实例的补丁合规性，请[ListComplianceItems](#)改用[DescribeInstancePatchStates](#)或。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) 要修补的实例的 ID。不要指定配置为在维护时段期间运行的实例 ID。

- LambdaRoleArn

类型：字符串

说明：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- WaitForInstance

类型：字符串

默认值：PT2M

说明：(可选) Automation 应休眠以允许实例重新进入运行状态的持续时间。

- WaitForReboot

类型：字符串

默认值：PT5M

说明：(可选) Automation 应休眠以允许修补后的实例进行重启的持续时间。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ssm:GetParameter
- ssm:SendCommand
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks

- `ec2:CreateTags`
- `ec2:DescribeInstances`
- `ec2:RunInstances`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`

AWS-PatchInstanceWithRollback

描述

使 EC2 实例符合适用的补丁基准。失败时对根卷进行回滚。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) EC2 InstanceId，我们对其应用补丁基线。

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- ReportS3Bucket

类型：字符串

说明：(可选) 过程期间生成的合规性报告的 Amazon S3 存储桶目标。

文档步骤

步骤编号	步骤名称	自动化操作
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand

步骤编号	步骤名称	自动化操作
5	SleepThruInstallation	aws:invokeLambdaFunction
6	CheckCompliance	aws:invokeLambdaFunction
7	SaveComplianceReportToS3	aws:invokeLambdaFunction
8	ReportSuccessOrFailure	aws:invokeLambdaFunction
9	RestoreFromSnapshot	aws:invokeLambdaFunction
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormation模板	aws:deleteStack

输出

IdentifyRootVolume. 有效载荷

PrePatchSnapshot。输出

SaveComplianceReportToS3. 有效载荷

RestoreFromSnapshot. 有效载荷

CheckCompliance. 有效载荷

AWS-QuarantineEC2Instance

描述

使用AWS-QuarantineEC2Instance运行手册，您可以为不允许任何入站或出站流量的亚马逊弹性计算云 (Amazon EC2) 实例分配安全组。

⚠ Important

在运行此运行手册前，应仔细检查对 RDP 设置的更改。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) 要管理其 RDP 设置的托管实例的 ID。

- IsolationSecurityGroup

类型：字符串

描述：(必需) 您要分配给实例以防止入站或出站流量的安全组的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:DescribeAutoScalingInstances
- autoscaling:DetachInstances
- ec2:CreateSecurityGroup
- ec2:CreateSnapshot
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:ModifyInstanceAttribute
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文档步骤

- aws:executeAwsApi - 收集有关该实例的详细信息。
- aws:executeScript - 验证该实例是否为自动扩缩组的一部分。
- aws:executeAwsApi - 创建附加到该实例的根卷的一个快照。
- aws:waitForAwsResourceProperty - 等待快照状态处于 completed。
- aws:executeAwsApi - 将 IsolationSecurityGroup 参数中指定的安全组分配给您的实例。

输出

GetEC2InstanceResources.RevokedSecurityGroupsIds

GetEC2InstanceResources.RevokedSecurityGroupsNames

createSnapshot.SnapId

AWS-ResizeInstance

描述

更改亚马逊弹性计算云 (Amazon EC2) 实例的实例类型。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) 实例的 ID。

- InstanceType

类型：字符串

说明：(必需) 实例类型。

AWS-RestartEC2Instance

描述

重启一个或多个亚马逊弹性计算云 (Amazon EC2) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceIds

类型：StringList

描述：(必填) 要重启 IDs 的 Amazon EC2 实例。

AWS-SetupJupyter

描述

AWS-SetupJupyter运行手册可帮助您在亚马逊弹性计算云 (亚马 EC2实例) 实例上设置 Jupyter Notebook。您可以指定现有实例，也可以提供 Amazon Machine Image (AMI) 用于启动和设置新实例的自动化的 ID。开始之前，您必须先在 Parameter Store 中创建一个 SecureString 参数，用作 Jupyter 笔记本的密码。参数存储是一个工具 AWS Systems Manager。有关创建参数的更多信息，请参阅AWS Systems Manager 用户指南中的[创建参数](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- Amild

类型：字符串

描述：(可选) 的 ID AMI 你想用它来启动新实例和设置 Jupyter Notebook。

- InstanceId

类型：字符串

说明：(必需) 您想要设置 Jupyter 笔记本的实例的 ID。

- InstanceType

类型：字符串

默认：t3.medium

描述：(可选) 如果您要启动新实例来设置 Jupyter 笔记本，则指定要使用的实例类型。

- JupyterPasswordSSMKey

类型：字符串

描述：(必填) Parameter Store 中要用作 Jupyter 笔记本密码的 SecureString 参数的名称。

- KeyPairName

类型：字符串

描述：(可选) 要与新启动实例关联的密钥对。

- RemoteAccessCidr

类型：字符串

默认：0.0.0.0/0

描述：(可选) 您希望允许 SSH 流量来自的 CIDR 范围。

- RoleName

类型：字符串

默认：SSMManagedInstanceProfileRole

描述：(可选) 新启动实例的实例配置文件的名称。

- StackName

类型：字符串

默认：CreateManagedInstanceStack{{自动化:execution_ID}}

描述：(可选) 您希望自动化使用的 CloudFormation 堆栈名称。

- SubnetId

类型：字符串

默认：Default

描述：(可选) 您希望启动新实例以便使用的子网。

- VpcId

类型：字符串

默认：Default

描述：(可选) 要将新实例启动到的虚拟私有云 (VPC) 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ssm:GetParameter
- ssm:SendCommand
- ssm:StartAutomationExecution
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- ec2:DescribeInstances
- ec2:DescribeKeyPairs
- ec2:RunInstances
- iam:AttachRolePolicy
- iam:CreateRole
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:PassRole
- iam:PutRolePolicy
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction

文档步骤

- aws:executeScript - 使用您为运行手册输入参数指定的值，在您指定的实例上或新启动的实例上设置 Jupyter 笔记本。

AWS-StartEC2Instance

描述

启动一个或多个亚马逊弹性计算云 (Amazon EC2) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceIds

类型：StringList

描述：要启动的 (必需) EC2 实例。

AWS-StopEC2Instance

描述

停止一个或多个亚马逊弹性计算云 (Amazon EC2) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceIds

类型：StringList

描述：(必需) 要停止的 EC2 实例。

AWS-TerminateEC2Instance

描述

终止一个或多个亚马逊弹性计算云 (Amazon EC2) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceIds

类型：StringList

描述：(必填) 要终止 IDs 的一个或多个 EC2 实例。

AWS-UpdateLinuxAmi

描述

使用 Linux 分发软件包和 Amazon 软件更新 Amazon Machine Image (AMI) 。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

允许的模式：`^$|^arn:aws[a-z0-9-]*:iam::(\d{12}|\{\global:ACCOUNT_ID\})\:role/[w/.@+,-]{1,1017}$`

- 必须是有效的 IAM 角色 ARN 或空字符串。系统变量 `{global:ACCOUNT_ID}` 可用来代替 `arn` 中的 AWS 账户 ID。

- ExcludePackages

类型：字符串

默认：无

说明：(可选) 在所有情况下从更新中排除的软件包的名称。默认值 ("none") 不排除任何软件包。

允许的模式：`^(none|[a-zA-Z0-9\s,._+:=<>()\[ \]/*-]+)$`

- 必须为 "none" 或由字母、数字、空格和以下字符组成的以逗号分隔的项目列表：, . _ + : = < > () [] / * -

- IamInstanceProfileName

类型：字符串

默认：ManagedInstanceProfile

说明：(必需) 启用 Systems Manager 以管理实例的实例配置文件。

允许的模式：`^[w+=, .@-]{1,128}$`

- 必须介于 1 到 128 个字符之间，并且仅包含字母、数字和以下字符：+ = , . @ - _

- IncludePackages

类型：字符串

默认：all

说明：(可选) 仅更新这些指定的软件包。默认值 ("all") 将应用所有可用的更新。

允许的模式：`^(all|[a-zA-Z0-9\s,._+:=<>()\[\]/*-]+)$`

- 必须为“all”或由字母、数字、空格和以下字符组成的以逗号分隔的项目列表：`, . _ + : = < > ( ) [ ] / * -`

• InstanceType

类型：字符串

默认：t2.micro

说明：（可选）启动作为工作区主机的实例的类型。实例类型因区域而异。

允许的模式：`^[a-z0-9]+(-[a-z0-9]+)*\.[a-z0-9]+$`

- 必须采用 prefix.suffix 格式，其中两个部分都包含小写字母和数字，前缀可以包含连字符

• MetadataOptions

类型：StringMap

默认：`{"HttpEndpoint": "已启用", "HttpTokens": "可选"}`

说明：（可选）实例的元数据选项。有关更多信息，请参阅 [InstanceMetadataOptionsRequest](#)。

允许的模式：`^\{[^<>\$;|&\\]*\}$`

- 必须用大括号 `{}` 括起来，并且不能包含以下字符：`< > $ ; | & \`

• PostUpdateScript

类型：字符串

默认：无

说明：（可选）在应用软件包更新后要运行的脚本的 URL。默认值 ("none") 不运行脚本。

允许的模式：`^(none|https?:\/\/[\w\-.~:\/?#\[\]@!$&'()*+,\;=%]+)$`

- 必须为“无”或有效的 HTTP/HTTPS 网址

• PreUpdateScript

类型：字符串

默认：无

说明：(可选) 在更新前应用要运行的脚本的 URL。默认值 ("none") 不运行脚本。

允许的模式：`^(none|https?:\/\/[\w\-.~:\/?#\[\]\@!$&'()*+,\;=%]+)$`

- 必须为“无”或有效的 HTTP/HTTPS 网址

- SecurityGroupIds

类型：字符串

描述：(必填) 要应用于的安全组 IDs 的列表，以逗号分隔。AMI

允许的模式：`^sg-[a-z0-9]{8,17}$`

- 必须以“sg-”开头，后跟 8-17 个小写字母或数字

- SourceAmiId

类型：字符串

说明：(必需) 源 Amazon 系统映像 ID。

允许的模式：`^ami-[a-z0-9]{8,17}$`

- 必须以“ami-”开头，后跟 8-17 个小写字母或数字

- SubnetId

类型：字符串

描述：(可选) 您希望启动实例以便使用的子网 ID。如果您已删除默认 VPC，则此参数是必需的。

允许的模式：`^$|^subnet-[a-z0-9]{8,17}$`

- 必须为空或者以“subnet-”开头，后跟 8-17 个小写字母或数字

- TargetAmiName

类型：字符串

默认：`UpdateLinuxAmi_from_ {{SourceAmiId}} _on_ {global: date_Time}`

说明：(可选) 将创建的新 AMI 的名称。默认为系统生成的字符串，其中包括源 AMI ID 以及创建时间和日期。

允许的模式：`^[a-zA-Z0-9() \[\] \{ \} . / ' @ _ : - ] { 3 , 1 2 8 } $`

- 必须介于 3 到 128 个字符之间，并且仅包含字母、数字、空格和以下字符：() [] { } . / ' @ _ : -

AWS-UpdateWindowsAmi

描述

更新 Microsoft Windows Amazon Machine Image (AMI)。默认情况下，此运行手册安装所有 Windows 更新、Amazon 软件和 Amazon 驱动程序。然后，它运行 Sysprep 以创建新的 AMI。支持 Windows Server 2008 R2 到 Windows Server 2022。

Important

本运行手册不支持 Windows Server 2025 及更高版本，因为 AWS Paravirtual 驱动程序与这些版本不兼容。有关更多信息，请参阅适用于 [Windows 实例的半虚拟化驱动程序](#)。

Important

如果您的实例 AWS Systems Manager 使用 VPC 终端节点连接，则除非在 us-east-1 区域中使用，否则本运行手册将失败。实例必须启用 TLS 1.2 才能使用此运行手册。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 类别

类型：字符串

说明：(可选) 指定一个或多个更新类别。可以使用逗号分隔值筛选类别。选项：应用程序、连接器、、、CriticalUpdates DefinitionUpdates、驱动程序 DeveloperKits、、指南 FeaturePacks、Microsoft SecurityUpdates、ServicePacks、、工具UpdateRollups、、更新。有效格式包括单个条目，例如：CriticalUpdates。或者你可以指定一个以逗号分隔的列表：CriticalUpdates, SecurityUpdates。注意：逗号两边不能有任何空格。

- ExcludeKbs

类型：字符串

描述：(可选) 指定要排除的一篇或多篇 Microsoft 知识库 (KB) 文章 IDs 。IDs 您可以使用逗号分隔的值排除多个值。有效格式：KB9876543 或 9876543。

- IamInstanceProfileName

类型：字符串

默认：ManagedInstanceProfile

说明：(必需) 启用 Systems Manager 以管理实例的角色名称。

- IncludeKbs

类型：字符串

描述：(可选) 指定要包含的一篇或多篇 Microsoft 知识库 (KB) 文章 IDs 。IDs 您可以使用逗号分隔的值安装多个。有效格式：KB9876543 或 9876543。

- InstanceType

类型：字符串

默认：t2.medium

说明：(可选) 启动作为工作区主机的实例的类型。实例类型因区域而异。默认为 t2.medium。

- MetadataOptions

类型：StringMap

默认：{"HttpEndpoint": "已启用", "HttpTokens": "可选"}

说明：(可选) 实例的元数据选项。有关更多信息，请参阅 [InstanceMetadataOptionsRequest](#)。

- PostUpdateScript

类型：字符串

说明：(可选) 以字符串形式提供的脚本。它将在安装操作系统更新后运行。

- PreUpdateScript

类型：字符串

说明：(可选) 以字符串形式提供的脚本。它将在安装操作系统更新前运行。

- PublishedDateAfter

类型：字符串

说明：(可选) 指定查找在此日期后发布的更新。例如，如果指定 01/01/2017，则返回在 Windows 更新搜索期间找到的在 01/01/2017 当天或之后发布的所有更新。

- PublishedDateBefore

类型：字符串

说明：(可选) 指定查找在此日期前发布的更新。例如，如果指定 01/01/2017，则返回在 Windows 更新搜索期间找到的在 01/01/2017 当天或之前发布的所有更新。

- PublishedDaysOld

类型：字符串

说明：(可选) 指定更新在发行日期后必须经过的天数。例如，如果指定 10，则返回在 Windows 更新搜索期间找到的已发布 10 天或更多天的所有更新。

- SecurityGroupIds

类型：字符串

描述：(必填) 要应用于的安全组 IDs 的列表，以逗号分隔。AMI

- SeverityLevels

类型：字符串

说明：(可选) 指定一个或多个与更新关联的 MSRC 严重性级别。可以使用逗号分隔值筛选严重性级别。默认情况下，将选择所有安全级别的补丁。如果提供了值，则使用这些值对更新列表进行筛选。选项：关键、重要、低、中或未指定。有效格式包括单个条目，例如：关键。或者，可以指定逗号分隔列表：关键,重要,低。

- SourceAmild

类型：字符串

描述：(必填) 来源 AMI ID。

- SubnetId

类型：字符串

描述：(可选) 您希望启动实例以便使用的子网 ID。如果您已删除默认 VPC，则此参数是必需的。

- TargetAmiName

类型：字符串

默认：UpdateWindowsAmi_from_ {{SourceAmild}} _on_ {global: date_Time}}

说明：(可选) 将创建的新 AMI 的名称。默认为系统生成的字符串，其中包括源 AMI ID 以及创建时间和日期。

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

描述

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck运行手册为您指定的 Amazon A EC2 uto Scaling (Auto Scaling) 组启用运行状况检查。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- AutoScalingGroupARN

类型：字符串

描述：(必需) 您希望启用运行状况检查的自动扩缩组的 Amazon 资源名称 (ARN) 。

- HealthCheckGracePeriod

类型：整数

默认：300

描述：(可选) Auto Scaling 在检查已投入使用的亚马逊弹性计算云 (Amazon EC2) 实例的运行状况之前等待的时间 (以秒为单位) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeAutoScalingGroups
- ec2:UpdateAutoScalingGroup

文档步骤

- `aws:executeScript` - 对您在 `AutoScalingGroupARN` 参数中指定的自动扩缩组启用运行状况检查。

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

描述

AWSConfigRemediation-EnforceEC2InstanceIMDSv2运行手册要求您指定的亚马逊弹性计算云 (Amazon EC2) 实例使用实例元数据服务版本 2 (IMDSv2)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- `InstanceId`

类型：字符串

描述：(必填) 您要要求使用的 Amazon EC2 实例的 ID IMDSv2。

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `HttpPutResponseHopLimit`

类型：整数

描述：(可选) 从 IMDS 服务返回请求者的跳跃响应限制。对于托管容器的 EC2 实例，设置为 2 或更大。设置为 0 表示不更改 (默认)。

允许的模式：`^([1-5]?\d|6[0-4])$`

默认：0

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeInstances`
- `ec2:ModifyInstanceMetadataOptions`

文档步骤

- `aws:executeScript`-将您在 `InstanceId` 参数中指定的 Amazon EC2 实例 `required` 上的 `HttpTokens` 选项设置为。
- `aws:assertAwsResourceProperty`-需要对 Amazon EC2 实例进行验证 `IMDSv2`。

AWSEC2-CloneInstanceAndUpgradeSQLServer

描述

创建一个 AMI 来自一个 EC2 实例 Windows Server 运行 SQL Server 2008 或更高版本，然后将 AMI 升级到更高版本的 SQL Server。仅支持英文版本的 SQL Server。

支持的升级路径如下所示：

- SQL Server 2008 到 SQL Server 2017、2016 或 2014
- SQL Server 2008 R2 到 SQL Server 2017、2016 或 2014
- SQL Server 2012 到 SQL Server 2019、2017、2016 或 2014

- SQL Server 2014 到 SQL Server 2019、2017 或 2016
- SQL Server 2016 到 SQL Server 2019 或 2017

如果您使用的是与 SQL Server 2019 不兼容的早期版本 Windows Server，则自动化文档必须将你的 Windows Server 版本升级到 2016。

升级是一个多步骤过程，可能需要 2 个小时才能完成。自动化会从该实例创建 AMI，然后从新实例启动临时实例 AMI 在指定的 SubnetID。与您的原始实例关联的安全组将应用于临时实例。Automation 在临时实例上执行到 TargetSQLVersion 的就地升级。升级后，自动化会创建新的 AMI 从临时实例，然后终止临时实例。

您可以通过启动新应用程序来测试应用程序的功能 AMI 在你的 VPC 中。完成测试后，在执行下一次升级之前，请先计划应用程序停机时间，然后再完全切换到升级后的实例。

Note

如果你想修改从新启动的 EC2 实例的计算机名 AMI，请参见[重命名托管 SQL Server 独立实例的计算机](#)。

运行此自动化 (控制台)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

先决条件

- TLS 版本 1.2。
- 仅支持英文版本的 SQL Server。

- 该 EC2 实例必须使用一个版本 Windows Server 那是 Windows Server 2008 年 R2 (或更高版本) 和 SQL Server 2008 (或更高版本)。
- 验证实例上是否安装了 SSM Agent。有关更多信息，请参阅在 [Windows 服务器 EC2 实例上安装和配置 SSM 代理](#)。
- 将实例配置为使用 AWS Identity and Access Management (IAM) 实例配置文件角色。有关更多信息，请参阅 [Systems Manager 创建 IAM 实例配置文件](#)。
- 验证实例的实例启动盘具有 20 GB 的可用磁盘空间。
- 对于使用自带许可 (BYOL) SQL Server 版本的实例，以下额外的先决条件适用：
 - 提供包含目标 SQL Server 安装介质的 EBS 快照 ID。要实现此目的，应按照以下步骤进行：
 1. 确认该 EC2 实例运行的是 Windows Server 2008 R2 或更高版本。
 2. 在运行实例的同一可用区中创建一个 6 GB 的 EBS 卷。将卷附加到实例。例如，将其附加为驱动器 D。
 3. 例如，右键单击 ISO 并将其挂载为实例的驱动器 E。
 4. 将 ISO 的内容从驱动器 E:\ 复制到驱动器 D:\
 5. 创建在步骤 2 中创建的 6 GB 卷的 EBS 快照。

限制

- 只能在使用 Windows 身份验证的 SQL Server 上执行升级。
- 验证实例上没有待处理的安全补丁更新。打开控制面板，然后选择检查更新。
- 不支持 HA 和镜像模式下的 SQL Server 部署。

参数

- `IamInstanceProfile`

类型：字符串

说明：(必需) IAM 实例配置文件。

- `InstanceId`

类型：字符串

描述：(必填) 正在运行的实例 Windows Server 2008 年 R2 (或更高版本) 和 SQL Server 2008 (或更高版本)。

- KeepPreUpgradeImageBackUp

类型：字符串

说明：(可选) 如果设置为 `true`，则自动化不会删除在升级之前从实例中创建的 AMI。如果设置为 `true`，则必须由您删除此 AMI。默认情况下，将删除此 AMI。

- SubnetId

类型：字符串

说明：(必需) 为升级过程提供子网。验证子网是否具有与 AWS 服务、Amazon S3 和 Microsoft 的出站连接 (用于下载补丁)。

- SQLServerSnapshotId

类型：字符串

说明：(视情况而定) SQL Server 安装介质的快照 ID。对于使用 BYOL SQL Server 版本的实例，该参数是必需的。对于包含许可证的 SQL Server 实例 (使用为微软 SQL Server 提供的适用于 Windows 服务器的 AWS 亚马逊系统映像启动的实例)，此参数是可选的。

- RebootInstanceBeforeTakingImage

类型：字符串

说明：(可选) 如果设置为 `true`，则自动化在创建预升级 AMI 之前重新引导实例。默认情况下，自动化在升级前不重启。

- 目标 SQLVersion

类型：字符串

描述：(可选) 选择目标 SQL Server 版本。

可能的目标：

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014

默认目标：SQL Server 2016

输出

AMIId : 从升级到更高版本的 SQL Server 的实例创建的 AMI 的 ID。

AWSEC2-CloneInstanceAndUpgradeWindows

描述

从 Windows Server 2008 年 R2、2012 年 R2、2016 年、2019 年或 2022 年的实例创建 Amazon Machine Image (AMI)，然后将其升级 AMI 到 Windows Server 2016 年、2019 年、2022 年或 2025 年。支持的升级路径如下所示。

- Windows Server 2008 年 R2 到 Windows Server 2016 年。
- Windows Server 2012 R2 到 Windows Server 2016。
- Windows Server 2012 R2 到 Windows Server 2019。
- Windows Server 2012 R2 到 Windows Server 2022。
- Windows Server 2016 到 Windows Server 2019。
- Windows Server 2016 到 Windows Server 2022。
- Windows Server 2016 年到 Windows Server 2025 年。
- Windows Server 2019 到 Windows Server 2022。
- Windows Server 2019 年到 Windows Server 2025 年。
- Windows Server 2022 年到 Windows Server 2025 年。

升级操作是一个多步骤过程，可能需要 2 个小时才能完成。我们建议对内存至少为 2 v CPUs 和 4GB 的实例执行操作系统升级。自动化从实例创建一个 AMI，然后从新创建的 AMI，在您指定的 SubnetId 中启动一个临时实例。与您的原始实例关联的安全组将应用于临时实例。Automation 在临时实例上执行到 TargetWindowsVersion 的就地升级。要将 Windows Server 2008 R2 实例升级到 Windows Server 2016、2019 或 2022，请执行就地升级两次，因为不支持直接将 Windows Server 2008 R2 升级到 Windows Server 2016、2019 或 2022。自动化还会更新或安装临时实例所需的 AWS 驱动程序。升级后，自动化会从临时实例创建新 AMI，然后终止临时实例。

您可以通过在 Amazon Virtual Private Cloud (Amazon VPC) 中从升级后的 AMI 启动测试实例来测试应用程序的功能。完成测试后，在执行下一次升级之前，请先计划应用程序停机时间，然后再完全切换到升级后的 AMI。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows Server 2008 R2、2012 R2、2016、2019 或 2022 年标准版和数据中心版

先决条件

- TLS 版本 1.2。
- 验证实例上是否安装了 SSM Agent。有关更多信息，请参阅[在 EC2 实例中为 Windows Server 安装和配置 SSM Agent](#)。
- 必须在您的实例上安装 Windows PowerShell 3.0 或更高版本。
- 对于加入到某个 Microsoft Active Directory 域的实例，建议指定一个没有连接到您的域控制器的 SubnetId，以帮助避免主机名冲突。
- 实例子网必须具有与互联网的出站连接，这样可以访问 AWS 服务 诸如 Amazon S3 之类的网络，也可以访问从 Microsoft 下载补丁。如果子网是公有子网且实例具有公有 IP 地址，或者子网是私有子网并使用路由将互联网流量发送到公有 NAT 设备，即满足此要求。
- 此自动化仅适用于 Windows Server 2008 年 R2、2012 年 R2、2016 年、2019 年和 2022 年的实例。
- 使用为 Windows Server Systems Manager 提供必要权限的 AWS Identity and Access Management (IAM) 实例配置文件配置实例。有关更多信息，请参阅[为 Systems Manager 创建 IAM 实例配置文件](#)。
- 验证实例的启动盘具有 20 GB 的可用磁盘空间。
- 如果实例不使用 AWS 提供的 Windows 许可证，请指定包含 Windows Server 2012 R2 安装媒体的 Amazon EBS 快照 ID。要实现此目的，应按照以下步骤进行：
 - 确认 EC2 实例运行 Windows Server 2012 或更高版本。
 - 在运行实例的同一可用区中创建一个 6 GB 的 EBS 卷。将卷附加到实例。例如，将其附加为驱动器 D。
 - 例如，右键单击 ISO 并将其挂载为实例的驱动器 E。
 - 将 ISO 的内容从驱动器 E:\ 复制到驱动器 D:\
 - 为上面步骤 2 中创建的 6 GB 卷创建 EBS 快照。

- 对于 Windows Server 2025 年升级，源实例必须[基于 Nitro](#)。

限制

此 Automation 不支持升级 Windows 域控制器、集群或 Windows 桌面操作系统。该 Automation 也不支持安装了以下角色的 Windows Server EC2 实例。

- 远程桌面会话主机 (RDSH)
- 远程桌面连接代理 (RDCB)
- 远程桌面虚拟化主机 (RDVH)
- 远程桌面 Web 访问 (RDWA)

参数

- AlternativeKeyName

类型：字符串

描述：(可选) 升级过程中要使用的备用密钥对的名称。这在分配给初始实例的密钥对不可用的情况下很有用。如果没有为初始实例分配密钥对，则必须为此参数指定一个值。

- BYOLWindowsMediaSnapshotId

类型：字符串

描述：(可选) 复制包括 Windows Server 2012R2 安装介质的 Amazon EBS 快照的 ID。只有在升级 BYOL 实例时才需要。

- IamInstanceProfile

类型：字符串

描述：(必需) 启用 Systems Manager 以管理实例的 IAM 实例配置文件的名称。

- InstanceId

类型：字符串

描述：(必填) 运行 Windows Server 2008 R2、2012 R2、2016、2019 或 2022 年的 EC2 实例。

- KeepPreUpgradeImageBackUp

类型：字符串

描述：(可选) 如果设置为 True，则 Automation 不会删除在升级之前从 EC2 实例创建的 AMI。如果设置为 True，则必须由您删除此 AMI。默认情况下，将删除此 AMI。

- SubnetId

类型：字符串

描述：(必需) 这是执行升级过程的子网以及源 EC2 实例所在的位置。验证子网是否具有与 AWS 服务、Amazon S3 和 Microsoft 的出站连接 (用于下载补丁)。

- TargetWindowsVersion

类型：字符串

描述：(必需) 选择目标 Windows 版本。

默认值：2025

- RebootInstanceBeforeTakingImage

类型：字符串

描述：(可选) 如果设置为 True，则 Automation 会重启实例，然后再创建升级前 AMI。默认情况下，Automation 在升级前不重启。

AWSEC2-PatchLoadBalancerInstance

描述

升级并修补连接到任何负载均衡器 (经典、ALB 或 NLB) 的亚马逊 EC2 实例 (Windows 或 Linux) 的次要版本。在修补该实例之前，会应用默认的连接耗尽时间。您可以通过在 ConnectionDrainTime 参数中输入以分钟 (1-59) 为单位的自定义排水时间来覆盖等待时间。

自动化工作流程如下所示：

1. 确定实例所附加的负载均衡器或目标组，并验证该实例是否运行正常。
2. 该实例已从负载均衡器或目标组移除。
3. 此自动化将等待为连接耗尽时间指定的时间段。
4. 调用 [AWS RunPatchBaseline](#) 自动化来修补实例。
5. 该实例已从负载均衡器或目标组重新附加。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

先决条件

- 验证实例上是否安装了 SSM Agent。有关更多信息，[请参阅在 Windows 服务器 EC2 实例上使用 SSM 代理](#)。

参数

- InstanceId

类型：字符串

描述：(必需) 与负载均衡器 (经典、ALB 或 NLB) 关联的要修补的实例的 ID。

- ConnectionDrainTime

类型：字符串

描述：(可选) 负载均衡器的连接耗尽时间，以分钟 (1-59) 为单位。

- S3BucketLog

类型：字符串

描述：(可选) 用于存储命令输出响应的 Amazon S3 存储桶的名称。您可以指定自己拥有的存储桶或与您共享的存储桶。如果您提供此参数，则还必须提供 Role runCommandAssume。

- runCommandAssume 角色

类型：字符串

描述：(可选) 用于在实例上运行命令的 IAM 角色的 ARN。该角色必须与 **ssm.amazonaws.com** 服务委托人建立信任关系，必须附加了 Amazon SSMManaged InstanceCore 策略，并且必须对为 S3 指定的 Amazon S3 存储桶具有写入权限 BucketLog。

AWSEC2-SQLServerDBRestore

描述

AWSEC2-SQLServerDBRestore 运行手册将存储在 Amazon S3 中的 Microsoft SQL Server 数据库备份还原到在 Amazon Elastic Compute Cloud (EC2) Linux 实例上运行的 SQL Server 2017。您可以提供自己的运行 SQL Server 2017 Linux 的 EC2 实例。如果未提供 EC2 实例，自动化将启动，并使用 SQL Server 2017 配置新的 Ubuntu 16.04 EC2 实例。自动化支持还原完整、差异和事务日志备份。此自动化将接收多个数据库备份并自动还原所提供的文件中每个数据库的最近的有效备份。

要自动将本地 SQL Server 数据库备份和恢复到运行 SQL Server 2017 Linux 的 EC2 实例，您可以使用 AWS 签名的 PowerShell 脚本 [MigrateSQLServerToEC2Linux](#)。

Important

自动化每次运行时，此运行手册将重置 SQL Server 服务器管理员 (SA) 用户密码。自动化完成后，在连接到 SQL Server 实例之前，您必须重新设置您自己的 SA 用户密码。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

先决条件

要运行此自动化，您必须满足以下先决条件：

- 运行此自动化的 IAM 用户或角色必须拥有内联策略，并附有 [所需的 IAM 权限](#) 中概述的权限。
- 如果您提供自己的 EC2 实例：
 - 您提供的 EC2 实例必须是运行微软 SQL Server 2017 的 Linux 实例。

- 附加了 AmazonSSMManagedInstanceCore 托管策略的 AWS Identity and Access Management (IAM) 实例配置文件配置必须您提供的 EC2 实例。有关更多信息，请参阅[为 Systems Manager 创建 IAM 实例配置文件](#)。
- EC2 实例上必须安装 SSM 代理。有关更多信息，请参阅[在 Linux 的 EC2 实例上安装和配置 SSM 代理](#)。
- EC2 实例必须具有足够的可用磁盘空间来下载和还原 SQL Server 备份。

限制

此自动化不支持还原到在 Windows Server 的 EC2 实例上运行的 SQL Server。此自动化仅还原与 SQL Server Linux 2017 兼容的数据库备份。有关更多信息，请参阅[Linux 上的 SQL Server 2017 的版本和支持功能](#)。

参数

此自动化具有以下参数：

- DatabaseNames

类型：字符串

说明：(可选) 要还原的数据库的名称的逗号分隔列表。

- DataDirectorySize

类型：字符串

说明：(可选) 所需的新 EC2 实例的 SQL Server 数据目录的卷大小 (GiB)。

默认值：100

- KeyPair

类型：字符串

说明：(可选) 要在创建新 EC2 实例时使用的密钥对。

- IamInstanceProfileName

类型：字符串

说明：(可选) 要附加到新 EC2 实例的 IAM 实例配置文件。IAM 实例配置文件必须附加了 AmazonSSMManagedInstanceCore 托管策略。

- InstanceId

类型：字符串

说明：(可选) Linux 上的运行 SQL Server 2017 的实例。如果未提供，InstanceId 则自动化会使用提供的 InstanceType 和 SQLServer版本启动新的 EC2 实例。

- InstanceType

类型：字符串

说明：(可选) 要启动的 EC2 实例的实例类型。

- iss3 PresignedUrl

类型：字符串

说明：(可选) 如果 S3Input 是预签名 S3 URL，则表示 yes。

默认值：No

有效值：是 | 否

- LogDirectorySize

类型：字符串

说明：(可选) 所需的新 EC2 实例的 SQL Server 日志目录的卷大小 (GiB)。

默认值：100

- S3Input

类型：字符串

描述：(必填) S3 存储桶名称、以逗号分隔的 S3 对象密钥列表，或 URLs 包含要还原的 SQL 备份文件的以逗号分隔的预签名 S3 列表。

- SQLServer版本

类型：字符串

说明：(可选) 要安装在新创建的 EC2 实例上的 SQL Server 2017 版本。

有效值：Standard | Enterprise | Web | Express

- SubnetId

类型：字符串

说明：(可选) 要在其中启动新 EC2 实例的子网。子网必须与 AWS 服务有出站连接。如果未提供值，SubnetId 则自动化将使用默认子网。

- TempDbDirectorySize

类型：字符串

说明：(可选) 所需的新 EC2 实例的 SQL Server TempDB 目录的卷大小 (GiB)。

默认值：100

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ]
    }
  ],
}
```

```
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/ROLENAME"
      }
    ]
  }
}
```

文档步骤

要使用此自动化，请按照适用于实例类型的步骤进行操作：

对于新 EC2 实例：

1. `aws:executeAwsApi` - 在 Ubuntu 16.04 上检索 SQL Server 2017 的 AMI ID。
2. `aws:runInstances` - 启动适用于 Linux 的一个新 EC2 实例。
3. `aws:waitForAwsResourceProperty` - 等待新创建的 EC2 实例准备就绪。
4. `aws:executeAwsApi` - 如果实例未准备就绪，将重启实例。
5. `aws:assertAwsResourceProperty` - 验证安装了 SSM 代理。
6. `aws:runCommand`-在中运行 SQL Server 恢复脚本 PowerShell。

对于现有 EC2 实例：

1. `aws:waitForAwsResourceProperty` - 验证EC2 实例是否就绪。
2. `aws:executeAwsApi` - 如果实例未准备就绪，将重启实例。
3. `aws:assertAwsResourceProperty` - 验证安装了 SSM 代理。
4. `aws:runCommand`-在中运行 SQL Server 恢复脚本 PowerShell。

输出

获取实例。 `InstanceId`

`restoreToNew`实例. 输出

`restoreToExisting`实例. 输出

AWSSupport-ActivateWindowsWithAmazonLicense

描述

AWSSupport-ActivateWindowsWithAmazonLicense运行手册激活亚马逊弹性计算云 (Amazon EC2) 实例 Windows Server 使用 Amazon 提供的许可。Automation 验证和配置所需的密钥管理服务操作系统设置并尝试激活。这包括通往 Amazon 的密钥管理服务器的操作系统路由以及密钥管理服务操作系统设置。将AllowOffline参数设置为true允许自动化成功定位不受 AWS Systems Manager管理但需要停止和启动实例的实例。

Note

本运行手册不能用于“自带许可证”(BYOL) 模式 Windows Server 实例。有关使用自己的许可证的信息，请参阅 [AWS上的 Microsoft 许可](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AllowOffline

类型：字符串

有效值：true | false

默认：false

说明：(可选) 当在线故障排除失败或提供的实例不是托管实例时，如果允许进行离线 Windows 激活修复，请将其设置为 true。

 Important

离线方法要求先停止提供的 EC2 实例，然后再启动。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ForceActivation

类型：字符串

有效值：true | false

默认：false

说明：(可选) 若要在 Windows 已激活的情况下继续，请将其设置为 true。

- InstanceId

类型：字符串

描述：(必填) 您的托管 EC2 实例的 ID Windows Server.

- SubnetId

类型：字符串

默认：CreateNewVPC

描述：(可选) 仅限脱机-用于执行离线故障排除的 EC2 Rescue 实例的子网 ID。使用 SelectedInstanceSubnet 以使用同一子网作为您的实例，或使用 CreateNewVPC 创建一个新 VPC。重要：子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

我们建议接收命令的 EC2 实例具有 IAM 角色并附有 Amazon A SSMManagedInstanceCorema zon 托管策略。你必须至少有 ssm: StartAutomationExecution 和 ssm: SendCommand 才能运行自动化并将命令发送到实例，还必须有 s sm: GetAutomationExecution 才能读取自动化输出。对于离线修复息，请参阅 AWSSupport-StartEC2RescueWorkflow 所需的权限。

文档步骤

1. aws:assertAwsResourceProperty - 检查所提供的实例的平台是否为 Windows。
2. aws:assertAwsResourceProperty - 确认所提供的实例是托管实例：
 - a. (在线激活修复) 如果输入实例是托管实例，则运行 PowerShell脚本aws:runCommand以尝试修复 Windows 激活问题。
 - b. (离线激活修复) 如果输入实例不是托管实例：
 - i. aws:assertAwsResourceProperty - 验证AllowOffline旗帜是否设置为。true如果是，则启动离线修复，否则自动化将会结束。
 - ii. aws:executeAutomation - 使用 Windows 激活离线修复脚本调用 AWSSupport-StartEC2RescueWorkflow。该脚本使用 EC2 Config 或 EC2 Launch，具体取决于操作系统版本。
 - iii. aws:executeAwsApi - 阅读来自 AWSSupport-StartEC2RescueWorkflow 的结果。

输出

activateWindows.Output

getActivateWindowsOfflineResult。输出

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

描述

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2运行手册分析了从亚马逊弹性计算云 (Amazon EC2) 实例或弹性网络接口到终端节点的连接。AWS 服务 IPv6 不支持。运行手册使用您为 ServiceEndpoint 参数指定的值来分析与端点的连接。如果在您的 VPC 中找不到 AWS PrivateLink 端点，运行手册将使用当前 AWS 区域中的服务的公有 IP 地址。此自动化使用 Amazon Virtual Private Cloud 中的 Reachability Analyzer。有关更多信息，请参阅 Reachability Analyzer 中的 [什么是 Reachability Analyzer?](#)。

此自动化将检查以下事项：

- 检查您的虚拟私有云 (VPC) 是否配置为使用 Amazon 提供的 DNS 服务器。
- 检查您指定的 VPC 中是否存在 AWS PrivateLink 终端节点。AWS 服务 如果找到一个端点，自动化将验证 privateDns 属性是否已开启。
- 检查 AWS PrivateLink 终端节点是否使用默认终端节点策略。

注意事项

- 每次在来源和目标之间运行分析时，您需要支付费用。有关更多信息，请参阅 [Amazon VPC 定价](#)。
- 在自动化过程中，将创建网络洞察路径和网络洞察分析。如果自动化成功完成，运行手册将删除这些资源。如果清理步骤失败，则运行手册不会删除网络洞察路径，您需要手动将其删除。如果您不手动删除网络洞察路径，则该路径将继续计入您的 AWS 账户配额。有关 Reachability Analyzer 配额的更多信息，请参阅 Reachability Analyzer 中的 [Reachability Analyzer 配额](#)。
- 即使 Reachability Analyzer 返回 PASS，操作系统级配置（例如使用代理、本地 DNS 解析器或主机文件）也会影响连接。
- 查看对 Reachability Analyzer 执行的所有检查的评估。如果任何检查返回的状态为 FAIL，那么，即使整体可达性检查返回的状态为 PASS，也可能会影响连接性。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 来源

类型：字符串

描述：(必需) 您要分析自其的可达性的 Amazon EC2 实例或网络接口的 ID。

- ServiceEndpoint

类型：字符串

描述：(必需) 您要分析到其的可达性的服务端点的主机名。

- RetainVpcReachabilityAnalysis

类型：字符串

默认：false

描述：(可选) 确定是否保留所创建的网络洞察路径和相关分析。默认情况下，用于分析可达性的资源将在成功分析后删除。如果您选择保留分析，则运行手册不会删除该分析，您可以在 Amazon VPC 控制台将其可视化。自动化输出中提供了控制台链接。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateNetworkInsightsPath
- ec2>DeleteNetworkInsightsAnalysis
- ec2>DeleteNetworkInsightsPath
- ec2:DescribeAvailabilityZones
- ec2:DescribeCustomerGateways
- ec2:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeManagedPrefixLists

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribePrefixLists`
- `ec2:DescribeRegions`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTransitGatewayAttachments`
- `ec2:DescribeTransitGatewayPeeringAttachments`
- `ec2:DescribeTransitGatewayConnects`
- `ec2:DescribeTransitGatewayRouteTables`
- `ec2:DescribeTransitGateways`
- `ec2:DescribeTransitGatewayVpcAttachments`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `ec2:GetManagedPrefixListEntries`
- `ec2:GetTransitGatewayRouteTablePropagations`
- `ec2:SearchTransitGatewayRoutes`
- `ec2:StartNetworkInsightsAnalysis`
- `elasticloadbalancing:DescribeListeners`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeRules`
- `elasticloadbalancing:DescribeTags`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:DescribeTargetHealth`
- `tiros>CreateQuery`
- `tiros:GetQueryAnswer`
- `tiros:GetQueryExplanation`

文档步骤

1. `aws:executeScript` : 通过尝试解析主机名来验证服务端点。
2. `aws:executeScript` : 收集有关 VPC 和子网的详细信息。
3. `aws:executeScript` : 评估 VPC 的 DNS 配置。
4. `aws:executeScript` : 评估 VPC 端点检查。
5. `aws:executeScript` : 找到要连接到公共服务端点的互联网网关。
6. `aws:executeScript` : 确定要用于可达性分析的目的地。
7. `aws:executeScript` : 使用 Reachability Analyzer 分析从来源到端点的可达性，并在分析成功时清理资源。
8. `aws:executeScript` : 生成可达性评估报告。
9. `aws:executeScript` : 生成 JSON 形式的输出。

输出

- `generateReport.EvalReport` - 自动化系统所执行检查的结果，采用文本格式。
- `generateJsonOutput.Output` - 结果的最小版本，采用 JSON 格式。

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

描述

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 运行手册自动执行从英特尔支持的 Amazon Elastic Compute Cloud (Amazon EC2) 实例迁移到 AMD 支持的同等实例类型。此运行手册支

持基于 Nitro 系统构建的通用型 (M)、可突发性通用型 (T)、计算优化型 (C) 和内存优化型 (R) 实例。此运行手册可用于不由 Systems Manager 管理的实例。

为了降低数据丢失和停机的潜在风险，运行手册会检查实例的停止行为、实例是否在 Amazon EC2 Auto Scaling 组中、实例的运行状况，以及同一个可用区中是否有 AMD 支持的同等实例类型可用。默认情况下，如果已连接实例存储卷或实例是 AWS CloudFormation 堆栈的一部分，则此运行手册不会更改实例类型。如果要更改此行为，请为 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 参数中的任意一个指定 `yes`。

Important

访问 `AWSPremiumSupport-*` 运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持 计划](#)。

注意事项

- 我们建议您在`使用此运行手册之前先备份您的实例`。
- 更改实例类型需要运行手册来停止您的实例。当实例停止时，存储在 RAM 或实例存储卷中的所有数据都将丢失，并自动释放公有 IPv4 地址。有关更多信息，请参阅[停止和启动实例](#)。
- 如果您没有为 `TargetInstanceType` 参数指定值，则运行手册会尝试根据同一实例系列中的虚拟 CPUs 和内存来识别等效的 AMD 实例。如果运行手册无法识别等效的 AMD 实例类型，运行手册将结束。
- 使用 `DryRun` 选项，您可以捕获等效的 AMD 实例类型并验证需求，而无需实际更改实例类型。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 确认

类型：字符串

描述：(必填) 输入 yes 以确认您的目标实例将停止 (如果它正在运行)。

- InstanceId

类型：字符串

描述：(必填) 要更改其类型的 Amazon EC2 实例的 ID。

- TargetInstanceType

类型：字符串

默认：自动

描述：(可选) 要将您的实例更改为的 AMD 实例类型。默认automatic值在虚拟 CPUs 和内存方面使用等效的实例类型。例如，m5.large 将更改为 m5a.large。

- AllowInstanceStoreInstances

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果您指定 yes，运行手册将在已附加实例存储卷的实例上运行。

- AllowCloudFormationInstances

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果设置为 yes，则运行手册将在属于 CloudFormation 堆栈的实例上运行。

- AllowCrossGeneration

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果设置为 yes，运行手册将尝试在同一实例族中查找最新的等效 AMD 实例类型。

- DryRun

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果设置为 yes，运行手册将返回等效的 AMD 实例类型并验证迁移要求，而无需更改实例类型。

- SleepWait

类型：字符串

默认值：PT3S

描述：(可选) 运行手册在开始新的自动化之前应等待的时间。您为此参数提供的值必须符合 ISO 8601 标准。要了解有关创建 ISO 8601 字符串的更多信息，请参阅[为 Systems Manager 创建格式化的日期和时间字符串](#)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

- `ec2:GetInstanceTypesFromInstanceRequirements`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceState`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeTags`
- `ec2:ModifyInstanceAttribute`
- `ec2:StartInstances`
- `ec2:StopInstances`

文档步骤

1. `aws:assertAwsResourceProperty` : 确认目标 Amazon EC2 实例的状态为 `running`、`pending`、`stopped` 或 `stopping`。否则，自动化将结束。
2. `aws:executeAwsApi` : 从 Amazon EC2 目标实例收集属性。
3. `aws:branch` : 根据 Amazon EC2 实例的状态对自动化进行分支。
 - a. 如果为 `stopped` 或 `stopping`，则自动化会运行 `aws:waitForAwsResourceProperty`，直到 Amazon EC2 实例完全停止。
 - b. 如果为 `running` 或 `pending`，则自动化会运行 `aws:waitForAwsResourceProperty`，直到 Amazon EC2 实例通过状态检查。
4. `aws:assertAwsResourceProperty` : 通过检查 `aws:autoscaling:groupName` 标签是否已应用，确认 Amazon EC2 实例不是 Auto Scaling 组的一部分。
5. `aws:executeAwsApi` : 收集当前实例类型属性以查找等效的 AMD 实例类型。
6. `aws:assertAwsResourceProperty` : 确认 AWS Marketplace 产品代码未与 Amazon EC2 实例关联。某些产品类型并非在所有实例类型上都可用。
7. `aws:branch` : 根据您是否希望自动化检查 Amazon EC2 实例是否属于 CloudFormation 堆栈来分支自动化
 - a. 如果 `aws:cloudformation:stack-name` 标签应用于实例，则会运行自动化 `aws:assertAwsResourceProperty` 以确认该实例不是 CloudFormation 堆栈的一部分。
8. `aws:branch` : 根据实例根卷类型是否为 Amazon Elastic Block Store (Amazon EBS) 的实例对自动化进行分支。

9. `aws:assertAwsResourceProperty` : 确认实例关闭行为是 `stop` 且不是 `terminate`。
10. `aws:executeScript` : 确认此运行手册中只有一个针对当前实例的自动化。如果针对同一实例的另一个自动化已经在进行, 则它会返回错误并结束。
11. `aws:executeAwsApi`: 返回具有相同内存量和 v CPUs 的 AMD 实例类型的列表
12. `aws:executeScript` : 检查当前实例类型是否受支持并返回其等效的 AMD 实例类型。如果没有等效类型, 自动化将结束。
13. `aws:executeScript` : 确认 AMD 实例类型在同一可用区中可用, 并验证所提供的 IAM 权限。
14. `aws:branch` : 根据 `DryRun` 参数值是否为 `yes` 对自动化进行分支。
15. `aws:branch` : 检查原始和目标实例类型是否相同。如果它们相同, 自动化将结束。
16. `aws:executeAwsApi` : 获取当前实例状态。
17. `aws:changeInstanceState` : 停止 Amazon EC2 实例。
18. `aws:changeInstanceState`: 如果实例卡在了停止状态, 则强制其停止。
19. `aws:executeAwsApi` : 将实例类型更改为目标 AMD 实例类型。
20. `aws:sleep` : 更改实例类型后等待 3 秒钟以确保最终一致性。
21. `aws:branch` : 根据前实例的状态对自动化进行分支。如果是 `running`, 则实例已启动。
 - a. `aws:changeInstanceState` : 如果 Amazon EC2 实例在更改实例类型之前正在运行, 则启动该实例。
 - b. `aws:waitForAwsResourceProperty` : 等待 Amazon EC2 实例通过状态检查。如果实例未通过状态检查, 实例将变回其原始的实例类型。
 - i. `aws:changeInstanceState` : 停止 Amazon EC2 实例, 然后将其更改为原始实例类型。
 - ii. `aws:changeInstanceState` : 强制 Amazon EC2 实例停止, 然后再将其更改为原始实例类型, 以防它卡在停止状态。
 - iii. `aws:executeAwsApi` : 将 Amazon EC2 实例更改为其原始类型。
 - iv. `aws:sleep` : 更改实例类型后等待 3 秒钟以确保最终一致性。
 - v. `aws:changeInstanceState` : 如果 Amazon EC2 实例在更改实例类型之前正在运行, 则启动该实例。
 - vi. `aws:waitForAwsResourceProperty` : 等待 Amazon EC2 实例通过状态检查。
22. `aws:sleep` : 等待, 然后结束运行手册。

AWSsupport-CheckXenToNitroMigrationRequirements

描述

AWSSupport-CheckXenToNitroMigrationRequirements运行手册验证亚马逊弹性计算云 (Amazon EC2) 实例是否满足成功将实例类型从 Xen 类型实例更改为基于 Nitro 的实例类型的先决条件。此自动化将检查以下事项：

- 根设备是一个 Amazon Elastic Block Store (Amazon EBS) 卷。
- enaSupport 属性已启用。
- ENA 模块安装在实例上。
- 该 NVMe 模块已安装在实例上。如果是，则模块安装完毕，脚本将验证该模块是否加载到 `initramfs` 镜像中。
- 分析 `/etc/fstab` 并使用设备名称查找正在挂载的块设备。
- 确定操作系统 (OS) 是否默认使用可预测的网络接口名称。

此运行手册支持以下操作系统：

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian 服务器
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

默认：false

描述：(必填) 在迁移到基于 Nitro 的实例类型之前，您要检查其先决条件的 Amazon 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:StartAutomationExecution
- ssm:SendCommand
- iam:ListRoles

- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypes`

文档步骤

- `aws:executeAwsApi` - 收集有关该实例的详细信息。
- `aws:executeAwsApi` - 收集有关该实例虚拟机管理程序的信息。
- `aws:branch` - 根据目标实例是否已经在运行基于 Nitro 的实例类型进行分支。
- `aws:branch` - 检查基于 Nitro 的实例是否支持该实例的操作系统。
- `aws:assertAwsResourceProperty` - 验证您指定的实例是否由 Systems Manager 管理以及其状态是否为 Online。
- `aws:branch` - 根据实例的根设备是否是 Amazon EBS 卷进行分支。
- `aws:branch` - 根据是否为实例启用了 ENA 属性进行分支。
- `aws:runCommand` - 检查实例上是否有 ENA 驱动程序。
- `aws:runCommand` - 检查实例上的 NVMe 驱动程序。
- `aws:runCommand` - 检查 `fstab` 文件是否存在无法识别的格式。
- `aws:runCommand` - 检查实例上是否有可预测的接口名称配置。
- `aws:executeScript` - 根据上述步骤生成输出。

输出

`finalOutput.output` - 自动化执行的检查的结果。

AWSSupport-CloneXenEC2InstanceAndMigrateToNitro

描述

[这两InstanceAndMigrateToNitro本运行手册克隆、准备和迁移克隆的亚马逊弹性计算云 \(Amazon EC2 AWSSupport-CloneXenEC2\) Linux 实例，该实例目前在亚马逊 EC2 Xen 平台上运行，使其在亚马逊 EC2 Nitro 平台上运行。](#)这种自动化分为三个不同的分支：

- 初步检查：评估继续迁移的所有先决条件，包括检查目标 Amazon EC2 实例是否已在 Nitro 平台上运行、确定生命周期状态、验证操作系统以及验证 Systems Manager 连接。
- 测试：AMI从目标 Amazon EC2 实例创建测试并启动测试 Amazon EC2 实例以验证迁移过程，然后再继续。

- **CloneAndMigrate**：创建目标 Amazon EC2 实例的克隆，安装必要的驱动程序，为 Nitro 平台配置系统，并将实例类型更改为所需的 Nitro 类型。

 Important

在批准停止目标 Amazon EC2 实例之前，请确保该实例上运行的所有应用程序都已正常关闭。如果 Amazon EC2 实例没有关联弹性 IP 地址，则在实例停止和启动后，自动公有 IPv4 地址将发生变化。

 Important

免责声明：执行本运行手册可能会对您的账户收取额外费用，用于购买 Amazon EC2 实例、Amazon EBS Volumes 等。AMI 有关更多详细信息，请参阅[亚马逊 EC2 定价](#)和[亚马逊 EBS 定价](#)。

 Important

先决条件

目标 Amazon EC2 实例需要对存储库进行出站访问才能安装驱动程序和依赖项 `kernel-devel`，例如 `gcc`、`patch`、`rpm-build`、`wget`、`dracut`、`make`、`linux-headers`，并在需要时 `unzip` 使用包管理器。

受支持的操作系统

- Red Hat Enterprise Linux (RHEL) 8 和 9
- 亚马逊 Linux 2 和 AL2023
- Ubuntu Server 18.04 LTS、20.04 和 22.04
- Debian 11 和 12 (仅限 AWS 分区)
- SUSE12SP5 还有 SUSE15 SP (5,6)

如何工作？

运行手册执行以下高级步骤：

- 验证先决条件并检查实例是否适合迁移。
- 创建并测试AMI以确保迁移成功。
- 启用增强联网 (ENA) 属性并安装最新的 ENA 驱动程序。
- 在 initramfs 中验证和配置 NVMe 模块。
- 分析并修改 /etc/fstab 以将设备名称替换为。UUIDs
- 禁用可预测的接口命名并移除永久性网络规则。
- 将克隆的实例类型更改为所需的 Nitro 类型。
- 创建最终版AMI，可用作启动 Nitro 实例的黄金镜像。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:DescribeAutoScalingInstances
- ec2:CreateImage
- ec2:CreateTags
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes

- `ec2:DeregisterImage`
- `ec2:ModifyInstanceAttribute`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `iam:PassRole`
- `sns:Publish`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`

示例 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:CreateImage",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute:",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DeregisterImage",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "iam:PassRole",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
```

```

        "ssm:SendCommand"
      ],
      "Resource": "*"
    }
  ]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 **Execute automation**。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole（可选）：
 - 描述：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 ARN。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - TargetInstanceId（必填）：
 - 描述：（必填）您要迁移到 Nitro 平台的目标 Amazon EC2 实例的实例 ID。
 - 类型：AWS::EC2::Instance::Id
 - NitroInstanceType（可选）：
 - 描述：（可选）输入目标 Nitro 实例类型。仅支持 Nitro M5、M6、C5、C6、R5、R6 和 T3 实例（例如 t3.small）。默认值：m5.xlarge。
 - 类型：String
 - 允许的模式：`^(m5a?z?d?n?|c5a?d?n?|r5a?d?n?b?|(c|m|r)6(a|i)?d?)\\.(2|4|8|12|16|24|32)?xlarge$|^t3a?\\..((x|2x)?large|nano|micro|small|medium)$`
 - 默认值：m5.xlarge
 - SNSTopicArn（必填）：
 - 描述：（必填）提供亚马逊 SNS 主题的 ARN 以获取批准通知。此 Amazon SNS 主题用于在自动执行期间发送批准通知。

- 类型 : String
- 允许的模式 : `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:sns:(us(-gov|-isob)?|ap|ca|af|me|cn|eu|sa)-(central|(north|south)?(east|west)?)-\\d:\\d{12}:[a-zA-Z0-9_.-]{1,256}$`
- ApproverIAM (必填) :
 - 描述 : (必填) 提供能够批准或拒绝操作的 AWS 经过身份验证的委托人列表。最大审批者数量为 10。
 - 类型 : StringList
 - 允许的模式 : `^[a-zA-Z0-9_+=, .@\\-\\/] {1,128}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:(sts|iam)::[0-9]{12}:[a-zA-Z0-9_+=, .@\\-\\/] {1,256}$`
- MinimumRequiredApprovals (可选) :
 - 描述 : (可选) 恢复自动化所需的最低批准数量。默认值 : 1。
 - 类型 : 整数
 - 默认 : 1
- DeleteResourcesOnFailure (可选) :
 - 描述 : (可选) 是否终止克隆的 Amazon EC2 实例以及自动化AMI是否失败。
 - 类型 : Boolean
 - 允许的值 : [true, false]
 - 默认值 : true
- 致谢 (必填) :
 - 描述 : (必填) 请阅读本自动化运行手册执行的操作的完整详细信息，如果您确认这些步骤，请写上“是的，我理解并确认”。
 - 类型 : String
 - 允许的模式 : `^Yes, I understand and acknowledge$`
- AllowInstanceStoreInstances (可选) :
 - 描述 : (可选) 如果您指定 yes，运行手册将在已附加实例存储卷的实例上运行。警告：实例停止后，实例存储卷中的数据将丢失。此参数有助于避免数据意外丢失。
 - 类型 : Boolean
 - 允许的值 : [yes, no]

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **checkConcurrency:**

确保只有一次针对当前 Amazon EC2 实例执行此运行手册。

- **getTargetInstanceProperties:**

获取目标 Amazon EC2 实例的详细信息。

- **checkIfNitroInstanceTypeIsSupportedInAZ:**

确定目标 Nitro 实例类型是否在与目标 Amazon EC2 实例相同的可用区中受支持。

- **createTestImage:**

AMI从提供的实例创建测试。

- **launchTestInstanceInSameSubnet:**

AMI使用与目标 Amazon EC2 实例相同的配置从测试中启动测试版 Amazon EC2 实例。

- **approvalToStopTargetInstance:**

等待指定委托人批准后停止目标实例。

- **createBackupImage:**

AMI从提供的实例创建用于备份。

- **launchInstanceInSameSubnet:**

AMI使用与源 Amazon EC2 实例相同的配置，从备份中启动一个新的 Amazon EC2 实例。

- **checkAndInstallENADrivers:**

确定 Amazon EC2 实例上增强型联网适配器 (ENA) 驱动程序的可用性，如果缺少则进行安装。

- **checkAndAddNVMEDrivers:**

确定克隆的 Amazon EC2 实例上的 NVMe 驱动程序的可用性，如果缺少则进行安装。

- **checkAndModifyFSTABEntries:**

确定中/etc/fstab是否使用了设备名称，如果找到 UUIDs，则将其替换为其名称。

- **setNitroInstanceTypeForClonedInstance:**

为克隆的亚马逊 EC2 实例设置提供的目标 Amazon EC2 实例类型。

- **approvalForCreatingImageAfterDriversInstallation:**

如果克隆的 Amazon EC2 实例在 Nitro 平台上成功启动，则等待用户批准。

- **createImageAfterDriversInstallation:**

仅当新的 Amazon EC2 实例在 Nitro 平台上成功启动时，才会从新的 Amazon EC2 实例创建映像。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

AWS Systems Manager 自动化

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-CollectSAPHANALogs

描述

该AWSSupport-CollectSAPHANALogs运行手册在部署时从 SAP HANA 收集亚马逊弹性计算云 (Amazon EC2) 实例上的系统日志，该实例是 SAP 的一部分。AWS Amazon EC2 实例必须由 AWS Systems Manager (Systems Manager) 管理。运行手册会检查所需的软件包并在缺失时进行安装，针对检测到的操作系统运行相应的日志收集工具，并可选择将收集的日志上传到亚马逊简单存储服务 (Amazon S3) 存储桶。

Important

此运行手册要求/var/log分区上至少有 200 MB 的可用磁盘空间。运行此运行手册可能会在目标 Amazon EC2 实例上安装其他软件包。您必须通过将Acknowledgement参数设置为来确认这一点Yes。在 Amazon S3 中存储日志会产生标准的 Amazon S3 存储和请求费用。

支持的操作系统

- Red Hat Enterprise Linux 8.4 及更高版本
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 15 SP3 及更高版本

如果缺少软件包，则已安装

SUSE Linux Enterprise Server:

- supportutils
- yast2-support
- supportutils-plugin-suse-public-cloud
- supportutils-plugin-ha-sap
- crmsh
- unzip
- curl
- aws-cli (可选，如果设置InstallAWSCLI为，则安装Yes)

Red Hat Enterprise Linux:

- sos
- crm_report
- unzip
- curl
- aws-cli (可选，如果设置InstallAWSCLI为，则安装Yes)

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型:: AWS::EC2::Instance: ID

描述：(必填) 运行 SAP 工作负载的 Amazon EC2 实例的 ID，应从中收集日志。

- 确认

类型：字符串

有效值：是

描述：(必填) 我确认本运行手册可能会在目标 Amazon EC2 实例中安装其他软件包以进行日志收集。

- S3 LogDestination

类型:: AWS::S3::Bucket: 姓名

描述：(可选) 将日志上传到的 Amazon S3 存储桶的名称。存储桶不能是公开的，并且必须属于同一个 AWS 账户。如果未提供，则日志存储在实例本地存储中。

- S3Prefix

类型：字符串

默认：AWSSupport-CollectSAPHANALogs

允许的模式：`^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$`

描述：(可选) 存储日志的 Amazon S3 存储桶前缀。如果未提供，则默认为AWSSupport-CollectSAPHANALogs。

- 安装 AWSCLI

类型：字符串

有效值：是 | 否

默认：否

描述：(可选) 是否在实例上安装 AWS CLI。如果是Yes，则运行手册会安装 AWS CLI (如果还没有)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- s3:GetBucketPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketOwnershipControls
- s3:GetEncryptionConfiguration
- s3:PutObject

文档步骤

1. AssertInstanceIsSSMManaged-验证目标 Amazon EC2 实例是否由 Systems Manager 管理并且为PingStatus. Online如果实例未被托管，则运行手册将被取消。
2. GetInstanceInformation-检索有关指定 Amazon EC2 实例的信息，包括用于确定适当的日志收集方法的平台名称。
3. CollectLogs-在实例上运行 shell 脚本以收集日志。例如SUSE Linux Enterprise Server，脚本使用supportconfig。例如Red Hat Enterprise Linux，它使用sos report。对于 HA 集群，该脚本还使用crm report命令收集过去 7 天内的其他 HA 日志。如果缺少必需的软件包，则安装完毕。

4. BranchOnS3BucketProvided-根据中是否提供了 Amazon S3 存储桶来分支执行S3LogDestination。如果未提供存储桶，则运行手册将跳至。GenerateReport否则，它会继续CheckS3BucketPublicStatus。
5. CheckS3BucketPublicStatus-检查中指定的 Amazon S3 存储桶S3LogDestination是否配置了服务器端加密 (SSE)，以及它是否允许匿名或公开读取或写入访问权限。还会验证实际的存储桶所有者是否与预期的存储桶所有者相同。如果此步骤失败，则运行手册将继续运行GenerateReport而不上传。
6. UploadLogsToS3-将收集的日志上传到指定的 Amazon S3 存储桶。如果设置InstallAWSCLI为Yes，但未安装 AWS CLI，则脚本会在上传之前安装 AWS CLI。
7. GenerateReport-生成日志收集过程报告。如果提供了 Amazon S3 存储桶，则它会包含上传日志的 Amazon S3 存储桶名称和前缀。如果不是，则表示日志存储在实例本地。它还会报告任何先前步骤失败的原因。

输出

GenerateReport.Summary-日志收集结果摘要。

GenerateReport.LogLocation-存储日志的位置，可以是实例上的本地路径，也可以是 Amazon S3 URI。

GenerateReport.Status-日志收集执行的总体状态。

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-CollectSAPHANALogs](#)在 Systems Manager 的“文档”下导航至。

2. 选择 Execute automation (执行自动化) 。

3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表你执行操作的 IAM 角色的 ARN。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 实例 ID (必填)：

运行 SAP 工作负载的 Amazon EC2 实例的 ID。

- 致谢 (必填)：

输入Yes以确认运行手册可能会在目标 Amazon EC2 实例上安装其他软件包。

- **S3LogDestination** (可选) :

要将日志上传到的 Amazon S3 存储桶的名称。如果未提供, 则日志存储在实例本地。

- **S3Prefix** (可选) :

存储日志的 Amazon S3 存储桶前缀。默认值为 `AWSSupport-CollectSAPHANALogs`。

- **InstallAWSCLI** (可选) :

如果实例上没有 AWS CLI, 请选择Yes自动安装 CLI。默认值为 No。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤:

- **AssertInstanceIsSSMManaged**

验证目标 Amazon EC2 实例是否由 Systems Manager 管理并且为 `PingStatus`。Online

- **GetInstanceInformation**

检索有关指定 Amazon EC2 实例的信息, 包括平台名称。

- **CollectLogs**

运行 shell 脚本以使用 `for SLES` 或 `sos report f supportconfig or` 收集日志 `RHEL`。对于 HA 集群, 还可以使用收集过去 7 天的 HA 日志 `crm report`。

- **BranchOnS3BucketProvided**

`GenerateReport`如果未提供 Amazon S3 存储桶, 则跳至, 否则继续执行。`CheckS3BucketPublicStatus`

- **CheckS3BucketPublicStatus**

验证 Amazon S3 存储桶已启用 SSE、不允许公开访问且归同一个 AWS 账户所有。

- **UploadLogsToS3**

将收集的日志上传到指定的 Amazon S3 存储桶。如果 `InstallAWSCLI` 是, 则安装 AWS CLI `Yes`, 但它还不存在。

- **GenerateReport**

生成日志收集结果的摘要，包括日志位置和任何步骤失败。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSsupport-ConfigureEC2Metadata

描述

本运行手册可帮助您为亚马逊弹性计算云 (Amazon) 实例配置实例元数据服务 (IMDS EC2) 选项。使用此运行手册，您可以执行以下配置：

- IMDSv2 例如，强制使用元数据。
- 配置 `HttpPutResponseHopLimit` 值。
- 允许或拒绝访问实例元数据。

有关实例元数据的更多信息，请参阅 Amazon EC2 用户指南中的[配置实例元数据服务](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 强制执行 IMDSv2

类型：字符串

有效值：必需 | 可选

默认：可选

描述：(可选) 强制执行 IMDSv2。如果您愿意required，Amazon EC2 实例将仅使用 IMDSv2。如果您愿意optional，则可以在 IMDSv1 和之间进行选择，IMDSv2 以访问元数据。

Important

如果强制执行 IMDSv2，使用的应用程序 IMDSv1 可能无法正常运行。在强制执行之前 IMDSv2，请确保使用 IMDS 的应用程序已升级到支持的 IMDSv2 版本。有关实例元数据服务版本 2 (IMDSv2) 的信息，请参阅 Amazon EC2 用户指南中的[配置实例元数据服务](#)。

- HttpPutResponseHopLimit

类型：整数

有效值：0-64

默认：0

描述：(可选) 实例元数据请求的所需 HTTP PUT 响应跃点限制值 (1-64)。此值控制 PUT 响应可以遍历的跳点数。为防止响应在实例之外传播，请为参数值指定 1。

- InstanceId

类型：字符串

描述：(必填) 您要配置其元数据设置的 Amazon EC2 实例的 ID。

- **MetadataAccess**

类型：字符串

有效值：启用 | 禁用

默认值：启用

描述：(可选) 允许或拒绝访问 Amazon 实例中的 EC2 实例元数据。如果您指定 disabled，则所有其他参数将被忽略，且实例的元数据访问将被拒绝。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:ModifyInstanceMetadataOptions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

文档步骤

1. branchOnMetadataAccess-根据MetadataAccess参数值进行分支自动化。
2. disableMetadataAccess -调用 ModifyInstanceMetadataOptions API 操作以禁用元数据端点访问权限。
3. branchOnHttpPutResponseHopLimit -根据HttpPutResponseHopLimit参数的值分支自动化。
4. maintainHopLimitAndConfigureImdsVersion -如果HttpPutResponseHopLimit为 0，则保持当前跳跃限制并更改其他元数据选项。
5. waitBeforeAssertingIMDSv2状态-在断言 IMDSv2状态之前等待 30 秒。
6. setHopLimitAndConfigureImdsVersion -如果大HttpPutResponseHopLimit于 0，则使用给定的输入参数配置元数据选项。
7. waitBeforeAssertingHopLimit -在断言元数据选项之前等待 30 秒。
8. assertHopLimit -断言该HttpPutResponseHopLimit属性已设置为您指定的值。
9. branchVerificationOnIMDSv2选项-根据EnforceIMDSv2参数的值进行分支验证。
- 10断言 IMDSv2 IsOptional -将HttpTokens值设置为。optional
- 11断言 IMDSv2 IsEnforced -将HttpTokens值设置为。required

12.waitBeforeAssertingMetadataState -等待 30 秒后才断言元数据状态已禁用。

13.assertMetadataIs已禁用-断言元数据为。disabled

14.describeMetadataOptions -在应用您指定的更改后获取元数据选项。

输出

describeMetadataOptions.State

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

AWSSupport-ContainEC2Instance

描述

该AWSSupport-ContainEC2Instance运行手册为文章中概述的程序提供了自动解决方案，[当面临潜在的入侵或可疑情况时，如何隔离 Amazon EC2 实例](#)？自动化的分支取决于您指定的值。

如何工作？

本自动化运行手册通过一系列协调步骤对 Amazon EC2 实例AWSSupport-ContainEC2Instance进行网络控制。在Contain模式下执行时，它首先验证输入参数并检查实例是否未终止。然后，它将当前的安全组配置备份到 Amazon S3 存储桶，以便日后恢复。运行手册创建了两个安全组：临时的“所有访问权限”安全组和最后一个“遏制”安全组。它会逐渐将实例的网络接口从其原始安全组过渡到所有访问安全组，最后过渡到包含安全组。如果指定，它将创建实例的未加密和加密AMI备份。对于 Auto Scaling 组中的实例，它会处理必要的 Auto Scaling 组修改并将实例置于待机状态。在Release模式下执行时，它会使用 Amazon S3 中的备份设置将实例恢复到其原始网络配置。运行手册支持无需进行实际更改即可预览操作的DryRun参数，并在整个容器和发布工作流程中包括全面的错误处理和报告机制。

Important

- 此运行手册执行各种需要提升权限的操作，例如修改安全组、创建安全组以及与 Auto AMI Scaling 组进行交互。这些操作可能会导致权限提升或影响您账户中的其他工作负载。您应查看向AutomationAssumeRole参数指定的角色授予的权限，并确保这些权限适用于预期用例。您可以参考以下 AWS 文档，了解有关 IAM 权限的更多信息：[AWS Identity and](#)

[Access Management \(IAM\) Permissions](#)[AWS Systems Manager Automation Permissions](#)。

- 此运行手册执行的变异操作可能会导致您的工作负载不可用或中断。具体而言，它会修改与目标 Amazon EC2 实例关联的安全组，这可能会影响网络连接。此外，如果该实例是 Auto Scaling 组的一部分，则运行手册可能会修改该组的配置，从而可能影响其扩展行为。
- 在控制过程中，此运行手册会创建其他资源，例如安全组和 AMI。虽然这些资源被标记为用于识别，但您应该知道它们的创建，并确保在控制过程完成后进行适当的清理或管理。
- 如果将 Action 参数设置为 Release，则此运行手册会尝试将 Amazon EC2 实例的配置恢复到其原始状态。但是，还原过程有可能失败，从而使实例处于不一致的状态。运行手册提供了在出现此类故障时手动恢复的说明，但您应该做好在恢复过程中处理潜在问题的准备。

建议在生产环境中执行运行手册之前，请仔细阅读运行手册，了解其潜在影响，并在非生产环境中对其进行测试。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- 自动缩放：CreateOrUpdateTags
- 自动缩放：DeleteTags
- 自动缩放：DescribeAutoScalingGroups
- 自动缩放：DescribeAutoScalingInstances
- 自动缩放：DescribeTags
- 自动缩放：EnterStandby

- 自动缩放 : ExitStandby
- 自动缩放 : UpdateAutoScalingGroup
- ec2: AuthorizeSecurityGroupEgress
- ec2: AuthorizeSecurityGroupIngress
- ec2: CopyImage
- ec2: CreateImage
- ec2: CreateSecurityGroup
- ec2: CreateSnapshot
- ec2: CreateTags
- ec2: DeleteSecurityGroup
- ec2: DeleteTags
- ec2: DescribeImages
- ec2: DescribeInstances
- ec2: DescribeSecurityGroups
- ec2: DescribeSnapshots
- ec2: DescribeTags
- ec2: ModifyNetworkInterfaceAttribute
- ec2: RevokeSecurityGroupEgress
- kms: CreateGrant
- kms: DescribeKey
- kms: GenerateDataKeyWithoutPlaintext
- kms: ReEncryptFrom
- kms: ReEncryptTo
- s3 : CreateBucket
- s3 : DeleteObjectTagging
- s3 : GetAccountPublicAccessBlock
- s3 : GetBucketAcl
- s3 : GetBucketLocation
- s3 : GetBucketOwnershipControls
- s3 : GetBucketPolicy

- s3 : GetBucketPolicyStatus
- s3 : GetBucketPublicAccessBlock
- s3 : GetObject
- s3 : ListBucket
- s3 : PutAccountPublicAccessBlock
- s3 : PutBucketPolicy
- s3 : PutBucketVersioning
- s3 : PutObject
- s3 : PutObjectTagging

策略示例：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOperations",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "kms:DescribeKey",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
```

```
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": "*"
},
{
  "Sid": "WriteOperations",
  "Effect": "Allow",
  "Action": [
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:DeleteTags",
    "autoscaling:EnterStandby",
    "autoscaling:ExitStandby",
    "autoscaling:UpdateAutoScalingGroup",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CopyImage",
    "ec2:CreateImage",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSnapshot",
    "ec2:CreateTags",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTags",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:RevokeSecurityGroupEgress",
    "kms:CreateGrant",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:ReEncryptFrom",
    "kms:ReEncryptTo",
    "s3:CreateBucket",
    "s3>DeleteObjectTagging",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketPolicy",
    "s3:PutBucketVersioning",
    "s3:PutObject",
    "s3:PutObjectTagging"
  ],
  "Resource": "*"
}
]
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-ContainEC2Instance](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - 操作 (必填)：
 - 描述：(必填) 选择Contain隔离 Amazon EC2 实例或Restore尝试从先前的备份中恢复 Amazon EC2 实例配置的原始配置。
 - 类型：字符串
 - 允许的模式：Contain|Restore
 - DryRun (可选)：
 - 描述：(可选) 设置为true，自动化将不执行任何命令，而是报告其本来会尝试执行的操作，详细说明每个步骤。默认值：true。
 - 类型：布尔值
 - 允许的值：true|false
 - 创建AMIBackup (可选)：
 - 描述：(可选) 如果设置为true，则将在执行控制操作之前创建一个 AMI Amazon EC2 实例。
 - 类型：布尔值
 - 允许的值：true|false
 - KmsKey (可选)：
 - 描述：(可选) 将用于创建加密的目标 Amazon EC2 实例AMI的 AWS KMS 密钥的 ID。默认值设置为alias/aws/ebs。
 - 类型：字符串
 - 允许的模式：`^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]{1}-[0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-`

```
f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32}))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}: [0-9]{12}:)?alias/.{1,})$
```

- BackupS3BucketName (视情况而定) :
 - 描述 : (视情况而定) Amazon Amazon S3 存储桶, Action用于在配置时上传配置Contain或在配置Action时恢复配置Release。注意: 如果提供的存储桶在账户中不存在, 自动化系统 will 代表您创建一个 Amazon S3 存储桶。
 - 类型 : AWS::S3::Bucket::Name
- TagIdentifier (可选) :
 - 描述 : (可选) 一种标记Key=BatchId, Value=78925, 其格式将添加到此 Runbook 在包含工作流程中创建或修改的 AWS 资源中。此标签可用于识别和管理在控制过程中关联的资源。在还原工作流程中, 此参数指定的标签将从资源中删除。注意: 标签键和值区分大小写。
 - 类型 : 字符串
 - 允许的模式 : ^\$|^([Kk][Ee][Yy]=\\+\\-\\=\\._\\:\\\\/@a-zA-Z0-9]{1,128}, [Vv][Aa][Ll][Uu][Ee]=\\+\\-\\=\\._\\:\\\\/@a-zA-Z0-9]{0,128})\$
- BackupS3BucketAccess (视情况而定) :
 - 描述 : (视情况而定) 运行控制操作后允许访问备份 Amazon S3 存储桶的 IAM 用户或角色的 ARN。当是时, 此参数是必需Action的Contain。自动将AutomationAssumeRole正在其上下文中运行自动化的用户添加到列表中。
 - 类型 : 字符串
 - 允许的模式 : ^\$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\\\/([\\w+\\\\/=. ,@-]+)\$
- IngressTrafficRules (可选) :
 - 描述 : (可选) 以逗号分隔的安全组入口规则映射, 格式为 [{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}] Cidr IpProtocol、FromPort 和 ToPort, 将应用于 Amazon EC2 实例。如果未提供任何规则, 则会将没有任何入口规则的安全组附加到 Amazon EC2 实例, 从而有效地将其与任何传入流量隔离开来。
 - 类型 : MapList
 - 允许的模式 : ^\\{\\}\$|^\\{\\["Cidr\\":\\["\\x00-\\x7F+]{1,128}\\", \\["IpProtocol\\":\\["\\x00-\\x7F+]{1,128}\\", \\["FromPort\\":\\["\\x00-\\x7F+]{1,128}\\", \\["ToPort\\":\\["\\x00-\\x7F+]{0,255}\\}\\}\\}
- EgressTrafficRules (可选) :

- 描述：(可选) 以逗号分隔的安全组出站规则映射，其中包含 Cidr IpProtocol、FromPort 和 ToPort，格式[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]将应用于 Amazon EC2 实例。如果未提供任何规则，则会将没有任何出口规则的安全组附加到 Amazon EC2 实例，从而有效地阻止所有传出流量。
- 类型：MapList
- 允许的模式：`^\\{\\}$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"}\\\"\\\"}`
- BackupS3KeyName (可选) :
 - 描述：(可选) 如果设置Action为Restore，则指定自动化用于尝试恢复目标 Amazon EC2 实例配置的 Amazon S3 密钥。Amazon S3 密钥通常遵循以下格式：`{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json`。密钥可以从之前的控制自动化执行的输出中获得。
 - 类型：字符串
 - 允许的模式：`^[a-zA-Z0-9\\.\\-\\_\\!\\*\\'\\(\\)/]{0,1024}$`

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- ValidateRequiredInputs

验证是否提供了所有必需的输入。

- AssertInstanceIsNotTerminated

检查目标 Amazon EC2 实例是否未终止 (已删除)。

- GetAutoScalingInstanceInfo

如果目标 Amazon EC2 实例是 Auto Scaling 组的一部分，则获取 Amazon EC2 实例生命周期和组名称。

- CheckBackupS3BucketName

检查目标 Amazon S3 存储桶是否可能向其对象授予read或write公开访问权限。如果存储桶不存在，则会创建一个新的 Amazon S3 BackupS3BucketName 存储桶。

- BranchOnActionAndMode

根据输入参数对自动化进行分支Action和DryRun。

- BranchOnAutoScalingGroupMembership

根据目标 Amazon EC2 实例是否属于 Auto Scaling 组及其生命周期状态来分支自动化。

- DescribeAutoScalingGroups

获取并存储关联的 Amazon EC2 Auto Scaling 组配置。

- ModifyAutoScalingGroup

修改包含操作的关联的 Amazon EC2 Auto Scaling 组配置，将 Amazon EC2 实例设置为Standby状态并调整 Auto Scaling 组MinSize容量。

- BackupInstanceSecurityGroups

获取并存储目标 Amazon EC2 实例安全组的配置。

- CreateAllAccessSecurityGroup

创建一个临时安全组，允许取代目标 Amazon EC2 实例的安全组的所有入口流量。

- CreateContainmentSecurityGroup

使用指定的入口和出口规则创建限制性容器安全组，并用它替换临时的全部访问安全组。

- BranchOnCreateAMIBackup

根据CreateAMIBackup输入参数对自动化进行分支。

- AssertSourceInstanceRootVolumelsEbs

检查目标 Amazon EC2 实例根卷是否是 Amazon EBS。

- CreateImage

创建目标 Amazon EC2 实例。AMI

- RestoreInstanceConfiguration

从备份中恢复目标 Amazon EC2 实例配置。

- ReportContain

输出遏制操作的试运行详细信息。

- ReportRestore

输出恢复操作的试运行详细信息。

- ReportRestoreFailure

提供在恢复工作流程失败的情况下恢复目标 Amazon EC2 实例原始配置的说明。

- ReportContainmentFailure

提供在控制工作流程失败的情况下恢复目标 Amazon EC2 实例原始配置的说明。

- FinalOutput

输出遏制操作的详细信息。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果：

- FinalOutput。输出

当设置为 False 时DryRun，输出此运行手册执行的遏制操作的详细信息。

- RestoreInstanceConfiguration。输出

当设置为 False 时，输出此运行手册执行DryRun的还原操作。

- ReportContain。输出

设置为 Tr DryRun ue 时，输出此运行手册执行的遏制操作的详细信息。

- ReportRestore。输出

设置为 True 时DryRun，输出此运行手册执行的还原操作的详细信息。

- ReportContainmentFailure。输出

提供在控制工作流程失败的情况下恢复目标 Amazon EC2 实例原始配置的说明。

- ReportRestoreFailure。输出

提供在恢复工作流程失败的情况下恢复目标 Amazon EC2 实例原始配置的说明。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行简单的自动化](#)

[设置自动化](#)

- [Support 自动化工作流程](#)

AWSsupport-CopyEC2Instance

描述

该AWSsupport-CopyEC2Instance运行手册为知识中心文章中概述的程序提供了自动解决方案。[如何将我的 EC2实例移动到另一个子网、可用区或 VPC？](#) 自动化的分支取决于您为 Region 和 SubnetId 参数指定的值。

如果您为参数指定值但未为SubnetId参数指定值，Region则自动化会创建一个 Amazon Machine Image (AMI) 的目标实例并从中启动一个新实例 AMI 在您指定的子网中。

如果您为SubnetId参数和参数指定值，Region则自动化会创建一个 AMI 在目标实例中，复制 AMI 到 AWS 区域 您指定的，然后从中启动一个新实例 AMI 在您指定的子网中。

如果您为参数指定值但未为Region参数指定值，SubnetId则自动化会创建一个 AMI 在目标实例中，复制 AMI 到您指定的区域，然后从中启动一个新实例 AMI 位于目标区域的虚拟私有云 (VPC) 的默认子网中。

如果没有为Region或SubnetId参数指定任何值，则自动化会创建一个 AMI 的目标实例，并从中启动一个新实例 AMI 在您的 VPC 的默认子网中。

要复制 AMI 对于不同的区域，您必须为AutomationAssumeRole参数提供一个值。如果在waitForAvailableDestinationAmi步骤期间自动化超时，AMI 可能还在复制。在这种情况下，您可以等待复制完成，然后手动启动该实例。

在运行此自动化之前，请注意以下事项：

- AMI 是基于Amazon Elastic Block Store (Amazon EBS) 快照。对于之前没有快照的大型文件系统，AMI 创建可能需要几个小时。要减少 AMI 创建时间，请在创建 Amazon EBS 快照之前创建 AMI。
- 创建一个 AMI 不会为实例上的实例存储卷创建快照。有关将实例存储卷备份到 Amazon EBS 的信息，请参阅[如何将我的亚马逊实例上的实例存储卷备份到 Amazon EC2 EBS？](#)
- 新的 Amazon EC2 实例具有不同的私有 IPv4 或公 IPv6 有 IP 地址。您必须使用分配给新实例的新 IP 地址，更新对旧 IP 地址的所有引用（例如，在 DNS 条目中）。如果您在源实例上使用弹性 IP 地址，请务必将其附加到新实例。

- 当副本启动并尝试联系域时，可能会出现域安全标识符 (SID) 冲突问题。在捕获 AMI 之前，请使用 Sysprep 或从域中移除已加入域的实例，以防止出现冲突问题。有关更多信息，请参阅[如何使用 Sysprep 创建和安装自定义的可重复使用的 Windows ? AMIs](#)

[运行此自动化 \(控制台 \)](#)

Important

我们不建议使用此运行手册来复制 Microsoft Active Directory Domain Controller 实例。

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要复制的实例的 ID。

- KeyPair

类型：字符串

描述：(可选) 要与新复制的实例关联的密钥对。如果您要将实例复制到其他区域，请确保指定的区域存在密钥。

- 区域

类型：字符串

描述：(可选) 要将实例复制到的区域。如果您为此参数指定一个值，但未为 SubnetId 和 SecurityGroupIds 参数指定值，自动化将尝试使用默认安全组在默认的 VPC 中启动实例。如果在目标区域启用 EC2-Classic，则启动将失败。

- SubnetId

类型：字符串

描述：(可选) 要将实例复制到的子网的 ID。如果目标区域启用了 EC2-Classic，则必须为此参数提供一个值。

- InstanceType

类型：字符串

描述：(可选) 复制的实例应当启动的目标实例类型。如果您没有为此参数指定一个值，则使用源实例类型。如果要将实例复制到的区域不支持源实例类型，自动化将失败。

- SecurityGroupIds

类型：字符串

描述：(可选) IDs 要与复制的实例关联的安全组列表，以逗号分隔。如果您未为此参数指定一个值，且该实例未被复制到其他区域，则使用与源实例关联的安全组。如果您要将实例复制到其他区域，则使用目的地区域中默认 VPC 的默认安全组。

- KeepImageSourceRegion

类型：布尔值

有效值：true | false

默认：True

描述：(可选) 如果您 true 为此参数指定，则自动化不会删除 AMI 源实例的。如果您 false 为此参数指定，则自动化会取消注册 AMI 并删除关联的快照。

- KeepImageDestinationRegion

类型：布尔值

有效值：true | false

默认：True

描述：(可选) 如果您true为此参数指定，则自动化不会删除 AMI 它将被复制到您指定的区域。如果您false为此参数指定，则自动化会取消注册 AMI 并删除关联的快照。

- NoRebootInstanceBeforeTakingImage

类型：布尔值

有效值：true | false

默认：false

描述：(可选) 如果您true为此参数指定，则在创建源实例之前，不会重新启动源实例 AMI。使用此选项时，无法保证所创建映像的文件系统的完整性。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateImage
- ec2:DeleteSnapshot
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeImages
- ec2:RunInstances

如果您要将实例复制到其他区域，则还需要具有以下权限。

- ec2:CopyImage

文档步骤

- describeOriginalInstance详细信息-从要复制的实例中收集详细信息。

- `assertRootVolumeIsEbs` -检查根卷设备类型是否为ebs，如果不是，则结束自动化。
- `evalInputParameters` -评估为输入参数提供的值。
- `createLocalAmi` -创建一个 AMI 源实例的。
- `tagLocalAmi` -标记 AMI 在上一步中创建。
- `branchAssertRegionIsSame` -根据实例是在同一区域内复制还是复制到其他区域进行分支。
- `branchAssertSameRegionWithKeyPair` -根据是否为在同一区域内复制的实例的KeyPair参数提供了值进行分支。
- `sameRegionLaunchInstanceWithKeyPair` -从启动 Amazon EC2 实例 AMI 源实例位于您使用指定的 key pair 指定的子网或子网中。
- `sameRegionLaunchInstanceWithoutKeyPair` -从启动 Amazon EC2 实例 AMI 源实例位于同一子网或不带密钥对 (key pair) 的子网中。
- `copyAmiToRegion` -复制 AMI 到目标地区。
- `waitForAvailableDestinationAmi` -等待复制的内容 AMI 要成为的状态available。
- `destinationRegionLaunchInstance` -使用复制的 EC2 实例启动 Amazon 实例 AMI。
- `branchAssertDestinationAmiToDelete` -根据您为KeepImageDestinationRegion参数提供的值进行分支。
- `deregisterDestinationAmiAndDeleteSnapshots` -注销复制的内容 AMI 并删除关联的快照。
- `branchAssertSourceAmiToDelete` -根据您为KeepImageSourceRegion参数提供的值进行分支。
- `deregisterSourceAmiAndDeleteSnapshots` -注销 AMI 从源实例创建并删除关联的快照。
- `sleep` - 使自动化休眠 2 秒钟。这是最终步骤。

输出

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunchInstance`实例。 `DestinationInstanceId`

AWSPremiumSupport-DiagnoseDiskUsageOnLinux

描述

该AWSPremiumSupport-DiagnoseDiskUsageOnLinux运行手册分析了目标亚马逊弹性计算云 (Amazon EC2) 实例的亚马逊弹性区块存储 (Amazon EBS) 卷，以确定它们是否需要扩展。它会根据运

行手册输入参数中定义的阈值检查每个卷的使用情况、文件系统类型和扩展历史记录。该脚本会考虑诸如最近的修改、支持的文件系统和 AWS 音量限制等因素。然后，它会输出可供扩展的卷（如果有），以及每卷的相关细节。

如何工作？

此运行手册执行以下操作：

- 验证目标实例是否由 Systems Manager 管理且未运行 Windows
- 检索实例详细信息，包括平台和根设备类型
- 获取 Amazon EC2 实例使用的卷
- 在 Linux 上运行预检查以分析磁盘使用情况并确定扩展候选对象
- 输出有待扩展的数量以及相关的细节

Important

访问 `AWSPremiumSupport-*` 运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持计划](#)。

[运行此自动化（控制台）](#)

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm : DescribeInstanceInformation`
- `ec2: DescribeInstances`
- `ec2: DescribeVolumes`
- `ssm : SendCommand`
- `ssm : ListCommandInvocations`

策略示例：

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

```

    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceInformation",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ssm:SendCommand",
        "ssm:ListCommandInvocations"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - InstanceId (必填)：
 - 说明：(必需) 您的 Amazon EC2 实例的 ID。
 - 类型：String
 - 允许模式：`^i-[0-9a-f]{8,17}$`
 - VolumeExpansionUsageTrigger (必填)：
 - 描述：(必填) 触发扩展所需的分区空间的最小使用量 (百分比)。
 - 类型：String
 - 允许模式：`^[0-9]{1,2}$`
 - VolumeExpansionCapSize (必填)：

- 描述：(必填) Amazon EBS 卷将增加到的最大大小 (以 GiB 为单位)。
 - 类型：String
 - 允许模式：`^[0-9]{1,4}$`
 - VolumeExpansionGibIncrease (必填)：
 - 描述：(必填) 增加音量的 GiB。VolumeExpansionPercentageIncrease将使用VolumeExpansionGibIncrease和之间最大的净增幅。
 - 类型：String
 - 允许模式：`^[0-9]{1,4}$`
 - VolumeExpansionPercentageIncrease (必填)：
 - 描述：(必填) 增加音量的百分比。VolumeExpansionPercentageIncrease将使用VolumeExpansionGibIncrease和之间最大的净增幅。
 - 类型：String
 - 允许模式：`^[0-9]{1,2}$`
4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
- AssertInstanceIsManagedInstance:

检查目标实例是否由 Systems Manager 管理。
 - DescribeInstance:

描述目标 Amazon EC2 实例并检索实例的详细信息Platform，包括、和。RootDeviceType
 - BranchOnPlatform:

在平台类型上进行分支，如果平台与 Windows 不同，则继续执行。
 - DescribeVolumes:

获取 Amazon EC2 实例使用的卷。
 - RunPreChecksOnLinux:

对上一步中收集的卷进行检查。
7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-EnableWindowsEC2SerialConsole

描述

该运行手册AWSSupport-EnableWindowsEC2SerialConsole可帮助您在亚马逊 EC2 Windows 实例上启用亚马逊 EC2 串行控制台、特殊管理控制台 (SAC) 和启动菜单。借助 Amazon Elastic Compute Cloud (Amazon EC2) 串行控制台功能，您可以访问亚马逊 EC2 实例的串行端口，以解决启动、网络配置和其他问题。运行手册自动执行在处于运行状态并由管理的实例以及处于停止状态或未由 AWS Systems Manager管理的实例上启用该功能所需的步骤。AWS Systems Manager

如何工作？

AWSSupport-EnableWindowsEC2SerialConsole自动化运行手册有助于在运行微软 Windows Server 的亚马逊 EC2 实例上启用 SAC 和启动菜单。对于处于运行状态且由管理的实例 AWS Systems Manager，运行手册会运行 R AWS Systems Manager un Command PowerShell 脚本来启用 SAC 和启动菜单。对于处于停止状态或未由管理的实例 AWS Systems Manager，运行手册使用 [AWSSupport-StartEC2 RescueWorkflow](#) 创建临时 Amazon EC2 实例，以离线执行所需的更改。

有关更多信息，请参阅适用于 [Windows 实例的 Amazon EC2 串行控制台](#)。

Important

- 如果您在实例上启用 SAC，则依赖密码检索的 Amazon EC2 服务将无法在 Amazon EC2 控制台上运行。有关更多信息，请参阅[使用 SAC 排查 Windows 实例的问题](#)。
- 要配置对串行控制台的访问权限，您必须在账户级别授予串行控制台访问权限，然后配置 AWS Identity and Access Management (IAM) 策略以向您的用户授予访问权限。您还必须在每个实例上配置基于密码的用户，以使您的用户能够使用串行控制台进行故障排查。有关更多信息，请参阅[配置对 Amazon EC2 串行控制台的访问权限](#)。
- 要查看您的账户是否启用了串行控制台，请参阅[查看串行控制台的账户访问状态](#)。
- 只有在 [Nitro 系统](#)上构建的虚拟化实例才支持串行控制台访问。

有关更多信息，请参阅 Amazon EC2 串行控制台 [先决条件](#)。

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:Describe*",
        "ec2:createTags",
        "ec2:createImage",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetInstanceProfile",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ec2:us-east-1:111122223333:volume/vol-049df61146EXAMPLE",
        "arn:aws:iam:111122223333:instance-profile/instance-profile-name",
        "arn:aws:ssm:us-east-1:111122223333:parameter/aws/service/*",
        "arn:aws:ssm:us-east-1:*:document/AWSSupport-StartEC2RescueWorkflow",
        "arn:aws:ssm:us-east-1:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:us-east-1:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "AWSSupport-EC2Rescue-AutomationExecution",
                "Name"
            ]
        }
    }
},
},

```

```

{
  "Effect": "Allow",
  "Action": [
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStacks",
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:RebootInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ssm:SendCommand"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateLaunchTemplate",
    "ec2>DeleteLaunchTemplate",
    "ec2:RunInstances"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": [

```

```
}
  ]
}
}
}
  "ssm.amazonaws.com",
  "ec2.amazonaws.com"
]
```

说明

按照这些步骤对自动化进行配置：

1. 导航到 AWS Systems Manager 控制台 `AWSSupport-EnableWindowsEC2SerialConsole` 中的。
2. 选择 `Execute automation` (执行自动化) 。
3. 对于输入参数，请输入以下内容：

- `InstanceId`: (必填)

您要启用亚马逊 EC2 串行控制台、(SAC) 和启动菜单的 Amazon EC2 实例的 ID。

- `AutomationAssumeRole`: (可选)

允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `HelperInstanceType`: (视情况而定)

运行手册预配置的 Amazon EC2 实例的类型，用于为离线实例配置 Amazon EC2 串行控制台。

- `HelperInstanceProfileName`: (视情况而定)

帮助程序实例的现有 IAM 实例配置文件的名称。如果您在处于停止状态或不由管理的实例上启用 SAC 和启动菜单 AWS Systems Manager，则这是必需的。如果未指定 IAM 实例配置文件，则自动化会代表您创建一个。

- `SubnetId`: (视情况而定)

帮助程序实例的子网 ID。默认情况下，它使用的子网与提供的实例所在的子网相同。

 Important

如果您提供自定义子网，则该子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 Systems Manager 端点。只有当目标实例处于停止状态或不是由管理时，才需要这样做 AWS Systems Manager。

- CreateInstanceBackupBeforeScriptExecution: (可选)

指定 True 可在启用 SAC 和启动菜单之前创建 Amazon EC2 实例的亚马逊系统映像 (AMI) 备份。Automation 完成后，AMI 仍将存在。您有责任保护对 AMI 的访问权限或将其删除。

- BackupAmazonMachineImagePrefix: (视情况而定)

如果将CreateInstanceBackupBeforeScriptExecution参数设置为，则创建的 Amazon 系统映像 (AMI) 的前缀True。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- CheckIfEc2SerialConsoleAccessEnabled:

检查是否在账户级别启用了 Amazon EC2 串行控制台访问权限。注意：默认情况下，无法访问串行控制台。有关更多信息，请参阅[配置对 Amazon EC2 串行控制台的访问权限](#)。

- CheckIfEc2InstanceIsWindows:

断言目标实例平台是否是 Windows。

- GetInstanceType:

检索目标实例的实例类型。

- CheckIfInstanceTypeIsNitro:

检查实例类型虚拟机管理程序是否基于 Nitro。仅在 Nitro 系统上构建的虚拟化实例支持串行控制台访问。

- CheckIfInstanceIsInAutoScalingGroup:

通过调用 DescribeAutoScalingInstances API 来检查 Amazon EC2 实例是否属于亚马逊 EC2 Auto Scaling 组。如果该实例是 Amazon EC2 Auto Scaling 组的一部分，则它可以确保.NET 实例的移植助手处于待机生命周期状态。

- `WaitForEc2InstanceStateStablized`:

等待实例进入运行或停止状态。

- `GetEc2InstanceState`:

获取实例的当前状态。

- `BranchOnEc2InstanceState`:

基于上一步中检索到的实例状态进行分支。如果该实例状态正在运行，则进入 `CheckIfEc2InstanceIsManagedBySSM` 步骤，如果没有，则进入该 `CheckIfHelperInstanceProfileIsProvided` 步骤。

- `CheckIfEc2 InstanceIsManagedBy SSM` :

检查实例是否由管理 AWS Systems Manager。如果是托管的，则运行手册使用 PowerShell 运行命令启用 SAC 和启动菜单。

- `BranchOnPreEC2RescueBackup`:

基于 `CreateInstanceBackupBeforeScriptExecution` 输入参数进行分支。

- `CreateAmazonMachineImageBackup`:

创建实例的 AMI 备份。

- `启用 SACAndBootMenu` :

通过 PowerShell 运行命令脚本启用 SAC 和启动菜单。

- `RebootInstance`:

重新启动 Amazon EC2 实例以应用配置。如果实例处于联机状态并且由管理，则这是最后一步 AWS Systems Manager。

- `CheckIfHelperInstanceProfileIsProvided`:

在使用临时 Amazon EC2 实例离线启用 SAC 和启动菜单之前，请检查 `HelperInstanceProfileName` 指定的是否存在。

- `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`:

当实例处于停止状态或未由 AWS Systems Manager 管理时，运行启用 SAC 和启动菜单。`AWSSupport-StartEC2RescueWorkflow`

- `GetExecutionDetails`:

检索备份和脱机脚本输出的图像 ID。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- 启用SACAndBootMenu。输出：

EnableSACAndBootMenu步骤中执行命令的输出。

- GetExecutionDetails.OfflineScriptOutput:

RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu步骤中执行的离线脚本的输出。

- GetExecutionDetails.BackupBeforeScriptExecution:

如果CreateInstanceBackupBeforeScriptExecution输入参数为 True，则拍摄的 AMI 备份的映像 ID。

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSPremiumSupport-ExtendVolumesOnWindows

描述

该AWSPremiumSupport-ExtendVolumesOnWindows运行手册在目标亚马逊弹性计算云 (Amazon EC2) 实例上扩展了亚马逊弹性块存储 (Amazon EBS) 卷、其分区和文件系统。

重要注意事项

- 操作影响和交易量状态：Amazon EBS 卷修改分三个阶段进行：modifyingoptimizing、和completed。当卷达到optimizing状态时，这种自动化会继续进行文件系统扩展。在此optimizing状态下，在调整分区大小期间，您可能会遇到暂时的性能影响和潜在的文件系统级中断。您可以[监控 Amazon EBS 卷修改的进度](#)。

- **成本和限制：**增加 Amazon EBS 卷大小将导致每月存储成本增加。有关更多信息，请参阅 [Amazon EBS 定价](#)。本运行手册创建的备份 AMI 和关联快照将根据其大小和您保存的时间长短产生额外费用。对于某些卷类型，如果您需要在扩展后保持相同的每 GB IOPS 比率，则可能需要修改预配置的 IOPS。
- **备份和恢复：**在对卷进行任何更改之前，运行手册会创建备份 AMI。AMI 和关联的快照不会自动从您的账户中删除。如果不再需要这些备份，则应手动删除这些备份。如果出现故障，可以从相关 AMI 的快照中恢复卷，如 [使用快照替换 Amazon EBS 卷](#) 中所述。

如何工作？

此运行手册执行以下操作：

- 验证目标实例是否由 Systems Manager 管理并且正在运行 Windows Server
- 确保只有一次针对当前 Amazon EC2 实例执行此运行手册
- 从目标实例创建备份 Amazon 系统映像 (AMI)
- 扩展指定用于扩展的 Amazon EBS 卷
- 使用命令扩展目标实例上的文件系统 PowerShell

Important

访问 AWS Premium Support - * 运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅 [比较 AWS 支持计划](#)。

[运行此自动化 \(控制台\)](#)

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:CreateImage
- ec2:DescribeImages
- ec2:DescribeVolumes
- ec2:ModifyVolume

- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:DescribeInstanceInformation`

示例 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:CreateImage",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolume",
        "ssm:SendCommand",
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSPremiumSupport-ExtendVolumesOnWindows](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 类型 : AWS::IAM::Role::Arn
- InstanceId (必填) :
 - 说明 : (必需) Amazon EC2 实例的 ID。
 - 类型 : String
 - 允许模式 : ^i-[0-9a-f]{8,17}\$
- VolumeExpansionCapSize (必填) :
 - 描述 : (必填) Amazon EBS 卷将增加的最大大小 (以 GiB 为单位)。
 - 类型 : String
 - 允许模式 : ^[0-9]{1,4}\$
- DiagnosticResults (必填) :
 - 描述 : (必填) DiagnoseDiskUsage 文档中预检脚本的结果，格式为单行 CSV。字符串以开头，EXTEND; 后面是每个卷的以逗号分隔的卷信息，卷之间用分号分隔。每个卷的信息包括：卷 ID、驱动器号、扩展标志 (1 表示扩展，0 表示跳过)、以 GB 为单位的新大小、AWS 区域和原因/操作。
 - 类型 : String
 - 允许模式 : ^EXTEND;[0-9a-zA-Z\\.\;_:\-\/,\\s]{7,5400}\$

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- AssertInstanceIsManagedInstance:

验证目标实例是否由 Systems Manager 管理。

- DescribeInstance:

检索目标 Amazon EC2 实例的平台信息。

- BranchOnPlatform:

确认目标 Amazon EC2 实例平台是 Windows 服务器。

- CheckConcurrency:

确保只有一次针对当前 Amazon EC2 实例执行此运行手册。

- CreateImage:

- WaitUntillImageReady:

等待 Amazon 系统映像 (AMI) 完成创建并进入available状态。

- 扩展 EBSVolume :

扩展指定用于扩展的目标实例的 Amazon EBS 卷。

- DescribeVolumes:

描述指定用于扩展的目标实例的 Amazon EBS 卷。

- ExtendFilesystem:

使用 PowerShell 命令扩展目标实例的文件系统。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)
- [请求修改 Amazon EBS 交易量](#)

AWSsupport-ExecuteEC2Rescue

描述

本运行手册使用 EC2Rescue 工具，用于对指定的 Linux 版亚马逊弹性计算云 (Amazon EC2) 实例进行故障排除并在可能的情况下修复常见的连接问题或 Windows Server。 不支持带有加密根卷的实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EC2RescueInstanceType

类型：字符串

有效值：t2.small | t2.medium | t2.large

默认值：t2.small

描述：(必填) 的 EC2 实例类型 EC2Rescue 实例。推荐大小：t2.small

- LogDestination

类型：字符串

描述：(可选) 您账户中用于上传故障排除日志的 Amazon S3 存储桶的名称。请确存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

类型：字符串

默认：CreateNewVPC

描述：(可选) 的子网 ID EC2Rescue 实例。默认情况下，AWS Systems Manager 自动化会创建一个新的 VPC。或者，您也可以使用 SelectedInstanceSubnet 来使用与您的实例相同的子网，或指定一个自定义的子网 ID。

⚠ Important

子网必须与 `UnreachableInstanceId` 位于同一可用区中，并且必须允许访问 SSM 端点。

- `UnreachableInstanceId`

类型：字符串

描述：(必填) 您无法访问的 EC2 实例的 ID。

⚠ Important

Systems Manager Automation 会停止此实例，并在尝试任何操作前创建一个 AMI。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP 地址，则公有 IP 地址将发生更改。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

您必须至少拥有 `ssm:StartAutomationExecution` 和 `ssm:GetAutomationExecution` 才能读取自动化输出。有关所需权限的更多信息，请参阅 [AWSSupport-StartEC2RescueWorkflow](#)。

文档步骤

1. `aws:assertAwsResourceProperty`-断言提供的实例是否为 Windows Server:
 - a. (EC2Rescue for Windows Server) 如果提供的实例是 Windows Server 实例：
 - i. `aws:executeAutomation`-使用救援 `AWSSupport-StartEC2RescueWorkflow` 调用 EC2 Windows Server 离线脚本。
 - ii. `aws:executeAwsApi` - 从嵌套的 Automation 检索备份 AMI ID。
 - iii. `aws:executeAwsApi`-从嵌套自动化中检索 EC2 救援摘要。
 - b. (EC2Rescue 对于 Linux) 如果提供的实例是 Linux 实例：
 - i. `aws:executeAutomation`-`AWSSupport-StartEC2RescueWorkflow` 使用 Rescue for Linux EC2 离线脚本调用
 - ii. `aws:executeAwsApi` - 从嵌套的 Automation 检索备份 AMI ID。
 - iii. `aws:executeAwsApi`-从嵌套自动化中检索 EC2 救援摘要。

输出

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSsupport-ListEC2Resources

描述

AWSsupport-ListEC2Resources运行手册返回有关您指定的亚马逊 EC2 实例和相关资源的信息，例如亚马逊弹性块存储 (Amazon EBS) 卷、弹性 IP 地址和亚马逊 A EC2 uto Scaling 组。AWS 区域 默认情况下，信息从所有区域收集，并在在自动化的输出中显示。或者，您可以指定要将信息以逗号分隔值 (.csv) 文件形式上传到的 Amazon Simple Storage Service (Amazon S3) 存储桶。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(可选) 要将所收集的信息上传到的 S3 存储桶的名称。

- `DisplayResourceDeletionDocumentation`

类型：字符串

默认：True

描述：(可选) 如果设置为 true，此自动化会在输出中创建指向与删除资源相关的文档的链接。

- `RegionsToQuery`

类型：字符串

默认：全部

描述：(可选) 您要从中收集亚马逊 EC2 相关信息的地区。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

此外，要成功将收集到的信息上传到您指定的 S3 存储桶，`AutomationAssumeRole` 需要执行以下操作：

- `s3:GetBucketAcl`

- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

文档步骤

- `aws:executeAwsApi` - 收集为该账户启用的区域。
- `aws:executeScript` - 确认为账户启用的区域支持 `RegionsToQuery` 参数中指定的区域。
- `aws:branch` - 如果未对账户启用任何区域，自动化将结束。
- `aws:executeScript` - 列出您指定的账户和区域的所有 EC2 实例。
- `aws:executeScript` - 列出您指定的账户和区域的所有亚马逊机器映像 (AMI)。
- `aws:executeScript` - 列出您指定的账户和区域的所有 EBS 卷。
- `aws:executeScript` - 列出您指定的账户和区域的所有弹性 IP 地址。
- `aws:executeScript` - 列出您指定的账户和区域的所有弹性网络接口。
- `aws:executeScript` - 列出您指定的账户和区域的所有自动扩缩组。
- `aws:executeScript` - 列出您指定的账户和区域的所有负载均衡器。
- `aws:executeScript` - 在您为 `Bucket` 参数提供值时将收集到的信息上传到指定的 S3 存储桶。

AWSsupport-ManageRDPSettings

描述

AWSsupport-ManageRDPSettings 运行手册能够让用户管理常见的远程桌面协议 (RDP) 设置，例如 RDP 端口和网络层身份验证 (NLA)。默认情况下，此运行手册读取和输出这些设置的值。

Important

在运行此运行手册前，应仔细检查对 RDP 设置的更改。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) 要管理其 RDP 设置的托管实例的 ID。

- NLASetting 操作

类型：字符串

有效值：Check | 启用 | 禁用

默认值：Check

说明：(必需) 要对 NLA 设置执行的操作：Check、Enable、Disable。

- RDPPort

类型：字符串

默认值：3389

说明：(可选) 指定新的 RDP 端口。仅在操作设置为 Modify 时使用。端口号必须介于 1025-65535 之间。注意：更改端口后，将重启 RDP 服务。

- RDPPort 操作

类型：字符串

有效值：Check | 修改

默认值：Check

说明：(必需) 要应用于 RDP 端口的操作。

- RemoteConnections

类型：字符串

有效值：Check | 启用 | 禁用

默认值：Check

描述：(必需) 要对 fDeny TSConnections 设置执行的操作。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

接收命令的 EC2 实例必须具有 IAM 角色并附有 Amazon A SSManagedInstanceCoreamazon 托管策略。用户必须至少有 ssm: 才能将命令发送SendCommand到实例，还必须有 ssm: GetCommandInvocation 才能读取命令输出。

文档步骤

aws:runCommand-运行 PowerShell 脚本以更改或检查目标实例上的 RDP 设置。

输出

管理 RDPSettings .Output

AWSSupport-ManageWindowsService

描述

AWSSupport-ManageWindowsService 运行手册允许您在目标实例上停止、启动、重启、暂停或禁用任何 Windows 服务。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要管理其服务的托管实例的 ID。

- ServiceAction

类型：字符串

有效值：Check | 重启 | 强制重启 | 启动 | 停止 | 前置停止 | 暂停

默认值：Check

描述：(必填) 要应用于 Windows 服务的操作。注意：Force-Restart 和 Force-Stop 可用于重启和停止具有从属服务的服务。

- StartupType

类型：字符串

有效值：选中 | 自动 | 需求 | 已禁用 | DelayedAutoStart

默认值：Check

描述：(必填) 要应用于 Windows 服务的启动类型。

- WindowsServiceName

类型：字符串

描述：(必需) 有效的 Windows 服务名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议接收命令的 EC2 实例具有 IAM 角色并附有 Amazon A SSManagedInstanceCoreamazon 托管策略。用户必须至少有 ssm: StartAutomationExecution 和 ssm: SendCommand 才能运行自动化并将命令发送到实例，还必须有 ssm: GetAutomationExecution 才能读取自动化输出。

文档步骤

aws:runCommand-运行 PowerShell 脚本将所需的配置应用于目标实例上的 Windows 服务。

输出

manageWindowsService。输出

AWSSupport-MigrateEC2ClassicToVPC

描述

AWSSupport-MigrateEC2ClassicToVPC运行手册将亚马逊弹性计算云 (Amazon EC2) 实例从 EC2-Classic 迁移到虚拟私有云 (VPC)。本运行手册支持使用亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 根卷迁移硬件虚拟机 (HVM) 虚拟化类型的亚马逊 EC2 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- ApproverIAM

类型：StringList

描述：(可选) 可以批准或拒绝操作的 IAM 用户的 Amazon 资源名称 (ARNs)。如果您为 MigrationType 参数指定 CutOver 值，则此参数才应用。

- DestinationSecurityGroupId

类型：StringList

描述：(可选) 您要与在您的 VPC 中启动的 Amazon EC2 实例关联的安全组的 ID。如果您未为此参数指定值，则自动化会在您的 VPC 中创建一个安全组，并从 EC2-Classic 中的安全组中复制规则。如果无法将规则复制到新的安全组，则您的 VPC 的默认安全组将与 Amazon EC2 实例关联。

- DestinationSubnetId

类型：字符串

描述：(可选) 您要将 Amazon EC2 实例迁移到的子网的 ID。如果您没有为此参数指定一个值，则自动化将从 VPC 中随机选择一个子网。

- InstanceId

类型：字符串

描述：(必填) 您要迁移的 Amazon EC2 实例的 ID。

- MigrationType

类型：字符串

有效值：CutOver | 测试

描述：(必需) 要执行的迁移的类型。

该CutOver选项需要获得批准才能停止在 EC2-Classic中运行的Amazon EC2 实例。此操作获得批准
后，Amazon EC2 实例将停止，并且自动化会创建一个 Amazon Machine Image (AMI)。当 AMI

状态为 `available`，从此启动了一个新的 Amazon EC2 实例 AMI 在 `DestinationSubnetId` 您的 VPC 中指定的中。如果您在 EC2-Classic 中运行的 Amazon EC2 实例附加了弹性 IP 地址，则该实例将被移至您的 VPC 中新创建的亚马逊 EC2 实例。如果在您的 VPC 中启动的 Amazon EC2 实例由于任何原因未能创建，则该 EC2 实例将被终止并请求批准以 EC2-Classic 启动您的亚马逊实例。

该 `Test` 选项创建了一个 AMI 您的 Amazon EC2 实例，该实例在 EC2-Classic 中运行，无需重启。由于 Amazon EC2 实例不会重启，因此我们无法保证所创建映像的文件系统的完整性。当 AMI 状态为 `available`，从此启动了一个新的 Amazon EC2 实例 AMI 在您 `DestinationSubnetId` 的 VPC 中指定的中。如果您在 EC2-Classic 中运行的 Amazon EC2 实例附加了弹性 IP 地址，则自动化会验证 `DestinationSubnetId` 您指定的地址是否公开。如果在您的 VPC 中启动的 Amazon EC2 实例由于任何原因未能创建，则该实例将被终止并终止自动运行。

- `SNSNotificationARNfor批准`

类型：字符串

描述：(必需) 要向其发送批准通知的 Amazon Simple Notification Service (Amazon SNS) 主题的 ARN。如果您为 `MigrationType` 参数指定 `CutOver` 值，则此参数才应用。

- `TargetInstanceType`

类型：字符串

默认：t2.2xlarge

描述：(可选) 您要在您的 VPC 中启动的 Amazon EC2 实例的类型。仅支持基于 Xen 的实例类型，例如 T2、M4 或 C4。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetDocument`
- `ssm:ListDocumentVersions`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:ListSubscriptions`
- `sns:ListTopics`

- `sns:Publish`
- `ec2:AssociateAddress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateImage`
- `ec2:CreateSecurityGroup`
- `ec2>DeleteSecurityGroup`
- `ec2:MoveAddressToVpc`
- `ec2:RunInstances`
- `ec2:StopInstances`
- `ec2:CreateTags`
- `ec2:DescribeAddresses`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceState`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroupReferences`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTags`
- `ec2:DescribeVpcs`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`

文档步骤

- `aws:executeAwsApi`-收集您在`InstanceId`参数中指定的 Amazon EC2 实例的详细信息。
- `aws:assertAwsResourceProperty` - 确认您在 `TargetInstanceType` 参数中指定的实例类型是基于 XEN。
- `aws:assertAwsResourceProperty`-确认您在`InstanceId`参数中指定的 Amazon EC2 实例属于 HVM 虚拟化类型。

- `aws:assertAwsResourceProperty`-确认您在`InstanceId`参数中指定的亚马逊 EC2 实例具有 Amazon EBS 根卷。
- `aws:executeScript` - 根据您为 `DestinationSecurityGroupId` 参数指定的值视需要创建一个安全组。
- `aws:branch` - 根据您在 `DestinationSubnetId` 参数中指定的值进行分支。
- `aws:executeAwsApi` - 标识您运行此自动化所在 AWS 区域 的默认 VPC。
- `aws:executeAwsApi` - 随机选择位于默认 VPC 中的子网的 ID。
- `aws:createImage`-创建一个 AMI 无需重新启动 Amazon EC2 实例。
- `aws:branch` - 根据您为 `MigrationType` 参数指定的值进行分支。
- `aws:branch` - 根据您为 `DestinationSubnetId` 参数指定的值进行分支。
- `aws:runInstances`-从启动新实例 AMI 在 EC2-Classic 中启动 Amazon EC2 实例即可创建。
- `aws:changeInstanceState`-如果上一步由于任何原因失败，则终止新启动的 Amazon EC2 实例。
- `aws:runInstances`-从启动新实例 AMI 创建时无需在 EC2-Classic 中重启亚马逊 EC2 实例 (如果提供)。 `DestinationSubnetId`
- `aws:changeInstanceState`-如果上一步由于任何原因失败，则终止新启动的 Amazon EC2 实例。
- `aws:assertAwsResourceProperty`-确认在 EC2-Classic 中运行的 Amazon EC2 实例的停止行为。
- `aws:approve`-等待批准才能停止 Amazon EC2 实例。
- `aws:changeInstanceState`-停止在 EC2-Classic 中运行的 Amazon EC2 实例。
- `aws:changeInstanceState`-如果需要，强制停止在 EC2-Classic 中运行的 Amazon EC2 实例。
- `aws:createImage`-创建一个 AMI Amazon EC2 实例停止后的数据。
- `aws:branch` - 根据为 `DestinationSubnetId` 参数指定的值进行分支。
- `aws:runInstances`-从启动新实例 AMI 在 EC2-Classic 中由已停止的 Amazon EC2 实例创建。
- `aws:approve`-如果上一步由于任何原因失败，则等待批准终止新启动的 Amazon EC2 实例，并在 EC2-Classic 中启动 Amazon 实例。
- `aws:changeInstanceState`-终止新启动的 Amazon EC2 实例。
- `aws:runInstances`-从启动新实例 AMI 由 `DestinationSubnetId` 参数中的 EC2-Classic 中已停止的 Amazon EC2 实例创建。
- `aws:approve`-如果上一步由于任何原因失败，则等待批准终止新启动的 Amazon EC2 实例，并在 EC2-Classic 中启动 Amazon 实例。

- `aws:changeInstanceState`-终止新启动的 Amazon EC2 实例。
- `aws:changeInstanceState`-启动在-C EC2 classic 中停止的 Amazon EC2 实例。
- `aws:branch`-基于 Amazon EC2 实例是否具有公有 IP 地址进行分支。
- `aws:executeAwsApi` - 验证公有 IP 地址是否为弹性 IP 地址。
- `aws:branch` - 根据您在 `MigrationType` 参数中指定的值进行分支。
- `aws:executeAwsApi` - 将弹性 IP 地址移至您的 VPC。
- `aws:executeAwsApi` - 收集已移至 VPC 的弹性 IP 地址的分配 ID。
- `aws:branch`-分支基于在您的 VPC 中运行的 Amazon EC2 实例启动的子网。
- `aws:executeAwsApi` - 将弹性 IP 地址附加到 VPC 中新启动的实例。
- `aws:executeScript`-确认您在您的 VPC 中运行的新启动的 Amazon EC2 实例的子网是公有的。

输出

`getInstanceProperties.virtualizationType`-在-C EC2 classic 中运行的 Amazon EC2 实例的虚拟化类型。

`getInstanceProperties.rootDeviceType`-在-C EC2 classic 中运行的 Amazon EC2 实例的根设备类型。

`createAMIWithoutReboot.ImageId`-的身份证 AMI 创建时无需重启在-Classic 中 EC2 运行的 Amazon EC2 实例。

`getDefaultVPC.VpcId`-如果未提供 `DestinationSubnetId` 参数值，则为启动新 Amazon EC2 实例的默认 VPC 的 ID。

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`-如果未提供 `DestinationSubnetId` 参数值，则在默认 VPC 中启动新 Amazon EC2 实例的子网的 ID。

`launchTestInstanceDefaultVPC.InstanceIds-Test` 迁移类型期间在您的默认 VPC 中新启动的 Amazon EC2 实例的 ID。

`launchTestInstanceProvidedSubnet.InstanceIds`-您在 `Test` 迁移类型期间指定的新启动 `DestinationSubnetId` 的 Amazon EC2 实例的 ID。

`createAMIAfterStoppingInstance.ImageId`-的身份证 AMI 在停止在 EC2-Classic 中运行的 Amazon EC2 实例之后创建。

`launchCutOverInstanceProvidedSubnet.InstanceIds`-您在CutOver迁移类型期间指定的新启动DestinationSubnetId的 Amazon EC2 实例的 ID。

`launchCutOverInstanceDefaultVPC.InstanceIds`-CutOver 迁移类型期间在您的默认 VPC 中新启动的 Amazon EC2 实例的 ID。

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic` - 在默认 VPC 中由自动化选择的子网是否为公有子网。

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic` - 您在 DestinationSubnetId 中指定的子网是否为公有子网。

AWSsupport-MigrateXenToNitroLinux

描述

AWSsupport-MigrateXenToNitroLinux运行手册将亚马逊弹性计算云 (Amazon EC2) Linux Xen 实例克隆、准备和迁移到 [Nitro 实例类型](#)。此运行手册为操作类型提供了两个选项：

- **Clone&Migrate**— 此选项的工作流程包括初步检查、测试和 Clone&Migrate阶段。工作流程使用 AWSsupport-CloneXenEC2InstanceAndMigrateToNitro 运行手册运行。
- **FullMigration** – 此选项运行 Clone&Migrate 工作流程，然后执行 替换 Amazon EBS 根卷的额外步骤。

Important

使用此运行手册会给您的账户带来亚马逊 EC2实例的运行时间、亚马逊弹性区块存储 (Amazon EBS) 存储卷的创建以及 AMIs。有关更多详情，请参阅[亚马逊 EC2 定价](#)和[亚马逊 EBS 定价](#)。

初步检查

在继续迁移之前，自动化会执行以下初步检查。如果任何检查失败，自动化将结束。此阶段只是 Clone&Migrate 工作流程的一部分。

- 检查目标实例是否已经是 Nitro 实例类型。
- 检查竞价型实例购买选项是否用于目标实例。
- 检查实例存储卷是否附加到目标实例。

- 验证目标实例操作系统 (OS) 是否为 Linux。
- 检查目标实例是否是 Amazon A EC2 uto Scaling 组的一部分。如果它是自动扩缩组的一部分，自动化操作将验证该实例是否处于 standby 状态。
- 验证实例是否由管理。AWS Systems Manager

测试

自动化会创建一个 Amazon Machine Image (AMI) 从目标实例启动测试实例，并从新创建的实例启动测试实例 AMI。此阶段只是工作Clone&Migrate流程的一部分。

如果测试实例通过了所有状态检查，则自动化将暂停，并通过 Amazon Simple Notification Service (Amazon SNS) 通知请求指定委托人批准。如果提供了批准，则自动化会终止测试实例，停止目标实例，并继续迁移，同时新创建的 AMI 在Clone&Migrate工作流程结束时取消注册。

Note

在提供批准之前，我们建议您确认目标实例上运行的所有应用程序均已正常关闭。

克隆和迁移

自动化创造了另一个 AMI 从目标实例，然后启动一个新实例以更改为 Nitro 实例类型。在继续迁移之前，自动化会完成以下先决条件。如果任何检查失败，自动化将结束。此阶段也只是 Clone&Migrate 工作流程的一部分。

- 开启增强联网 (ENA) 属性。
- 安装最新版本的 ENA 驱动程序（如果尚未安装），或者将 ENA 驱动程序版本更新至最新版本。为确保最佳网络性能，如果出现以下情况，则需要更新到最新的 ENA 驱动程序版本 Nitro 实例类型是第 6 代。
- 验证 NVMe 模块是否已安装。如果模块安装完毕，自动化将验证该模块是否加载到 initramfs 中。
- 使用区块设备名称（ /dev/sd*或/dev/xvd* ）分析/etc/fstab条目并将其替换为相应的条目 UUIDs。在修改配置之前，自动化会在路径 /etc/fstab* 上创建文件的备份。
- 关闭可预测的接口命名，方法是将 net.ifnames=0 选项添加到 /etc/default/grub 文件（如果存在）中的 GRUB_CMDLINE_LINUX 行，或添加到 /boot/grub/menu.lst 中的内核。
- 如果 /etc/udev/rules.d/70-persistent-net.rules 文件存在，则将其移除。在移除文件之前，自动化会在路径 /etc/udev/rules.d/ 上创建文件的备份。

验证所有要求后，实例类型更改为 Nitro 您指定的实例类型。自动化会等待新创建的实例在启动后通过所有状态检查 Nitro 实例类型。然后，自动化会等待指定负责人的批准后再创建 AMI 成功推出的 Nitro 实例。如果批准被拒绝，自动化将结束，从而让新创建的实例保持运行状态，目标实例将保持停止状态。

替换根 Amazon EBS 卷

如果您选择 FullMigration 作为 OperationType，则自动化会将目标 Amazon EC2 实例迁移到 Nitro 您指定的实例类型。Automation 会请求指定委托人的批准，以将目标 Amazon EC2 实例的 Amazon EBS 根卷替换为克隆的 EC2 亚马逊实例的根卷。成功迁移后，克隆的 Amazon EC2 实例将终止。如果自动化失败，则原始的 Amazon EBS 根卷将附加到目标亚马逊 EC2 实例。如果连接到目标 Amazon EC2 实例的 Amazon EBS 根卷具有应用 aws: 前缀的标签，则不支持该 FullMigration 操作。

开始之前

目标实例必须具有出站互联网访问权限。这是为了访问驱动程序和依赖项的存储库，比如 kernel-devel, gcc, patch, rpm-build, wget, dracut, make, linux-headers，以及 unzip。如果需要，可以使用 Package 管理器。

需要使用 Amazon SNS 主题才能发送批准和更新的通知。有关如何创建 Amazon SNS 主题的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 [创建 Amazon SNS 主题](#)。

此运行手册支持以下操作系统：

- RHEL 7.x-8.5
- Amazon Linux (2018.03)、Amazon Linux 2
- Debian 服务器
- Ubuntu Server 18.04 LTS、20.04 LTS 和 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 确认

类型：字符串

描述：(必需) 阅读此自动化运行手册所执行操作的完整详细信息，然后输入 **Yes, I understand and acknowledge** 以继续使用运行手册。

- ApproverIAM

类型：字符串

描述：(必填) 可以批准自动化的 IAM 角色、用户或用户名。ARNs 您可以指定最多 10 个批准者。

- DeleteResourcesOnFailure

类型：布尔值

描述：(可选) 确定新创建的实例是否和 AMI 因为如果自动化失败，则会删除迁移。

有效值：True | False

默认值：True

- MinimumRequiredApprovals

类型：字符串

描述：(可选) 在请求批准时继续运行自动化所需的最低批准数。

有效值：1-10

默认值：1

- NitroInstanceType

类型：字符串

描述：(必填) Nitro 您要将实例更改为的实例类型。支持的实例类型包括 M5、M6、C5、C6、R5、R6 和 T3。

默认：m5.xlarge

- OperationType

类型：字符串

描述：(必需) 希望执行的操作。FullMigration 选项执行的任务与 Clone&Migrate 的相同，还会替换目标实例的根卷。迁移过程结束后，目标实例的根卷将替换为来自新创建实例的根卷。FullMigration 操作不支持逻辑卷管理器 (LVM) 定义的根卷。

有效值：克隆并迁移 | FullMigration

- SNSTopicArn

类型：字符串

说明：(必需) 用于批准通知的 Amazon SNS 主题的 ARN。Amazon SNS 主题用于在自动化期间发送所需的批准通知。

- TargetInstanceId

类型：字符串

描述：(必填) 要迁移的 Amazon EC2 实例的 ID。

Clone&Migrate 工作流

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation

- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`
- `ec2:CreateImage`
- `ec2:RunInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DeregisterImage`
- `ec2>DeleteSnapshot`
- `ec2:TerminateInstances`
- `ec2:StartInstances`
- `ec2:DescribeKeyPairs`
- `ec2:StopInstances`
- `kms:CreateGrant*`
- `kms:ReEncrypt`
- `ec2:ModifyInstanceAttribute`
- `autoscaling:DescribeAutoScalingInstances`
- `iam:passRole`
- `iam:ListRoles`

文档步骤

- `startOfPreliminaryChecksBranch` - 分支到初步检查工作流程。
- `getTargetInstanceProperties` - 从目标实例收集详细信息。
- `checkIfNitroInstanceTypeIsSupportedInAZ` - 确定目标的 Amazon EC2 实例类型是否在与目标实例相同的可用区中受支持。

- `getXenInstanceTypeDetails` - 收集有关源实例类型的详细信息。
- `checkIfInstanceHypervisorIsNitroAlready` - 检查目标实例是否已作为一个实例运行 Nitro 实例类型。
- `checkIfTargetInstanceLifecycleIsSpot` - 检查目标实例的购买选项是否为 Spot。
- `checkIfOperatingSystemIsLinux` - 检查目标实例操作系统是否为 Linux。
- `verifySSMConnectivityForTargetInstance` - 验证目标实例是否由 Systems Manager 管理。
- `checkIfEphemeralVolumeAreSupported` - 检查目标实例的当前实例类型是否支持实例存储卷。
- `verifyIfTargetInstanceHasEphemeralVolumesAttached` - 检查目标实例是否包含附加的实例存储卷。
- `checkIfRootVolumeIsEBS` - 检查目标实例的根卷类型是否为 EBS。
- `checkIfTargetInstanceIsInASG` - 检查目标实例是否是自动扩缩组的一部分。
- `endOfPreliminaryChecksBranch` - 初步检查分支结束。
- `startOfTestBranch` - 分支到测试工作流程。
- `createTestImage` - 创建测试 AMI 目标实例的。
- `launchTestInstanceInSameSubnet` - 从测试中启动测试实例 AMI 使用与目标实例相同的配置。
- `cleanupTestInstance` - 终止测试实例。
- `endOfTestBranch` - 测试分支结束。
- `checkIfTestingBranchSucceeded` - 检查测试分支的状态。
- `approvalToStopTargetInstance` - 等待指定委托人的批准才能停止目标实例。
- `stopTargetEC2Instance` - 停止目标实例。
- `forceStopTargetEC2Instance` - 只有在上一步未能停止目标实例时才强制停止该实例。
- `startOfCloneAndMigrateBranch` - 分支到 Clone&Migrate 工作流程。
- `createBackupImage` - 创建一个 AMI 要用作备份的目标实例。
- `launchInstanceInSameSubnet` - 从备份中启动新实例 AMI 使用与源实例相同的配置。
- `waitForClonedInstanceToPassStatusChecks` - 等待新创建的实例通过所有状态检查。
- `verifySSMConnectivityForClonedInstance` - 验证新创建的实例是否由 Systems Manager 管理。
- `checkAndInstallENADrivers` - 检查新创建的实例上是否安装了 ENA 驱动程序，并在需要时安装驱动程序。

- `checkAndAddNVMeDrivers`-检查新创建的实例上是否安装了 NVMe 驱动程序，并在需要时安装驱动程序。
- `checkAndModifyFSTABEntries`-检查中是否使用了设备名称，`/etc/fstab`并在需要时将其替 UUIDs 换为。
- `stopClonedInstance` - 停止新创建的实例。
- `forceStopClonedInstance` - 只有在上一步未能停止实例时才强制停止新创建的实例。
- `checkENAAtributeForClonedInstance` - 检查是否为新创建的实例启用了增强联网属性。
- `setNitroInstanceTypeForClonedInstance`-将新创建的实例的实例类型更改为 Nitro 您指定的实例类型。
- `startClonedInstance` - 启动您已更改其实例类型的新创建实例。
- `approvalForCreatingImageAfterDriversInstallation`-如果实例成功启动为 Nitro 实例类型，自动化将等待所需委托人的批准。如果提供了批准，AMI 是为了用作金牌而创建的 AMI。
- `createImageAfterDriversInstallation`-创建一个 AMI 可用作金牌 AMI。
- `endOfCloneAndMigrateBranch`-结束 Clone&Migrate 分支。
- `cleanupTestImage`-注销 AMI 为测试而创建。
- `failureHandling` - 检查您是否选择在出现故障时终止资源。
- `onFailureTerminateClonedInstance` - 在自动化失败时终止新创建的实例。
- `onFailurecleanupTestImage`-注销 AMI 为测试而创建。
- `onFailureApprovalToStartTargetInstance` - 在自动化失败时等待指定主体的批准以启动目标实例。
- `onFailureStartTargetInstance` - 在自动化失败时启动目标实例。

FullMigration 工作流

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`
- `ssm:GetAutomationExecution`

- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`
- `ec2:CreateImage`
- `ec2:RunInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DeregisterImage`
- `ec2>DeleteSnapshot`
- `ec2:TerminateInstances`
- `ec2:StartInstances`
- `ec2:DescribeKeyPairs`
- `ec2:StopInstances`
- `kms:CreateGrant*`
- `kms:ReEncrypt`
- `ec2:ModifyInstanceAttribute`
- `ec2:DetachVolume`
- `ec2:AttachVolume`
- `ec2:DescribeVolumes`
- `autoscaling:DescribeAutoScalingInstances`
- `iam:PassRole`
- `ec2:CreateTags`
- `cloudformation:DescribeStackResources`

文档步骤

FullMigration 工作流程运行的步骤与 Clone&Migrate 工作流程运行的相同，另外还执行以下步骤：

- `checkConcurrency`-验证此运行手册中是否只有一个针对您指定的 Amazon EC2 实例的自动化。如果运行手册发现另一个针对同一实例的自动化正在进行，自动化将结束。
- `getTargetInstanceProperties` - 从目标实例收集详细信息。
- `checkRootVolumeTags`-确定目标 Amazon EC2 实例的根卷是否包含任何 AWS 预留标签。
- `cloneTargetInstanceAndMigrateToNitro` - 使用 `AWS-CloneXenInstanceToNitro` 运行手册启动儿童自动化。
- `branchOnTheOperationType` - 根据您为 `OperationType` 参数指定的值进行分支。
- `getClonedInstanceId` - 从子自动化中检索新启动的实例的 ID。
- `checkIfRootVolumeIsBasedOnLVM` - 确定根分区是否由 LVM 管理。
- `branchOnTheRootVolumeLVMStatus` - 如果从主体收到了要求的最低限度批准，自动化将继续执行根卷替换。
- `manualInstructionsInCaseOfLVM` - 如果根卷由 LVM 管理，自动化将发送包含如何手动替换根卷说明的输出。
- `startOfReplaceRootEBSVolumeBranch` - 启动“替换根 EBS 卷”分支工作流。
- `checkIfTargetInstanceIsManagedByCFN`-确定目标实例是否由 AWS CloudFormation 堆栈管理。
- `branchOnCFNStackStatus`-基于 CloudFormation 堆栈状态的分支。
- `approvalForRootVolumesReplacement(WithCFN)`-如果目标实例是由启动的 CloudFormation，则在新启动的实例成功启动后，自动化将等待批准 Nitro 实例类型。获得批准后，目标实例的 Amazon EBS 卷将替换为新启动实例的根卷。
- `approvalForRootVolumesReplacement`-在新启动的实例成功启动后等待批准 Nitro 实例类型。获得批准后，目标实例的 Amazon EBS 卷将替换为新启动实例的根卷。
- `assertIfTargetEC2InstanceIsStillStopped` - 在更换根卷之前，验证目标实例是否处于 `stopped` 状态。
- `stopTargetInstanceForRootVolumeReplacement` - 如果目标实例正在运行，则自动化会在替换根卷之前停止该实例。
- `forceStopTargetInstanceForRootVolumeReplacement` - 在上一步失败时强制停止目标实例。
- `stopClonedInstanceForRootVolumeReplacement` - 停止新创建的实例后再替换 Amazon EBS 卷。
- `forceStopClonedInstanceForRootVolumeReplacement` - 在上一步失败时强制停止新创建的实例。

- `getBlockDeviceMappings` - 检索目标实例和新创建实例的块设备映射。
- `replaceRootEbsVolumes` - 将目标实例的根卷替换为新创建实例的根卷。
- `EndOfReplaceRootEBSVolumeBranch` - 结束“替换根 EBS 卷”分支工作流。
- `checkENAAttributeForTargetInstance`-检查目标 Amazon EC2 实例的增强联网 (ENA) 属性是否已开启。
- `enableENAAttributeForTargetInstance`-如果需要，可为目标 Amazon EC2 实例开启 ENA 属性。
- `setNitroInstanceTypeForTargetInstance`-将目标实例更改为 Nitro 您指定的实例类型。
- `replicateRootVolumeTags`-从目标亚马逊实例复制根 Amazon EBS 卷上的标签。EC2
- `startTargetInstance`-更改 EC2 实例类型后启动目标 Amazon 实例。
- `onFailureStopTargetEC2Instance`-如果目标 Amazon EC2 实例启动失败，则将其停止 Nitro 实例类型。
- `onFailureForceStopTargetEC2Instance`-如果上一步失败，则强制停止目标 Amazon EC2 实例。
- `OnFailureRevertOriginalInstanceType`-如果目标 EC2实例启动失败，则将目标 Amazon 实例恢复为原始实例类型 Nitro 实例类型。
- `onFailureRollbackRootVolumeReplacement` - 必要时还原 `replaceRootEbsVolumes` 步骤所做的所有更改。
- `onFailureApprovalToStartTargetInstance`-在回退之前的更改后，等待指定委托人的批准才能启动目标 Amazon EC2 实例。
- `onFailureStartTargetInstance`-启动目标 Amazon EC2 实例。
- `terminateClonedEC2Instance`-更换根 Amazon EBS 卷后，终止克隆的 Amazon EC2 实例。

AWSsupport-ResetAccess

描述

本运行手册将在指定 EC2 实例上使用 EC2救援工具使用 EC2 控制台 (Windows) 重新启用密码解密，或者生成和添加新的 SSH 密钥对 (Linux)。如果您丢失了密钥对，此自动化将创建一个启用密码的 AMI，您可以使用该AMI启动带有您拥有的密钥对 EC2 的新实例 (Windows)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EC2RescueInstanceType

类型：字符串

有效值：t2.small | t2.medium | t2.large

默认值：t2.small

描述：(必填) EC2救援 EC2 实例的实例类型。建议大小：t2.small。

- InstanceId

类型：字符串

描述：(必填) 您要重置访问权限的 EC2 实例的 ID。

 Important

Systems Manager Automation 会停止此实例，并在尝试任何操作前创建一个 AMI。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- SubnetId

类型：字符串

默认：CreateNewVPC

描述：（可选）EC2救援实例的子网 ID。默认情况下，Systems Manager Automation 会创建一个新 VPC。或者，SelectedInstanceSubnet 使用与您的实例使用相同的子网，或者指定自定义子网 ID。

 Important

子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

您必须至少具有 ssm: StartAutomationExecution、ssm: GetParameter（用于检索 SSH 密钥参数名称）和 ssm: GetAutomationExecution 才能读取自动化输出。有关所需权限的更多信息，请参阅 [AWSSupport-StartEC2RescueWorkflow](#)。

文档步骤

1. aws:assertAwsResourceProperty - 断言 提供的实例是否是 Windows。
 - a. （适用于 Windows 的 EC2 救援）如果提供的实例是 Windows：
 - i. aws:executeAutomation-AWSSupport-StartEC2RescueWorkflow 使用 Windows 版 R EC2 rescue 离线密码重置脚本进行调用
 - ii. aws:executeAwsApi - 从嵌套的 Automation 检索备份 AMI ID
 - iii. aws:executeAwsApi - 从嵌套的 Automation 检索启用了密码的 AMI ID
 - iv. aws:executeAwsApi-从嵌套自动化中检索 EC2救援摘要
 - b. （适用于 Linux 的 EC2 救援）如果提供的实例是 Linux：
 - i. aws:executeAutomation-AWSSupport-StartEC2RescueWorkflow 使用适用于 Linux 的 EC2 救援离线 SSH 密钥注入脚本调用
 - ii. aws:executeAwsApi - 从嵌套的 Automation 检索备份 AMI ID
 - iii. aws:executeAwsApi - 检索注入的 SSH 密钥的 SSM 参数名称
 - iv. aws:executeAwsApi-从嵌套自动化中检索 EC2救援摘要

输出

获取 EC2 RescueForWindowsResult .Output

getWindowsBackup阿米。ImageId

getWindowsPasswordEnabledAmi.ImageId

获取 EC2 RescueForLinuxResult .Output

getLinuxBackup阿米。ImageId

获取 Linux 参数.Name SSHKey

AWSSupport-ResetLinuxUserPassword

描述

AWSSupport-ResetLinuxUserPassword 运行手册可帮助您重置本地操作系统 (OS) 用户的密码。对于需要使用串行控制台访问其 Amazon Elastic Compute Cloud (Amazon EC2) 实例的用户，此运行手册尤其有用。运行手册 AWS 账户 使用自动生成的 AWS Identity and Access Management (IAM) 角色或您指定的自定义 IAM 实例配置文件在您的中创建一个临时 Amazon EC2 实例。自定义 (IAM) 实例配置文件必须有权检索包含密码的 AWS Secrets Manager 密钥值。

运行手册可停止您的目标 Amazon EC2 实例，分离 Amazon Elastic Block Store (Amazon EBS) 根卷，并将其附加到临时 Amazon EC2 实例。利用运行命令，可以在临时实例上运行脚本，以设置您指定的操作系统用户的密码。然后，Amazon EBS 根卷会重新附加到您的目标实例。此运行手册还提供了在自动化开始时创建根卷快照的选项。

开始之前

使用您要分配给操作系统用户的密码的值创建一个 Secrets Manager 密钥。该值必须为纯文本。有关更多信息，请参阅《AWS Secrets Manager 用户指南》中的[创建 AWS Secrets Manager 密钥](#)。

注意事项

- 我们建议您在**使用此运行手册之前先备份您的实例**。考虑将 CreateSnapshot 参数的值设置为 **Yes**。
- 更改本地用户密码需要运行手册停止您的实例。停止实例后，存储在内存或实例存储卷上的数据将丢失。此外，任何自动分配的公用 IPv4 地址都会被释放。有关停止实例时会发生什么情况的更多信息，请参阅 Amazon EC2 用户指南中的[停止和启动实例](#)。
- 如果连接到您的目标 Amazon EC2 实例的 Amazon EBS 卷使用客户托管 AWS Key Management Service (AWS KMS) 密钥进行加密，请确保 AWS KMS 密钥未加密，deleteddisabled否则您的实例将无法启动。

- 使用自定义 IAM 实例配置文件需要拥有 IAM GetInstanceProfile 权限AutomationAssumeRole才能进行验证，而自定义实例配置文件本身必须包含 Systems Manager 和 Secrets Manager 访问权限。运行手册会预先验证实例配置文件是否存在，但如果实例配置文件缺少所需的访问权限，则在辅助实例操作期间将失败。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 包含您要重置的操作系统用户密码的 Amazon EC2 Linux 实例的 ID。

- LinuxUserName

类型：字符串

默认：ec2-user

描述：(可选) 要重置其密码的操作系统用户账户。

- SecretArn

类型：字符串

描述：(必需) 包含新密码的 Secrets Manager 密钥的 ARN。

- SecurityGroupId

类型：字符串

描述：(可选) 要附加到临时 Amazon EC2 实例的安全组的 ID。如果您没有为此参数提供一个值，将使用默认的 Amazon Virtual Private Cloud (Amazon VPC) 安全组。

- SubnetId

类型：字符串

描述：(可选) 要将 Amazon EC2 临时实例启动到的子网的 ID。默认情况下，自动化会选择与您的目标实例相同的子网。如果您选择提供不同的子网，则它必须与目标实例位于同一可用区，并且可以访问 Systems Manager 端点。

- CreateSnapshot

类型：字符串

有效值：是 | 否

默认：是

描述：(可选) 确定是否在自动化运行之前创建目标 Amazon EC2 实例根卷的快照。

- StopConsent

类型：字符串

有效值：是 | 否

默认：否

描述：输入 **Yes** 以确认目标 Amazon EC2 实例将在此自动化期间停止。当 Amazon EC2 实例停止时，存储在内存或实例存储卷中的所有数据都将丢失，并自动释放公有 IPv4 地址。有关更多信息，请参阅 Amazon EC2 用户指南中的[停止和启动您的实例](#)。

- InstanceProfileName

类型：字符串

描述：(可选) 要附加到帮助程序 Amazon EC2 实例的 IAM 实例配置文件的名称。如果未提供，则将自动创建具有所需权限的临时实例配置文件。自定义实例配置文件必须有权访问指定的 Secrets Manager 密钥和 Systems Manager。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeInstanceInformation
- ssm:ListTagsForResource
- ssm:SendCommand
- ec2:AttachVolume
- ec2:CreateSnapshot
- ec2:CreateSnapshots
- ec2:CreateVolume
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeSnapshotAttribute
- ec2:DescribeSnapshots
- ec2:DescribeSnapshotTierStatus
- ec2:DescribeVolumes
- ec2:DescribeVolumeStatus
- ec2:DetachVolume
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStackResource

- `cloudformation:DescribeStacks`
- `cloudformation:ListStacks`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`
- `iam:GetInstanceProfile`

文档步骤

1. `aws:branch` – 根据您是否同意停止目标 Amazon EC2 实例进行分支。
2. `aws:assertAwsResourceProperty`— 确保 Amazon EC2 实例的状态为 `running` 或 `stopped` 状态。否则，自动化将结束。
3. `aws:executeAwsApi`— 获取 Amazon EC2 实例的属性。
4. `aws:executeAwsApi`— 获取根卷属性。
5. `aws:branch`— 根据是否提供了临时 Amazon EC2 实例的子网 ID 来分支自动化。
6. `aws:assertAwsResourceProperty`— 确保您在 `SubnetId` 参数中指定的子网与目标 Amazon EC2 实例位于同一个可用区中。
7. `aws:assertAwsResourceProperty`— 确保目标 Amazon EC2 实例根卷是亚马逊 EBS 卷。
8. `aws:assertAwsResourceProperty`— 确保 Amazon EC2 实例架构为 `arm64` 或 `x86_64`。
9. `aws:assertAwsResourceProperty`— 确保 Amazon EC2 实例的关闭行为是 `stop` 而不是 `terminate`。
10. `aws:branch`— 确保 Amazon EC2 实例不是竞价型实例。否则，自动化将结束。
11. `aws:executeScript`— 确保 Amazon EC2 实例不属于自动扩展组。如果该实例是自动扩缩组的一部分，则自动化会确认 Amazon EC2 实例是否处于 `Standby` 生命周期状态。
12. `aws:branch`— 根据是否提供了自定义 IAM 实例配置文件名称来分支自动化
13. `aws:assertAwsResourceProperty`— 确保自定义 IAM 实例配置文件存在并验证其名称是否与输入参数匹配。
14. `aws:createStack`— 创建临时的 Amazon EC2 实例，用于重置您指定的操作系统用户的密码。

- 15aws:waitForAwsResourceProperty— 等待直到新启动的临时 Amazon EC2 实例开始运行。
- 16aws:executeAwsApi— 获取临时亚马逊 EC2 实例的 ID。
- 17aws:waitForAwsResourceProperty— 等待临时 Amazon EC2 实例报告为由 Systems Manager 管理。
- 18aws:changeInstanceState— 停止目标 Amazon EC2 实例。
- 19aws:changeInstanceState— 强制目标 Amazon EC2 实例停止，以防它陷入停止状态。
- 20aws:branch— 根据是否请求了目标 Amazon EC2 实例的根卷快照来分支自动化。
- 21aws:executeAwsApi— 创建目标 Amazon EC2 实例根亚马逊 EBS 卷的快照。
- 22aws:waitForAwsResourceProperty— 等待快照进入completed状态。
- 23aws:executeAwsApi— 将 Amazon EBS 根卷与目标 Amazon EC2 实例分离。
- 24aws:waitForAwsResourceProperty— 等待亚马逊 EBS 根卷与目标 Amazon EC2 实例分离。
- 25aws:executeAwsApi— 将根 Amazon EBS 卷附加到临时亚马逊 EC2 实例。
- 26aws:waitForAwsResourceProperty— 等待 Amazon EBS 根卷连接到临时的 Amazon EC2 实例。
- 27aws:runCommand— 通过在临时 Amazon EC2 实例上使用运行命令运行 shell 脚本来重置目标用户密码。
- 28aws:executeAwsApi— 将 Amazon EBS 根卷与临时亚马逊 EC2 实例分离。
- 29aws:waitForAwsResourceProperty— 等待 Amazon EBS 根卷与临时的 Amazon EC2 实例分离。
- 30aws:executeAwsApi— 出错后，将 Amazon EBS 根卷与临时的 Amazon EC2 实例分离。
- 31aws:waitForAwsResourceProperty— 等待出错后将 Amazon EBS 根卷与临时的 Amazon EC2 实例分离。
- 32aws:branch— 根据是否请求根卷的快照来确定出现错误时的恢复路径，对自动化进行分支。
- 33aws:executeAwsApi— 将根 Amazon EBS 卷重新连接到目标 Amazon EC2 实例。
- 34aws:waitForAwsResourceProperty— 等待亚马逊 EBS 根卷连接到亚马逊 EC2 实例。
- 35aws:executeAwsApi— 根据目标 Amazon EC2 实例根卷快照创建新的 Amazon EBS 卷。
- 36aws:waitForAwsResourceProperty— 等到新的 Amazon EBS 卷处于状态为止。available
- 37aws:executeAwsApi— 将新的 Amazon EBS 卷作为根卷附加到目标实例。
- 38aws:waitForAwsResourceProperty— 等待 Amazon EBS 交易量处于状态。attached
- 39aws:executeAwsApi— 描述运行手册无法创建或更新 CloudFormation 堆栈时的 CloudFormation 堆栈事件。

40aws:branch— 根据之前的 Amazon EC2 实例状态对自动化进行分支。如果状态为 `running`，则实例已启动。如果处于 `stopped` 状态，则自动化会继续。

41aws:changeInstanceState— 如果需要，启动 Amazon EC2 实例。

42aws:waitForAwsResourceProperty— 等待 CloudFormation 堆栈处于终端状态后再删除。

43aws:executeAwsApi— 删除包括临时 Amazon EC2 实例在内的 CloudFormation 堆栈。

AWSupport-RunEC2RescueForWindowsTool

描述

AWSupport-RunEC2 RescueForWindowsTool 运行手册在目标亚马逊弹性计算云 (Amazon EC2) Windows 托管实例上运行适用于 Windows 服务器的 Amazon EC2 Rescue 故障排除工具，以帮助解决常见问题。本运行手册支持三个主要操作：

- **ResetAccess**：重置本地管理员密码。密码是随机生成的，并安全地存储在 P AWS Systems Manager parameter Store 中 `/EC2Rescue/Password/<instance_id>`。如果未提供任何参数，则使用默认 AWS Key Management Service (AWS KMS) 密钥对密码进行加密 `alias/aws/ssm`。或者，您可以指定 AWS KMS 密钥 ID 以使用自己的密钥对密码进行加密。
- **CollectLogs**：通过运行带选项的 Amazon EC2 Rescue，从操作系统收集日志和配置文件，然后将其上传到您账户中的亚马逊简单存储服务 (Amazon S3) 存储桶。 `/collect:all`
- **FixAll**：尝试通过运行带 `/rescue:all` 选项的 Amazon EC2 Rescue 来检测 and 解决连接到当前实例的离线 Windows 根卷上的问题。

Important

本运行手册要求目标实例是 PowerShell 安装了适用于 Windows 的 AWS 工具的 Windows 托管实例。运行手册使用 Systems Manager Distributor 软件包 `AWSupport-EC2Rescue` 安装适用于 Windows 服务器的 Amazon EC2 救援工具。

如何工作？

运行手册执行以下步骤：

- 使用 Systems Manager 分销商包安装适用于 Windows 服务器的 Amazon EC2 Rescue 疑难解答工具。

- 使用提供的参数执行指定的操作 (ResetAccessCollectLogs、或FixAll)。
- ForResetAccess：生成安全密码并将其存储在参数存储中。
- 用于CollectLogs：收集系统日志并将其上传到指定的 Amazon S3 存储桶。
- ForFixAll：尝试修复指定脱机卷上的问题。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:SendCommand
- ssm:ListCommandInvocations
- ssm:DescribeInstanceInformation
- ssm:GetCommandInvocation
- ssm:PutParameter (供 ResetAccess 采取行动)
- kms:Encrypt (用于使用自定义 AWS KMS 键进行 ResetAccess 操作)
- s3:PutObject (供 CollectLogs 采取行动)
- s3:GetBucketAcl (供 CollectLogs 采取行动)
- s3:GetBucketPolicy (供 CollectLogs 采取行动)
- s3:GetBucketPolicyStatus (供 CollectLogs 采取行动)

策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:PutParameter",
        "kms:Encrypt",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-RunEC2RescueForWindowsTool](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - 命令 (必填)：
 - 描述：(必填) 要执行的操作。
 - 类型：String
 - 允许值：[ResetAccess, CollectLogs, FixAll]
 - 默认值：ResetAccess
 - 参数 (必填)：
 - 描述：(必填) 命令的参数：
 - 用于ResetAccess：AWS KMS 密钥 ID 或别名 (默认：alias/aws/ssm)

- 收件人CollectLogs：要将日志上传到的 Amazon S3 存储桶名称
- 用于FixAll：离线修复的设备名称（例如，xvdf）
- 类型：String
- 允许模式：`^[0-9a-z][a-z0-9-.]{3,63}$|^(dev\[a-z0-9]{2,10}|xv[a-z0-9]{1,10})$|^(alias\\aws\\ssm[a-zA-Z0-9-/_]{1,32})$`

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- 安装EC2救援：

使用 Systems Manager 分销商包安装适用于 Windows 服务器的 Amazon EC2 Rescue 疑难解答工具AWSSupport-EC2Rescue。

- 运行 EC2 RescueForWindows：

使用命令参数中指定的操作运行 PowerShell 脚本以执行请求的操作。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)
- [使用适用于 Windows 服务器的 Amazon EC2 Rescue 和 Systems Manager 运行命令](#)

AWSPremiumSupport-ResizeNitroInstance

描述

AWSPremiumSupport-ResizeNitroInstance 运行手册提供了一种自动化的解决方案，用于调整基于 Nitro 系统构建的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的大小。

为了降低数据丢失和停机的潜在风险，运行手册对以下事项进行验证：

- 实例停止行为。
- 实例是否是 Amazon EC2 Auto Scaling 组的一部分且处于 standby 模式。
- 实例状态和租赁。
- 您要更改成的实例类型支持当前附加到您实例的网络接口的数量。
- 当前实例类型和目标实例类型的处理器架构和虚拟化类型相同。
- 如果实例正在运行，则表明它正在通过所有状态检查。
- 您要更改的实例类型在相同可用区中是可用的。

如果 Amazon EC2 在更改实例类型后未通过状态检查，运行手册将自动回退到以前的实例类型。

默认情况下，如果实例正在运行以及已附加实例存储卷，则此运行手册不会更改实例类型。如果实例是 AWS CloudFormation 堆栈的一部分，运行手册也不会更改实例类型。如果要更改这些行为中的任意一个，请为 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 参数指定 `yes`。

运行手册提供了两种不同的方法来指定要更改为的实例类型：

- 对于针对单个实例的简单自动化，请使用 `TargetInstanceTypeFromParameter` 参数指定要更改为的实例类型。
- 要大规模运行自动化以更改多个实例的实例类型，请使用 `TargetInstanceTypeFromTagValue` 参数指定实例类型。有关大规模运行自动化的信息，请参阅[大规模运行自动化](#)。

如果您没有为任一参数指定一个值，自动化将失败。

Important

访问 `AWSPremiumSupport` - *运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持计划](#)。

注意事项

- 我们建议您在运行手册之前先备份您的实例。
- 有关更改实例类型的兼容性的信息，请参阅[更改实例类型的兼容性](#)。
- 如果自动化失败并回退到初始实例类型，请参阅[更改实例类型疑难解答](#)。

- 更改实例类型需要运行手册来停止您的实例。停止实例后，存储在内存或实例存储卷上的数据将丢失。此外，任何自动分配的公用 IPv4 地址都会被释放。有关停止实例时会发生什么的更多信息，请参阅[停止和启动您的实例](#)。
- 使用 `SkipInstancesWithTagKey` 参数，您可以跳过应用了特定 Amazon EC2 标签键的实例。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 确认

类型：字符串

描述：(必需) 输入 **yes** 以确认如果您的实例当前正在运行，则该实例将停止。

- `AllowInstanceStoreInstances`

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果您指定 `yes`，您将允许运行手册在已附加实例存储卷的实例上运行。

- `AllowCloudFormationInstances`

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果您指定 `yes`，则运行手册将在属于 CloudFormation 堆栈的实例上运行。

- `DryRun`

类型：字符串

有效值：否 | 是

默认值：no

描述：(可选) 如果您指定 `yes`，运行手册将验证大小调整要求，而不会更改实例类型。

- `InstanceId`

类型：字符串

描述：(必填) 要更改其类型的 Amazon EC2 实例的 ID。

- `SkipInstancesWithTagKey`

类型：字符串

描述：(可选) 如果您指定的标签键应用于目标实例，自动化将跳过该实例。

- `SleepTime`

类型：字符串

原定设置值：3

描述：(可选) 此运行手册在完成后应处于休眠状态的秒数。

- `TagInstance`

类型：字符串

描述：(可选) 使用您选择的密钥和价值标记实例，格式如

下：*Key=ChangingType, Value=True*。此选项允许您跟踪此运行手册所针对的实例。标签键和价值区分大小写。

- TargetInstanceTypeFromParameter

类型：字符串

描述：(可选) 要将您的实例更改为的实例类型。如果您要使用

TargetInstanceTypeFromTagValue 参数中提供的标签键的值，请将此参数留空。

- TargetInstanceTypeFromTagValue

类型：字符串

描述：(可选) 应用于目标实例的标签键，其值包含您要更改为的实例类型。如果您为

TargetInstanceTypeFromParameter 参数指定值，那么它将替换您为此参数指定的任何值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:DescribeAutoScalingInstances
- cloudformation:DescribeStackResources
- ssm:GetAutomationExecution
- ssm:DescribeAutomationExecutions
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeTags
- ec2:ModifyInstanceAttribute
- ec2:StartInstances
- ec2:StopInstances

文档步骤

1. `aws:assertAwsResourceProperty` : 确保 Amazon EC2 实例未使用 `SkipInstancesWithTagKey` 参数中指定的资源标签键进行标记。如果发现标签键应用于该实例，该步骤将失败，自动化将结束。
2. `aws:assertAwsResourceProperty` : 确认目标 Amazon EC2 实例的状态为 `running`、`pending`、`stopped` 或 `stopping`。否则，自动化将结束。
3. `aws:executeAwsApi` : 从 Amazon EC2 实例收集属性。
4. `aws:executeAwsApi` : 收集有关当前 Amazon EC2 实例类型的详细信息。
5. `aws:branch` : 检查当前实例类型和 `TargetInstanceTypeFromParameter` 参数中指定的实例类型是否相同。如果相同，自动化将结束。
6. `aws:assertAwsResourceProperty` : 确保实例在 Nitro 系统上运行。
7. `aws:branch` : 确保 Amazon EC2 实例根卷类型为 Amazon Elastic Block Store (Amazon EBS) 卷。
8. `aws:assertAwsResourceProperty` : 确认实例关闭行为是 `stop` 且不是 `terminate`。
9. `aws:branch` : 确保 Amazon EC2 实例不是竞价型实例。
10. `aws:branch` : 确保 Amazon EC2 实例的租赁是默认的，而不是专属主机或专用实例。
11. `aws:executeScript` : 确认此运行手册中只有一个针对当前实例 ID 的自动化。如果针对同一实例的另一个自动化已经在进行，则它会返回错误并结束。
12. `aws:branch` : 根据 Amazon EC2 实例的状态对自动化进行分支。
 - a. 如果为 `stopped` 或 `stopping`，则自动化会运行 `aws:waitForAwsResourceProperty`，直到 Amazon EC2 实例完全停止。
 - b. 如果为 `running` 或 `pending`，则自动化会运行 `aws:waitForAwsResourceProperty`，直到 Amazon EC2 实例通过状态检查。
13. `aws:assertAwsResourceProperty` : 通过调用 `DescribeAutoScalingInstances` API 操作，确认 Amazon EC2 实例不是自动扩缩组的一部分。如果实例是自动扩缩组的一部分，确保 Amazon EC2 实例处于 `standby` 模式。
14. `aws:branch` : 根据您是否希望自动化检查 Amazon EC2 实例是否属于 CloudFormation 堆栈来分支自动化：
 - a. `aws:executeScript` 通过调用 `DescribeStackResources` API 操作确保 Amazon EC2 实例不属于 CloudFormation 堆栈。
15. `aws:executeAwsApi` : 返回具有相同处理器架构类型、虚拟化类型且支持当前附加到目标实例的网络接口数量的实例类型列表。

- 16aws:executeAwsApi : 从 TargetInstanceTypeFromTagValue 参数中指定的标签键获取目标实例类型值。
- 17aws:executeScript : 确认当前实例类型和目标实例类型兼容。确保目标实例类型在同一个子网中可用。验证已启动运行手册的主体是否拥有更改实例类型的权限，以及是否拥有当实例正在运行时停止和启动该实例的权限。
- 18aws:branch : 根据 DryRun 参数值是否设置为 yes，对自动化进行分支。如果是 yes，自动化将结束。
- 19aws:branch : 检查原始和目标实例类型是否相同。如果它们相同，自动化将结束。
- 20aws:executeAwsApi : 获取当前实例状态。
- 21aws:changeInstanceState : 停止 Amazon EC2 实例。
- 22aws:changeInstanceState : 如果实例卡在了 stopping 停止状态，则强制其停止。
- 23aws:executeAwsApi : 将实例类型更改为目标实例类型。
- 24aws:sleep : 更改实例类型后等待 3 秒钟以确保最终一致性。
- 25aws:branch : 根据前实例的状态对自动化进行分支。如果是 running，则实例已启动。
- a. aws:changeInstanceState : 如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
 - b. aws:waitForAwsResourceProperty : 等待 Amazon EC2 实例通过状态检查。如果实例未通过状态检查，实例将变回其原始的实例类型。
 - i. aws:changeInstanceState : 停止 Amazon EC2 实例，然后将其更改为原始实例类型。
 - ii. aws:changeInstanceState : 强制 Amazon EC2 实例停止，然后再将其更改为原始实例类型，以防它卡在停止状态。
 - iii. aws:executeAwsApi : 将 Amazon EC2 实例更改为其原始类型。
 - iv. aws:sleep : 更改实例类型后等待 3 秒钟以确保最终一致性。
 - v. aws:changeInstanceState : 如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
 - vi. aws:waitForAwsResourceProperty : 等待 Amazon EC2 实例通过状态检查。
- 26aws:sleep : 等待，然后结束运行手册。

AWSsupport-ShareEncryptedAMI0rEBSSnapshot

描述

本操作手册自动执行与其他亚马逊云科技账户共享加密Amazon Machine Image或亚马逊弹性区块存储快照的过程。本运行手册处理跨账户共享加密资源的复杂要求，包括 AWS Key Management Service 密钥策略修改和资源权限更新。

此自动化会执行 AWS 安全博客文章[如何在账户之间共享加密的以启动加密AMI的 Amazon Elastic Compute Cloud 实例](#)中概述的步骤。

重要注意事项

- 本运行手册将修改您的资源：运行手册将向您的 AWS KMS 客户托管密钥 (CMK) 策略添加跨账户权限，并向目标账户授予启动AMI权限或 Amazon EBS 快照创建卷权限。
- 可能会产生额外费用：复制资源（不同区域或 AWS 托管密钥加密）时，新的快照AMI或 Amazon EBS 快照以及任何跨区域数据传输都将产生额外费用。
- 请验证目标账户 ID：请仔细检查目标账户 ID，因为此操作手册无法验证账户是否存在。
- 通过手动验证自动回滚：如果更改失败，此运行手册会尝试自动回滚更改。但是，如果回滚本身失败，请确认您的账户中没有剩余的 AMI /Snapshot 副本，资源 LaunchPermission/ CreateVolumePermission 属性不包括非预期账户，并且 AWS KMS 密钥策略处于其原始状态。

如何工作？

运行手册执行以下高级步骤：

- 验证输入资源的存在、状态和加密配置
- 检查目标账户当前的资源共享权限
- 分析 AWS KMS 关键策略并创建所有必需更改的全面预览
- 在进行任何更改之前，请先征得指定负责人的批准
- 执行已批准的更改，包括资源复制（如果需要）、权限更新和 AWS KMS 密钥策略修改
- 如果需要，提供包含回滚信息的全面执行报告

[运行此自动化（控制台）](#)

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

该 AutomationAssumeRole 参数需要以下操作：

- ec2: DescribeImages
- ec2: DescribeSnapshots
- ec2: DescribeImageAttribute
- ec2: DescribeSnapshotAttribute
- ec2: ModifyImageAttribute
- ec2: ModifySnapshotAttribute
- ec2: CopyImage
- ec2: CopySnapshot
- ec2: DeregisterImage
- ec2: DeleteSnapshot
- kms: DescribeKey
- kms: GetKeyPolicy
- kms: PutKeyPolicy
- kms: CreateGrant
- kms: GenerateDataKey *
- kms: ReEncrypt *
- kms: Decrypt
- 访问分析器：CheckAccessNotGranted

说明

按照这些步骤对自动化进行配置：

1. [AWSsupport-ShareEncryptedAMI0rEBSSnapshot](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management 角色的亚马逊资源名称。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 批准者 (必填) :

能够批准或拒绝操作的 AWS 经过身份验证的委托人列表。最大审批者数量为 10。您可以使用以下任一格式指定委托人：用户名、用户 ARN、IAM 角色 ARN 或 IAM 代入角色 ARN。

- ResourceId (必填) :

AMI 或者要共享的亚马逊 EBS 快照 ID (例如 ami-123456789012 或 snap-123456789012)。

- DestinationAccountId (必填) :

将在其中共享资源的 12 位 AWS 账户 ID。

- CustomerManagedKeyId (可选) :

AWS KMS 用于重新加密资源的 CMK ID。如果资源使用 AWS 托管密钥加密，或者指定要进行跨区域复制，DestinationRegion 则为必填项。要进行跨区域复制，此密钥必须存在于目标区域。

- DestinationRegion (可选) :

资源将被复制到的 AWS 区域。默认值为当前区域。如果指定了其他区域，则将使用 CustomerManagedKeyId 参数中指定的 AWS KMS CMK 将资源复制到目标区域。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **ValidateResources:**

验证输入资源的存在、状态、加密配置，并确定共享所需的更改。

- **BranchOnResourcePermission:**

根据是否需要检查资源共享权限来分支工作流程。

- **CheckResourcePermission:**

检查目标账户是否拥有资源所需的共享权限。

- **AnalyzeChanges:**

分析 AWS KMS 关键策略并创建所有必需更改的全面预览。

- **BranchOnChanges:**

根据更改是否需要批准来分支工作流程。

- **GetApproval:**

等待指定的 AWS IAM 委托人在批准后才能继续进行所需的更改。

- **ExecuteChanges:**

执行已批准的更改，并在失败时进行回滚。

- **Results:**

生成一份全面的执行报告，总结在加密AMI或快照共享过程中采取的所有操作。

7. 完成后，查看“输出”部分以了解执行的详细结果。

目标账户的必填 AWS AWS Identity and Access Management 政策

目标账户中的 IAM 角色或用户必须配置以下 IAM 权限，才能从共享加密的 Amazon EC2 实例启动加密的 Amazon EC2 实例，AMI或者从共享的加密的 Amazon EBS 快照创建卷：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:<region>:<account-id>:key/<key-id>"
      ]
    }
  ]
}
```

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)

- [设置自动化](#)
- [Support 自动化工作流程](#)
- [共享密 AWS KMS 钥](#)

AWSSupport-RestoreEC2InstanceFromSnapshot

描述

该AWSSupport-RestoreEC2InstanceFromSnapshot运行手册可帮助您从亚马逊弹性区块存储 (Amazon EBS EC2) 根卷的有效快照中识别和恢复亚马逊弹性计算云 (Amazon) 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EndDate

类型：字符串

描述：(可选) 要自动化查看快照的最后日期。

- InplaceSwap

类型：布尔值

有效值：true | false

描述：(可选) 如果此参数的值设置为 true，则从快照中新创建的卷将替换附加到您的实例的现有根卷。

- InstanceId

类型：字符串

说明：(必需) 要从快照复原的实例的 ID。

- LookForInstanceStatusCheck

类型：布尔值

有效值：true | false

默认：True

描述：(可选) 如果此参数的值设置为 true，则自动化将检查从快照启动的测试实例的实例状态检查是否失败。

- SkipSnapshotsBy

类型：字符串

描述：(可选) 搜索快照以恢复实例时跳过快照的时间间隔。例如，如果有 100 个快照可用，且您为此参数指定的值为 2，则每三张快照就会被审查一次。

默认：0

- SnapshotId

类型：字符串

描述：(可选) 要从中复原实例的快照的 ID。

- StartDate

类型：字符串

描述：(可选) 要自动化查看快照的最早日期。

- TotalSnapshotsToLook

类型：字符串

描述：(可选) 自动化审查的快照数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation
- ec2:AttachVolume
- ec2:CreateImage
- ec2:CreateTags
- ec2:CreateVolume
- ec2>DeleteTags
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeImages
- ec2:DescribeSnapshots
- ec2:DescribeVolumes
- ec2:DetachVolume
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudwatch:GetMetricData

文档步骤

1. aws:executeAwsApi - 收集有关目标实例的详细信息。
2. aws:assertAwsResourceProperty - 验证目标实例是否存在。
3. aws:assertAwsResourceProperty - 验证根卷是否为 Amazon EBS 卷。

4. `aws:assertAwsResourceProperty` - 验证另一个针对此实例的自动化是否尚未运行。
5. `aws:executeAwsApi` - 标记目标实例。
6. `aws:executeAwsApi`-创建一个 AMI 实例的。
7. `aws:executeAwsApi`-收集有关以下内容的详细信息 AMI 在上一步中创建。
8. `aws:waitForAwsResourceProperty`-等着 AMI available在继续操作之前先要变成。
9. `aws:executeScript`-从新创建的实例启动新实例 AMI。
- 10`aws:assertAwsResourceProperty` - 验证实例状态为 available。
- 11`aws:executeAwsApi` - 收集有关新启动实例的详细信息。
- 12`aws:branch` - 根据您是否为 `SnapshotId` 参数提供了值进行分支。
- 13`aws:executeScript` - 返回指定时间段内快照的列表。
- 14`aws:executeAwsApi` - 停止实例。
- 15`aws:waitForAwsResourceProperty` - 等待卷状态处于 available。
- 16`aws:waitForAwsResourceProperty` - 等待实例状态处于 stopped。
- 17`aws:executeAwsApi` - 分离根卷。
- 18`aws:waitForAwsResourceProperty` - 等待根卷被分离。
- 19`aws:executeAwsApi` - 附加新的根卷。
- 20`aws:waitForAwsResourceProperty` - 等待新卷被附加。
- 21`aws:executeAwsApi` - 启动实例。
- 22`aws:waitForAwsResourceProperty` - 等待实例状态处于 available。
- 23`aws:waitForAwsResourceProperty` - 等待通过实例的系统和实例状态检查。
- 24`aws:executeScript` - 运行脚本以查找可用于成功创建卷的快照。
- 25`aws:executeScript` - 运行脚本，以使用根据自动化识别的快照新创建的卷，或使用根据您在 `SnapshotId` 参数中指定的快照创建的卷来恢复实例。
- 26`aws:executeScript` - 删除此自动化创建的资源。

输出

`launchCloneInstance.InstanceIds`

`ListSnapshotByDate.finalSnapsh`

`ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange`

findWorkingSnapshot. 工作快照

InstanceRecovery。结果

AWSSupport-SendLogBundleToS3Bucket

描述

AWSSupport-SendLogBundleToS3Bucket运行手册将 EC2救援工具生成的日志包从目标实例上传到指定的 S3 存储桶。运行手册根据目标实例的平台安装特定于平台的 R EC2 rescue 版本。EC2然后使用 Rescue 来收集所有可用的操作系统 (OS) 日志。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

说明：(必需) 要从此收集日志的 Windows 或 Linux 托管实例的 ID。

- S3 BucketName

类型：字符串

说明：(必需) 要将日志上传到的 S3 存储桶。

- S3Path

类型：字符串

默认：AWSsupport-SendLogBundleToS3Bucket/

说明：(可选) 收集的日志的 S3 路径。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议接收命令的 EC2 实例具有 IAM 角色并附有 Amazon A SSMMangedInstanceCorema zon 托管策略。用户必须至少有 ssm: StartAutomationExecution 和 ssm: SendCommand 才能运行自动化并将命令发送到实例，还必须有 ssm: GetAutomationExecution 才能读取自动化输出。

文档步骤

1. aws:runCommand-通过安装 R EC2 escue AWS-ConfigureAWSPackage。
2. aws:runCommand-运行 PowerShell 脚本以使用 R EC2 escue 收集 Windows 故障排除日志。
3. aws:runCommand-使用 R EC2 escue 运行 bash 脚本收集 Linux 故障排除日志。

输出

collectAndUploadWindowsLogBundle。输出

collectAndUploadLinuxLogBundle。输出

AWSSupport-StartEC2RescueWorkflow

描述

AWSSupport-StartEC2RescueWorkflow 运行手册在创建的帮助程序实例上运行提供 base64 编码脚本 (Bash 或 Powershell) 以修复实例。您的实例的根卷已连接并挂载到辅助实例，也称为 R EC2 escue 实例。如果实例是 Windows，请提供 Powershell 脚本。否则，请使用 Bash。运行手册会设置一些可供脚本使用的环境变量。环境变量包含有关您提供的输入的信息，以及有关离线根卷的信息。离线卷已挂载，可供使用。例如，您可以将 Desired State Configuration 文件保存到离线 Windows 根卷，或 chroot 到一个离线 Linux 根卷并执行离线修复。

运行此自动化 (控制台)

⚠ Important

此自动化不支持从 Marketplace Amazon 系统映像 (AMIs) 创建的 Amazon EC2 实例。

附加信息

要对脚本进行 base64 编码，可以使用 Powershell 或 Bash。Powershell：

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash：

```
base64 PATH_TO_FILE
```

下面是您可以在离线脚本中使用的环境变量列表，具体视目标操作系统而定

Windows：

变量	说明	示例值
\$env：救援账户_ID EC2	{{ global:ACCOUNT_ID }}	123456789012
\$env：救援日期 EC2	{{ global:DATE }}	2018-09-07
\$env：救援_日期_时间 EC2	{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$env：EC2RESCUE_ RW_DIR EC2	EC2Windows 版 Rescue 安装 路径	C:\Program Files\ Amazon\ R EC2 escue
\$env：EC2RESCUE_ RW_DIR EC2	EC2Windows 版 Rescue 安装 路径	C:\Program Files\ Amazon\ R EC2 escue
\$env：RESCUE_EXECUT ION_ID EC2	{{ automation:EXECUTI ON_ID }}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
\$env：救援_OFFLINE_CU RRENT_CONTROL_SET EC2	离线 Windows 目前控制设置路 径	HKLM:\AWSTempSystem \ControlSet001

变量	说明	示例值
\$env : 救援_OFFLINE_DRIVE EC2	离线 Windows 驱动器号	D:\
\$env : RESCUE_OFFLINE _EBS_DEVICE EC2	离线根卷 EBS 设备	xvdf
\$env : RESCUE_OFFLIN E_KERNEL_VER EC2	离线 Windows 内核版本	6.1.7601.24214
\$env : RESCUE_OFFLINE _OS_ARCHITECTUR EC2	离线 Windows 架构	AMD64
\$env : RESCUE_OFFLIN E_OS_CAPTION EC2	离线 Windows 标题	Windows Server 2008 R2 (数 据中心版)
\$env : RESCUE_OFFLIN E_OS_TYPE EC2	离线 Windows 操作系统类型	服务器
\$env : RESCUE_OFFLINE _PROGRAM_FILES_DIR EC2	离线 Windows 程序文件目录路 径	D:\Program Files
\$env : RESCUE_OFFLIN E_PROGRAM_FILES_X8 6_DIR EC2	离线 Windows 程序文件 x86 目录路径	D:\Program Files (x86)
\$env : 救援_OFFLINE_RE GISTRY_DIR EC2	离线 Windows 注册表目录路径	D:\Windows\System32\config
\$env : RESCUE_OFFLIN E_SYSTEM_ROOT EC2	离线 Windows 系统根目录路径	D:\Windows
\$env : RESCUE_REGION EC2	{{ global:REGION }}	us-west-1
\$env : RESCUE_S3_BUCKET EC2	{{ S3BucketName }}	amzn-s3 demo-bucket

变量	说明	示例值
\$env : RESCUE_S3_PREFIX EC2	{{ S3Prefix }}	myprefix/
\$env : 救援_SOURCE_INS TANCE EC2	{{ InstanceId }}	i-abcdefgh123456789
\$script : EC2救援_离线_W INDOWS_INSTALL	离线 Windows 安装元数据	客户 Powershell 对象

Linux :

变量	说明	示例值
EC2救援账号	{{ global:ACCOUNT_ID }}	123456789012
EC2救援日期	{{ global:DATE }}	2018-09-07
EC2救援日期_时间	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_ri_DIR EC2	EC2Linux 版的救援安装路径	/usr/local/ec2ri-1.1.3
EC2救援_执行_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2离线救援设备	离线设备名称	/dev/xvdf1
EC2离线救援_EBS_设备	离线根卷 EBS 设备	/dev/sdf
EC2救援离线系统根目录	离线根卷挂载点	/mnt/mount
EC2救援_蟒蛇	Python 版本	python2.7
EC2救援区域	{{ global:REGION }}	us-west-1
EC2救援_S3_BUCKET	{{ S3BucketName }}	amzn-s3 demo-bucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/

变量	说明	示例值
EC2救援源实例	{{ InstanceId }}	i-abcdefgh123456789

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AMIPrefix

类型：字符串

默认：AWSsupport-EC2Rescue

描述：(可选) 备份 AMI 名称的前缀。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CreatePostEC2RescueBackup

类型：字符串

有效值：true | false

默认：false

描述：(可选) 将其设置为 `true` 以便 `InstanceId` 在运行脚本之后、启动脚本之前创建 AMI。Automation 完成后，AMI 仍将存在。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。

- `CreatePreEC2RescueBackup`

类型：字符串

有效值：`true` | `false`

默认：`false`

描述：(可选) 将其设置为 `true`，以便 `InstanceId` 在运行脚本之前创建的 AMI。Automation 完成后，AMI 仍将存在。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。

- `EC2RescueInstanceType`

类型：字符串

有效值：`t2.small` | `t2.medium` | `t2.large` | `t3.small` | `t3.medium` | `t3.large` | `i3.large` | `i3.xlarge`

默认：`t3.medium`

描述：(可选) EC2 救援实例的 EC2 实例类型。

- `InstanceId`

类型：字符串

描述：(必需) 您的 EC2 实例的 ID。重要：AWS Systems Manager 自动化会停止此实例。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- `OfflineScript`

类型：字符串

描述：(必需) 将对帮助程序实例运行的 Base64 编码的脚本。如果你的源实例是 Linux，如果是 Windows，PowerShell 则使用 Bash。

- `S3 BucketName`

类型：字符串

描述：(可选) 您账户中用于上传故障排除日志的 S3 存储桶的名称。确保存储桶策略不会向不需要访问所收集日志的各方授予不必要的 read/write 权限。

- S3Prefix

类型：字符串

默认：AWSsupport-EC2Rescue

描述：(可选) S3 日志的前缀。

- SubnetId

类型：字符串

默认：SelectedInstanceSubnet

描述：(可选) EC2救援实例的子网 ID。默认情况下，使用提供的实例所在的同一子网。重要：如果您提供自定义子网，则该子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 终端节点。

- UniqueId

类型：字符串

默认值：{{ automation:EXECUTION_ID }}

描述：(可选) 用于自动化的唯一标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议运行自动化的用户附加 Amazon Role SSMAutomation IAM 托管策略。除了此策略以外，用户还必须：

JSON

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

```

        "Action": [
            "lambda:InvokeFunction",
            "lambda:DeleteFunction",
            "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-
EC2Rescue-*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": [
            "arn:aws:s3:::awssupport-ssm.*/*.template",
            "arn:aws:s3:::awssupport-ssm.*/*.zip"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:CreateRole",
            "iam:CreateInstanceProfile",
            "iam:GetRole",
            "iam:GetInstanceProfile",
            "iam:PutRolePolicy",
            "iam:DetachRolePolicy",
            "iam:AttachRolePolicy",
            "iam:PassRole",
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam>DeleteInstanceProfile"
        ],
        "Resource": [
            "arn:aws:iam:*:111122223333:role/AWSSupport-EC2Rescue-*",
            "arn:aws:iam:*:111122223333:instance-profile/AWSSupport-EC2Rescue-
*"
        ],
        "Effect": "Allow"
    },
    {

```

```

        "Action": [
            "lambda:CreateFunction",
            "ec2:CreateVpc",
            "ec2:ModifyVpcAttribute",
            "ec2:DeleteVpc",
            "ec2:CreateInternetGateway",
            "ec2:AttachInternetGateway",
            "ec2:DetachInternetGateway",
            "ec2:DeleteInternetGateway",
            "ec2:CreateSubnet",
            "ec2:DeleteSubnet",
            "ec2:CreateRoute",
            "ec2:DeleteRoute",
            "ec2:CreateRouteTable",
            "ec2:AssociateRouteTable",
            "ec2:DisassociateRouteTable",
            "ec2:DeleteRouteTable",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteVpcEndpoints",
            "ec2:ModifyVpcEndpoint",
            "ec2:Describe*"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }
}

```

文档步骤

1. aws:executeAwsApi - 描述提供的实例
2. aws:executeAwsApi - 描述提供的实例的根卷
3. aws:assertAwsResourceProperty - 检查根卷设备类型是否为 EBS
4. aws:assertAwsResourceProperty - 检查根卷是否未加密
5. aws:assertAwsResourceProperty - 检查提供的子网 ID
 - a. (使用当前实例子网) -如果 * SubnetId = SelectedInstanceSubnet * 则运行aws:createStack部署 EC2救援 CloudFormation 堆栈
 - b. (创建新 VPC) -如果 * SubnetId = CreateNew VPC* 则运行部署aws:createStack救援堆栈 EC2 CloudFormation

c. (使用自定义子网) - 在所有其他情况下 :

aws:assertAwsResourceProperty - 检查提供的子网是否与提供的实例位于同一可用区中

aws:createStack-部署 EC2救援 CloudFormation 堆栈

6. aws:invokeLambdaFunction - 执行额外输入验证

7. aws:executeAwsApi-更新 EC2救援 CloudFormation 堆栈以创建 EC2救援助手实例

8. aws:waitForAwsResourceProperty-等待 EC2救援 CloudFormation 堆栈更新完成

9. aws:executeAwsApi-描述用于获取 EC2 Rescue 助手实例 ID 的 EC2救援 CloudFormation 堆栈输出

10aws:waitForAwsResourceProperty-等待 R EC2 escue 助手实例变为托管实例

11aws:changeInstanceState - 停止提供的实例

12aws:changeInstanceState - 停止提供的实例

13aws:changeInstanceState - 强制停止提供的实例

14aws:assertAwsResourceProperty-检查 CreatePreEC2RescueBackup输入值

a. (创建EC2救援前备份) -如果* CreatePre EC2 RescueBackup = true*

b. aws:executeAwsApi - 创建提供的实例的 AMI 备份

c. aws:createTags - 标记 AMI 备份

15aws:runCommand-在 EC2救援助手实例上安装 EC2 Rescue

16aws:executeAwsApi - 从提供的实例分离根卷

17aws:assertAwsResourceProperty - 检查提供的实例平台

a. (实例为 Windows) :

aws:executeAwsApi-将根卷作为 *xvdf* 连接到 R EC2 escue 助手实例

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Powershell 中运行提供的离线脚本

b. (实例为 Linux) :

aws:executeAwsApi-将根卷作为 */dev/sdf* 连接到 R EC2 escue 助手实例

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Bash 中运行提供的离线脚本

- 18aws:changeInstanceState-停止 EC2救援助手实例
- 19aws:changeInstanceState-强制停止 EC2救援助手实例
- 20aws:executeAwsApi-将根卷与 R EC2 rescue 助手实例分离
- 21aws:executeAwsApi - 将根卷附加回提供的实例
- 22aws:assertAwsResourceProperty-检查 CreatePostEC2RescueBackup输入值
 - a. (创建EC2救援后备份) -如果* CreatePost EC2 RescueBackup = true*
 - b. aws:executeAwsApi - 创建提供的实例的 AMI 备份
 - c. aws:createTags - 标记 AMI 备份
- 23aws:executeAwsApi - 为提供的实例的根卷恢复初始的终止时删除状态
- 24aws:changeInstanceState - 将提供的实例恢复为初始状态 (运行/停止)
- 25aws:deleteStack-删除 EC2救援 CloudFormation 堆栈

输出

runScriptForLinux.Outp

runScriptForWindows. Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSSupport-TroubleshootActiveDirectoryReplication

描述

该AWSSupport-TroubleshootActiveDirectoryReplication运行手册通过检查目标域控制器实例上的常用设置来帮助解决 Microsoft Active Directory (AD) 域控制器复制故障。本运行手册对提供的域控制器实例运行一系列 PowerShell 命令，以检查当前的复制状态并报告可能导致域复制问题的错误。如果复制关键服务 (Netlogon、和KDC) 已停止 RPCSSW32Time，运行手册可以选择启动这些服务，并通过在目标实例w32tm /resync /force上运行来同步系统时间。

Important

AWS 托管 Microsoft AD 不在本运行手册的范围之内。

Important

当自动化在目标实例上运行命令时，会对目标实例文件系统进行更改。这些更改包括创建日志目录 (\$env:ProgramData\TroubleshootActiveDirectoryReplication) 和报告文件。

如何工作？

运行手册执行以下检查和操作：

- 验证目标实例是否运行 Windows 并且由 Systems Manager 管理。
- 运行 PowerShell 脚本以检查 Active Directory 复制配置和状态。
- 检查安全组和网络 ACL 设置是否存在复制伙伴连接。
- 对时间同步和关键服务状态进行故障排除。
- 将日志文件上传到指定的 Amazon S3 存储桶进行分析。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- secretsmanager:GetSecretValue
- ssm:DescribeInstanceInformation

- ssm:SendCommand
- ssm:GetCommandInvocation
- s3:GetBucketAcl
- s3:GetBucketPolicy
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:PutObject

策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "secretsmanager:GetSecretValue",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Secrets Manager 设置

支票复制 PowerShell 脚本通过运行时调用来检索用户名和密码，从而连接到目标 Microsoft Active Directory 域控制器。AWS Secrets Manager按照[创建 AWS Secrets Manager 密钥](#)中的步骤创建新 AWS Secrets Manager 密钥。确保用户名和密码使用一 key/value 对格式存

储{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}。创建密钥后，请确保将 AWS Secrets Manager 机密 ARN 的 `secretsmanager:GetSecretValue` 权限授予目标域控制器 IAM 实例配置文件角色。

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootActiveDirectoryReplication](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选) :
 - 描述：(可选) AWS 身份和访问管理 (IAM) Access Management 角色的亚马逊资源名称 (ARN)，允许系统管理员自动化代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - InstanceId (必填) :
 - 描述：(必填) 您要解决活动目录复制问题的 Amazon EC2 域控制器实例的 ID。请注意，提供的实例必须是域控制器。
 - 类型：AWS::EC2::Instance::Id
 - SecretsManagerArn (必填) :
 - 描述：(必填) 您的 AWS Secrets Manager 密钥的 ARN，其中包含具有企业管理员或访问您的 Active Directory 域和林配置的同等权限的 Active Directory 用户名和密码。确保用户名和密码使用一 key/value 对格式存储 {"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}。确保将机密 ARN 的 `secretsmanager:GetSecretValue` 权限附加到您的目标域控制器 IAM 实例配置文件角色。
 - 类型：String
 - 允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z0-9-]{2,20}:[0-9]{12}:secret:[a-zA-Z0-9]{1}[a-zA-Z0-9\\/_+=.@-]{1,256}$`
 - TimeSync (可选) :

- 描述：(可选) 选择Check或Sync。如果选择Check，运行手册将打印出当前的系统时间同步状态。Sync如果选中，运行手册将尝试通过在目标实例w32tm /resync /force上运行来强制时间重新同步。
 - 类型：String
 - 允许的值：[Check, Sync]
 - 默认值：Check
 - ServiceAction (可选) :
 - 描述：(可选) 选择Check或Fix。如果选择Check，运行手册会打印出Netlogon、Windows Time service (W32Time)Remote Procedure Call (RPC) Service、和Key Distribution Center (KDC)服务的当前状态。如果Fix选中，则运行手册将尝试启动这些服务 (如果有任何服务已停止)。
 - 类型：String
 - 允许的值：[Check, Fix]
 - 默认值：Check
 - LogDestination (必填) :
 - 描述：(必填) 您 AWS 账户中用于上传命令输出的 Amazon S3 存储桶。
 - 类型：String
4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
- assertIfOperatingSystemIsWindows:

检查所提供的目标 Amazon EC2 实例的操作系统是否为 Windows。
 - assertIfInstanceIsSsmManaged:

确保 Amazon EC2 实例由 Systems Manager 管理，否则自动化将结束。
 - 检查复制：

在指定的域控制器实例上运行 PowerShell 脚本以获取 Active Directory 域复制配置和状态。
 - checkInstanceSgAndNACL:

检查与目标域控制器实例关联的安全组和网络 ACL 是否允许发送到复制伙伴的流量。

运行 PowerShell 脚本以排除时间同步和关键服务状态故障。

- `verifys3 BucketPublicStatus` :

检查中指定的 Amazon S3 存储桶是否 `LogDestination` 允许匿名或公开读取或写入访问权限。

- **`runUploadScript`**:

运行 PowerShell 脚本将日志存档上传到 `LogDestination` 参数中指定的 Amazon S3 存储桶，并从操作系统中删除存档的日志文件。日志文件可用于故障排除，也可以在排除复制问题时与 S AWS support 共享。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSPremiumSupport-TroubleshootEC2DiskUsage

描述

`AWSPremiumSupport-TroubleshootEC2DiskUsage` 运行手册可帮助您调查并有可能纠正 Amazon Elastic Compute Cloud (Amazon EC2) 实例根磁盘和非根磁盘使用方面的问题。如果可能，运行手册会尝试通过扩展卷及其文件系统来纠正问题。为执行这些任务，此运行手册会根据受影响实例的操作系统协调执行多个运行手册。

第一个运行手册 (`AWSPremiumSupport-DiagnoseDiskUsageOnWindows` 或 `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`) 确定是否可以通过扩展卷来缓解磁盘问题。

第二个运行手册 (`AWSPremiumSupport-ExtendVolumesOnWindows` 或 `AWSPremiumSupport-ExtendVolumesOnLinux`) 使用第一个运行手册的输出来运行可修改卷的 Python 代码。修改卷后，运行手册会扩展受影响卷的分区和文件系统。

⚠ Important

访问AWSPremiumSupport-*运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持 计划](#)。

本文档是与 AWS Managed Services (AMS) 合作编写的。AMS 可帮助您更高效、更安全地管理 AWS 基础设施。AMS 还提供操作灵活性、增强的安全性和合规性、容量优化和成本节约识别功能。有关更多信息，请参阅 [AWS Managed Services](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- InstanceId

类型：字符串

允许的值：`^i-[a-z0-9]{8,17}$`

说明：(必需) 您的 Amazon EC2 实例的 ID。

- VolumeExpansionEnabled

类型：布尔值

描述：(可选) 用于控制文档是否扩展受影响的卷和分区的标志。

默认：True

- VolumeExpansionUsageTrigger

类型：字符串

描述：(可选) 触发扩展所需的分区空间的最小使用量 (以百分比表示)。

允许的值：^[0-9]{1,2}\$

默认：85

- VolumeExpansionCapSize

类型：字符串

(可选)：(可选) 可以将 Amazon Elastic Block Store (Amazon EBS) 卷增加到的最大大小 (以 GiB 为单位)。

允许的值：^[0-9]{1,4}\$

默认：2048

- VolumeExpansionGibIncrease

类型：字符串

Description (描述)：(可选) 卷容量增加，以 GiB 为单位。VolumeExpansionPercentageIncrease 将使用 VolumeExpansionGibIncrease 和之间最大的净增幅。

允许的值：^[0-9]{1,4}\$

默认值：20

- VolumeExpansionPercentageIncrease

类型：字符串

描述：(可选) 卷的百分比增大。VolumeExpansionPercentageIncrease 将使用 VolumeExpansionGibIncrease 和之间最大的净增幅。

允许的值：^[0-9]{1,2}\$

默认值：20

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeVolumes
- ec2:DescribeVolumesModifications
- ec2:ModifyVolume
- ec2:DescribeInstances
- ec2:CreateImage
- ec2:DescribeImages
- ec2:DescribeTags
- ec2:CreateTags
- ec2>DeleteTags
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationExecutions
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations

文档步骤

1. aws:assertAwsResourceProperty - 检查实例是否由 Systems Manager 管理
2. aws:executeAwsApi - 描述要获取平台的实例。
3. aws:branch - 根据实例平台对自动化进行分支。

- a. 如果实例是 Windows :
 - i. `aws:executeAutomation` - 运行 `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` 运行手册以诊断实例上的磁盘使用问题。
 - ii. `aws:executeAwsApi` - 获取上一个自动化的输出。
 - iii. `aws:branch` - 根据诊断结果进行分支，以及是否存在可以扩展以缓解警报的音量。
 - A. 没有需要扩展的卷：结束自动化。
 - B. 以下是需要扩展的卷：
 - I. `aws:executeAwsApi` - 创建实例的 Amazon Machine Image (AMI)。
 - II. `aws:waitForAwsResourceProperty` - 等待 AMI 状态变为 `available`。
 - III. `aws:executeAutomation` - 运行 `AWSPremiumSupport-ExtendVolumesOnWindows` 运行手册以执行卷修改以及在操作系统 (OS) 中执行使新空间可用的所需步骤。
- b. (平台不是窗口) 如果输入实例不是 Windows :
 - i. `aws:executeAutomation` - 运行 `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` 运行手册以诊断实例上的磁盘使用问题。
 - ii. `aws:executeAwsApi` - 获取上一个自动化的输出。
 - iii. `aws:branch` - 根据诊断结果进行分支，以及是否存在可以扩展以缓解警报的音量。
 - A. 没有需要扩展的卷：结束自动化。
 - B. 以下是需要扩展的卷：
 - I. `aws:executeAwsApi` - 创建实例的 AMI。
 - II. `aws:waitForAwsResourceProperty` - 等待 AMI 状态变为 `available`。
 - III. `aws:executeAutomation` - 运行 `AWSPremiumSupport-ExtendVolumesOnLinux` 运行手册以执行卷修改以及在操作系统中执行使新空间可用所需的步骤。

输出

`diagnoseDiskUsageAlertOnWindows`。输出

`extendVolumesOnWindows`。Output

`diagnoseDiskUsageAlertOnLinux`。输出

`extendVolumesOnLinux`。Output

Backup AMILinux。ImageId

Backup AMI Windows。 ImageId

AWSsupport-TroubleshootEC2InstanceConnect

描述

AWSsupport-TroubleshootEC2InstanceConnect 自动化有助于分析和检测阻止使用 Amazon EC2 Instance Connect 连接到亚马逊弹性计算云 (Amazon EC2) 实例的错误。它可以识别由不支持的 Amazon 系统映像 (AMI)、缺少 OS-level 软件包安装或配置、缺少 AWS Identity and Access Management (IAM) 权限或网络配置问题导致的问题。

如何工作？

该运行手册采用 IAM 角色或在 Amazon EC2 Instance Connect 中遇到问题的用户的 Amazon EC2 实例 ID、用户名、连接模式、源 IP CIDR、SSH 端口和亚马逊资源名称 (ARN)。然后，它会检查使用 Amazon EC2 Instance Connect 连接到 Amazon EC2 实例的[先决条件](#)：

- 实例正在运行且处于正常状态。
- 该实例位于 Amazon EC2 Instance Connect 支持的 AWS 区域。
- Amazon EC2 Instance Connect 支持该实例的 AMI。
- 该实例可以访问实例元数据服务 (imds v2)。
- Amazon EC2 Instance Connect 软件包已在操作系统级别正确安装和配置。
- 网络配置（安全组、网络 ACL 和路由表规则）允许通过 Amazon EC2 Instance Connect 连接到实例。
- 用于利用 Amazon EC2 Instance Connect 的 IAM 角色或用户有权将密钥推送到 Amazon EC2 实例。

Important

- 要检查实例 AMI、imds v2 的可访问性和 Amazon EC2 Instance Connect 软件包的安装，该实例必须由 SSM 托管。否则，它会跳过这些步骤。有关更多信息，请参阅[为什么我的 Amazon EC2 实例没有显示为托管节点](#)。
- 只有将 SourceIp CIDR 作为输入参数提供时，网络检查才会检测安全组和网络 ACL 规则是否会阻止流量。否则，它只会显示 SSH-related 规则。
- 本运行手册中未验证使用 [Amazon EC2 Instance Connect 终端节点](#) 的连接。

- 对于私有连接，自动化不会检查源计算机上是否安装了 SSH 客户端，以及它是否可以访问实例的私有 IP 地址。

文档类型

自动化

所有者

Amazon

平台

Linux

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand

说明

按照这些步骤对自动化进行配置：

1. 导航到 AWS Systems Manager 控制台 [AWSsupport-TroubleshootEC2InstanceConnect](#) 中的。

2. 选择 Execute automation (执行自动化) 。

3. 对于输入参数，请输入以下内容：

- InstanceId (必填)：

您无法使用 Amazon EC2 Instance Connect 连接到的目标 Amazon EC2 实例的 ID。

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表你执行操作的 IAM 角色的 ARN。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 用户名 (必填)：

用于使用 Amazon EC2 Instance Connect 连接到亚马逊 EC2 实例的用户名。它用于评估是否向该特定用户授予 IAM 访问权限。

- EC2InstanceConnectRoleOrUser (必填)：

利用 Amazon EC2 Instance Connect 向实例推送密钥的 IAM 角色或用户的 ARN。

- sshPort (可选)：

在 Amazon EC2 实例上配置的 SSH 端口。默认值为 22。端口号必须介于1-65535。

- SourceNetworkType (可选)：

Amazon EC2 实例的网络访问方法：

- 浏览器：您可以从 AWS 管理控制台进行连接。
- 公用：您通过 Internet 连接到位于公有子网中的实例（例如，您的本地计算机）。
- 私有：您通过实例的私有 IP 地址进行连接。
- SourceIpCIDR (可选)：

源 CIDR，包括您将使用 Amazon EC2 Instance Connect 登录的设备（例如您的本地计算机）的 IP 地址。示例：172.31.48。6/32。如果公有或私有访问模式未提供任何值，则运行手册将不会评估 Amazon EC2 实例安全组和网络 ACL 规则是否允许 SSH 流量。它将改为显示 SSH-related 规则。

Input parameters	
InstanceId (Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect. ☒ Show interactive instance picker	
AWS::EC2::instance::Id	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	Username (Required) The username used to connect to the EC2 instance using EC2 Instance Connect. It is used to evaluate if IAM access is granted for this particular user.
String	String
EC2InstanceConnectRoleOrUser (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role or user that is being used to leverage EC2 Instance Connect and push keys to the instance.	SSHPort (Optional) The SSH port configured on the EC2 instance. Default value is '22'. The port number must be between '1-65535'.
String	22
SourceNetworkType (Optional) The network access method to the EC2 instance: "Browser" : you are connecting to the EC2 instance using your browser by clicking the connect button from the console. "Public" : you are accessing the EC2 instance located in a public subnet over the Internet (example: from your local computer). "Private" : you are connecting to your instance through its private IP address.	SourceIpCIDR (Optional) The source CIDR that includes the IP address of the device you will be logging from using EC2 Instance Connect (such as your local computer). Example: 172.31.48.0/20.
Browser	None

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- AssertInitialState:

确保 Amazon EC2 实例的状态处于运行状态。否则，自动化将结束。

- GetInstanceProperties:

获取当前 Amazon EC2 实例的属性 (PlatformDetails PublicIpAddress VpcId、 SubnetId 和 MetadataHttpEndpoint)。

- GatherInstanceInformationFromSSM:

如果该实例由 SSM 托管，则获取 Systems Manager 实例的 ping 状态和操作系统详细信息。

- CheckIfAWSRegionSupported:

检查 Amazon EC2 实例是否位于 Amazon EC2 Instance Connect 支持的 AWS 区域。

- BranchOnIfAWSRegionSupported:

如果 Amazon EC2 Instance Connect 支持该区域，则继续执行。否则，它会创建输出并退出自动化。

- CheckIfInstanceAMIsSupported:

检查 Amazon EC2 Instance Connect 是否支持与该实例关联的 AMI。

- BranchOnIfInstanceAMIsSupported:

如果支持实例 AMI，它将执行 OS-level 检查，例如元数据可访问性以及 Amazon EC2 Instance Connect 软件包的安装和配置。否则，它会使用 AWS API 检查是否启用了 HTTP 元数据，然后进入网络检查步骤。

- CheckIMDSReachabilityFromOs:

在目标 Amazon EC2 Linux 实例上运行 Bash 脚本以检查它是否能够访问 imdsv2。

- CheckEICPackageInstallation:

在目标 Amazon EC2 Linux 实例上运行 Bash 脚本，以检查 Amazon EC2 Instance Connect 软件包是否已正确安装和配置。

- CheckSSHConfigFromOs:

在目标 Amazon EC2 Linux 实例上运行 Bash 脚本，以检查配置的 SSH 端口是否与输入参数 “sshPort” 相匹配。

- CheckMetadataHTTPEndpointIsEnabled:

检查实例元数据服务 HTTP 端点是否已启用。

- CheckEICNetworkAccess:

检查网络配置（安全组、网络 ACL 和路由表规则）是否允许通过 Amazon EC2 Instance Connect 连接到实例。

- CheckIAMRoleOrUserPermissions:

检查用于利用 Amazon EC2 Instance Connect 的 IAM 角色或用户是否有权使用提供的用户名将密钥推送到 Amazon EC2 实例。

- MakeFinalOutput:

合并所有先前步骤的输出。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

目标实例具有所有必需先决条件的执行：

▼ Outputs

```
MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
SUCCESS: The instance AMI 'Ubuntu 22.04' is supported by EC2 Instance Connect

### Checking if Instance Metadata service (IMDSv2) is reachable ###
SUCCESS: Instance metadata is reachable.

### Checking if EC2 Instance Connect package is installed and configured on the instance: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-set-up.html ###
SUCCESS: 'ec2-instance-connect' package is installed
SUCCESS: 'ec2-instance-connect' is properly configured

|

### Checking SSH configuration at the OS-level ###
WARNING: If you configured a firewall in the EC2 instance make sure that it allows SSH traffic from the source ip CIDR
INFO: SSH is configured to listen on port 22.
SUCCESS: The configured SSH port (22) matches the provided input port (22).

### Checking Network configuration requirements to access the instance through EC2 Instance Connect using 'Browser' access mode and port '22' ###
SUCCESS: The instance has a public IPv4 address.
SUCCESS: Subnet subnet-██████████ is public.
SUCCESS: SSH access is allowed by security group id 'sg-██████████'
SUCCESS: 'Inbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: 'Outbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: Network requirements to connect to the instance 'i-██████████' using EC2 instance connect are satisfied

### Checking if the required permissions are granted to the IAM identity 'arn:aws:iam:██████████:role/Admin' used to connect to the instance 'i-██████████' through EC2 Instance Connect with the username 'ubuntu' ###
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:DescribeInstances' access permission
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:SendSSHPublicKey' access permission
```

在不支持目标实例的 AMI 的情况下执行：

▼ Outputs

```
MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
ERROR: The instance AMI 'SLES 15.5' is not supported by EC2 Instance Connect. Please make sure to use one of the AMIs listed here: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html#ec2-prereqs-ami:
```

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

AWS 服务文档

- [如何解决使用 Amazon EC2 Instance Connect 连接到我的 Amazon EC2 实例的问题？](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

描述

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs` 自动化运行手册用于检测在 Linux 服务器中安装 AWS Transform MGN (AWS MGN) 和 AWS 弹性灾难恢复 (AWS DRS) 复制代理以将源服务器迁移到云端时的常见错误。AWS

如何工作？

运行手册 `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs` 采用亚马逊简单存储服务 (Amazon S3) Service 路径，其中 AWS 将 MGN AWS 或 DRS 安装 `aws_replication_agent_installer.log` 日志作为参数上传。然后，它会执行以下任务：

- 验证：检查提供的日志文件是否有效以及其中是否包含至少一个代理安装。
- 解析：彻底解析日志文件中最新安装的代理，以查找已知的 AWS MGN 或 AWS DRS 错误。
- 错误检测 and 解决：根据解析，它会检测并列出代理安装过程中出现的任何错误或问题。对于检测到的每个错误，运行手册都提供了帮助解决或缓解问题的详细步骤。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `s3:GetObject`
- `s3:ListBucket`

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName (必填)：

存储复制代理日志的 Amazon S3 存储桶的名称。

- S3ObjectKey (必填)：

存储复制代理安装程序日志文件的 Amazon S3 对象的密钥。示例：如果 Amazon S3 的 URI 是 `s3://bucket_name/path/to/file/aws_replication_agent_installer.log`，则您应该输入 `path/to/file/aws_replication_agent_installer.log`。

- ServiceName (必填)：

为其安装了复制代理的服务的名称。允许的值：AWS MGN 或 AWS DRS

Input parameters

AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. 	BucketName (Required) The name of the Amazon S3 bucket where the replication agent log is stored. s3bucket-name 
S3ObjectKey (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is `s3://bucket_name/path/to/file/aws_replication_agent_installer.log` then you should provide `path/to/file/aws_replication_agent_installer.log` as input. aws_replication_agent_installer.log	ServiceName (Required) The name of the service for which the Replication agent is done: **AWS MGN** : AWS Application Migration Service. **AWS DRS** : AWS Elastic Disaster Recovery. AWS MGN

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- **ValidateInput**

使用提供的 Amazon S3 存储桶名称和对象路径确保复制代理日志文件有效且可访问，然后返回最新代理安装的字节号。

- **CheckReplicationAgentLogErrors**

从最新的安装字节开始读取复制代理日志文件并搜索已知的 AWS MGN 或 AWS DRS 错误。

- **MakeFinalOutput**

创建先前检查的输出，包括有关发现的错误和故障排除建议的信息。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

▼ Outputs

```
MakeFinalOutput.Output
### Input Validation Step ###

✅ The replication agent log file is valid and accessible using the provided S3 path.

### Log file error checking results ###

❌ Detected error: Kernel development package for ██████████ are missing from repositories

✅ Recommendations and troubleshooting steps:

During agent installation, the installer downloads a matching "kernel-devel/linux-headers" package from the repository configured in your Linux operating system.
This error occurs when the agent installation workflow can't install the matching "kernel-devel/linux-headers" package to the Linux OS current running kernel.

1. Check the current kernel version on the source server:

$ sudo uname -r

2. Make sure to install the version that corresponds exactly to the current kernel version that you are running (displayed in the output of "sudo uname -r" command).

Use the following commands to install "kernel-devel/linux-headers" package for the running kernel:

+ For all Red Hat and CentOS source servers:

$ sudo yum install kernel-devel-`uname -r`

+ For all Ubuntu/Debian source servers:

$ sudo apt-get install linux-headers-`uname -r`

+ For all SUSE source servers:

$ sudo zypper install kernel-default-devel-`uname -r`

Note: When the "kernel-devel/linux-headers" packages are installed for both the running kernel and other installed kernels, you will find the following directories generated for each installed kernel.
They are located under "/usr/src/kernels" for all Red Hat-based operating systems and under "/usr/src" for Ubuntu and Debian-based operating systems:

$ sudo ls -la /usr/src/kernels

$ sudo ls -la /usr/src

3. Sometimes, you will find that the "kernel-devel/linux-headers" package for the running kernel is not available in your server repositories.
In that case, you have three options:
```

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSsupport-TroubleshootRDP

描述

AWSSupport-TroubleshootRDP 运行手册允许用户检查或修改目标实例上可能影响远程桌面协议 (RDP) 连接的常规设置，如 RDP 端口、网络层身份验证 (NLA) 和 Windows 防火墙配置文件。(可选) 如果用户明确允许进行离线修复，则可以通过停止和启动实例来离线应用更改。默认情况下，此运行手册读取和输出这些设置的值。

Important

在使用此运行手册之前，应仔细检查对 RDP 设置、RDP 服务和 Windows 防火墙配置文件的更改。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- 操作

类型：字符串

有效值：CheckAll | FixAll | 自定义

默认值：Custom

描述：(可选) [自定义] 使用“防火墙”、“操作”RDPService StartupType、“RDPService操作”、“RDPPort操作”和“NLASetting操作”中的值RemoteConnections 来管理设置。[CheckAll] 读取设置的值而不进行更改。[FixAll] 恢复 RDP 默认设置，然后禁用 Windows 防火墙。

- AllowOffline

类型：字符串

有效值：true | false

默认：false

说明：(可选) 仅修复 - 如果当在线故障排除失败或提供的实例不是托管实例时允许进行离线 RDP 修复，请将其设置为 true。注意：对于离线修复，SSM Automation 会停止实例，并在尝试任何操作前创建一个 AMI。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 防火墙

类型：字符串

有效值：Check | 禁用

默认值：Check

说明：(可选) 检查或禁用 Windows 防火墙 (所有配置文件)。

- InstanceId

类型：字符串

说明：(必需) 要对其 RDP 设置进行故障排除的实例的 ID。

- NLASetting 操作

类型：字符串

有效值：Check | 禁用

默认值：Check

说明：(可选) 检查或禁用网络层身份验证 (NLA)。

- RDPPort 操作

类型：字符串

有效值：Check | 修改

默认值：Check

说明：(可选) 检查用于 RDP 连接的当前端口，或将 RDP 端口修改回 3389 并重启服务。

- RDPService 操作

类型：字符串

有效值：Check | 启动 | 重启 | 强制重启

默认值：Check

描述：(可选) 检查、启动、重新启动或强制重启 RDP 服务 ()。TermService

- RDPServiceStartupType

类型：字符串

有效值：Check | 自动

默认值：Check

说明：(可选) 检查或设置 RDP 服务在 Windows 启动时自动启动。

- RemoteConnections

类型：字符串

有效值：Check | 启用

默认值：Check

描述：(可选) 要对 fDeny TSConnections 设置执行的操作：选中，启用。

- S3 BucketName

类型：字符串

说明：(可选) 仅离线 - 您账户中用于上传故障排除日志的 S3 存储桶的名称。请确保存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

类型：字符串

默认：SelectedInstanceSubnet

描述：（可选）仅限脱机-用于执行离线故障排除的 EC2 Rescue 实例的子网 ID。如果未指定子网 ID，AWS Systems Manager 自动化将创建一个新的 VPC。重要：子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议接收命令的 EC2 实例具有 IAM 角色并附有 Amazon A SSManagedInstanceCoreamazon 托管策略。要进行在线修复，用户必须至少有 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution 和 ssm: SendCommand 才能运行自动化并将命令发送到实例，还必须有 ssm: GetAutomationExecution 才能读取自动化输出。要进行离线修复，用户必须至少具有 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution、ec2: 和 ssm: DescribeInstances，GetAutomationExecution 才能读取自动化输出。AWSSupport-TroubleshootRDP调用AWSSupport-ExecuteEC2Rescue以执行离线修复-请查看的权限AWSSupport-ExecuteEC2Rescue以确保您可以成功运行自动化。

文档步骤

1. aws:assertAwsResourceProperty-检查实例是否是 Windows Server 实例
2. aws:assertAwsResourceProperty - 检查实例是否为托管实例
3. （在线故障排除）如果实例为托管实例，则：
 - a. aws:assertAwsResourceProperty - 检查提供的操作值
 - b. （在线检查）如果动作 = CheckAll，那么：

aws:runPowerShellScript-运行 PowerShell 脚本以获取 Windows 防火墙配置文件状态。

aws:executeAutomation - 调用 AWSSupport-ManageWindowsService 以获取 RDP 服务状态。

aws:executeAutomation - 调用 AWSSupport-ManageRDPSettings 以获取 RDP 设置。

- c. （在线修复）如果动作 = FixAll，那么：

aws:runPowerShellScript-运行 PowerShell 脚本以禁用所有 Windows 防火墙配置文件。

`aws:executeAutomation` - 调用 `AWSSupport-ManageWindowsService` 以启动 RDP 服务。

`aws:executeAutomation` - 调用 `AWSSupport-ManageRDPSettings` 以启用远程连接并禁用 NLA。

d. (在线管理) 如果 `Action = Custom` , 则 :

`aws:runPowerShellScript`-运行 PowerShell 脚本以管理 Windows 防火墙配置文件。

`aws:executeAutomation` - 调用 `AWSSupport-ManageWindowsService` 以管理 RDP 服务。

`aws:executeAutomation` - 调用 `AWSSupport-ManageRDPSettings` 以管理 RDP 设置。

4. (离线修复) 如果实例并非托管实例 , 则 :

a. `aws:assertAwsResourceProperty`-断言 `AllowOffline = 真`

b. `aws:assertAwsResourceProperty`-断言操作 = `FixAll`

c. `aws:assertAwsResourceProperty`-断言的价值 `SubnetId`

(使用提供的实例的子网) 如果 `SubnetId` 为 `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi` - 检索当前实例的子网。

`aws:executeAutomation` - 使用提供的实例的子网运行 `AWSSupport-ExecuteEC2Rescue`。

d. (使用提供的自定义子网) 如果未选中 `SELECTED_INSTANCE_SUBNET`

`aws:executeAutomation-AWSSupport-ExecuteEC2Rescue` 使用提供的 `SubnetId`值运行。

输出

`manageFirewallProfiles`。输出

管理 `RDPService` 设置。输出

管理 `RDPSettings` .Output

`checkFirewallProfiles`。输出

检查RDPService设置。输出

检查 RDPSettings .Output

disableFirewallProfiles。输出

恢复默认设置RDPService。输出

恢复默认. RDPSettings Output

疑难解答RDPOffline。输出

疑难解答RDPOfflineWithSubnetId。输出

AWSSupport-TroubleshootSSH

描述

AWSSupport-TroubleshootSSH运行手册安装适用于 Linux 的 Amazon EC2 Rescue 工具，然后使用 EC2救援工具检查或尝试修复阻止通过 SSH 远程连接到 Linux 计算机的常见问题。（可选）如果用户明确允许进行离线修复，则可以通过停止和启动实例来离线应用更改。默认情况下，运行手册以只读模式运行。

[运行此自动化（控制台）](#)

有关使用 AWSSupport-TroubleshootSSH 运行手册的信息，请参阅来自 AWS Premium Support 的此 [AWSSupport-TroubleshootSSH故障排除主题](#)。

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- 操作

类型：字符串

有效值：CheckAll | FixAll

默认：CheckAll

说明：(必需) 指定只检查而不修复问题还是检查并自动修复任何发现的问题。

- AllowOffline

类型：字符串

有效值：true | false

默认：false

说明：(可选) 仅修复 - 如果当在线故障排除失败或提供的实例不是托管实例时允许进行离线 SSH 修复，请将其设置为 true。注意：对于离线修复，SSM Automation 会停止实例，并在尝试任何操作前创建一个 AMI。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 您的 Linux 版 EC2 实例的 ID。

- S3 BucketName

类型：字符串

说明：(可选) 仅离线 - 您账户中用于上传故障排除日志的 S3 存储桶的名称。请确存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

类型：字符串

默认：SelectedInstanceSubnet

描述：（可选）仅限脱机-用于执行离线故障排除的 EC2 Rescue 实例的子网 ID。如果未指定子网 ID，AWS Systems Manager Automation 将创建一个新的 VPC。

 Important

子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议接收命令的 EC2 实例具有 IAM 角色并附有 Amazon A SSManagedInstanceCoreamazon 托管策略。要进行在线修复，用户必须至少有 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution 和 ssm: SendCommand 才能运行自动化并将命令发送到实例，还必须有 ssm: GetAutomationExecution 才能读取自动化输出。要进行离线修复，用户必须至少有 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution、ec2: DescribeInstances，GetAutomationExecution才能读取自动化输出。AWSSupport-TroubleshootSSH调用AWSSupport-ExecuteEC2Rescue以执行离线修复-请查看的权限AWSSupport-ExecuteEC2Rescue以确保您可以成功运行自动化。

文档步骤

1. aws:assertAwsResourceProperty - 检查实例是否为托管实例

a. （在线修复）如果实例为托管实例，则：

- i. aws:configurePackage-通过安装适用于 Linux 的 EC2救援AWS-ConfigureAWSPackage。
- ii. aws:runCommand-运行 bash 脚本运行 Linux 版 R EC2 rescue。

b. （离线修复）如果实例并非托管实例，则：

- i. aws:assertAwsResourceProperty-断言 AllowOffline = 真
- ii. aws:assertAwsResourceProperty-断言操作 = FixAll
- iii. aws:assertAwsResourceProperty-断言的价值 SubnetId

- iv. (使用提供的实例的子网) SubnetId 如果SelectedInstanceSubnet 我们aws:executeAutomation要使用提供的实例的子网运行AWSSupport-ExecuteEC2Rescue。
- v. (使用提供的自定义子网) SubnetId If 不SelectedInstanceSubnet aws:executeAutomationAWSSupport-ExecuteEC2Rescue使用提供的SubnetId 值运行。

输出

troubleshootSSH.Output

疑难解答SSHOffline。输出

疑难解答SSHOfflineWithSubnetId。输出

AWSSupport-TroubleshootSUSERegistration

描述

该AWSSupport-TroubleshootSUSERegistration运行手册可帮助您确定注册亚马逊弹性计算云 (Amaz EC2 on) 的原因 SUSE Linux Enterprise Server 具有 SUSE 更新基础设施的实例失败。此自动化输出提供了解决问题或帮助您排查问题的步骤。如果实例在自动化期间通过了所有检查，该实例将注册到 SUSE Update Infrastructure。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 您要执行故障排除的 Amazon EC2 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:DescribeInstanceProperties
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:ListCommands

文档步骤

- aws:assertAwsResourceProperty-检查 Amazon EC2 实例是否由管理 AWS Systems Manager。
- aws:runCommand-检查 Amazon EC2 实例平台是否为 SLES。
- aws:runCommand - 检查软件包 cloud-regionsrv-client 版本是否高于或等于所需的版本 9.0.10。
- aws:runCommand - 检查基础产品的符号链接是否损坏，并在链接损坏时修复链接。
- aws:runCommand - 检查主机文件 (/etc/hosts) 是否包含 smt-ec2-suscloud.net 的记录。自动化将删除所有重复的条目。
- aws:runCommand - 检查 curl 命令是否已安装。
- aws:runCommand-检查亚马逊 EC2 实例是否可以访问实例元数据服务 (IMDS) 地址 169.254.169.254。

- `aws:runCommand`-检查 Amazon EC2 实例是否有账单代码或 AWS Marketplace 产品代码。
- `aws:runCommand`-检查 Amazon EC2 实例是否可以通过 HTTPS 访问至少 1 台区域服务器。
- `aws:runCommand`-检查 Amazon EC2 实例是否可以通过 HTTP 访问订阅管理工具 (SMT) 服务器。
- `aws:runCommand`-检查亚马逊 EC2 实例是否可以通过 HTTPS 访问订阅管理工具 (SMT) 服务器。
- `aws:runCommand`-检查亚马逊 EC2 实例是否可以通过 HTTPS 到达该 `smt-ec2.susecloud.net` 地址。
- `aws:runCommand`-向 SUSE 更新基础设施注册 Amazon EC2 实例。
- `aws:executeScript` - 收集并输出所有先前步骤的输出。

AWSSupport-TroubleshootWindowsPerformance

描述

该运行手册 `AWSSupport-TroubleshootWindowsPerformance` 有助于解决亚马逊弹性计算云 (Amazon EC2) Windows 实例上持续存在的性能问题。运行手册从目标实例捕获日志，并分析 CPU、内存、磁盘和网络性能指标。或者，自动化可以捕获进程转储，以帮助确定性能下降的潜在原因。如果您允许安装此运行手册，则自动化还会使用最新的 [EC2Rescue](#) 工具捕获事件和系统日志。

如何工作？

运行手册执行以下步骤：

- 检查 Amazon EC2 实例的先决条件。
- 在 Amazon EC2 Windows 实例的根磁盘中生成性能日志
- 将捕获的日志存储在文件夹中 `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- 如果提供了亚马逊简单存储服务 (Amazon S3) Service 存储桶，并且自动代入角色具有所需的权限，则捕获的日志将上传到 Amazon S3 存储桶。
- 将最新 `EC2Rescue` 工具安装到 Amazon EC2 Windows 实例，用于捕获事件和系统日志（如果您选择安装），但它不会分析所捕获的进程转储和日志 `EC2Rescue`。

Important

- 要执行本运行手册，Amazon EC2 Windows 实例必须由 AWS Systems Manager 管理。有关更多信息，请参阅 [为什么我的 Amazon EC2 实例没有显示为托管节点](#)。

- 要执行本运行手册，Amazon EC2 Windows 实例必须在 Windows 8.1/ Windows Server 2012 R2 (6.3) 或更高版本上运行 PowerShell 4.0 或更高版本。有关更多信息，请参阅 [Windows 操作系统版本](#)。
- 要生成性能日志，根设备上至少需要 10 GB 的可用空间。如果根磁盘大于 100 GB，则可用空间必须大于磁盘大小的 10%。如果您在执行过程中转储进程，则可用空间必须大于 10 GB，再加上该进程消耗的内存总量（当该进程消耗的内存超过 10 GB 时）。
- 根设备上生成的日志不会自动删除。
- 运行手册不会卸载该EC2Rescue工具。有关更多信息，请参阅[用EC2Rescue于 Windows 服务器](#)。
- 最佳做法是在性能影响期间运行此自动化。您也可以使用 AWS Systems Manager 状态管理器关联或通过安排 AWS Systems Manager 维护窗口来定期运行它。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ec2:DescribeInstances`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`

- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `s3:ListBucket`
- `s3:GetEncryptionConfiguration`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:GetAccountPublicAccessBlock`

(可选) 在实例配置文件上附加的 IAM 角色或在实例上配置的 IAM 用户需要执行以下操作才能将日志上传到为参数指定的 Amazon S3 存储桶 `LogUploadBucketName` :

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

说明

按照这些步骤对自动化进行配置 :

1. [AWSSupport-TroubleshootWindowsPerformance](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：

- `AutomationAssumeRole` (可选) :

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `InstanceId` (必填) :

您要在其中运行自动化的目标 Amazon EC2 Windows 实例的 ID。该实例必须由 Systems Manager 管理才能执行自动化。

- `CaptureProcessDump` (可选) :

要捕获的进程转储类型。自动化可以为可能在自动化开始时造成性能影响的流程捕获一个进程转储。实例根卷需要至少 10 GB 的可用空间 (当根卷大小大于 100 GB 时，需要大于磁盘大小的 10%；如果进程消耗的内存超过 10 GB，则需要加上 10 GB 加上进程消耗的总内存大小)。

- **LogCaptureDuration** (可选) :

问题出现时，此自动化将捕获日志的分钟数，介于1和15之间。默认值为 5。

- **LogUploadBucketName** (可选) :

您账户中您要上传日志的 Amazon S3 存储桶。存储桶必须配置服务器端加密 (SSE)，并且存储桶策略不得向不需要访问捕获日志的各方授予不必要的 read/write 权限。亚马逊 EC2 Windows 实例必须有权访问亚马逊 S3 存储桶。

- **InstallEC2RescueTool** (可选) :

设置为Yes允许运行手册安装该EC2Rescue工具的最新版本以捕获 Windows 事件和系统日志。默认值为 No。

- **致谢** (必填) :

阅读本自动化操作手册所执行操作的完整详细信息，如果您同意，请键入Yes, I understand and acknowledge。

Input parameters	
InstanceId (Required) The ID of the Amazon EC2 Windows instance you want to troubleshoot performance issues. ☒ Show interactive instance picker AWS::EC2::Instance::Id	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. 	CaptureProcessDump (Optional) The process dump type to capture. The automation can capture one process dump for the process which is potentially causing the performance impact in the beginning of the automation. The instance root volume will require to have at least 10 GB free space (greater than 10% of the disk size when the root volume size is bigger than 100 GB and 10GB plus the total memory size consumed by the process when the process consumes more than 10GB memory). None
LogCaptureDuration (Optional) The number of minutes this automation should capture logs while the issue is present. Default is '5' minutes. You can specify a value between '1' and up to '15' minutes. 5	LogUploadBucketName (Optional) The Amazon S3 bucket in your account to upload the logs to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.
InstallEC2RescueTool (Optional) Set it to 'True' if you allow the runbook to install the latest version of the 'EC2Rescue' tool to capture the Windows Events and System logs. Default value 'No'. No	Acknowledgement (Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps. String

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **CheckConcurrency:**

确保只有一次针对该实例执行此运行手册。如果运行手册发现另一个针对同一实例的执行，它将返回错误并结束。

- **AssertInstanceIsWindows:**

断言 Amazon EC2 实例在 Windows 操作系统上运行。否则，自动化将结束。

- **AssertInstanceIsManagedInstance:**

断言 Amazon EC2 实例由管理。AWS Systems Manager 否则，自动化将结束。

- **VerifyPrerequisites:**

验证实例操作系统上的 PowerShell 版本，并确保可以通过 Systems Manager 连接实例以运行 PowerShell 命令。此自动化支持在 Windows 8.1 /Server 2012 R2 (6.3) 或更高版本上运行 PowerShell 4.0 及更高版本。如果版本较旧，则自动化将失败。当您选择将日志上传到 Amazon S3 存储桶时，此自动操作会检查“AWS 工具”PowerShell 模块是否可用。否则，自动化将结束。

- **BranchOnProcessDump:**

分支取决于您是否将其设置为捕获影响性能的进程的转储。

- **CaptureProcessDump:**

检查实例是否有足够的空间来运行此自动化（当您选择“最高 CPU /内存”时）。

- **CapturePerformanceLogs:**

再次检查磁盘空间并在实例上运行 PowerShell 脚本以创建 perfmon 计数器并启动性能监视器和 Windows 性能记录器日志记录。脚本在满足定义 LogCaptureDuration 后停止。

- **SummarizePerformanceLogs:**

汇总上一步生成的 XML 报告 CapturePerformanceLogs，找出自动化输出中显示的消耗最多 WorkingSet 64（内存）和处理器时间（CPU）百分比的负责进程。它会生成类似的网络接口、内存 LogicalDisk、TCPv4、IPv4 和 UDPv4 的使用信息，并将其保存到 analysis_output.log 输出文件夹中。

- **BranchOnInstallEC2Rescue:**

分支（如果您将其设置为在 Amazon EC2 实例中安装最新 EC2Rescue 工具）。

- **InstallEC2RescueTool:**

在实例操作系统中安装该EC2Rescue工具以使用捕获EC2Rescue日志AWS-ConfigureAWSPackage。

- **RunEC2RescueTool:**

在实例操作系统中运行该EC2Rescue工具以捕获所需的所有日志。EC2Rescue仅捕获所需的日志以节省空间。

- **BranchOnIfS3BucketProvided:**

根据用户的输入进行分支LogUploadBucketName，以查看是否有可用于上传日志的存储桶名称。

- **GetS3BucketPublicStatus:**

确定是否提供了 Amazon S3 存储桶，如果提供，则确认该 Amazon S3 存储桶不是公有的，并且已使用 SSE 进行配置。

- **UploadLogResult:**

将日志上传到提供的 Amazon S3 存储桶。如果 PowerShell 版本为 5.0 或更高版本，它会将日志压缩为 ZIP 存档并上传。它会在上传完成后删除 ZIP 文件。如果 PowerShell 版本低于 5.0，则会将文件直接上传到文件夹。

- **CleanUpLogsOnFailure:**

当步骤失败时，清除该CapturePerformanceLogs步骤生成的所有日志。如果 SSM 代理无法正常工作或 Windows 系统没有响应，则该CleanUpLogsOnFailure步骤可能会失败或超时。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

在目标实例具有所有必需先决条件的情况下执行。

▼ Outputs

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance [REDACTED] was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance [REDACTED]
Data Collector Set TroubleshootWindowsPerformance [REDACTED] created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance [REDACTED]
Data Collector Set TroubleshootWindowsPerformance [REDACTED] started successfully.
Current CPU usage is '54.73%' and Memory usage is '17.15%'
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.
Starting Windows Performance Recording (WPR) capture process.
Stopping WPR capture process.
WPR capture process is in 'Stopped' state.
The Data Collector Set TroubleshootWindowsPerformance [REDACTED] is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance [REDACTED] has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance [REDACTED]
Data Collector Set TroubleshootWindowsPerformance [REDACTED] deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\ [REDACTED]
The captured log files will not be deleted by this automation, please manually delete it after analysis.
|

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\ [REDACTED]_EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.

Process	Counter	Min %	Max %	Avg %
sppsv	Processor	0.00	106.00	9.00
WmiPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenVulObj	Processor	0.00	30.00	0.28
svchost#42	Processor	0.00	29.00	0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):

Process	Counter	Min MB	Max MB	Avg MB
MsMpEng	WorkingSet	220.00	260.00	236.00
Registry	WorkingSet	78.00	193.00	120.00
powershell	WorkingSet	90.00	92.00	92.00
LogonUI	WorkingSet	43.00	43.00	43.00
dwm	WorkingSet	38.00	38.00	38.00

目标实例在 Linux 平台上执行且执行失败。您可以选择步骤 ID 以查看失败详情。

▼ Outputs

CapturePerformanceLogs.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output

No output available yet because the step is not successfully executed

VerifyPrerequisites.Output

No output available yet because the step is not successfully executed

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

No output available yet because the step is not successfully executed

UploadLogResult.Output

No output available yet because the step is not successfully executed

Execution status

Overall status

🔴 Failed

Failed

1

All executed steps

2

Cancelled

0

Succeeded

1

TimedOut

0

Executed steps (2)

Find Steps

1

Step ID	Step #	Step name	Action	Status	Start time	End time
[REDACTED]	1	CheckConcurrency	aws:executeScript	🟢 Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
[REDACTED]0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	🔴 Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

步骤的失败详情AssertInstanceIsWindows。

Failure details

 **Failure message**
Step fails when it is Execute/Cancelling action. Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows']. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

FailureType	FailureStage
Verification	Invocation
VerificationErrorMessage	
Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].	

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSSupport-TroubleshootWindowsUpdate

描述

该AWSSupport-TroubleshootWindowsUpdate运行手册用于识别可能导致亚马逊弹性计算云 (Amazon EC2) Windows 实例的 Windows 更新失败的问题。

如何工作？

运行手册执行以下步骤：

- 检查目标 Amazon EC2 实例是否由管理 AWS Systems Manager。
- 检查 Systems Manager 的修补操作是否支持代 AWS Systems Manager 理（SSM 代理）和 Windows Server 版本。
- 检查为 Windows 更新推荐的可用磁盘空间以及是否正在等待重启。待重启通常表示更新处于待处理状态，并且在执行其他更新之前需要重新启动。
- 在操作系统级别配置代理设置，这有助于解决连接问题。
- 执行亚马逊简单存储服务 (Amazon S3) Simple Service 终端节点连接测试，并调用 [GetDeployablePatchSnapshotForInstance](#) API 操作来检索托管节点使用的补丁基准的当前快照。
- 如果连接失败，则提供AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2运行手册的选项，以分析实例与 Amazon S3 终端节点的连接。

- 验证 Windows 更新配置并测试 Windows 服务器更新服务 (WSUS) (如果适用) 。

Important

- 不支持活动目录域控制器。
- 不支持 Windows Server 版本 2008 R2 或之前的版本。
- 不支持 SSM Agent 1.2.371 或之前的版本。
- AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2运行手册[VPC Reachability Analyzer](#)用于分析源端点和服务端点之间的网络连接。每次在来源和目标之间运行分析时，您需要支付费用。有关详细信息，请参阅 [Amazon VPC 定价](#)。
- 并非所有支持 Systems Manager 的地区都提供该操作手册AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2册。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation

- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

 Note

要运行子运行手册 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`，请添加[本文档](#)中列出的权限。

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootWindowsUpdate](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId (必填)：

输入 Windows 更新失败的亚马逊 EC2 实例的 ID。

- RunVpcReachabilityAnalyzer (可选)：

如果网络问题是由扩展检查确定的，或者指定的 `true` 实例 ID 不是托管实例，则指定运行 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 自动化。有关此子自动化的更多信息，请参阅[文档](#)。默认值为 `false`。

- RetainVpcReachabilityAnalysis (可选)：

只有在 `RunVpcReachabilityAnalyzer` 是的情况下才相关 `true`。指定 `true` 保留由创建的网络洞察路径和相关分析 `Reachability Analyzer`。默认情况下，这些资源将在成功分析后删除。如果您选择保留分析，则子运行手册不会删除该分析，您可以在 Amazon VPC 控制台中将其可视化。控制台链接将在儿童自动化输出中可用。默认值 `false`。

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance.
☒ Show interactive instance picker

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

RunVpcReachabilityAnalyzer
(Optional) Specify 'true' to run the 'AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

RetainVpcReachabilityAnalysis
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **getWindowsServerAndSSMAgentVersion:**

验证目标实例是否由管理，AWS Systems Manager 并获取有关 SSM 代理版本和 Windows 版本的详细信息。

- **assertIfInstanceIsSsmManaged:**

确保 Amazon EC2 实例由 AWS Systems Manager (SSM) 管理，否则自动化将结束。

- **CheckProxy:**

检查 Windows 实例的所有代理类型。

- **CheckPrerequisites:**

获取 SSM 代理版本和 Windows 版本，并确定它是否是 Active Directory 域控制器 (DC)。如果实例是 DC 或者不支持 SSM 代理或 Windows 版本，则运行手册将停止。

- **CheckDiskSpace:**

获取并验证 Windows 实例上的可用磁盘空间是否足以执行 Windows 更新。

- **CheckPendingReboot:**

在 Windows 实例上检查是否有任何待重启的任务。

- **CheckS3Connectivity:**

检查实例是否可以访问的 Amazon S3 终端节点Patchbaseline。

- **branchOnRunVpcReachabilityAnalyzer:**

如果RunVpcReachabilityAnalyzer为 true，则它会分支自动化以对调试 Amazon S3 连接进行更深入的分析。

- **GenerateEndpoints:**

生成一个终端节点，以便对 Amazon S3 终端节点进行扩展连接检查。

- **analyzeAwsEndpointReachabilityFromEC2:**

调用自动化运行手册，AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2. 以检查所选实例与所需终端节点的可访问性。

- **CheckWindowsUpdateServices:**

检查 Windows 更新服务状态和启动类型。

- **CheckWindowsUpdateSettings:**

检查是否在 Windows 实例上配置了 Windows 更新策略。

- **CheckWSUSSettings:**

检查 Windows 更新是使用 WSUS 还是微软更新目录配置的，并验证连接。

- **CheckWUGlobalSettings:**

检查通过 Windows 实例配置的 Windows 更新全局设置。

- **GenerateLogs:**

将 Windows 更新日志和 CBS 日志下载到实例桌面，并检查 Windows 事件日志是否出现故障。

- **FinalReport:**

生成所有步骤的完整报告。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

```

FinalReport.Results
"

=====Prerequisites Check=====
Result: [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

=====Disk Space Check=====
Result: [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

=====Pending Reboot Check=====
Result: [PASSED]
INFO: There is no pending reboot.

=====Amazon S3 Connectivity Check=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====Windows Update Services Status=====
Result: [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

=====Windows Proxy Settings=====
Result: [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.

=====Windows Update Settings=====
Result: [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\Administrative Template\Windows Component\Windows
Update\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

=====Windows Update Global Settings=====
Result: [PASSED]
Windows Update Client has no restrictions

=====Copy of Windows Update and CBS logs=====
Result: [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\Windows\TEMP\c176a507-d074-4402-8a5b-631dd643f33a folder
"

```

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)

- [设置自动化](#)
- [支持自动化工作流登录页面](#)

与 AWS 服务相关的文档

- 有关更多信息，请参阅文章《[Troubleshoot Windows 更新](#)》。

AWSSupport-UpgradeWindowsAWSDrivers

描述

AWSSupport-UpgradeWindowsAWSDrivers 运行手册升级或修复指定 EC2 实例上的存储和网络 AWS 驱动程序。运行手册尝试通过调用 SSM 代理在线安装最新版本的 AWS 驱动程序。如果无法联系 SSM 代理，则如果明确要求，运行手册可以脱机安装 AWS 驱动程序。

此运行手册支持以下操作系统：

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note

注意：在线和离线升级都将在尝试任何操作前创建一个 AMI，此 AMI 在 Automation 完成后予以保留。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。在线方法在升级过程中会重启实例，而离线方法则需要停止然后启动提供的 EC2 实例。

Important

如果您的实例 AWS Systems Manager 使用 VPC 终端节点连接，则除非在 us-east-1 区域中使用，否则本运行手册将失败。此运行手册也将在域控制器上失败。要更新域控制器上的 AWS PV 驱动程序，请参阅[升级域控制器 \(AWS PV 升级\)](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AllowOffline

类型：字符串

有效值：true | false

默认：false

说明：(可选) 如果允许在无法执行在线安装时进行离线驱动程序升级，请将其设置为 true。注意：离线方法需要停止提供的 EC2 实例然后启动。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ForceUpgrade

类型：字符串

有效值：true | false

默认：false

说明：(可选) 仅离线 - 如果允许离线驱动程序升级在实例已安装最新驱动程序的情况下继续，请将其设置为 true。

- InstanceId

类型：字符串

说明：(必需) 您的 Windows Server EC2 实例的 ID。

- SubnetId

类型：字符串

默认：SelectedInstanceSubnet

描述：(可选) 仅限脱机-用于执行离线驱动程序升级的 R EC2 rescue 实例的子网 ID。如果未指定子网 ID，Systems Manager Automation 将创建一个新 VPC。

 Important

子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

接收命令的 EC2 实例必须至少具有一个 IAM 角色，该角色包括 ssm: StartAutomationExecution 和 ssm: SendCommand 的权限，用于运行自动化并将命令发送到实例，以及 ssm: GetAutomationExecution 才能读取自动化输出。您可以将 AmazonSSMManagedInstanceCore Amazon 托管策略附加到 IAM 角色以提供这些权限。不过，我们建议使用 Automation IAM 角色 AmazonSSMAutomationRole 以实现该目的。有关更多信息，请参阅 [使用 IAM 为自动化配置角色](#)。

如果要执行离线升级，请参阅 [AWSSupport-StartEC2RescueWorkflow](#) 所需的权限。

文档步骤

1. aws:assertAwsResourceProperty - 验证输入实例是否为 Windows。
2. aws:assertAwsResourceProperty - 验证输入实例是否为托管实例。如果是托管实例，则启动在线升级，否则将评估离线升级。
 - a. (在线升级) 如果输入实例为托管实例：
 - i. aws:createImage - 创建 AMI 备份。
 - ii. aws:createTags - 标记 AMI 备份。

- iii. `aws:runCommand`-安装 ENA 网络驱动程序。
- iv. `aws:runCommand`-安装 NVMe 驱动程序。
- v. `aws:runCommand`-安装 AWS 光伏驱动程序。
- b. (离线升级) 如果输入实例不为托管实例 :
 - i. `aws:assertAwsResourceProperty` - 验证 `AllowOffline` 旗帜是否设置为 `true`。如果是，则启动离线升级，否则自动化流程结束。
 - ii. `aws:changeInstanceState` - 停止源实例。
 - iii. `aws:changeInstanceState` - 强制停止源实例。
 - iv. `aws:createImage` - 创建源实例的 AMI 备份。
 - v. `aws:createTags` - 标记源实例的 AMI 备份。
 - vi. `aws:executeAwsApi` - 为实例启用 ENA
 - vii. `aws:assertAwsResourceProperty`-宣称 `ForceUpgrade` 旗帜。
 - viii. 强制离线升级) 如果 `ForceUpgrade` 为 `true` `aws:executeAutomation`，则 `AWSsupport-StartEC2RescueWorkflow` 使用驱动程序强制升级脚本运行调用。不管当前安装的是何种版本，都将安装驱动程序
 - ix. (离线升级) 如果 `ForceUpgrade` 为 `false` `aws:executeAutomation`，则 `AWSsupport-StartEC2RescueWorkflow` 使用驱动程序升级脚本运行调用。

输出

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup. ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline. 输出`

`forceUpgradeDrivers` 离线。 输出

Amazon ECS

AWS Systems Manager Automation 为 Amazon 弹性容器服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

AWSSupport-CollectECSInstanceLogs

描述

AWSSupport-CollectECSInstanceLogs 运行手册从 Amazon Elastic Compute Cloud (Amazon EC2) 实例收集操作系统和 Amazon Elastic Container Service (Amazon ECS) 相关日志文件，以帮助解决常见的 Amazon ECS 问题。当自动化收集关联的日志文件时，会对文件系统进行更改。这些更改包括创建临时目录和日志目录、将日志文件复制到这些目录，以及将日志文件压缩到档案中。

如果您为 LogDestination 参数指定值，则目标实例必须安装适用于 Linux 实例的 AWS 命令行界面 (AWS CLI) 或适用 PowerShell 于 Windows 的 Windows AWS 工具。自动化会评估您指定的亚马逊简单存储服务 (Amazon S3) 存储桶的策略状态。为了帮助保护从 Amazon EC2 实例收集的日志的安全，如果策略状态 isPublic 设置为 true，或者如果访问控制列表 (ACL) 向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，日志将不会上传。此外，如果提供的存储桶在您的账户中不可用，日志将不会上传。有关 Amazon S3 预定义组的更多信息，请参阅[亚马逊简单存储服务用户指南中的 Amazon S3 预定义组](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ECSInstanceid

类型：字符串

描述：(必需) 需要收集日志的实例 ID。指定的实例必须由 Systems Manager 托管。

- LogDestination

类型：字符串

描述：(可选) 您中 AWS 账户 用于上传存档日志的 Amazon S3 存储桶。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- ssm:DescribeInstanceInformation

建议您在 ECSInstanceid 参数中指定的 Amazon EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。要将日志档案上传到您在 LogDestination 参数中指定的 Amazon S3 存储桶，您必须添加以下权限：

- s3:PutObject
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl

文档步骤

- `assertInstanceIsManaged` - 验证您在 `ECSInstanceId` 参数中指定的实例是否由 Systems Manager 管理。
- `getInstancePlatform` - 获取您在 `ECSInstanceId` 参数中指定的实例的操作系统 (OS) 平台的相关信息。
- `verifyInstancePlatform` - 根据 OS 平台对自动化进行分支。
- `runLogCollectionScriptOnLinux` - 在 Linux 实例上收集操作系统和 Amazon ECS 相关日志文件，并在 `/var/log/collectECSlogs` 目录中创建一个归档文件。
- `runLogCollectionScriptOnWindows` - 在 Windows 实例上收集操作系统和 Amazon ECS 相关日志文件，并在 `C:\ProgramData\collectECSlogs` 目录中创建一个归档文件。
- `verifyIfS3BucketProvided` - 验证是否为 `LogDestination` 参数指定了一个值。
- `runUploadScript` - 基于操作系统平台对自动化步骤进行分支。
- `runUploadScriptOnLinux` - 将日志档案上传到 `LogDestination` 参数中指定的 Amazon S3 存储桶，并从操作系统中删除归档的日志文件。
- `runUploadScriptOnWindows` - 将日志档案上传到 `LogDestination` 参数中指定的 Amazon S3 存储桶，并从操作系统中删除归档的日志文件。

AWS-InstallAmazonECSAgent

描述

AWS-InstallAmazonECSAgent 运行手册将 Amazon Elastic Container Service (Amazon ECS) 代理安装在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例上。此运行手册仅支持 Amazon Linux 和 Amazon Linux 2 实例。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceIds

类型：StringList

描述：(必需) 要在其上安装 Amazon ECS 代理的 Amazon EC2 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

文档步骤

aws:executeScript - 将 Amazon ECS 代理安装到您在 InstanceIds 参数中指定的 Amazon EC2 实例上。

输出

InstallAmazonECSAgent.SuccessfullInstances -成功安装 Amazon ECS 代理的实例的 ID。

InstallAmazonECSAgent.FailedInstances -安装 Amazon ECS 代理失败的实例的 ID。

InstallAmazonECSAgent.InProgressInstances -正在安装 Amazon ECS 代理的实例的 ID。

AWS-ECSRunTask

描述

运行AWS-ECSRunTask手册运行您指定的亚马逊弹性容器服务 (Amazon ECS) 任务。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 容量 ProviderStrategy

类型：字符串

描述：(可选) 用于任务的容量提供者策略。

- cluster

类型：字符串

描述：(可选) 用于运行任务的集群的短名称或 ARN。如果未指定集群，则使用默认集群。

- count

类型：字符串

描述：(可选) 要在集群上放置的指定任务的实例化次数。您最多可以为每个请求指定 10 个任务。

- 启用 ECSManagedTags

类型：布尔值

描述：(可选) 指定是否对任务使用 Amazon ECS 托管标签。有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的[标记 Amazon ECS 资源](#)。

- 启用 ExecuteCommand

类型：布尔值

描述：(可选) 确定是否激活此任务中容器的执行命令功能。如果为 true，则将在任务中的所有容器上激活执行命令功能。

- 组

类型：字符串

描述：(可选) 要与任务关联的任务组的名称。默认值为任务定义的姓氏。例如 family:my-family-name。

- 启动类型

类型：字符串

有效值：EC2 | FARGATE | EXTERNAL

描述：(可选) 运行独立任务的基础架构。

- networkConfiguration

类型：字符串

描述：(可选) 任务的网络配置。使用awsvpc网络模式接收自己的 elastic network interface 的任务定义必须使用此参数，其他网络模式则不支持此参数。

- 覆盖

类型：字符串

描述：(可选) JSON 格式的容器覆盖列表，用于指定任务定义中指定容器的名称以及容器应接收的替代项。您可以使用命令替换在任务定义或 Docker 镜像中指定的容器的默认命令。您还可以覆盖任务定义或容器上的 Docker 镜像中指定的现有环境变量。此外，您还可以使用环境覆盖来添加新的环境变量。

- placementConstraints

类型：字符串

描述：(可选) 用于任务的放置约束对象数组。您最多可以为每项任务指定 10 个约束条件，包括任务定义中的约束条件和运行时指定的约束条件。

- placementStrategy

类型：字符串

描述：(可选) 用于任务的放置策略对象。您最多可以为每个任务指定 5 条策略规则。

- platformVersion

类型：字符串

描述：(可选) 任务使用的平台版本。仅为 Fargate 上托管的任务指定平台版本。如果未指定任何版本，将使用 LATEST 平台版本。

- propagateTags

类型：字符串

描述：(可选) 确定标签是否从任务定义传播到任务。如果未指定任何值，则不会传播标签。只能在任务创建过程中将标签传播到任务。

- referenceld

类型：字符串

描述：(可选) 用于任务的参考 ID。参考 ID 的最大长度可以为 1024 个字符。

- 起始者

类型：字符串

描述：(可选) 任务启动时指定的可选标签。这有助于您通过筛选 ListTasks API 操作的结果来确定哪些任务属于特定作业。最多允许 36 个字母 (大写和小写)、数字、连字符 (-) 和下划线 (_)。

- 标签

类型：字符串

描述：(可选) 要应用于任务的元数据，以帮助您对任务进行分类和组织。每个标签都由用户定义的键和值组成。

- 任务定义

类型：字符串

描述：(可选) 要family运行的任务定义的和 revision (family:revision) 或完整 ARN。如果未指定修订版，则使用最新的ACTIVE修订版。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ecs:RunTask

文档步骤

aws:executeScript-根据您为运行手册输入参数指定的值运行 Amazon ECS 任务。

AWSSupport-TroubleshootECSContainerInstance

描述

AWSSupport-TroubleshootECSContainerInstance 运行手册可帮助排除无法向 Amazon ECS 集群注册的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的问题。此自动化会检查实例的用户数据是否包含正确的集群信息、实例配置文件是否包含所需的权限，还会检查网络配置问题。

Important

要成功运行此自动化，Amazon EC2 实例的状态必须为 running，Amazon ECS 集群的状态必须为 ACTIVE。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必需) 实例未能向其注册的 Amazon ECS 集群的名称。

- InstanceId

类型：字符串

描述：(必需) 需要排除故障的 Amazon EC2 实例 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`

文档步骤

`aws:executeScript` : 审查 Amazon EC2 实例是否满足向 Amazon ECS 集群注册所需的先决条件。

AWSsupport-TroubleshootECSTaskFailedToStart

描述

AWSsupport-TroubleshootECSTaskFailedToStart 运行手册可帮助解决 Amazon ECS 集群中的 Amazon Elastic Container Service (Amazon ECS) 任务无法启动的问题。您必须以与未能启动的任务 AWS 区域 相同的方式运行此运行手册。运行手册分析了以下可能导致任务无法启动的常见问题：

- 与已配置的容器注册表的网络连接
- 缺少任务执行角色所需的 IAM 权限
- VPC 端点连接
- 安全组规则配置
- AWS Secrets Manager 秘密参考
- 日志配置

Note

如果分析确定需要对网络连接进行测试，则会在您的账户中创建 Lambda 函数和必要的 IAM 角色。这些资源用于模拟失败任务的网络连接。当这些资源不再需要时，此自动化会将其删除。但是，如果此自动化无法删除这些资源，则必须手动将其删除。

提供 Lambda IAM 角色后，自动化将使用该角色而不是创建新角色。提供的 Lambda IAM 角色必须包含 AWS 托管策略，AWSLambdaVPCAccessExecutionRole 并且具有允许该策略由 Lambda 服务委托人担任的信任策略。`lambda.amazonaws.com`

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaRoleArn

类型：字符串

描述：(可选) 允许该 AWS Lambda 函数访问所需 AWS 服务和资源的 IAM 角色的 ARN。如果未指定任何角色，则此 Systems Manager Automation 将在您的账户中为 Lambda 创建一个 IAM 角色 `NetworkToolSSMRunbookExecution<ExecutionId>`，其名称包含托管策略：`。AWSLambdaVPCAccessExecutionRole`

- ClusterName

类型：字符串

描述：(必需) 任务启动失败的 Amazon ECS 集群的名称。

- CloudwatchRetentionPeriod

类型：整数

描述：(可选) 要存储在 Amazon CloudWatch Logs 中的 Lambda 函数日志的保留期，以天为单位。只有在分析确定需要测试网络连通性时，才需要这样做。

有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

默认：30

- TaskId

类型：字符串

描述：(必需) 失败任务的 ID。使用最近失败的任务。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudtrail:LookupEvents
- ec2:DeleteNetworkInterface
- ec2:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVpcAttribute
- elasticfilesystem:DescribeFileSystems
- elasticfilesystem:DescribeMountTargets

- elasticfilesystem:DescribeMountTargetSecurityGroups
- elasticfilesystem:DescribeFileSystemPolicy
- ecr:DescribeImages
- ecr:GetRepositoryPolicy
- ecs:DescribeContainerInstances
- ecs:DescribeServices
- ecs:DescribeTaskDefinition
- ecs:DescribeTasks
- iam:AttachRolePolicy
- iam:CreateRole
- iam>DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:ListUsers
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:GetFunctionConfiguration
- lambda:InvokeFunction
- lambda:TagResource
- logs:DescribeLogGroups
- logs:PutRetentionPolicy
- secretsmanager:DescribeSecret
- ssm:DescribeParameters
- sts:GetCallerIdentity

如果LambdaRoleArn提供了自动化，则无需创建角色，并且可以排除以下权限：

- iam:CreateRole
- iam>DeleteRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy

文档步骤

- aws:executeScript - 验证启动此自动化的用户或角色是否具有所需的 IAM 权限。如果您没有足够的权限来使用此运行手册，则缺少的必需权限将包含在此自动化的输出中。
- aws:branch - 根据您是否对运行手册的所有必要操作拥有权限进行分支。
- aws:executeScript - 如果分析确定需要测试网络连通性，则会在 VPC 中创建 Lambda 函数。
- aws:branch - 根据上一步的结果进行分支。
- aws:executeScript - 分析启动任务失败的可能原因。
- aws:executeScript - 删除此自动化创建的资源。
- aws:executeScript - 格式化此自动化的输出，将分析结果返回到控制台。在此步骤之后，您可以在自动化完成前查看分析。
- aws:branch - 根据 Lambda 函数和关联资源是否已创建以及是否需要删除进行分支。
- aws:sleep - 休眠 30 分钟，使得可以删除 Lambda 函数的弹性网络接口。
- aws:executeScript - 删除 Lambda 函数网络接口。
- aws:executeScript - 格式化 Lambda 函数网络接口删除步骤的输出。

AWS-UpdateAmazonECSAgent

描述

AWS-UpdateAmazonECSAgent 运行手册更新了您指定的Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Container Service (Amazon ECS) 代理。此运行手册仅支持 Amazon Linux 和 Amazon Linux 2 实例。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterARN

类型：StringList

描述：(必需) 容器实例所注册的 Amazon ECS 集群的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeImage
- ec2:DescribeInstance
- ec2:DescribeInstanceAttribute
- ecs:DescribeContainerInstances
- ecs:DescribeClusters

- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

文档步骤

`aws:executeScript` - 更新您在 `ClusterARN` 参数中指定的 Amazon ECS 集群上的 Amazon ECS 代理。

输出

`UpdateAmazonECSAgent.UpdatedContainers` - 成功更新 Amazon ECS 代理的实例的 ID。

`UpdateAmazonECSAgent.FailedContainers` - Amazon ECS 代理更新失败的实例的 ID。

`UpdateAmazonECSAgent.InProgressContainers` - 正在更新 Amazon ECS 代理的实例的 ID。

Amazon EFS

AWS Systems Manager Automation 为亚马逊 Elastic File System 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-CheckAndMountEFS](#)

AWSSupport-CheckAndMountEFS

描述

`AWSSupport-CheckAndMountEFS` 运行手册验证挂载 Amazon Elastic File System (Amazon EFS) 文件系统并在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例上挂载文件系统的先决条件。此运行手册支持使用 DNS 名称或使用挂载目标的 IP 地址来挂载 Amazon EFS 文件系统。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 处理建议

类型：字符串

有效值：选中 | CheckAndMount

描述：(必需) 确定运行手册是验证先决条件，还是验证先决条件并装载文件系统。

- EfsId

类型：字符串

描述：(必选) 要挂载的文件系统的 ID。

- InstanceId

类型：字符串

描述：(必需) 要在其上挂载文件系统的 Amazon EC2 实例的 ID。

- MountOptions

类型：字符串

描述：(可选) 要在挂载文件系统时使用的 Amazon EFS 挂载帮助程序支持的选项。如果您指定 `tls` 选项，则验证目标实例上的 `stunnel` 是否已升级。

- MountPoint

类型：字符串

描述：(可选) 要挂载文件系统的目录。如果为 Action 参数指定了 Check 值，则不应指定此参数。

- MountTarget知识产权

类型：字符串

描述：(可选) 挂载目标的 IP 地址。通过 IP 地址挂载适用于 DNS 被禁用的环境，例如禁用 DNS 主机名的虚拟私有云 (VPC)。此外，如果您的环境使用 Amazon Route 53 (Route 53) 以外的 DNS 提供商，则可以使用此选项。

- Region

类型：字符串

描述：(必填) Amazon EC2 实例和文件系统所在的位置。AWS 区域

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:StartAutomationExecution
- iam:ListRoles
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups

- elasticfilesystem:DescribeFileSystemPolicy
- elasticfilesystem:DescribeMountTargets
- elasticfilesystem:DescribeMountTargetSecurityGroups
- resource-groups:*

文档步骤

- aws:executeScript - 收集有关您在 InstanceId 参数中指定的 Amazon EC2 实例的详细信息。
- aws:executeScript - 收集有关您在 EfsId 参数中指定的文件系统的详细信息。
- aws:executeScript - 验证与文件系统关联的安全组是否允许来自您在 InstanceId 参数中指定的 Amazon EC2 实例的端口 2049 上的流量。
- aws:assertAwsResourceProperty - 验证您在 InstanceId 参数中指定的 Amazon EC2 实例是否由 Systems Manager 管理以及其状态是否为 Online。
- aws:branch - 根据您为 Action 参数指定的值进行分支。
- aws:runCommand - 验证挂载您在 EfsId 参数中指定的文件系统的先决条件。
- aws:runCommand - 验证挂载您在 EfsId 参数中指定的文件系统的先决条件，并将文件系统挂载到您在 InstanceId 参数中指定的 Amazon EC2 实例上。

Amazon EKS

AWS Systems Manager 自动化为亚马逊 Elastic Kubernetes Service 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)

- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-CollectEKSLinuxNodeStatistics](#)
- [AWSSupport-CollectEKSInstanceLogs](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)
- [AWSSupport-TroubleshootEKSSALBControllerIssues](#)
- [AWSSupport-TroubleshootEKSDNSFailure](#)

AWS-CreateEKSClusterWithFargateProfile

描述

AWS-CreateEKSClusterWithFargateProfile运行手册使用创建了亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 集群。 AWS Fargate

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必填) 集群的唯一名称。

- ClusterRoleArn

类型：字符串

描述：(必填) IAM 角色的 ARN，该角色为 Kubernetes 控制平面提供代表您调用 AWS API 操作的权限。

- FargateProfileName

类型：字符串

描述：(必填) Fargate 配置文件的名称。

- FargateProfileRoleArn

类型：字符串

描述：(必填) 亚马逊 EKS Pod 执行 IAM 角色的 ARN。

- FargateProfileSelectors

类型：字符串

描述：(必填) 用于将吊舱与 Fargate 配置文件进行匹配的选择器。

- SubnetIds

类型：StringList

描述：(必填) 您要用于 Amazon EKS 集群的子网的 ID。Amazon EKS 在这些子网中创建弹性网络接口，用于您的节点与 Kubernetes 控制平面之间的通信。您必须指定至少两个子网 ID。

- EKSEndpointPrivateAccess

类型：布尔值

默认值：True

描述：(可选) 将此值设置为，True以允许对集群的 Kubernetes API 服务器终端节点进行私有访

问。如果启用私有访问，集群的 VPC 内的 Kubernetes API 请求将使用私有 VPC 端点。如果您禁用

私有访问并且集群中有节点或 AWS Fargate Pod，请确保 `publicAccessCidrs` 其中包含与节点或 Fargate Pod 通信所必需的 CIDR 块。

- `EKSEndpointPublicAccess`

类型：布尔值

默认值：False

描述：（可选）将此值设置为 `False` 以禁用对集群的 Kubernetes API 服务器端点的公共访问权限。如果您禁用公共访问，则集群的 Kubernetes API 服务器只能接收来自其启动的 VPC 内部请求。

- `PublicAccessCIDRs`

类型：StringList

描述：（可选）允许访问集群的公共 Kubernetes API 服务器端点的 CIDR 块。拒绝从您指定的 CIDR 块之外的地址与端点的通信。如果您已禁用私有终端节点访问并且集群中有节点或 Fargate pod，请确保指定必要的 CIDR 块。

- `SecurityGroupIds`

类型：StringList

描述：（可选）指定一个或多个安全组以与 Amazon EKS 在您的账户中创建的弹性网络接口相关联。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:CreateCluster`
- `eks:CreateFargateProfile`
- `eks:DescribeCluster`

- `eks:DescribeFargateProfile`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

文档步骤

- `createeksCluster` (aws: execute) `AwsApi`-创建亚马逊 EKS 集群。
- `VerifyEKSClusterIsActive` (aws: waitForAwsResourceProperty t)-验证集群状态为。ACTIVE
- `CreateFargateProfile` (aws: executeAwsApi)-为集群创建 Fargate。
- `VerifyFargateProfileIsActive` (aws: waitForAwsResourceProperty)-验证 Fargate 配置文件状态为。ACTIVE

输出

`CreateEKSCluster.CreateClusterResponse`

描述：从 `CreateCluster` API 调用中收到的响应。

`CreateFargateProfile.CreateFargateProfileResponse`

描述：从 `CreateFargateProfile` API 调用中收到的响应。

AWS-CreateEKSClusterWithNodegroup

描述

该AWS-CreateEKSClusterWithNodegroup运行手册使用容量节点组创建了亚马逊 Elastic Kubernetes Service (Amazon EKS) 集群。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必填) 集群的唯一名称。

- ClusterRoleArn

类型：字符串

描述：(必填) IAM 角色的 ARN，该角色为 Kubernetes 控制平面提供代表您调用 AWS API 操作的权限。

- NodegroupName

类型：字符串

描述：(必填) 节点组的唯一名称。

- NodegroupRoleArn

类型：字符串

描述：(必填) 要与您的节点组关联的 IAM 角色的 ARN。Amazon EKS 工作节点 kubelet 守护程序代表你调用 AWS API。节点通过 IAM 实例配置文件和关联的策略获得这些 API 调用的权限。您必须先为节点创建 IAM 角色以在启动它们时使用，然后才能启动这些节点并在集群中注册它们。

- SubnetIds

类型：StringList

描述：(必填)您要用于 Amazon EKS 集群的子网的 ID。Amazon EKS 在这些子网中创建弹性网络接口，用于您的节点与 Kubernetes 控制平面之间的通信。您必须指定至少两个子网 ID。

- EKSEndpointPrivateAccess

类型：布尔值

默认值：True

描述：(可选)将此值设置为，True以允许对集群的 Kubernetes API 服务器终端节点进行私有访问。如果启用私有访问，集群的 VPC 内的 Kubernetes API 请求将使用私有 VPC 端点。如果您禁用私有访问并且集群中有节点或 AWS Fargate Pod，请确保publicAccessCidrs其中包含与节点或 Fargate Pod 通信所必需的 CIDR 块。

- EKSEndpointPublicAccess

类型：布尔值

默认值：False

描述：(可选)将此值设置为，False以禁用对集群的 Kubernetes API 服务器端点的公共访问权限。如果您禁用公共访问，则集群的 Kubernetes API 服务器只能接收来自其启动的 VPC 内部请求。

- PublicAccessCIDRs

类型：StringList

描述：(可选)允许访问集群的公共 Kubernetes API 服务器端点的 CIDR 块。拒绝从您指定的 CIDR 块之外的地址与端点的通信。如果您已禁用私有终端节点访问并且集群中有节点或 Fargate pod，请确保指定必要的 CIDR 块。

- SecurityGroupIds

类型：StringList

描述：(可选)指定一个或多个安全组以与 Amazon EKS 在您的账户中创建的弹性网络接口相关联。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

文档步骤

- `createeksCluster` (aws: execute) `AwsApi`-创建亚马逊 EKS 集群。
- `VerifyEKSClusterIsActive` (aws: waitForAwsResourceProperty t)-验证集群状态为。ACTIVE
- `CreateNodegroup` (aws: executeAwsApi)-为群集创建节点组。
- `VerifyNodegroupIsActive` (aws: waitForAwsResourceProperty)-验证节点组的状态为。ACTIVE

输出

- `CreateEKSCluster.CreateClusterResponse`: 从 `CreateCluster` API 调用中收到的响应。
- `CreateNodegroup.CreateNodegroupResponse`: 从 `CreateNodegroup` API 调用中收到的响应。

AWS-DeleteEKSCluster

描述

此运行手册将删除与 Amazon EKS 集群关联的资源，包括节点组和 Fargate 配置文件。或者，您可以选择删除所有自管理节点、用于创建节点的 CloudFormation 堆栈以及集群的 VPC CloudFormation 堆栈。有关删除集群的更多信息，请参阅《Amazon EKS 用户指南》中的[删除集群](#)。

 Note

如果集群中具有与负载均衡器关联的有效服务，则必须先删除这些服务，然后再删除集群。否则，系统将无法删除负载均衡器。在运行 AWS-DeleteEKSCluster 运行手册之前，请通过以下过程查找和删除服务。

查找和删除集群中的服务

1. 安装 Kubernetes 命令行实用程序 kubectl。有关更多信息，请参阅《Amazon EKS 用户指南》中的[安装 kubectl](#)。
2. 运行以下命令列出集群中运行的所有服务。

```
kubectl get svc --all-namespaces
```

3. 运行以下命令以删除任何具有关联 EXTERNAL-IP 值的服务。这些服务的前面配置了一个负载均衡器，您必须从 Kubernetes 中将其删除才能释放负载均衡器和关联资源。

```
kubectl delete svc  
service-name
```

现在您可以运行 AWS-DeleteEKSCluster 运行手册了。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EKSClusterName

类型：字符串

描述：(必需) 要删除的 Amazon EKS 集群的名称。

- VPCCloudFormationStack

类型：字符串

描述：(可选) 要删除的 EKS 集群的 VPC CloudFormation 堆栈名称。这将删除 VPC 的 CloudFormation 堆栈以及该堆栈创建的所有资源。

- VPCCloudFormationStackRole

类型：字符串

描述：(可选) CloudFormation 假定删除 VPC CloudFormation 堆栈的 IAM 角色的 ARN。CloudFormation 使用该角色的凭据代表您拨打电话。

- SelfManagedNodeStacks

类型：字符串

描述：(可选) 自管节点的 CloudFormation 堆栈名称 Comma-separated 列表，这将删除自管理节点的 CloudFormation 堆栈。

- SelfManagedNodeStacksRole

类型：字符串

描述：(可选) CloudFormation 假定删除 Self-managed 节点堆栈的 IAM 角色的 ARN。CloudFormation 使用该角色的凭据代表您拨打电话。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- sts:AssumeRole
- eks:ListNodegroups
- eks>DeleteNodegroup
- eks:ListFargateProfiles
- eks>DeleteFargateProfile
- eks>DeleteCluster
- cfn:DescribeStacks
- cfn>DeleteStack

文档步骤

- aws:executeScript- DeleteNodeGroups : 查找并删除 EKS 集群中的所有节点组。
- aws:executeScript- DeleteFargateProfiles : 在 EKS 集群中查找并删除所有 Fargate 配置文件。
- aws:executeScript- DeleteSelfManagedNodes : 删除所有自行管理的节点和用于创建节点的 CloudFormation 堆栈。
- aws:executeScript - DeleteEKSCluster : 删除 EKS 集群。
- aws:executeScript- DeleteVPCCloudFormationStack : 删除 VPC CloudFormation 堆栈。

AWS-MigrateToNewEKSSelfManagedNodeGroup

描述

该AWS-MigrateToNewEKSSelfManagedNodeGroup运行手册可帮助您创建一个新的亚马逊 Elastic Kubernetes Service (Amazon EKS) Linux 节点组，以将现有应用程序迁移到该节点组。有关更多信息，请参阅 Amazon EKS 用户指南中的[迁移到新节点组](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- OldStackName

类型：字符串

描述：(必填) 现有堆栈的名称或 CloudFormation 堆栈 ID。

- NewStackName

类型：字符串

描述：(可选) 为您的新节点组创建的新 CloudFormation 堆栈的名称。如果您未为此参数指定值，则使用以下格式创建堆栈名称：NewNodeGroup-*ClusterName*-*AutomationExecutionID*。

- ClusterControlPlaneSecurityGroup

类型：字符串

描述：(可选) 您希望节点用于与 Amazon EKS 控制平面通信的安全组的 ID。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的安全组。

- NodeInstanceType

类型：字符串

描述：(可选) 您要用于新节点组的实例类型。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的实例类型。

- NodeGroupName

类型：字符串

描述：(可选) 您的新节点组的名称。如果您未为此参数指定值，则使用在现有 CloudFormation 堆栈中指定的节点组名称。

- NodeAutoScalingGroupDesiredCapacity

类型：字符串

描述：(可选) 创建新堆栈时要扩展到的所需节点数量。此数字必须大于或等于该NodeAutoScalingGroupMinSize值且小于或等于NodeAutoScalingGroupMaxSize。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的节点组所需容量。

- NodeAutoScalingGroupMaxSize

类型：字符串

描述：(可选) 您的节点组可以扩展到的最大节点数。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的节点组最大大小。

- NodeAutoScalingGroupMinSize

类型：字符串

描述：(可选) 您的节点组可以扩展到的最小节点数。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的节点组最小大小。

- NodeImageId

类型：字符串

描述：(可选) 希望节点组使用的 Amazon Machine Image (AMI) 的 ID。

- NodeImageIdSSMParam

类型：字符串

描述：(可选) 希望节点组使用的 AMI 的公共 Systems Manager 参数。

- NodeVolumeSize

类型：字符串

描述：(可选) 节点的根卷大小 (以 GiB 为单位)。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的节点卷大小。

- NodeVolumeType

类型：字符串

描述：(可选) 您要用于节点根卷的 Amazon EBS 卷的类型。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的卷类型。

- KeyName

类型：字符串

描述：(可选) 您要分配给节点的密钥对。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的密钥对。

- 子网

类型：StringList

描述：(可选) 要用于新节点组的子网 ID 的逗号分隔列表。如果您未为此参数指定值，则使用现有 CloudFormation 堆栈中指定的子网。

- DisableIMDSv1

类型：布尔值

描述：(可选) 指定禁用实例元数据服务版本 1 (imds v1)。默认情况下，节点支持 imds v1 和 imds v2。

- BootstrapArguments

类型：字符串

描述：(可选) 要传递给节点引导脚本的其他参数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetParameters
- autoscaling:CreateAutoScalingGroup
- autoscaling:CreateOrUpdateTags

- `autoscaling:DeleteTags`
- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `autoscaling:DescribeScheduledActions`
- `autoscaling:SetDesiredCapacity`
- `autoscaling:TerminateInstanceInAutoScalingGroup`
- `autoscaling:UpdateAutoScalingGroup`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateLaunchTemplateVersion`
- `ec2:CreateLaunchTemplate`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2>DeleteLaunchTemplate`
- `ec2>DeleteSecurityGroup`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstanceState`
- `ec2:DescribeInstances`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`

- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:PassRole`

文档步骤

- `DetermineParameterValuesForNewNodeGroup` (aws: ExecuteScript)-收集用于新节点组的参数值。
- `CreateStack` (aws: CreateStack)-为新节点组创建 CloudFormation 堆栈。
- `GetNewStackNodeInstanceRole` (aws: executeAwsApi)-获取节点实例角色。
- `GetNewStackSecurityGroup` (aws: executeAwsApi)-该步骤获取节点安全组。
- `AddIngressRulesToNewNodeSecurityGroup` (aws: executeAwsApi)-向新创建的安全组添加入口规则，使其可以接受来自分配给您先前节点组的安全组的流量。
- `AddIngressRulesToOldNodeSecurityGroup` (aws: executeAwsApi)-向先前的安全组添加入口规则，使其可以接受来自分配给您新创建的节点组的流量。
- `VerifyStackComplete` (aws: assertAwsResourceProperty)-验证新的堆栈状态为 `CREATE_COMPLETE`

输出

`DetermineParameterValuesForNewNodeGroup.NewStackParameters` -用于创建新堆栈的参数。

`GetNewStackNodeInstanceRole.NewNodeInstanceRole` -新节点组的节点实例角色。

`GetNewStackSecurityGroup.NewNodeSecurityGroup` -新节点组的安全组的 ID。

`DetermineParameterValuesForNewNodeGroup.NewStackName` -新节点组的 CloudFormation 堆栈名称。

CreateStack.StackId -新节点组的 CloudFormation 堆栈 ID。

AWSPremiumSupport-TroubleshootEKSCluster

描述

AWSPremiumSupport-TroubleshootEKSCluster 运行手册诊断 Amazon Elastic Kubernetes Service (Amazon EKS) 集群和底层基础架构的常见问题，并提供建议的修复步骤。

Important

访问AWSPremiumSupport-*运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持 计划](#)。

如果您为 S3BucketName 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 EC2 实例收集的日志的安全性，如果策略状态 isPublic 设置为 true，或者访问控制列表 (ACL) 向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，则不会上传日志。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 [Amazon S3 预定义组](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必需) 要排除问题的 Amazon EKS 集群的名称。

- S3BucketName

类型：字符串

描述：(必填) 应上传运行手册生成的报告的私有 Amazon S3 存储桶的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeVpcs
- ec2:DescribeNetworkAcls
- iam:GetInstanceProfile
- iam:ListInstanceProfiles
- iam:ListAttachedRolePolicies
- eks:DescribeCluster
- eks:ListNodegroups
- eks:DescribeNodegroup

- `autoscaling:DescribeAutoScalingGroups`

此外，附加到启动自动化的用户或角色的 AWS Identity and Access Management (IAM) 策略必须允许对以下公共 AWS Systems Manager 参数进行 `ssm:GetParameter` 操作，才能为工作节点获取最新推荐的 Amazon EKS Amazon Machine Image (AMI)。

- `arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2/recommended/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-1909-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2-gpu/recommended/image_id`

要将运行手册生成的报告上传到 Amazon S3 存储桶，需要对指定的指定 Amazon S3 存储桶拥有以下权限。

- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`
- `s3:PutObject`

文档步骤

- `aws:executeAwsApi` - 收集指定 Amazon EKS 集群的详细信息。
- `aws:executeScript` - 收集 Amazon Elastic Compute Cloud (Amazon EC2) 实例、Auto Scaling 组、AMI 和 Amazon EC2 GPU 图形实例类型的详细信息。
- `aws:executeScript` - 收集 Amazon EKS 集群的虚拟私有云 (VPC)、子网、网络地址转换 (NAT) 网关、子网路由、安全组和网络访问控制列表 (ACL) 的详细信息。
- `aws:executeScript` - 收集附加的 IAM 实例配置文件和角色策略的详细信息。
- `aws:executeScript` - 收集您在 `S3BucketName` 参数中指定的 Amazon S3 存储桶的详细信息。
- `aws:executeScript` - 将 Amazon VPC 子网分类为公共或私有子网。

- `aws:executeScript` - 检查 Amazon VPC 子网中是否有需要作为 Amazon EKS 集群一部分的标签。
- `aws:executeScript` - 检查 Amazon VPC 子网中是否有 Elastic Load Balancing 子网所需的标签。
- `aws:executeScript` - 检查 Worker 节点 Amazon EC2 实例是否使用最新的 Amazon EKS 优化的 AMI
- `aws:executeScript` - 检查 Amazon VPC 安全组是否已附加到所需标签的 Worker 节点。
- `aws:executeScript` - 检查 Amazon EKS 集群和 Worker 节点 Amazon VPC 安全组规则中是否有建议的 Amazon EKS 集群入口规则。
- `aws:executeScript` - 检查 Amazon EKS 集群和 Worker 节点 Amazon VPC 安全组规则中是否有建议的 Amazon EKS 集群出口规则。
- `aws:executeScript` - 检查 Amazon VPC 子网的网络 ACL 配置。
- `aws:executeScript` - 检查 Worker 节点 Amazon EC2 实例是否具有所需的托管策略。
- `aws:executeScript` - 检查 Auto Scaling 组是否具有集群自动扩展所需的标签。
- `aws:executeScript` - 检查 Worker 节点 Amazon EC2 实例是否已连接到互联网。
- `aws:executeScript` - 根据前面步骤的输出生成报告。如果为 `S3BucketName` 参数指定了一个值，则生成的报告将上传到 Amazon S3 存储桶。

AWSSupport-TroubleshootEKSTaskNode

描述

AWSSupport-TroubleshootEKSTaskNode 运行手册分析 Amazon Elastic Compute Cloud (Amazon EC2) Worker 节点和 Amazon Elastic Kubernetes Service (Amazon EKS) 集群，以帮助识别和解决阻碍 Worker 节点加入集群的常见原因。运行手册会输出指南，以帮助解决已发现的任何问题。

Important

要成功运行此自动化，Amazon EC2 Worker 节点的状态必须为 `running`，Amazon EKS 集群的状态必须为 `ACTIVE`。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必需) Amazon EKS 集群的名称。

- WorkerID

类型：字符串

描述：(必需) 未能加入集群的 Amazon EC2 Worker 节点的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeDhcpOptions
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeNatGateways

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`

文档步骤

- `aws:assertAwsResourceProperty` - 确认您在 `ClusterName` 参数中指定的 Amazon EKS 集群存在且处于 `ACTIVE` 状态。
- `aws:assertAwsResourceProperty` - 确认您在 `WorkerID` 参数中指定的 Amazon EC2 Worker 节点存在且处于 `running` 状态。
- `aws:executeScript` - 运行 Python 脚本以帮助确定 Worker 节点未能加入集群的可能原因。

AWS-UpdateEKSCluster

描述

AWS-UpdateEKSCluster 运行手册可帮助你将在亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 集群更新到你要使用的 Kubernetes 版本。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必填) 您的 Amazon EKS 集群的名称。

- 版本

类型：字符串

描述：(必填) 你要将集群更新到的 Kubernetes 版本。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- eks:DescribeUpdate
- eks:UpdateClusterVersion

文档步骤

- `aws:executeAwsApi`-更新您的亚马逊 EKS 集群使用的 Kubernetes 版本。
- `aws:waitForAwsResourceProperty`-等待更新状态变为 `Successful`

AWS-UpdateEKSMangedNodeGroup

描述

AWS-UpdateEKSMangedNodeGroup 运行手册可帮助您更新 Amazon Elastic Kubernetes Service (Amazon EKS) 托管节点组。您可以选择 `Version` 或 `Configuration` 更新。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `ClusterName`

类型：字符串

描述：(必需) 要更新其节点组的集群的名称。

- `NodeGroupName`

类型：字符串

描述：(必选) 要更新的节点组的名称。

- UpdateType

类型：字符串

有效值：更新节点组版本 | 更新节点组配置

默认：更新节点组版本

描述：(必需) 要对节点组执行的更新的类型。

以下参数仅适用于 Version 更新类型：

- AMIReleaseVersion

类型：字符串

描述：(可选) 要使用的 Amazon EKS 优化 AMI 的版本。默认情况下会使用最新版本。

- ForceUpdate

类型：布尔值

描述：(可选) 如果为真，则更新不会因容器组中断预算违规而失败。

- KubernetesVersion

类型：字符串

描述：(可选) 要将节点组更新到的 Kubernetes 版本。

- LaunchTemplateId

类型：字符串

描述：(可选) 启动模板的 ID。

- LaunchTemplateName

类型：字符串

描述：(可选) 启动模板的名称。

- LaunchTemplateVersion

类型：字符串

描述：(可选) Amazon Elastic Compute Cloud (Amazon EC2) 启动模板版本。此参数仅在节点组是根据启动模板创建时才有效。

以下参数仅适用于 Configuration 更新类型：

- AddOrUpdateNodeGroupLabels

类型：StringMap

描述：(可选) 要添加或更新的 Kubernetes 标签。

- AddOrUpdateKubernetesTaintsEffect

类型：StringList

描述：(可选) 要添加或更新的 Kubernetes 污点。

- MaxUnavailableNodeGroups

类型：整数

默认：0

描述：(可选) 版本更新期间一次不可用的最大节点数量。设置为 0 (默认) 以保留当前设置。

- MaxUnavailablePercentageNodeGroup

类型：整数

默认值：0

描述：(可选) 版本更新期间不可用的节点的最大百分比。设置为 0 (默认) 以保留当前设置。

- NodeGroupDesiredSize

类型：整数

默认值：-1

描述：(可选) 托管节点组应保留的当前节点数。设置为 -1 (默认) 以保留当前设置。

- NodeGroupMaxSize

类型：整数

默认值：0

描述：(可选) 托管节点组可以扩展到的最大节点数。设置为 0 (默认) 以保留当前设置。

- NodeGroupMinSize

类型：整数

默认值：-1

描述：(可选) 托管节点组可以缩减到的最小节点数。设置为 -1 (默认) 以保留当前设置。

- RemoveKubernetesTaintsEffect

类型：StringList

描述：(可选) 要删除的 Kubernetes 污点。

- RemoveNodeGroupLabels

类型：StringList

描述：(可选) 要删除的以逗号分隔的标签列表。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- eks:DescribeUpdate
- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

文档步骤

- aws:executeScript - 根据您为运行手册输入参数指定的值更新 Amazon EKS 集群节点组。
- aws:waitForAwsResourceProperty - 等待集群更新状态变为 Successful。

AWS-UpdateEKSSelfManagedLinuxNodeGroups

描述

AWS-UpdateEKSSelfManagedLinuxNodeGroups 运行手册使用 AWS CloudFormation 堆栈更新 Amazon Elastic Kubernetes Service (Amazon EKS) 集群中的自托管节点组。

如果您的集群使用自动扩缩，则我们建议在使用此运行手册之前将部署缩小到两个副本。

将部署扩展到两个副本

1. 安装 Kubernetes 命令行实用程序 kubectl。有关更多信息，请参阅 Amazon EKS 用户指南 中的 [安装 kubectl](#)。
2. 运行如下命令。

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. 运行 AWS-UpdateEKSSelfManagedLinuxNodeGroups 运行手册。
4. 运行以下命令，将部署缩回到所需的副本数。

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必需) Amazon EKS 集群的名称。

- NodeGroupName

类型：字符串

描述：(必需) 托管节点组的名称。

- ClusterControlPlaneSecurityGroup

类型：字符串

描述：(必需) 控制面板安全组的 ID。

- DisableIMDSv1

类型：布尔值

描述：(可选) 确定您是否要允许实例元数据服务版本 1 (IMDSv1) 和 IMDSv2。

- KeyName

类型：字符串

描述：(可选) 实例的密钥名称。

- NodeAutoScalingGroupDesiredCapacity

类型：字符串

描述：(可选) 节点组应保留的节点数。

- NodeAutoScalingGroupMaxSize

类型：字符串

描述：(可选) 节点组可以扩展到的最大节点数。

- NodeAutoScalingGroupMinSize

类型：字符串

描述：(可选) 节点组可以缩减到的最小节点数。

- **NodeInstanceType**

类型：字符串

默认：t3.large

描述：(可选) 要用于节点组的实例类型。

- **NodeImageId**

类型：字符串

描述：(可选) 希望节点组使用的 Amazon Machine Image (AMI) 的 ID。

- **NodeImageIdSSMParam**

类型：字符串

默认：/aws/service/eks/optimized-ami/1. 21/amazon-linux-2/recommended /image_id

描述：(可选) 希望节点组使用的 AMI 的公共 Systems Manager 参数。

- **StackName**

类型：字符串

描述：(必填) 用于更新节点组的 CloudFormation 堆栈的名称。

- **子网**

类型：字符串

描述：(必需) 要集群使用的子网的逗号分隔列表。

- **VpcId**

类型：字符串

默认：Default

描述：(必需) 部署集群的虚拟私有云 (VPC) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- eks:CreateCluster
- eks:CreateNodegroup
- eks>DeleteNodegroup
- eks>DeleteCluster
- eks:DescribeCluster
- eks:DescribeNodegroup
- eks:ListClusters
- eks:ListNodegroups
- eks:UpdateClusterConfig
- eks:UpdateNodegroupConfig

文档步骤

- aws:executeScript - 根据您为运行手册输入参数指定的值更新 Amazon EKS 集群节点组。
- aws:waitForAwsResourceProperty-等待 CloudFormation 堆栈更新状态返回。

AWSSupport-CollectEKSLinuxNodeStatistics

描述

AWSSupport-CollectEKSLinuxNodeStatistics运行手册从属于 Amazon EKS 集群的 Amazon EC2 实例以及该实例上运行的容器 (如果指定了容器 ID) 收集 Linux 统计数据。containerdAmazon EC2 实例必须由管理 AWS Systems Manager。

收集的主机级 Linux 统计数据包括：

- 操作系统信息。
- 网络接口统计信息-来自ethtool和/sys/class/net/interface/statistics目录。
- 文件描述符很重要。
- 临时端口很重要。
- 一堆iptables规则。

- 查看完整的 conntrack 表。

容器级 Linux 统计数据包括：

- 标识符信息-图片 URI 和标签。
- 网络接口统计信息-来自 ethtool 和 /sys/class/net/interface/statistics 目录。
- 如果 NetworkTargets 参数已填充，则会生成跟踪路径和 DNS 结果。
- 数据包捕获分析计数-TCP 重传、乱序数据包等

该运行手册收集来自各种 Linux 发行版的数据，包括亚马逊 Linux 2、亚马逊 Linux 2023 和 Debian/Ubuntu。它使用来自 Amazon ECR 公共图库的以下图像的最新版本：

- amazon-ecs-network-sidecar 图片以获取故障排除工具的访问权限。
- aws-cli 图片，用于将统计报告 JSON 文件和数据包捕获文件上传到指定的 Amazon S3 存储桶。

Important

本运行手册不支持 Fargate 实例。如果实例在执行期间关闭或断开连接，则此运行手册可能会失败。

如何工作？

运行手册执行以下操作：

- 验证目标 Amazon S3 存储桶是否未授予公共读取或写入权限。
- 确保目标 Amazon EC2 实例由 Systems Manager 管理并处于运行状态。
- 验证实例是否运行 Linux 操作系统。
- 从 Amazon EC2 实例收集全面的 Linux 统计数据，也可以从指定的容器中收集全面的 Linux 统计数据。
- 将收集的统计数据上传到指定的 Amazon S3 存储桶。

[运行此自动化 \(控制台\)](#)

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

该AutomationAssumeRole参数需要以下操作：

- s3:GetAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketLocation
- s3:GetEncryptionConfiguration
- s3:PutObject
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- ec2:DescribeInstances

示例 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration"
      ],
    },
  ],
}
```

```

        "Resource": "arn:aws:s3:::S3_BUCKET_NAME"
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::S3_BUCKET_NAME/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeInstanceInformation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ssm:SendCommand"
        ],
        "Resource": [
            "arn:aws:ssm:*:*:document/AWS-RunShellScript",
            "arn:aws:ec2:*:111122223333:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ssm:GetCommandInvocation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances"
        ],
        "Resource": "*"
    }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-CollectEKSLinuxNodeStatistics](#) 在 Systems Manager 的“文档”下导航至。

2. 选择 Execute automation (执行自动化) 。

3. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId (必填)：

用于收集统计数据的 Amazon EC2 实例的 ID。

- S3BucketName (必填)：

用于将 JSON 输出从亚马逊 EC2 实例导出为文件的 Amazon S3 存储桶的名称。

- S3KeyPrefix (可选)：

用于将 Amazon EC2 实例的 JSON 输出作为文件导出的 Amazon S3 密钥前缀 (子文件夹)。默认值：AWSSupport-CollectEKSLinuxNodeStatistics。

- S3BucketOwnerRoleArn (可选)：

有权获取 Amazon S3 存储桶和账户封禁公开访问设置、存储桶加密配置、存储桶、存储桶策略状态以及将对象上传到存储桶的 IAM 角色的 ARN。ACLs 如果未指定此参数，则运行手册将使用 AutomationAssumeRole (如果已指定) 或用户启动此 runbook (如果 AutomationAssumeRole 未指定)。

- S3BucketOwnerAccount (可选)：

拥有 Amazon S3 存储桶的 AWS 账户。如果您未指定此参数，则运行手册会假定存储桶位于此账户中。

- ContainerId (可选)：

在指定的 Amazon EC2 实例上运行的容器的 ID。

- NetworkTargets (可选)：

以逗号分隔 IPv4 的地址、用于测试 and/or DNS 解析的 DNS 名称以及使用 traceroute 进行连接的列表。

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **CheckBucketAccess:**

检查目标 Amazon S3 存储桶是否有可能授予对其对象的读 and/or 写公共访问权限。

- **AssertInstanceIsSSMManaged:**

确保目标 Amazon EC2 实例由 Systems Manager 管理，否则自动化将结束。

- **VerifyInstanceState:**

在尝试收集统计数据之前，验证 Amazon EC2 实例是否处于运行状态。

- **BranchOnVerifyLinuxInstance:**

在继续操作之前，请验证该实例是否为 Linux 实例。

- **BranchOnVerifyInstanceRunning:**

在继续操作之前，请验证实例是否处于运行状态。

- **CollectEKSLinuxNodeStatistics:**

从 Amazon EC2 实例收集全面的 Linux 统计数据，包括操作系统信息、网络接口统计信息、文件描述符、临时端口、防火墙规则以及可选的容器级统计信息。

- **GenerateStatisticsOutputS3Uri:**

生成 Linux 统计文件的完整 Amazon S3 URI，用作自动化文档的输出。

7. 完成后，查看“输出”部分以了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-CollectEKSIInstanceLogs

描述

AWSSupport-CollectEKSIInstanceLogs 运行手册从 Amazon Elastic Compute Cloud (Amazon EC2) 实例收集操作系统和 Amazon Elastic Kubernetes Service (Amazon EKS) 相关日志文件，以帮助解决常见问题。在此自动化收集关联的日志文件时，会对文件系统结构进行更改，包括创建临时目录、将日志文件复制到临时目录以及将日志文件压缩到档案中。此活动可能会导致 Amazon EC2 实例上的 CPUUtilization 增加。有关更多信息 CPUUtilization，请参阅 Amazon CloudWatch 用户指南中的[实例指标](#)。

如果您为 LogDestination 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 Amazon EC2 实例收集的日志的安全，如果策略状态 isPublic 设置为 true，或者如果访问控制列表 (ACL) 向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，日志将不会上传。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的[Amazon S3 预定义组](#)。

Note

这种自动化需要连接到您的亚马逊 EC2 实例的亚马逊弹性块存储 (Amazon EBS) 根卷上至少 10% 的可用磁盘空间。如果根卷上没有足够的可用磁盘空间，此自动化将停止。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EKSInstance我是

类型：字符串

描述：(必填) 您要从中收集日志的 Amazon EKS Amazon EC2 实例的 ID。

- LogDestination

类型：字符串

描述：(可选) 您账户中用于上传存档日志的亚马逊简单存储服务 (Amazon S3) 存储桶。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand

亚马逊 EC2 实例配置文件所需的 IAM 权限

使用的实例配置文件EKSInstanceId必须附有 Amazon SSMManaged InstanceCore Amazon 托管策略。

它还必须能够访问 LogDestination Amazon S3 存储桶，这样它才能上传收集的日志。以下是可以附加到该实例配置文件的 IAM 策略的示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
```

```

        "s3:GetBucketAcl"
    ],
    "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
    ]
}
]
}

```

如果LogDestination使用 AWS KMS 加密，则必须在 IAM 策略中添加一条额外的声明，授予对加密中使用的 AWS KMS 密钥的访问权限：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KMS-KEY-ID"
    }
  ]
}

```

文档步骤

- `aws:assertAwsResourceProperty` - 确认您在 `EKSInstanceId` 参数中指定的值的操作系统为 Linux。

- `aws:runCommand` - 收集操作系统和 Amazon EKS 相关日志文件，从而将其压缩到 `/var/log` 目录中的档案中。
- `aws:branch` - 确认是否为 `LogDestination` 参数指定了一个值。
- `aws:runCommand`-将日志档案上传到您在`LogDestination`参数中指定的 Amazon S3 存储桶。

AWSsupport-SetupK8sApiProxyForEKS

描述

AWSsupport-SetupK8sApiProxyForeKs 自动化运行手册提供了一种创建函数的方法，该 AWS Lambda 函数充当对亚马逊 Elastic Kubernetes Service 集群终端节点进行控制平面 API 调用的代理。它可以作为运行手册的构建块，这些运行手册需要调用控制平面 API 来自动执行任务和排除 Amazon EKS 集群的问题。

Important

此自动化创建的所有资源都已标记，因此可以轻松找到它们。使用的标签是：

- `AWSsupport-SetupK8sApiProxyForEKS : true`

Note

- 自动化是一个辅助运行手册，不能作为独立运行手册执行。对于需要对 Amazon EKS 集群进行控制平面 API 调用的运行手册，它被当作子级自动化调用。
- 请确保在使用后进行Cleanup操作，以免产生不必要的费用。

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必填) 亚马逊 Elastic Kubernetes Service 集群的名称。

- 操作

类型：字符串

描述：(必需) 要执行的操作：Setup在账户中配置 Lambda 函数，Cleanup将取消配置在设置阶段创建的资源。

允许的值：Setup| Cleanup

默认：设置

- LambdaRoleArn

类型：字符串

描述：(可选) 允许该 AWS Lambda 函数访问所需 AWS 服务和资源的 IAM 角色的 ARN。如果未指定任何角色，则此 Systems Manager Automation 将在您的账户中为 Lambda 创建一个 IAM 角色Automation-K8sProxy-Role-`<ExecutionId>`，其名称包含托管策略：AWSLambdaBasicExecutionRole和。AWSLambdaVPCAccessExecutionRole

如何工作？

运行手册执行以下步骤：

- 验证自动化是否作为子执行运行。当作为独立运行手册调用时，运行手册将不起作用，因为它本身无法执行任何有意义的工作。
- 检查指定集群的代理 Lambda 函数的现有 CloudFormation 堆栈。

- 如果堆栈存在，则会重复使用现有基础架构，而不是重新创建它。
- 参考计数器使用标签进行维护，以确保如果运行手册被同一集群的另一个 runbook 重复使用，则该运行手册不会删除该基础架构。
- 执行为调用指定的操作类型 (Setup/Cleanup) :
 - 设置：创建或描述现有资源。
 - 清理：如果任何其他 runbook 未使用基础架构，则移除已配置的资源。

所需的 IAM 权限

该AutomationAssumeRole参数需要以下权限 LambdaRoleArn未通过：

- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation>DeleteStack
- cloudformation:UpdateStack
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2>DeleteNetworkInterface
- eks:DescribeCluster
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:ListTags
- lambda:GetFunction
- lambda:ListTags
- lambda:TagResource
- lambda:UntagResource
- lambda:UpdateFunctionCode

- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:TagResource
- logs:UntagResource
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:ListTagsForResource
- iam:CreateRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy
- iam:PassRole
- iam:GetRole
- iam>DeleteRole
- iam:TagRole
- iam:UntagRole
- tag:GetResources
- tag:TagResources

如果LambdaRoleArn提供了自动化，则无需创建角色，并且可以排除以下权限：

- iam:CreateRole
- iam>DeleteRole
- iam:TagRole
- iam:UntagRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy

以下是一个策略示例，演示了未通过 AutomationAssumeRoleLambdaRoleArn时所需的权限：

JSON

```
{
```



```

"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "tag:GetResources",
      "tag:TagResources",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2>DeleteNetworkInterface",
      "eks:DescribeCluster",
      "iam:GetRole",
      "cloudformation:DescribeStacks",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "lambda:GetFunction",
      "lambda:ListTags",
      "logs:ListTagsForResource"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowActionsWithoutConditions"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    },
    "Action": "iam:CreateRole",
    "Resource": [
      "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AllowCreateRoleWithRequiredTag"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    }
  }
]

```

```

    },
    "Action": [
        "iam:DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "IAMActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        },
        "StringLike": {
            "iam:PolicyARN": [
                "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaBasicExecutionRole",
                "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaVPCLambdaAccessExecutionRole"
            ]
        }
    },
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AttachRolePolicy"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "lambda:CreateFunction",

```

```

        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode"
    ],
    "Resource": "arn:aws:lambda:us-east-1:111122223333:function:Automation-K8sProxy*",
    "Effect": "Allow",
    "Sid": "LambdaActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack"
    ],
    "Resource": "arn:aws:cloudformation:us-east-1:111122223333:stack/AWSSupport-SetupK8sApiProxyForEKS*",
    "Effect": "Allow",
    "Sid": "CloudFormationActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*",

```

```

        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/
Automation-K8sProxy*:*"
    ],
    "Effect": "Allow",
    "Sid": "LogsActions"
  },
  {
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": "lambda.amazonaws.com"
      }
    },
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "arn:aws:iam::111122223333:role/Automation-K8sProxy-Role*"
    ],
    "Effect": "Allow",
    "Sid": "PassRoleToLambda"
  }
]
}

```

如果通过，请确保它已为公共集群以及私有集群附加了 [AWSLambdaBasicExecutionRole](#) 策略。LambdaRoleArn [AWSLambdaVPCAccessExecutionRole](#)

资源已创建

以下资源是在Setup操作期间创建的：

1. AWS Lambda 函数
2. IAM 角色：Lambda 执行角色（如果未提供）。
3. CloudWatch 日志组（Lambda 日志）

在执行Cleanup操作之前，Lambda 函数和执行角色将一直保留。Lambda 日志组将保留 30 天或直到手动删除。

说明

运行手册是一个辅助工具，旨在作为子自动化从其他运行手册中执行。它促进了基础设施的创建，使父运行手册能够调用 Amazon EKS K8s 控制平面 API。要使用运行手册，您可以在父自动化的上下文中执行以下步骤。

1. 设置阶段：使用运行手册中的 `aws:executeAutomation` 操作调用自动化，该操作要在操作设置为的情况下进行 Amazon EKS K8s 控制平面 API 调用。Setup

输入参数示例：

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

该 `aws:executeAutomation` 步骤的输出将包含代理 Lambda 函数的 ARN。

2. 使用 Lambda 代理：使用 `Lambda.Client.invoke(...)` 带有 API 调用路径列表和持有者令牌 `boto3` 的，在 `aws:executeScript` 操作中调用 Lambda 函数。Lambda 函数将通过将持有者令牌作为授权标头的一部分传递来对指定路径执行 HTTP GET 调用。

Lambda 调用事件的示例：

```
{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "... "
}
```

Note

持有者令牌必须作为父级自动化脚本的一部分生成。您需要确保执行父运行手册的委托人拥有对指定 Amazon EKS 集群的只读权限。

3. 清理阶段：使用运行手册中的 `aws:executeAutomation` 操作调用自动化，该操作要在操作设置为的情况下进行 Amazon EKS K8s 控制平面 API 调用。Cleanup

输入参数示例：

```
{
  "AutomationAssumeRole": "<role-arn>",
```

```
"ClusterName": "<eks-cluster-name>",  
"Operation": "Cleanup"  
}
```

自动化步骤

1. ValidateExecution

- 验证自动化是否未作为独立执行运行。

2. CheckForExistingStack

- 检查是否已经为指定的集群名称配置了 CloudFormation 堆栈。
- 返回堆栈存在状态以及是否可以安全删除。

3. BranchOnIsStackExists

- 基于堆栈存在情况进行分支的决策步骤。
- 更新现有堆栈名称或继续操作分支的路由。

4. UpdateStackName

- 使用现有堆栈的名称更新 StackName 变量。
- 仅在堆栈已经存在时才执行。

5. BranchOnOperation

- 根据 Operation 参数 (Setup/Cleanup) 对自动化进行路由。
- For Setup : 创建新堆栈或描述现有资源的路由。
- For Cleanup : 如果可以安全删除, 则继续删除堆栈。

6. GetClusterNetworkConfig

- 描述用于获取 VPC 配置的 Amazon EKS 集群。
- 检索终端节点、VPC ID IDs、子网、安全组 ID 和 CA 数据。

7. ProvisionResources

- 使用所需资源创建 CloudFormation 堆栈。
- 使用必要的网络配置配置 Lambda 函数。
- 为所有资源添加标签以进行跟踪和管理。

8. DescribeStackResources

- 检索有关 created/existing 堆栈的信息。

9. BranchOnIsLambdaDeploymentRequired

- 确定是否需要部署 Lambda 代码。
- 仅对新创建的堆栈进行部署。

10DeployLambdaFunctionCode

- 使用部署包部署 Lambda 函数代码。
- 使用代理实现更新函数。

11AssertLambdaAvailable

- 验证 Lambda 函数代码更新是否成功。
- 等待函数进入Successful状态。

12PerformStackCleanup

- 删除 CloudFormation 堆栈和相关资源。
- 在Cleanup操作期间或操作失败时执行。 Setup

输出

LambdaFunctionArn: 代理 Lambda 函数的 ARN

参考

Systems Manager Automation

- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSsupport-TroubleshootEbsCsiDriversForEks

描述

该AWSsupport-TroubleshootEbsCsiDriversForEks运行手册有助于解决亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 中的亚马逊 Elastic Block Store 卷装载问题和亚马逊 EBS 容器存储接口 (CSI) 驱动程序问题

Important

目前不支持在上 AWS Fargate 运行的 Amazon EBS CSI 驱动程序。

如何工作？

运行手册AWSsupport-TroubleshootEbsCsiDriversForEks执行以下高级步骤：

- 验证目标 Amazon EKS 集群是否存在且处于活动状态。
- 根据插件是 Amazon EKS 管理的还是自行管理的，部署必要的身份验证资源，用于调用 Kubernetes API。
- 执行 Amazon EBS CSI 控制器运行状况检查和诊断。
- 对节点角色和服务账号角色运行 IAM 权限检查。
- 诊断指定应用程序 Pod 的持续卷创建问题。
- 检查 node-to-pod调度并检查 pod 事件。
- 收集相关的 Kubernetes 和应用程序日志，并将它们上传到指定的 Amazon S3 存储桶。
- 执行节点运行状况检查并验证与 Amazon EC2 终端节点连接。
- 查看永久音量块设备附件和安装状态。
- 清理故障排除期间创建的身份验证基础架构。
- 生成包含所有诊断结果的全面故障排除报告。

Note

- Amazon EKS 集群的身份验证模式必须设置为API或API_AND_CONFIG_MAP。我们建议使用 Amazon EKS Access 入口。运行手册需要 Kubernetes 基于角色的访问控制 (RBAC) 权限才能执行必要的 API 调用。
- 如果您没有为 Lambda 函数 (LambdaRoleArn参数) 指定 IAM 角色，则自动化会在您的账户Automation-K8sProxy-Role-<ExecutionId>中创建一个名为的角色。此角色包括托管策略AWSLambdaBasicExecutionRole和AWSLambdaVPCLambdaAccessExecutionRole。
- 某些诊断步骤要求将 Amazon EKS 工作节点设为 Systems Manager 托管实例。如果节点不是 Systems Manager 托管实例，则会跳过需要 Systems Manager 访问权限的步骤，但会继续进行其他检查。
- 自动化包括一个清理步骤，用于删除身份验证基础架构资源。即使之前的步骤失败，此清理步骤也会运行，这有助于防止您的 AWS 账户中出现孤立资源。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceStatus
- ec2:GetEbsEncryptionByDefault
- eks:DescribeAddon
- eks:DescribeAddonVersions
- eks:DescribeCluster
- iam:GetInstanceProfile
- iam:GetOpenIDConnectProvider
- iam:GetRole
- iam:ListOpenIDConnectProviders
- iam:SimulatePrincipalPolicy
- s3:GetBucketLocation
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:ListBucket
- s3:ListBucketVersions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetDocument

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

说明

按照这些步骤对自动化进行配置：

1. 在您的账户 `TroubleshootEbsCsiDriversForEks-SSM-Role` 中创建 SSM 自动化角色。验证信任关系是否包含以下策略。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 将以下策略附加到 IAM 角色，以授予对指定资源执行指定操作所需的权限。

- 如果您希望将执行和资源日志上传到同一 AWS 区域的 Amazon S3 存储桶，请在中替换 `arn:{partition}:s3:::BUCKET_NAME/*` 为您的日志 `OptionalRestrictPutObjects`。
- 如果您要在 SSM 执行中选择 `S3BucketName`，Amazon S3 存储桶应指向正确的亚马逊 S3 存储桶。
- 如果您未指定，则此权限是可选的 `S3BucketName`
- Amazon S3 存储桶必须是私有的，并且位于执行 SSM 自动化的同一 AWS 区域。

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "OptionalRestrictPutObjects",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeIamInstanceProfileAssociations",
      "ec2:DescribeInstanceStatus",
      "ec2:GetEbsEncryptionByDefault",
      "eks:DescribeAddon",
      "eks:DescribeAddonVersions",
      "eks:DescribeCluster",
      "iam:GetInstanceProfile",
      "iam:GetOpenIDConnectProvider",
      "iam:GetRole",
      "iam:ListOpenIDConnectProviders",
      "iam:SimulatePrincipalPolicy",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketVersioning",
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "ssm:DescribeInstanceInformation",
      "ssm:GetAutomationExecution",
      "ssm:GetDocument",
      "ssm:ListCommandInvocations",
      "ssm:ListCommands",
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SetupK8sApiProxyForEKSActions",

```

```

    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole",
        "iam:TagRole",
        "iam:UntagRole",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",

```

```

        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
            "arn:aws:iam::*:role/Automation-K8sProxy-Role-*"
        ],
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": [
                    "lambda.amazonaws.com",
                    "ssm.amazonaws.com"
                ]
            }
        }
    },
    {
        "Sid": "AttachRolePolicy",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:DetachRolePolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
            }
        }
    }
]
}

```

3. 授予 Amazon EKS 集群 RBAC (基于角色的访问控制) 所需的权限。推荐的方法是在您的 Amazon EKS 集群中创建访问入口。

在 Amazon EKS 控制台中，导航到您的集群。对于 Amazon EKS 访问条目，请确认您的访问配置设置为 API_AND_CONFIG_MAP 或 API。有关为访问条目配置身份验证模式的步骤，请参阅 [设置访问条目](#)。

选择创建访问条目。

- 对于 IAM 委托人 ARN，请选择您在上一步中为 SSM 自动化创建的 IAM 角色。
- 对于类型，选择 Standard。

4. 添加访问策略：

- 在“访问范围”中，选择Cluster。
- 在“策略名称”中，选择AmazonEKSAAdminViewPolicy。

选择添加策略。

如果您不使用访问权限条目来管理 Kubernetes API 权限，则必须更新aws-auth ConfigMap 并在您的 IAM 用户或角色之间创建角色绑定。确保你的 IAM 实体拥有以下只读 Kubernetes API 权限：

- GET /apis/apps/v1/namespaces/{namespace}/deployments/{name}
- GET /apis/apps/v1/namespaces/{namespace}/replicasets/{name}
- GET /apis/apps/v1/namespaces/{namespace}/daemonsets/{name}
- GET /api/v1/nodes/{name}
- GET /api/v1/namespaces/{namespace}/serviceaccounts/{name}
- GET /api/v1/namespaces/{namespace}/persistentvolumeclaims/{name}
- GET /api/v1/persistentvolumes/{name}
- GET /apis/storage.k8s.io/v1/storageclasses/{name}
- GET /api/v1/namespaces/{namespace}/pods/{name}
- GET /api/v1/namespaces/{namespace}/pods
- GET /api/v1/namespaces/{namespace}/pods/{name}/log
- GET /api/v1/events

5. 运行自动化 [AWSSupport-TroubleshootEbsCsiDriversForEks](#) (控制台)

6. 选择 Execute automation (执行自动化)。

7. 对于输入参数，请输入以下内容：

- AutomationAssumeRole (可选) :
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。需要将该角色添加到您的 Amazon EKS 集群访问条目或 RBAC 权限中，才能允许 Kubernetes API 调用。
 - 类型：AWS::IAM::Role::Arn
 - 示例：TroubleshootEbsCsiDriversForEks-SSM-Role
- EksClusterName:
 - 描述：目标亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 集群的名称。
 - 类型：String

- **ApplicationPodName:**
 - 描述：在 Amazon EBS CSI 驱动程序中存在问题的 Kubernetes 应用程序容器的名称。
 - 类型：String
- **ApplicationNamespace:**
 - 描述：Amazon EBS CSI 驱动程序存在问题的应用程序容器的 Kubernetes 命名空间。
 - 类型：String
- **EbsCsiControllerDeploymentName (可选) :**
 - 描述：(可选) Amazon EBS CSI 控制器容器的部署名称。
 - 类型：String
 - 默认值：ebs-csi-controller
- **EbsCsiControllerNamespace (可选) :**
 - 描述：(可选) 亚马逊 EBS CSI 控制器舱的 Kubernetes 命名空间。
 - 类型：String
 - 默认值：kube-system
- **S3BucketName (可选) :**
 - 描述：(可选) 将上传故障排除日志的目标 Amazon S3 存储桶名称。
 - 类型：AWS::S3::Bucket::Name
- **LambdaRoleArn (可选) :**
 - 描述：(可选) 允许该 AWS Lambda 函数访问所需 AWS 服务和资源的 IAM 角色的 ARN。
 - 类型：AWS::IAM::Role::Arn

选择执行。

8. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)

有关亚马逊 EBS CSI 驱动程序的更多信息，请参阅[亚马逊 EBS CSI 驱动程序](#)。

AWSSupport-TroubleshootEKSALBControllerIssues

描述

AWSSupport-TroubleshootEKSALBControllerIssues 自动化运行手册可帮助诊断导致 AWS 负载均衡器控制器无法正确配置和管理适用于 Kubernetes 入口和服务的应用程序负载均衡器 (ALB) 和网络负载均衡器 (NLB) 的常见问题。

本运行手册对基本组件进行 end-to-end 验证，包括 OIDC 身份提供商设置、IRSA 配置、网络先决条件、ingress/service 配置和资源配额。它还会捕获控制器日志和相关的 Kubernetes 资源配置，以帮助识别错误配置或操作问题。

Important

本自动化运行手册专为使用亚马逊弹性计算云 (Amazon EC2) 节点组的亚马逊 EKS 集群而设计，目前不支持在上面运行的集群。AWS Fargate

如何工作？

运行手册 AWSSupport-TroubleshootEKSALBControllerIssues 执行以下高级步骤：

- 验证 Amazon EKS 集群状态、访问条目配置和 OIDC 提供商设置。
- 为 Kubernetes API 通信创建临时的 Lambda 代理。
- 检查 AWS Load Balancer Controller 部署和服务帐户配置。
- 验证 pod 身份 webhook 和 IAM 角色注入。
- 验证 Application Load Balancer 和 Network Load Balancer 配置的子网配置和标记。
- 根据当前使用情况检查应用程序负载均衡器和网络负载均衡器账户配额。
- 验证入口和服务资源注释。
- 检查工作节点安全组标记以实现负载均衡器集成。
- 收集控制器 pod 日志以进行诊断。
- 清理临时身份验证资源。
- 生成包含发现结果和补救步骤的诊断报告。

 Note

- Amazon EKS 集群必须为运行此自动化的 IAM 实体配置访问入口。集群的身份验证模式必须设置为API或API_AND_CONFIG_MAP。如果没有正确的访问权限条目配置，自动化将在初始验证期间终止。
- 该LambdaRoleArn参数是必需的，必须具有 AWS 托管策略AWSLambdaBasicExecutionRole并AWSLambdaVPCAccessExecutionRole附上该参数，以允许代理函数与 Kubernetes API 通信。
- Load Balancer 控制器必须是版本v2.1.1或更高版本。
- 自动化包括一个清理步骤，用于删除临时身份验证基础架构资源。即使之前的步骤失败，此清理步骤也会运行，从而确保您的 AWS 账户中没有孤立的资源。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:UpdateStack
- ec2:CreateNetworkInterface
- ec2>DeleteNetworkInterface
- ec2:DescribeInstances

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `eks:ListAssociatedAccessPolicies`
- `elasticloadbalancing:DescribeAccountLimits`
- `elasticloadbalancing:DescribeLoadBalancers`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:PassRole`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:ListTagsForResource`
- `logs:PutLogEvents`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `logs:UntagResource`
- `ssm:DescribeAutomationExecutions`

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `tag:GetResources`
- `tag:TagResources`

说明

按照以下步骤配置和运行自动化：

Note

在运行自动化之前，请按照以下步骤配置所需的 IAM 角色：一个角色让 Systems Manager Automation 执行运行手册，另一个角色让 Lambda 与 Kubernetes API 通信：

1. 在您的账户 `TroubleshootEKSALBController-SSM-Role` 中创建 SSM 自动化角色。验证信任关系是否包含以下策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 附上以下 IAM 策略以授予所需权限：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "TroubleshootEKSALBControllerIssuesActions",
        "Effect": "Allow",
        "Action": [
            "eks:DescribeCluster",
            "eks:ListAssociatedAccessPolicies",
```

```

        "iam:GetRole",
        "iam:ListOpenIDConnectProviders",
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeAccountLimits",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "SetupK8sApiProxyForEKSACTIONS",
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "iam:GetRole",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
    ]
}

```

```

        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "lambda.amazonaws.com",
                "ssm.amazonaws.com"
            ]
        }
    }
}
}]
}

```

3. 为您的 Amazon EKS 集群配置访问入口。这是自动化的强制性要求。有关为访问条目配置身份验证模式的步骤，请参阅[设置访问条目](#)。

在 Amazon EKS 控制台中，导航到您的集群并按照以下步骤操作：

- 在“访问权限”部分下，验证您的身份验证配置是否设置为API或API_AND_CONFIG_MAP。
- 选择创建访问条目并配置：
 - 对于 IAM 委托人 ARN，请选择您创建的 IAM 角色 () TroubleshootEKSSALBController-SSM-Role。
 - 对于类型，选择 Standard。
- 添加访问策略：
 - 在“策略名称”中，选择AmazonEKSSAdminViewPolicy。
 - 在“访问范围”中，选择Cluster。

- 选择添加策略。
 - 验证详细信息并选择“创建”。
4. 为 Lambda 函数创建一个 IAM 角色（在输入参数 `LambdaRoleArn` 中引用）：
- 使用以下信任策略创建新的 IAM 角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 将以下 AWS 托管策略附加到此角色：
- `AWSLambdaBasicExecutionRole`
- `AWSLambdaVPCLAccessExecutionRole`
- 请记住此角色的 ARN，因为 `LambdaRoleArn` 输入参数需要使用它。

1. [AWSSupport-TroubleshootEKSALBControllerIssues](#) 在 S AWS systems Manager 控制台中导航至。

2. 选择执行自动化。

3. 要输入参数，请输入以下内容：

- `AutomationAssumeRole`（可选）：

类型： `AWS::IAM::Role`: Arn

描述：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

允许的模式：`^arn:(?:aws|aws-cn|aws-us-gov):iam::\d{12}:role/?[a-zA-Z_0-9+=,.\@|-_/\]+`

- `EksClusterName`（必填）：

类型：字符串

描述：（必填）亚马逊 Elastic Kubernetes Service（亚马逊 EKS）集群的名称。

允许的模式：`^[0-9a-zA-Z][a-zA-Z0-9-]{0,99}$`

- ALBControllerDeploymentName（可选）：

类型：字符串

描述：（可选）您的 Amazon EKS 集群中部署的 AWS Load Balancer 控制器的名称。除非您在安装过程中对其进行了自定义，否则通常为 `aws-load-balancer-controller`。

允许的模式：`^[a-z0-9]([-a-z0-9]{0,251}[a-z0-9])?$`

默认：`aws-load-balancer-controller`

- ALBController命名空间（可选）：

类型：字符串

描述：（可选）部署 AWS 负载均衡器控制器的 Kubernetes 命名空间。默认情况下，这是 `kube-system`，但是如果您将控制器安装在自定义命名空间中，则可能会有所不同。

允许的模式：`^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?$`

默认：`kube-system`

- ServiceAccountName（可选）：

类型：字符串

描述：（可选）与 AWS 负载均衡器控制器关联的 Kubernetes 服务账户的名称。除非在安装过程中进行了自定义，否则通常为 `aws-load-balancer-controller`。

允许的模式：`^[a-z0-9]([-a-z0-9]{0,251}[a-z0-9])?$`

默认：`aws-load-balancer-controller`

- ServiceAccountNamespace（可选）：

类型：字符串

描述：（可选）AWS 负载均衡器控制器的服务帐户所在的 Kubernetes 命名空间。这通常是“kube-system”，但如果您使用了自定义命名空间，则可能会有所不同。

允许的模式：`^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?$`

默认：kube-system

- IngressName（可选）：

类型：字符串

描述：（可选）要验证的入口资源的名称（Application Load Balancer）。如果未指定，则将跳过 Ingress 验证。

允许的模式：`^$|^ [a-z0-9] [a-z0-9 .-]{0,251} [a-z0-9] $`

默认：“”（空字符串）

- IngressNamespace（可选）：

类型：字符串

描述：（可选）Ingress 资源的命名空间。在指定 IngressName 时是必需的。

允许的模式：`^$|^ [a-z0-9] [a-z0-9-]{0,61} [a-z0-9] $`

默认：“”（空字符串）

- ServiceName（可选）：

类型：字符串

描述：（可选）用于验证网络负载均衡器（网络负载均衡器）注释的特定服务资源的名称。如果未指定，则将跳过服务资源验证。

允许的模式：`^$|^ [a-z0-9] [a-z0-9 .-]{0,251} [a-z0-9] $`

默认：“”（空字符串）

- ServiceNamespace（可选）：

类型：字符串

描述：（可选）服务资源的命名空间。在指定 ServiceName 时是必需的。

允许的模式：`^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $`

默认："" (空字符串)

- LambdaRoleArn (必填) :

类型:: AWS::IAM::Role: Arn

描述：(必填) 允许 (AWS Lambda Lambda) 函数访问所需 AWS 服务和资源的 IAM 角色的 ARN。将 AWS 托管策

略：AWSLambdaBasicExecutionRole和AWSLambdaVPCLAccessExecutionRole与您的 lambda 函数执行 IAM 角色相关联。

允许的模式：`^arn:(?:aws|aws-cn|aws-us-gov):iam::\d{12}:role/?[a-zA-Z_0-9+=,.\@|-_]/+$`

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- a. ValidateAccessEntryAndOIDCProvider:

通过检查访问权限和 OIDC 提供商配置来验证 Amazon EKS 集群 IAM 设置。

- b. setupk8sAuthenticationClient :

执行 SAW Document AWSSupport-SetupK8sApiProxy forek 来设置 lambda 函数以在集群上运行 Amazon EKS API 调用。

- c. 验证ALBController并且IRSASetup :

检查给定的服务帐户和 Application Load Balancer 控制器是否存在于其各自的命名空间中。还要检查 Application Load Balancer 控制器的服务账户角色注释和信任策略。

- d. VerifyPodIdentityWebhookAndEnv:

检查是否 pod-identity-webhook正在运行。还会检查 IRSA 是否被注入到 pod 的 ENV 变量中。

- e. ValidateSubnetRequirements:

检查两个可用区中至少有两个子网，有 8 个可用 IP，public/private 负载均衡器有正确的子网标记。

- f. CheckLoadBalancerLimitsAndUsage:

将账户限制与 Application Load Balancer 和 Network Load Balancer 的数量进行比较。

g. CheckIngressOrServiceAnnotations:

检查 Ingress 和 Service 资源中的注释和规格是否正确，以确保它们针对应用程序负载均衡器和网络负载均衡器的使用进行了正确配置。

h. CheckWorkerNodeSecurityGroupTags:

验证连接到工作节点的安全组是否具有所需的集群标签。

i. 捕获ALBController日志：

从 Amazon EKS 集群中运行的 Load Balancer Controller 容器中检索最新的诊断日志。AWS

j. CleanupK8sAuthenticationClient：

使用“清理”操作执行 SAW 文档“AWSSupport-SetupK8sApiProxy Foreks”，以清理作为自动化一部分创建的资源。

k. GenerateReport:

生成自动化报告。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果：

a. 报告：

提供所有已执行检查的全面摘要，包括 Amazon EKS 集群的状态、Application Load Balancer 控制器设置、IRSA 配置、子网要求、负载均衡器限制、ingress/service 注释、工作节点安全组标签和应用程序负载均衡器控制器日志。它还包括所有已发现的问题和建议的补救步骤。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

与 Load Balancer 控制器相关的文档

- [AWS Load Balancer 控制器](#)
- [设置访问条目](#)

AWSSupport-TroubleshootEKSDNSFailure

描述

该AWSSupport-TroubleshootEKSDNSFailure运行手册可帮助解决应用程序或容器遇到 DNS 解析失败时，Amazon Elastic Kubernetes Service (Amazon EKS) 中的 CoreDNS 容器和配置问题。该运行手册验证 VPC DNS 设置，检查 CoreDNS 部署，检查水平容器自动扩缩器 (HPA) 配置 ConfigMap，收集 CoreDNS 日志，并在工作节点上执行 DNS 解析检查。或者，可以在问题工作节点所在的子网中创建探测型 Amazon Elastic Compute Cloud 实例，无需直接访问该节点即可执行 DNS 解析检查。

Important

Amazon EKS 集群的身份验证模式必须设置为API或API_AND_CONFIG_MAP。本运行手册部署了一个 (AWS Lambda Lambda) 函数作为代理，以进行经过身份验证的 Kubernetes API 调用，并在执行结束时清理所有创建的资源。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型:: AWS::IAM::Role: Arn

描述 : (可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EKSClusterName

类型：字符串

描述：(必填) 目标 Amazon EKS 集群的名称。

- DnsName

类型：字符串

默认：亚马逊

描述：(可选) 应用程序或 Pod 无法解析的域名的存根域后缀。

- ProblematicNodeInstanceId

类型:: AWS::EC2::Instance: ID

描述：(可选) 运行遇到 DNS 解析错误的应用程序的工作节点的实例 ID。如果提供，运行手册将在同一子网中创建一个探测型 Amazon EC2 实例，以执行 DNS 解析检查。如果工作节点不在公有子网中，或者不允许在工作节点bind-utils上安装，则使用此参数。

- CoreDnsNamespace

类型：字符串

默认：kube-system

描述：(可选) CoreDNS 容器的 Kubernetes 命名空间。

- S3 BucketName

类型:: AWS::S3::Bucket: 姓名

描述：(可选) 上传 CoreDNS 疑难解答日志的亚马逊简单存储服务存储桶的名称。

- LambdaRoleArn

类型:: AWS::IAM::Role: Arn

描述：(可选) Lambda 代理函数的 IAM 角色的 ARN。如果未提供，则运行手册将创建一个名为AWSLambdaBasicExecutionRole和AWSLambdaVPCAccessExecutionRole托管策略Automation-K8sProxy-Role-`<ExecutionId>`的角色。建议您提供自己的角色。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- eks:DescribeCluster
- ec2:DescribeVpcs
- ec2:DescribeInstances
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation>DeleteStack
- lambda:InvokeFunction
- s3:GetBucketPublicAccessBlock
- s3:GetBucketAcl
- s3:PutObject
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文档步骤

1. AssertIfTargetClusterExists-验证中指定的 Amazon EKS 集群EksClusterName是否存在且处于ACTIVE状态。如果未找到集群或集群未处于活动状态，则运行手册将跳至。GenerateReport
2. UpdateEksClusterExists-将内部eksClusterExists变量设置为true用于报告生成。
3. GetVpcDnsSettings-检索与亚马逊 EKS 集群关联的 Amazon Virtual Private Cloud 的enableDnsSupport和enableDnsHostnames设置。
4. BranchOnVpcDnsSettings-检查两个 VPC DNS 设置是否都已启用。如果其中一个被禁用，则运行手册将跳至。GenerateReport否则，请继续DeployK8sAuthApisResources。
5. DeployK8sAuthApisResources-执行AWSSupport-SetupK8sApiProxyForEKS以部署 Lambda 函数作为代理，用于对 Amazon EKS 集群进行经过身份验证的 Kubernetes API 调用。

6. RetrieveCoreDNSDeployment-检索有关 CoreDNS 部署的信息，包括容器就绪情况、容器状态以及托管 CoreDNS 容器的节点的准备情况。还会检索 CoreDNS 集群 IP。
7. RetrieveAndInspectCoreDNSConfigMap-从 Amazon EKS 集群检索 ConfigMap CoreDNS 并检查配置问题，包括中指定域的存根域设置。DnsName
8. ValidateHpaConfiguration-检查是否为指定命名空间中的 CoreDNS 部署配置了水平容器自动扩缩器 (HPA)。
9. CheckS3BucketPublicStatus-验证中指定的 Amazon S3 存储桶S3BucketName是否不允许公开或匿名读取或写入权限。
10. CollectLogToS3-收集 CoreDNS 容器日志并将其上传到指定的 Amazon S3 存储桶。
11. BranchOnProblematicNodeInstanceId-检查ProblematicNodeInstanceId是否已提供以及 CoreDNS 主机节点是否存在。如果两个条件都满足，则继续执行VerifyThatProblematicNodeInstanceBelongsToCluster。否则，分支到BranchOnCoreDnsDeployment。
12. VerifyThatProblematicNodeInstanceBelongsToCluster-确认中指定的实例ProblematicNodeInstanceId是 Amazon EKS 集群中的工作节点。
13. UpdateProblematicNodeInstanceStanding-将内部problematicNodeInstanceStanding变量设置为true。
14. GetProblematicInstanceDetails-检索有问题的工作节点的 AMI ID、实例类型、子网 ID 和安全组 ID，以便在创建探测型 Amazon EC2 实例时使用。
15. CreateProbingInfrastructure-创建实例配置文件并通过与有问题的工作节点位于同一子网中的 AWS CloudFormation 堆栈探测 Amazon EC2 实例。堆栈已命名AWSSupport-TroubleshootEKSDNSFailure-<ExecutionId>。
16. GetProbingInstanceId-从 CloudFormation 堆栈输出中检索正在探测的 Amazon EC2 实例 ID。
17. WaitForProbingInstanceSSMAgentStateToBeOnline-等待正在探测的亚马逊 EC2 实例上的 Amazon EC2 Systems Manager 代理报告Online状态，然后再继续。
18. RetrieveCoreDNSPodsIPFromProblematicNode-检索 CoreDNS 容器的 IP 地址，如有问题的工作节点所示。
19. PerformDNSResolutionOnProbingEC2Instance-使用集群 IP 和 CoreDNS 容器 IP 对正在探测的 Amazon EC2 实例运行 DNS 解析检查。
20. DeleteCloudFormationStack-删除创建探测 Amazon EC2 实例和实例配置文件的 CloudFormation 堆栈。
21. UpdateCfnStackDeleted-将内部cfnStackDeleted变量设置为true。

- 22.BranchOnCoreDnsDeployment-检查是否ProblematicNodeInstanceId未提供以及 CoreDNS 主机节点是否存在。如果两个条件都满足，则继续执行PerformDNSResolutionOnCoreDnsWorkerNodes。否则，请继续CleanupK8sAuthenticationInfrastructure。
- 23.BranchOnCoreDnsNodesExistForRunCommandSteps-在运行步骤之前检查 CoreDNS 主机节点是否存在。aws:runCommand如果不存在任何节点（例如，当 CoreDNS 的副本为零时），则跳到。CleanupK8sAuthenticationInfrastructure
- 24.PerformDNSResolutionOnCoreDnsWorkerNodes-使用集群 IP 和 CoreDNS 容器 IP 直接在 CoreDNS 工作节点上运行 DNS 解析检查。
- 25.VerifyNameserverMatchAndKubeProxyLogsAndIPTableEntries-验证域名服务器 IP 是否与集群 IP 匹配，检查 kube-proxy pod 对 API 服务器的访问权限，并验证 CoreDNS 工作节点上的 kube-dns iptables 条目。
- 26.VerifyPPSThrottlingOnENIs-检查 CoreDNS packets-per-second 工作节点上每个弹性网络接口 (ENI) 的 DNS (PPS) 限制，以确定潜在的限制。
- 27.UpdateChecksOnNodes-将内部checksOnNodes变量设置true为以表示已执行节点级检查。
- 28.CleanupK8sAuthenticationInfrastructure-执行删除AWSSupport-SetupK8sApiProxyForEKS自动化期间创建的 Lambda 代理函数和关联资源的Cleanup操作。
- 29.UpdateK8sInfrastructreDeleted-将内部K8sInfrastructreDeleted变量设置为true。
- 30.CleanUpAllResources-如果之前的清理步骤未成功完成，则对所有剩余资源执行全面清理，包括 CloudFormation 堆栈和 Lambda 代理函数。
- 31.CollectOutputFromAllRunCommandSteps-收集并合并自动化期间执行的所
有aws:runCommand步骤的输出。
- 32.GenerateReport-将前面所有步骤的结果汇编成一份全面的评估报告，涵盖VPC DNS设置、CoreDNS部署运行状况 ConfigMap、配置、HPA配置、日志收集状态和DNS解析检查结果。

输出

GenerateReport.EvalReport-关于所执行的所有 DNS 故障排除检查的全面报告，包括发现的结果和建议的补救措施。

Elastic Beanstalk

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Elastic Beanstalk有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)
- [AWSSupport-TroubleshootElasticBeanstalk](#)

AWSSupport-CollectElasticBeanstalkLogs

描述

AWSSupport-CollectElasticBeanstalkLogs 运行手册从 Elastic Beanstalk 启动的 Amazon Elastic Compute Cloud (Amazon EC2) Windows Server 实例收集 AWS Elastic Beanstalk 相关日志文件，以帮助解决常见问题。在此自动化收集关联的日志文件时，会对文件系统结构进行更改，包括创建临时目录、将日志文件复制到临时目录以及将日志文件压缩到档案中。此活动可能会导致 Amazon EC2 实例上的 CPUUtilization 增加。有关更多信息 CPUUtilization，请参阅 Amazon CloudWatch 用户指南中的[实例指标](#)。

如果您为 S3BucketName 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 Amazon EC2 实例收集的日志的安全，如果策略状态 isPublic 设置为 true，或者如果访问控制列表 (ACL) 向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，日志将不会上传。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的[Amazon S3 预定义组](#)。

如果您没有为 S3BucketName 参数指定一个值，此自动化会将日志捆绑包上传到您运行自动化所在 AWS 区域的默认 Elastic Beanstalk Amazon S3 存储桶。该目录根据以下结构 elasticbeanstalk- *region* - *accountID* 命名。*region* 和 *accountID* 值将因地区和 AWS 账户您在中运行自动化的不同而有所不同。日志捆绑包将保存到 resources/environments/logs/bundle/ *environmentID* / *instanceID* 目录。*environmentID* 和 *instanceID* 值将因您的 Elastic Beanstalk 环境和您从中收集日志的 Amazon EC2 实例而异。

默认情况下，附加到 Elastic Beanstalk 环境的 Amazon EC2 实例的 AWS Identity and Access Management (IAM) 实例配置文件具有将捆绑包上传到您的环境的默认 Elastic Beanstalk Amazon S3 存储桶所需的权限。如果您为 S3BucketName 参数指定一个值，则附加到 Amazon EC2 实例的实例配置文件必须允许对指定的 Amazon S3 存储桶和路径执行 s3:GetBucketAcl、s3:GetBucketPolicy、s3:GetBucketPolicyStatus 和 s3:PutObject 操作。

Note

此自动化要求附加到 Amazon EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 根卷上至少有 500 MB 的可用磁盘空间。如果根卷上没有足够的可用磁盘空间，此自动化将停止。

运行此自动化 (控制台)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EnvironmentId

类型：字符串

描述：(必需) 要从中收集日志捆绑包的 Elastic Beanstalk 环境的 ID。

- InstanceId

类型：字符串

(必需) 要从中收集日志捆绑包的 Amazon Beanstalk 环境中的 Amazon EC2 实例的 ID。

- S3BucketName

类型：字符串

(可选) 要将归档的日志上传到的 Amazon S3 存储桶。

- S3BucketPath

类型：字符串

(可选) 要将日志捆绑包上传到的 Amazon S3 存储桶路径。如果您没有为 S3BucketName 参数指定一个值，则忽略此参数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

文档步骤

- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例由 AWS Systems Manager 管理。
- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例是 Windows Server 实例。
- aws:runCommand - 检查该实例是否属于 Elastic Beanstalk 环境，是否有足够的磁盘空间来捆绑日志，以及要上传到的 Amazon S3 存储桶是否是公开的。
- aws:runCommand - 收集日志文件并将档案上传到 S3BucketName 参数中指定的 Amazon S3 存储桶，如果未指定一个值，则上传到 Elastic Beanstalk 环境的默认存储桶。

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

描述

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming运行手册允许在你指定的 AWS Elastic Beanstalk (Elastic Beanstalk) 环境中进行登录。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- EnvironmentId

类型：字符串

描述：(必需) 要对其启用日志记录的 Elastic Beanstalk 环境的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文档步骤

- `aws:executeAwsApi` - 允许对您在 `EnvironmentId` 参数中指定的 Elastic Beanstalk 环境启用日志记录。
- `aws:waitForAwsResourceProperty` - 等待环境状态变为 `Ready`。
- `aws:executeScript` - 验证是否对 Elastic Beanstalk 环境启用了日志记录。

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

描述

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications 运行手册为你指定的 AWS Elastic Beanstalk (Elastic Beanstalk) 环境启用通知。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `EnvironmentId`

类型：字符串

描述：(必需)要为之启用通知的 Elastic Beanstalk 环境的 ID。

- TopicArn

类型：字符串

描述：(必需)要向其发送通知的 Amazon Simple Notification Service (Amazon SNS) 主题的 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文档步骤

- aws:executeAwsApi - 为您在 EnvironmentId 参数中指定的 Elastic Beanstalk 环境启用通知。
- aws:waitForAwsResourceProperty - 等待环境状态变为 Ready。
- aws:executeScript - 验证是否已为 Elastic Beanstalk 环境启用通知。

AWSsupport-TroubleshootElasticBeanstalk

描述

AWSsupport-TroubleshootElasticBeanstalk运行手册可帮助您排除 AWS Elastic Beanstalk 环境处于Degraded或Severe状态的潜在原因。此自动检查与您的 Elastic Beanstalk 环境关联的以下 AWS 资源：

- 负载均衡器、AWS CloudFormation 堆栈、Amazon EC2 Auto Scaling 组、亚马逊弹性计算云 (Amazon EC2) 实例和虚拟私有云 (VPC) 的配置详细信息。
- 与子网关联的关联安全组规则、路由表和网络访问控制列表 (ACL) 存在网络配置问题。

- 验证与 Elastic Beanstalk 端点的连接以及公共互联网接入。
- 验证负载均衡器的状态。
- 验证 Amazon EC2 实例的状态。
- 从 Elastic Beanstalk 环境中检索日志包，也可以选择将文件上传到。支持

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ApplicationName

类型：字符串

描述：(必需) 您的 Elastic Beanstalk 应用程序的名称。

- EnvironmentName

类型：字符串

描述：(必需) 您的 Elastic Beanstalk 环境的名称。

- AWSS3UploaderLink

类型：字符串

描述：(可选) 向您提供的 支持 网址，用于将日志包从 Elastic Beanstalk 环境上传到。此选项仅适用于已购买 支持 计划并已提出 Support 案例的客户。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:Describe*
- cloudformation:Describe*
- cloudformation:Estimate*
- cloudformation:Get*
- cloudformation:List*
- cloudformation:Validate*
- cloudwatch:Describe*
- cloudwatch:Get*
- cloudwatch:List*
- ec2:Describe*
- elasticbeanstalk:Check*
- elasticbeanstalk:Describe*
- elasticbeanstalk:List*
- elasticbeanstalk:RetrieveEnvironmentInfo*
- elasticbeanstalk:RequestEnvironmentInfo*
- elasticloadbalancing:Describe*
- rds:Describe*
- s3:Get*
- s3:List*
- sns:Get*
- sns:List*

文档步骤

- `aws:executeScript`-验证启动自动化的 AWS Identity and Access Management (IAM) 委托人是否具有执行运行手册中定义的所有操作的必要权限。
- `aws:branch` - 根据上一步的结果对工作流进行分支。
- `aws:executeScript`-收集有关 Elastic Beanstalk 环境的信息，包括负载均衡器、CloudFormation 堆栈、Auto Scaling 组、Amazon EC2 实例和 VPC 配置。
- `aws:executeScript` - 检查与 VPC 中的子网关联的路由表和 ACL 是否存在网络连接问题。
- `aws:executeScript` - 检查与 Amazon EC2 实例关联的安全组规则是否存在网络连接问题。
- `aws:executeScript` - 验证 Amazon EC2 实例的状态检查。
- `aws:executeScript` - 为 Elastic Beanstalk 环境的日志捆绑包生成一个链接。
- `aws:executeScript`-将日志包上传到。支持
- `aws:executeScript` - 输出一份操作项报告，以帮助排除可能会影响 Elastic Beanstalk 环境状态的问题。

Elastic Load Balancing

AWS Systems Manager 自动化为 Elastic Load Balancing 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)
- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS-UpdateALBDesyncMitigationMode](#)
- [AWS-UpdateCLBDesyncMitigationMode](#)
- [AWSSupport-TroubleshootELBHealthChecks](#)

AWSConfigRemediation-DropInvalidHeadersForALB

描述

AWSConfigRemediation-DropInvalidHeadersForALB 运行手册能让指定的应用程序负载均衡器移除带无效标头的 HTTP 标头。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- LoadBalancerArn

类型：字符串

描述：(必需) 要丢弃无效标头的负载均衡器的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `aws:executeAwsApi` - 为您在 `LoadBalancerArn` 参数中指定的负载均衡器启用丢弃无效标头设置。
- `aws:executeScript` - 验证是否已对您指定的负载均衡器启用丢弃无效标头设置。

AWS-EnableCLBAccessLogs

描述

AWS-EnableCLBAccessLogs 运行手册启用 Classic Load Balancer 的访问日志。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `EmitInterval`

类型：整数

有效值：5 | 60

默认值：60

描述：(可选) 发布访问日志的时间间隔 (以分钟为单位)。

- LoadBalancerNames

类型：字符串

描述：(必填) 要为其启用访问日志的经典负载均衡器列表，以逗号分隔。

- S3BucketName

类型：字符串

描述：(必填) 存储访问日志的亚马逊简单存储服务 (Amazon S3) 存储桶的名称。

- S3BucketPrefix

类型：字符串

描述：(可选) 例如，您为 Amazon S3 存储桶创建的逻辑层次结构my-bucket-prefix/prod。如果未提供前缀，则将日志置于存储桶的根级别。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- elasticloadbalancing:ModifyLoadBalancerAttributes

文档步骤

- aws:executeAwsApi-启用您在LoadBalancerNames参数中指定的经典负载均衡器的访问日志。

输出

EnableCLBAccessLogs.SuccessesLoadBalancers -成功启用访问日志的负载均衡器名称列表。

EnableCLBAccessLogs.FailedLoadBalancers -启用访问日志失败 MapList 的负载均衡器名称以及失败的原因。

AWS-EnableCLBConnectionDraining

描述

AWS-EnableCLBConnectionDraining运行手册允许将 Classic Load Balancer (CLB) 上的连接耗尽到指定的超时值。连接耗尽使负载均衡能够完成向正在注销注册或运行状况不佳的实例发出的动态请求，指定的超时时间是它在报告实例已注销注册之前保持连接活跃的时间。有关 CLB 上连接耗尽的更多信息，请参阅 Classic Load Balancer 用户指南中的[为 Classic Load Balancer 配置连接耗尽](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LoadBalancerName

类型：字符串

描述：(必填) 要启用连接耗尽的负载均衡器的名称。

- ConnectionTimeout

类型：整数

有效值：1-3600

默认：300

描述：(必填) 负载均衡器的连接超时值。超时值可以设置在 1 到 3600 秒之间。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `ModifyLoadBalancerConnectionDraining` (aws: executeAwsApi)：启用连接耗尽并为您指定的负载均衡器设置指定的超时值。
- `VerifyLoadBalancerConnectionDrainingEnabled` (aws: assertAwsResourceProperty)：验证是否已为负载均衡器启用连接耗尽功能。
- `VerifyLoadBalancerConnectionDrainingTimeout` (aws: assertAwsResourceProperty)：验证负载均衡器的连接超时值是否与您指定的值相匹配。

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

描述

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing 运行手册为指定的经典负载均衡器 (CLB) 启用跨区域负载均衡。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- LoadBalancerName

类型：字符串

描述：(必需) 要对其启用跨区域负载平衡的 CLB 的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elb:DescribeLoadBalancerAttributes
- elb:ModifyLoadBalancerAttributes

文档步骤

- aws:executeAwsApi - 为您在 LoadBalancerName 参数中指定的 CLB 启用跨区域负载均衡。
- aws:assertAwsResourceProperty - 验证是否已对 CLB 启用跨区域负载均衡。

AWSConfigRemediation-EnableELBDeletionProtection

描述

AWSConfigRemediation-EnableELBDeletionProtection 运行手册为指定的弹性负载均衡器 (ELB) 启用删除保护。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- LoadBalancerArn

类型：字符串

描述：(必需) 要为其启用删除保护的 ELB 的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:ModifyLoadBalancerAttributes

文档步骤

- `aws:executeScript` - 对您在 `LoadBalancerArn` 参数中指定的 ELB 启用删除保护。

AWSConfigRemediation-EnableLoggingForALBAndCLB

描述

AWSConfigRemediation-EnableLoggingForALBAndCLB运行手册允许对指定的 Application Load Balancer 或 C AWS Iassc Load Balancer (CLB) 进行日志记录。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `LoadBalancerId`

类型：字符串

描述：(必需) 经典负载均衡器名称或应用程序负载均衡器 ARN。

- `S3BucketName`

类型：字符串

描述：(必需) Amazon S3 存储桶名称。

- S3BucketPrefix

类型：字符串

描述：(可选) 为 Amazon Simple Storage Service (Amazon S3) 存储桶创建的逻辑层次结构，例如 my-bucket-prefix/prod。如果未提供前缀，则将日志置于存储桶的根级别。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文档步骤

- aws:executeScript - 对经典负载均衡器或应用程序负载均衡器启用日志记录并验证。

AWSsupport-TroubleshootCLBConnectivity

描述

AWSsupport-TroubleshootCLBConnectivity 运行手册可帮助解决经典负载均衡器 (CLB) 和 Amazon Elastic Compute Cloud (Amazon EC2) 实例之间的连接问题。此外，还会审查客户端与 CLB 之间的连接问题。此运行手册还审查 CLB 的运行状况检查，验证是否遵循了最佳实践，并创建问题排查控制面板。或者，也可以将自动化输出上传到 Amazon Simple Storage Service (Amazon S3) 存储桶。但是，此运行手册不支持将输出上传到可公共访问的 S3 存储桶。我们建议为此自动化创建一个临时 S3 存储桶。

Important

使用此运行手册可能会对创建的控制面板产生费用。有关更多信息，请参阅 [Amazon CloudWatch 定价](#)

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InvestigationType

类型：字符串

有效值：最佳实践 | 连接问题 | 问题排除控制面板

描述：(必需) 希望运行手册执行的操作。

- LoadBalancerName

类型：字符串

描述：(必需) CLB 的名称。

- S3Location

类型：字符串

描述：(可选) 要将自动化结果发送到的 S3 存储桶的名称。不支持可公共访问的存储桶。如果 S3 存储桶使用服务器端加密，则运行此自动化的用户或角色必须拥有 AWS KMS 键的 kms:GenerateDataKey 权限。

- S3LocationPrefix

类型：字符串

描述：(可选) 要将自动化输出上传到的 Amazon S3 键前缀 (子文件夹)。

输出格式以以下格式存储：amzn-s3-demo-bucket/*S3LocationPrefix*/{} _
{{automation:*InvestigationType*}}.txt。 *EXECUTION_ID*

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerPolicies
- elasticloadbalancing:DescribeInstanceHealth
- elasticloadbalancing:DescribeLoadBalancerAttributes
- iam:ListRoles
- cloudwatch:PutDashboard
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:GetDocument
- ssm:ListCommands

- `ssm:ListCommandInvocations`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3:PutObject`

文档步骤

- `aws:executeScript` - 验证您在 `LoadBalancerName` 参数中指定的 CLB 是否存在。
- `aws:branch` - 根据为 `InvestigationType` 参数指定的值进行分支。
- `aws:executeScript` - 对 CLB 执行连接检查。
- `aws:executeScript` - 验证 CLB 配置是否符合 Elastic Load Balancing 最佳实践。
- `aws:executeScript` - 为您的 CLB 创建 Amazon CloudWatch 控制面板。
- `aws:executeScript` - 创建包含自动化结果的文本文件，并将其上传到您在 `S3Location` 参数中指定的 Amazon S3 存储桶。

输出

`RunBestPractices.Summary`

`RunConnectivityChecks.Summary`

`CreateTroubleshootingDashboard.Output`

`UploadOutputToS3.Output`

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

描述

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` 运行手册为指定的网络负载均衡器 (NLB) 启用跨区域负载平衡。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- LoadBalancerArn

类型：字符串

描述：(必需) 要为之启用跨区域负载均衡的 NLB 的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文档步骤

- aws:executeAwsApi - 为您在 LoadBalancerArn 参数中指定的 NLB 启用跨区域负载均衡。
- aws:executeScript - 验证是否已对 NLB 启用跨区域负载均衡。

AWS-UpdateALBDesyncMitigationMode

描述

AWS-UpdateALBDesyncMitigationMode运行手册会将 Application Load Balancer (ALB) 上的不同步缓解模式更新为指定的缓解模式。不同步缓解模式决定了负载均衡器如何处理可能对您的应用程序构成安全风险的请求。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LoadBalancerArn

类型：字符串

描述：(必填) 您要修改其不同步缓解模式的 ALB 的 Amazon 资源名称 (ARN)。

- DesyncMitigationMode

类型：字符串

有效值：监控 | 防御 | 最严格

描述：(必填) 您希望 ALB 使用的缓解模式。有关不同步缓解模式的信息，请参阅《应用程序负载均衡器用户指南》中的[不同步缓解模式](#)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文档步骤

- VerifyLoadBalancerType (aws: assertAwsResourceProperty)-在继续下一步之前，验证为LoadBalancerArn输入参数指定的值是否适用于应用程序负载均衡器。
- ModifyLoadBalancerDesyncMode (aws: executeAwsApi)-更新 ALB 以使用指定的。DesyncMitigationMode
- VerifyLoadBalancerDesyncMitigationMode (aws: executeScript)-验证目标 ALB 的不同步缓解模式是否已更新。

输出

VerifyLoadBalancerDesyncMitigationMode.ModificationResult -脚本的消息有效负载，用于验证对 ALB 的修改。

AWS-UpdateCLBDesyncMitigationMode

描述

AWS-UpdateCLBDesyncMitigationMode运行手册会将 Classic Load Balancer (CLB) 上的不同步缓解模式更新为指定的缓解模式。不同步缓解模式决定了负载均衡器如何处理可能对您的应用程序构成安全风险请求。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LoadBalancerName

类型：字符串

描述：(必填) 要修改其不同步缓解模式的 CLB 的名称。

- DesyncMitigationMode

类型：字符串

有效值：监控 | 防御 | 最严格

描述：(必填) 您希望 CLB 使用的防护模式。有关不同步缓解模式的信息，请参阅《应用程序负载均衡器用户指南》中的[不同步缓解模式](#)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `ModifyLoadBalancerDesyncMode` (aws: executeAwsApi)-更新负载均衡以使用指定的 `DesyncMitigationMode`
- `VerifyLoadBalancerDesyncMitigationMode` (aws: executeScript)-验证目标 CLB 的不同步缓解模式是否已更新。

输出

`VerifyLoadBalancerDesyncMitigationMode.ModificationResult` -脚本的消息有效负载，用于验证对 CLB 的修改。

AWSSupport-TroubleshootELBHealthChecks

描述

该AWSSupport-TroubleshootELBHealthChecks运行手册通过分析 AWS 弹性负载平衡 (Elastic Load Balancing) 的相关指标、验证网络连接以及在目标实例上执行诊断命令，帮助解决弹性负载平衡 CloudWatch (Elastic Load BalancingCloudWatch) 运行状况检查问题。

本运行手册解决了以下用例：

- 负载均衡器或目标组的目标实例中存在运行状况不佳的实例。
- 虽然没有运行状况不佳的实例，但 CloudWatch 指标表示的数据点 `UnHealthyHostCounts`

Important

重要注意事项：

- 自动化的重点是对实例类型目标进行故障排除。
- 允许进行故障排除的最大实例数为 50。
- 目标实例必须由 Systems Manager 管理，才能在实例级别执行诊断命令。
- 该 `S3BucketName` 参数是可选的，但某些诊断结果会直接上传到指定的 Amazon S3 存储桶，并且不会显示在自动化输出中。
- IPv6 不支持网络连接故障排除。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- cloudwatch:GetMetricStatistics
- ssm:SendCommand
- ssm:GetCommandInvocation
- ssm:DescribeInstanceInformation
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:PutObject

策略示例：

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeInstanceHealth",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "cloudwatch:GetMetricStatistics",
      "ssm:SendCommand",
      "ssm:GetCommandInvocation",
      "ssm:DescribeInstanceInformation",
      "s3:GetBucketLocation",
      "s3:GetBucketAcl",
      "s3:PutObject"
    ],
    "Resource": "*"
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootELBHealthChecks](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，SSM Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - LoadBalancerOrTargetGroupName (必填)：

- 描述：(必填) Classic Load Balancer 的名称，或者与应用程序负载均衡器或网络负载均衡器关联的目标组的名称。
- 类型：String
- 允许的模式：`^[a-zA-Z0-9-]+$`
- ExecutionMode (必填)：
 - 描述：(必填) 控制自动化执行模式。Complete在 Amazon EC2 实例上运行所有步骤，包括 runCommands。SkipRunCommands执行除在实例上运行命令之外的所有步骤。
 - 类型：String
 - 允许的值：`[Complete, SkipRunCommands]`
- S3BucketName (可选)：
 - 描述：(可选) 您账户中要上传疑难解答日志的 Amazon S3 存储桶的名称。
 - 类型：String
 - 默认值：""

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- getBucketPublic状态：

检查目标 Amazon S3 存储桶是否有可能授予对其对象的读取或写入公共访问权限。

- getLoadBalancer详细信息：

标识负载均衡器类型并返回统一负载均衡器详细信息对象。

- checkLoadBalancer类型：

检查负载均衡器是否存在。

- 获取目标：

根据不同类型的负载均衡器，查询描述了 APIs 如何返回健康和 unhealthy 目标详细信息的地图。

- checkCloudWatch指标：

检查 CloudWatch 指标HealthyHostCountsUnHealthyHostCounts并生成 CloudWatch 链接。

- checkUnhealthyReasons:

检查是否存在不健康的原因并筛选目标。

- 检查连接：

检查负载均衡器与其实例之间的连接。

- 运行命令：

在实例上运行故障排除命令并上传输出（如果提供了存储桶名称）。

- 生成报告：

根据前面步骤的输出生成最终报告，并将报告上传到 Amazon S3 存储桶（如果已指定）。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

诊断命令

运行手册对实例执行以下诊断命令：

- Linux Shell：top、free、ss、curl、iptables、tcpdump
- Windows PowerShell：Get-CimInstance、Get-、Get-NetFirewallProfile、Invoke-NetFirewallRule、netstat WebRequest、netsh、pktmon

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

Amazon EMR

AWS Systems Manager 自动化为 Amazon EMR 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-AnalyzeEMRLogs](#)

- [AWSSupport-DiagnoseEMRLogsWithAthena](#)

AWSSupport-AnalyzeEMRLogs

描述

此运行手册可帮助识别在 Amazon EMR 集群上运行任务时出现的错误。运行手册分析文件系统中已定义日志的列表，并查找预定义关键字的列表。这些日志条目用于创建 Amazon Events CloudWatch 事件，因此您可以根据事件采取任何必要的操作。或者，运行手册将日志条目发布到您选择的 Amazon Log CloudWatch s 日志组。此运行手册目前在日志文件中查找以下错误和模式：

- container_out_of_memory – YARN 容器内存不足，运行作业可能会失败。
- yarn_nodemanager_health：CORE 或 TASK 节点在磁盘中的运行空间不足，将无法运行任务。
- node_state_change：MASTER 节点无法访问核心或 TASK 节点。
- step_failure：EMR 步骤已失败。
- no_core_nodes_running：当前没有 CORE 节点在运行，集群运行状况不佳。
- hdfs_missing_blocks：缺少 HDFS 块可能会导致数据丢失。
- hdfs_high_util：HDFS 利用率较高，这可能会影响作业和集群运行状况。
- instance_controller_restart：进程已重新启动。Instance-Controller 此进程对集群运行状况至关重要。
- instance_controller_restart_legacy：进程已重新启动。Instance-Controller 此进程对集群运行状况至关重要。
- high_load：检测到平均负载过高，这可能会影响节点运行状况报告或导致超时或减速。
- yarn_node_blacklisted：CORE 或 TASK 节点已被 YARN 列入黑名单，无法运行任务。
- yarn_node_lost：CORE 或 TASK 节点已被 YARN 标记为丢失，这可能是连接问题。

与指定的关联的 ClusterID 实例必须由 AWS Systems Manager 管理。您可以运行此自动化一次，将此自动化安排为按特定的时间间隔运行，或者删除以前由某个自动化创建的时间安排。此运行手册支持 Amazon EMR 发行版 5.20 至 6.30。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterID

类型：字符串

描述：(必需) 要分析其节点日志的集群的 ID。

- 操作

类型：字符串

有效值：运行一次 | 计划 | 移除计划

描述：(必需) 要在集群上执行的操作。

- IntervalTime

类型：字符串

有效值：5 分钟 | 10 分钟 | 15 分钟

描述：(可选) 运行自动化的间隔时间。此参数仅在您为 Operation 参数指定 Schedule 时适用。

- LogToCloudWatchLogs

类型：字符串

有效值：是 | 否

描述：(可选) 如果您指定此参数yes的值，则自动化会使用CloudWatchLogGroup参数中指定的名称创建一个 CloudWatch 日志日志组，以存储任何匹配的日志条目。

- CloudWatchLogGroup

类型：字符串

描述：(可选) 您要在其中存储任何匹配的 CloudWatch 日志条目的日志组的名称。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

- CreateLogInsightsDashboard

类型：字符串

有效值：是 | 否

描述：(可选) 如果指定yes，则创建 CloudWatch 仪表板 (如果尚不存在)。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

- CreateMetricFilters

类型：字符串

有效值：是 | 否

描述：(可选) 指定yes是否要为 CloudWatch 日志组创建指标筛选器。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations

- `ssm:ListCommands`
- `ssm:SendCommand`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:GetRolePolicy`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `iam:passrole`
- `cloudformation:DescribeStacks`
- `cloudformation>DeleteStack`
- `cloudformation>CreateStack`
- `events>DeleteRule`
- `events:RemoveTargets`
- `events:PutTargets`
- `events:PutRule`
- `events:DescribeRule`
- `logs:DescribeLogGroups`
- `logs>CreateLogGroup`
- `logs:PutMetricFilter`
- `cloudwatch:PutDashboard`
- `elasticmapreduce:ListInstances`
- `elasticmapreduce:DescribeCluster`

文档步骤

- `aws:executeAwsApi` - 收集在 `ClusterID` 参数中指定的 Amazon EMR 集群的相关信息。
- `aws:branch` - 根据输入进行分支。
 - 如果提供的操作是 `Run Once` 或 `Schedule` :
 - `aws:assertAwsResourceProperty` - 验证集群是否可用。
 - `aws:executeAwsApi` - 收集集群中运行的所有实例的 ID。
 - `aws:assertAwsResourceProperty` - 验证 SSM 代理是否在集群中的所有实例上运行。

- `aws:branch` - 根据您指定运行自动化一次还是按计划运行进行分支。
- 如果提供的操作是 `Run Once` :
 - `aws:branch` - 根据在 `LogToCloudWatchLogs` 参数中指定的值进行分支。
 - 如果 `LogToCloudWatchLogs` 值为 `yes` :
 - `aws:executeScript`-检查参数中指定名称的 CloudWatch 日志组是否存在。如果不存在，则使用指定的名称创建组。
 - `aws:branch` - 根据在 `CreateMetricFilters` 参数中指定的值进行分支。
 - 如果 `CreateMetricFilters` 值为 `yes` :
 - `aws:executeAwsApi` - 为每个指标筛选器运行 12 个步骤
 - `aws:branch` - 根据在 `CreateLogInsightsDashboard` 参数中指定的值进行分支。
 - 如果 `CreateLogInsightsDashboard` 值为 `yes` :
 - `aws:executeAwsApi`-使用 `CloudWatchLogGroup` 参数中指定的相同名称创建 CloudWatch 仪表板 (如果尚不存在) 。
 - 如果 `CreateLogInsightsDashboard` 值为 `no` :
 - `aws:runCommand` - 运行 Shell 脚本以查找集群中每个实例的日志模式。
- 如果 `CreateMetricFilters` 值为 `no` :
 - `aws:branch` - 根据在 `CreateLogInsightsDashboard` 参数中指定的值进行分支。
 - 如果 `CreateLogInsightsDashboard` 值为 `yes` :
 - `aws:executeAwsApi`-使用 `CloudWatchLogGroup` 参数中指定的相同名称创建 CloudWatch 仪表板 (如果尚不存在) 。
 - 如果 `CreateLogInsightsDashboard` 值为 `no` :
 - `aws:runCommand` - 运行 Shell 脚本以查找集群中每个实例的日志模式。
- 如果 `LogToCloudWatchLogs` 值为 `no` :
 - `aws:executeAwsApi` - 运行 Shell 脚本以查找集群中每个实例的日志模式。
- 如果提供的操作是 `Schedule` :
 - `aws:createStack`-创建针对此运行手册的 Amazon EventBridge 事件。
- 如果提供的操作是 `Remove Schedule` :
 - `aws:executeAwsApi` - 验证集群是否存在时间表。
 - `aws:deleteStack` - 删除时间表。

输出

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.InstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.output

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

描述

该AWSSupport-DiagnoseEMRLogsWithAthena运行手册使用与数据目录集成的亚马逊 Athena 帮助诊断亚马逊 EMR 日志。AWS Glue Amazon Athena 用于查询 Amazon EMR 日志文件，以获取容器日志和/或节点日志以及特定日期范围或基于关键字的搜索的可选参数。

运行手册可以自动检索现有集群的 Amazon EMR 日志位置，或者您可以指定 Amazon S3 日志位置。为了分析日志，运行手册：

- 创建 AWS Glue 数据库并在 Amazon EMR Amazon S3 日志位置执行 Amazon Athena 数据定义语言 (DDL) 查询，为集群日志和已知问题列表创建表。
- 执行数据操纵语言 (DML) 查询，在 Amazon EMR 日志中搜索已知问题模式。这些查询会按照 Amazon S3 文件路径返回检测到的问题列表、出现次数以及匹配的关键词数量。
- 结果将上传到您在前缀下指定的 Amazon S3 存储桶saw_diagnose_EMR_known_issues。
- 运行手册返回 Amazon Athena 的查询结果，重点介绍来自预定义子集的调查结果、建议以及对亚马逊知识中心 (KC) 文章的引用。
- 完成或失败后，上传到 Amazon S3 存储桶的 AWS Glue 数据库和已知问题文件将被删除。

如何工作？

使用 Amazon Athena 对 Amazon EMR 日志AWSSupport-DiagnoseEMRLogsWithAthena进行分析，以检测错误并重点介绍调查结果、建议和相关知识中心文章。

运行手册执行以下步骤：

- 使用集群 ID 获取 Amazon EMR 集群日志位置或输入 Amazon S3 位置以检索日志位置和大小。
- 根据日志位置大小提供 Athena 成本估算。
- 在运行 Athena 查询并继续执行后续步骤之前，请向指定的 IAM 委托人申请批准，即可获得批准。
- 将已知问题上传到指定的 Amazon S3 存储桶，创建 AWS Glue 数据库和表。
- 对亚马逊 EMR 日志数据执行 Athena 查询。查询可以按日期范围、关键字和两个条件进行搜索，也可以根据提供的输入在不带筛选条件的情况下运行。
- 分析结果，重点介绍调查结果、建议和相关的 KC 文章。
- 亚马逊 Athena DML 的输出链接查询结果。
- 通过删除已创建的数据库、表和已上传的已知问题来清理环境。

文档类型

自动化

所有者

Amazon

平台

/

该 AutomationAssumeRole 参数需要以下操作才能成功使用运行手册：

- 雅典娜：GetQueryExecution
- 雅典娜：StartQueryExecution
- 雅典娜：GetPreparedStatement
- 雅典娜：CreatePreparedStatement
- 胶水：GetDatabase
- 胶水：CreateDatabase
- 胶水：DeleteDatabase
- 胶水：CreateTable
- 胶水：GetTable
- 胶水：DeleteTable

- 弹性地图减少 : DescribeCluster
- s3 : ListBucket
- s3 : GetBucketVersioning
- s3 : ListBucketVersions
- s3 : GetBucketPublicAccessBlock
- s3 : GetBucketPolicyStatus
- s3 : GetObject
- s3 : GetBucketLocation
- 定价 : GetProducts
- 定价 : GetAttributeValues
- 定价 : DescribeServices
- 定价 : ListPriceLists

Important

要限制仅访问此自动化所需的资源，请将以下策略附加到信任 SSM 服务的 IAM 角色。将“分区”、“区域”和“帐户”替换为执行运行手册的分区、区域和账号的相应值。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
```

```

        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
    ],
    "Resource": "*"
},
{
    "Sid": "RestrictPutObjects",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::*/*/results/*",
        "arn:aws:s3:::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Sid": "RestrictDeleteAccess",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
    ],
    "Resource": [
        "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*"

```

```

        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/*",
        "arn:aws:glue:us-east-1:111122223333:userDefinedFunction/
saw_diagnose_emr_database_*/*",
        "arn:aws:glue:us-east-1:111122223333:catalog"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "glue:CreateTable",
        "glue:GetTable",
        "glue>DeleteTable"
    ],
    "Resource": [
        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_known_issues",
        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_logs_table",
        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/j_*",
        "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
        "arn:aws:glue:us-east-1:111122223333:catalog"
    ]
}
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-DiagnoseEMRLogsWithAthena](#)在“文档”AWS Systems Manager 下方导航。
2. 选择 Execute automation (执行自动化)。
3. 要输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 集群 ID (必填) :

亚马逊 EMR 集群 ID。

- S3LogLocation (可选) :

亚马逊 S3 亚马逊 EMR 日志位置。输入亚马逊 S3 位置的 Path-style 网址，例如：s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/。如果 Amazon EMR 集群已终止超过30天数，请提供此参数。

- S3BucketName (必填) :

用于上传已知问题列表的 Amazon S3 存储桶名称，以及 Amazon Athena 查询的输出。该存储桶应[启用封锁公共访问功能](#)，并且与 Amazon EMR 集群位于同一 AWS 区域和账户。

- 批准者 (必填) :

能够批准或拒绝操作的 AWS 经过身份验证的委托人列表。您可以使用以下任一格式指定委托人：用户名、用户 ARN、IAM 角色 ARN 或 IAM 代入角色 ARN。最大审批者数量为 10。

- FetchNodeLogsOnly (可选) :

如果设置为true，则自动化会诊断 Amazon EMR 应用程序容器日志。默认值为 false。

- FetchContainersLogsOnly (可选) :

如果设置为true，则自动化会诊断 Amazon EMR 容器日志。默认值为 false。

- EndSearchDate (可选) :

日志搜索的结束日期。如果提供，则自动化将专门搜索在指定日期之前生成的日志，格式为 YYYY-MM-DD (例如：2024-12-30)。

- DaysToCheck (可选) :

如果EndSearchDate提供此参数，则需要使用此参数来确定追溯搜索指定日志的天数。EndSearchDate最大值为30天。默认值为 1。

- SearchKeywords (可选) :

要在日志中搜索的关键字列表，以逗号分隔。关键字不能包含单引号或双引号。

Input parameters

AutomationAssumeRole

(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

SSMAutomation

S3LogLocation

(Optional) The Amazon S3 URL that contains the Amazon EMR logs. Provide this parameter if the Amazon EMR cluster has been terminated for more than 30 days. Provide the full Amazon S3 path prefix for the EMR logs. Example s3://mybucket/myfolder/j-1K48XXXXXXHC8/.
String

Approvers

(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats: 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.
arn:awsiam::[redacted]:role/Approver

FetchContainersLogsOnly

(Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster.
false

DaysToCheck

(Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days.
1

ClusterID

(Required) The Amazon EMR cluster ID.
j-1K48XXXXXXHC8

S3BucketName

(Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have [Block Public Access Enabled](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) and be in the same AWS region as the Amazon EMR cluster provided.
[redacted]

FetchNodeLogsOnly

(Optional) If set to "true", the automation diagnoses the Amazon EMR node logs.
false

EndSearchDate

(Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30").
String

SearchKeywords

(Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes.
StringList

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- 得到LogLocation：

通过查询指定的 Amazon EMR 集群 ID 来检索 Amazon S3 日志位置。如果自动化无法从 Amazon EMR 集群 ID 中查询日志位置，则运行手册将使用输入参数。S3LogLocation

- 分支OnValidLog:

验证 Amazon EMR 日志的位置。如果位置有效，请继续估算对亚马逊 EMR 日志执行查询时的 Amazon Athena 潜在成本。

- 估计AthenaCosts：

确定 Amazon EMR 日志的大小，并提供对日志数据集执行 Athena 扫描的成本估算。对于非商业区域（非AWS分区），此步骤仅提供日志大小而不估算成本。可以使用指定区域的 Athena 定价文档计算成本。

- 批准自动化：

等待指定的 IAM 委托人批准后继续执行自动化的后续步骤。批准通知包含 Amazon EMR 日志上的 Amazon Athena 扫描的估计费用，以及有关自动配置的资源的信息。

- 上传KnownIssuesExecuteAthenaQueries：

将预定义的已知问题上传到S3BucketName参数中指定的 Amazon S3 存储桶。创建 AWS Glue 数据库和表。根据输入参数在数据库 AWS Glue 中执行 Amazon Athena 查询。

- 得到QueryExecutionStatus：

AWSSupport-DiagnoseEMRLogsWithAthena

512

一直等待，直到 Amazon Athena 查询执行处于状态。SUCCEEDED Amazon Athena DML 查询在亚马逊 EMR 集群日志中搜索错误和异常。

- 分析 AthenaResults :

分析 Amazon Athena 结果，提供来自一组预定义映射的调查结果、建议和知识中心 (KC) 文章。

- 得到 AnalyzeResultsQuery1ExecutionStatus :

等待，直到查询执行处于 SUCCEEDED 状态。Amazon Athena DML 查询分析了之前的 DML 查询的结果。此分析查询将返回匹配的异常以及解决方案和 KC 文章

- 得到 AnalyzeResultsQuery2ExecutionStatus :

等待，直到查询执行处于 SUCCEEDED 状态。Amazon Athena DML 查询分析了之前的 DML 查询的结果。此分析查询将返回在每个 Amazon S3 日志路径中 exceptions/errors 检测到的列表。

- 打印 AthenaQueriesMessage :

打印亚马逊 Athena DML 查询结果的链接。

- CleanupResources :

Clean-ups 资源，方法是删除已创建的 AWS Glue 数据库并删除在 Amazon EMR 日志存储桶中创建的已知问题文件。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

输出提供了 Athena 查询结果的三个链接：

- 列出在 Amazon EMR 集群日志中发现的所有错误和经常发生的异常以及相应的日志位置（Amazon S3 前缀）。
- Amazon EMR 日志中匹配的唯一已知异常摘要，以及建议的解决方案和 KC 文章，以帮助进行故障排除。
- 有关特定错误和异常在 Amazon S3 日志路径中出现位置的详细信息，以支持进一步诊断。

```

▼ Outputs

printAthenaQueriesMessage.QueriesLinkMessage
log Olive Query Link: This link provides a comprehensive view of all the exceptions encountered within your EMR logs.
https://

analyzeQuery 1 Link: This link provides a summary of unique issues detected from your logs, along with insights. It shows the issue ID, matched keywords for each issue, number of times the issue occurred, a summary of what the issue is, a description providing more details, and relevant links to knowledge center articles.
https://

analyzeQuery 2 Link: This link provides visibility into issues that have occurred, specified by S3 file path. It gives a breakdown of the number of times each unique issue has happened along with the keyword matched for that issue. The output allows precise tracing of exceptions and errors in each file, guiding remediation efforts and debugging
https://
  
```

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流登录页面](#)

AWS 服务文档

- 有关更多信息，请参阅 [Amazon EMR 集群故障排除](#)

亚马逊 OpenSearch 服务

AWS Systems Manager 自动化为亚马逊 OpenSearch 服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSONOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

AWSConfigRemediation-DeleteOpenSearchDomain

描述

AWSConfigRemediation-DeleteOpenSearchDomain运行手册使用 [DeleteDomain](#) API 删除给定的 Amazon OpenSearch 服务域。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- DomainName

类型：字符串

允许的值：(\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

描述：(必填) 您要删除的亚马逊 OpenSearch 服务域的名称。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DeleteDomain
- es:DescribeDomain

文档步骤

- aws:executeScript-接受 Amazon Serv OpenSearch ice 域名作为输入，将其删除，然后验证删除。

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

描述

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain运行手册使用 [UpdateDomainConfig](#) API EnforceHTTPS 在给定的亚马逊 OpenSearch 服务域上启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- DomainName

类型：字符串

允许的值：(\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

描述：(必填) 您要用于强制执行 HTTPS 的亚马逊 OpenSearch 服务域的名称。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

文档步骤

- `aws:executeScript`-在`DomainName`参数中指定的亚马逊 OpenSearch 服务域上启用`EnforceHTTPS`终端节点选项。

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

描述

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups运行手册使用[UpdateDomainConfig](#)API 更新给定 Amazon OpenSearch 服务域上的安全组配置。

Note

AWS 安全组只能应用于为亚马逊虚拟私有云 (VPC) Virtual Private Cloud 访问配置的亚马逊 OpenSearch 服务域，不能应用于配置为公共访问的 OpenSearch 亚马逊服务域。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `DomainName`

类型：字符串

描述：(必填) 您要用于更新安全组的 Amazon S OpenSearch ervice 域的名称。

- SecurityGroupList

类型：StringList

描述：(必填) 您要分配给 Amazon OpenSearch 服务域的安全组 ID。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

文档步骤

- aws:executeScript-更新您在DomainName参数中指定的亚马逊 OpenSearch 服务域上的安全组配置。

AWSSupport-TroubleshootOpenSearchRedYellowCluster

描述

AWSSupport-TroubleshootOpenSearchRedYellowClusterautomation runbook 用于识别[红色](#)或[黄色](#)集群运行状况的原因，并指导您将集群更改回绿色。

如何工作？

该运行手册AWSSupport-TroubleshootOpenSearchRedYellowCluster可帮助您排除红色或黄色群集的原因，并通过分析群集配置和资源利用率提供了解决此问题的后续步骤。

运行手册执行以下步骤：

- 对目标域调用 [DescribeDomain](#) API 以获取集群配置。
- 检查 OpenSearch 服务域是基于互联网（公共）还是基于[亚马逊虚拟私有云 \(VPC\)](#) 的。
- 根据集群配置创建公共 VPC-based AWS Lambda 函数或 [Amazon](#) 函数。注意：Lambda 函数包含故障排除代码，用于对集群运行 OpenSearch 服务 API，以确定集群为何处于红色或黄色状态。
- 删除 Lambda 函数。
- 显示已执行的检查以及解决红色或黄色群集问题的后续建议步骤。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation>DeleteStack`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `es:DescribeDomain`
- `es:DescribeDomainConfig`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:AttachNetworkInterface`
- `cloudwatch:GetMetricData`
- `iam:PassRole`

该 `LambdaExecutionRole` 参数需要以下操作才能成功使用运行手册：

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

`LambdaExecutionRole` 政策概述：

以下是 Lambda 函数的执行角色（AWS Identity and Access Management (IAM) 角色）的示例，该角色向该函数授予访问本运行手册所需的 AWS 服务和资源的权限。有关更多信息，请参阅 [Lambda 执行角色](#)。

Note

只有当您的 OpenSearch 服务集群 `ec2>DeleteNetworkInterface` 为 [亚马逊](#) 时 `ec2:DescribeNetworkInterfaces` `ec2:CreateNetworkInterface`，才需要使用、和，VPC-based 才能允许 Lambda 函数创建和管理 Amazon VPC 网络接口。有关更多信息，请参阅 [将出站互联网连接到 Amazon VPC 和 Lambda 执行角色中的资源](#)。

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "es:ESHttpGet",  
      "Resource": "arn:aws:es:us-east-1:123456789012:domain/*"
```

```

    {
      "Effect": "Allow",
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/
health",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/
indices",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/
allocation",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/
allocation/explain"
      ]
    },
    {
      "Condition": {
        "ArnLikeIfExists": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc_id"
        }
      },
      "Action": [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

说明

按照这些步骤对自动化进行配置：

1. 导航到 AWS Systems Manager 控制台 [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#) 中的。
2. 选择 Execute automation (执行自动化)。
3. 要输入参数，请输入以下内容：

- AutomationAssumeRole (可选) :

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色, Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaExecutionRole (必填) :

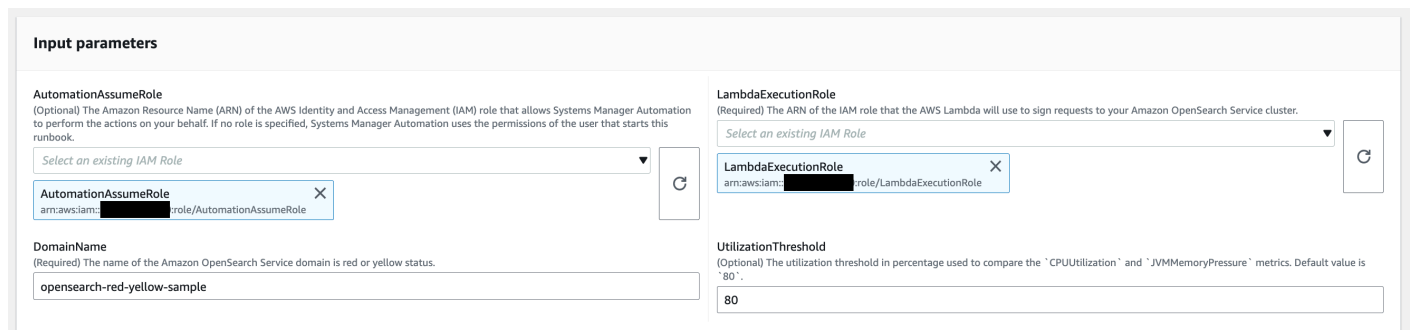
Lambda 将用于签署对您的亚马逊服务集群的请求的 IAM 角色的 ARN。OpenSearch

- DomainName (必填) :

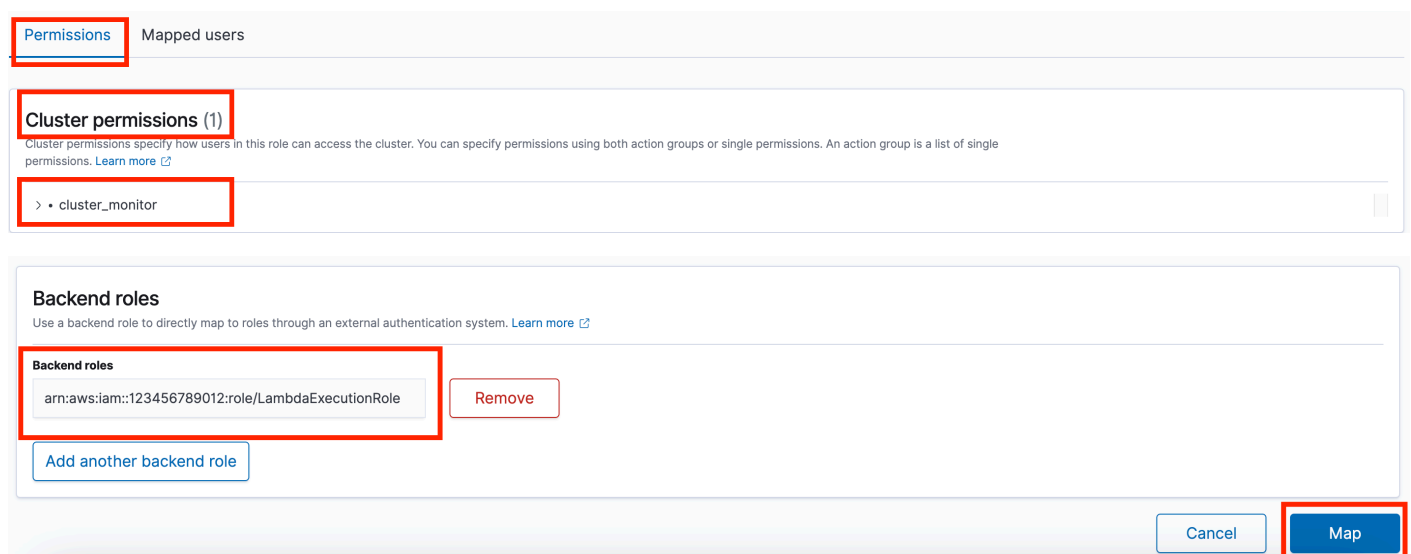
群集运行状况为红色或黄色的 OpenSearch 服务域的名称。

- UtilizationThreshold (可选) :

用于比较 CPU 利用率和 JVMMemoryPressure 指标的利用率阈值百分比。默认值为 80。



- 如果您已在 S OpenSearch ervice 集群上启用了[精细访问控制](#), 请确保将LambdaExecutionRole角色 arn 映射到至少具有权限的角色。cluster_monitor



- 选择执行。

6. 自动化启动。

7. 自动化运行手册执行以下步骤：

- GetClusterConfiguration:

获取 OpenSearch 服务集群配置。

- CreateAWSLambdaFunctionStack:

使用在您的账户中创建一个临时 Lambda 函数。CloudFormation Lambda 函数用于运行 OpenSearch 服务 API。

- WaitForAWSLambdaFunctionStack:

等待 CloudFormation 堆栈完成。

- GetClusterMetricsFromCloudWatch:

获取与亚马逊 CloudWatch ClusterStatus、CPU利用率和 JVMMemoryPressure OpenSearch 服务集群相关的指标及其创建日期。

- RunOpenSearchAPIs:

使用 Lambda 函数调用 OpenSearch 服务 API 并分析集群指标数据，以诊断红色或黄色集群状态的原因。

- DeleteAWSLambdaFunctionStack:

删除您的账户中由此自动化创建的 Lambda 函数。

8. 完成后，查看“输出”部分以了解执行的详细结果。

- RootCause:

概述已确定的集群运行状况处于红色或黄色状态的原因。

- IssueDescription:

提供有关集群为何处于红色或黄色状态以及使集群恢复到绿色状态的可能步骤的详细信息。

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)

- [支持自动化 workflow 登录页面](#)

AWS 服务文档

- 有关更多信息，请参阅 [Amazon OpenSearch 服务疑难解答](#)

AWSSupport-TroubleshootOpenSearchHighCPU

描述

该AWSSupport-TroubleshootOpenSearchHighCPU运行手册提供了一种自动解决方案，用于从 Amazon S OpenSearch ervice 域收集诊断数据，以解决[高 CPU](#) 问题。

如何工作？

该AWSSupport-TroubleshootOpenSearchHighCPU运行手册有助于排除 Amazon OpenSearch 服务域中 CPU 使用率过高的问题。

运行手册执行以下步骤：

- 对提供的亚马逊 OpenSearch 服务域运行 [DescribeDomain](#)API 以获取集群元数据。
- 检查亚马逊 OpenSearch 服务域是公共域还是亚马逊 CloudFormation，VPC-based 并在的帮助下创建公共 VPC-based AWS Lambda 函数或[亚马逊](#)函数。
- Lambda 函数从亚马逊 OpenSearch 服务域中获取诊断数据。
- 使用 AWS Step Functions 状态机协调多个 Lambda 函数执行，以收集更全面的数据。
- 默认情况下，将收集的数据存储在 Amazon CloudWatch 日志组中 24 小时。
- 删除已创建的资源，但 CloudWatch 日志组除外。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation>DeleteStack
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:InvokeFunction
- lambda:GetFunction
- lambda:TagResource
- es:DescribeDomain
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:DescribeInstances
- ec2:AttachNetworkInterface
- ec2>DeleteNetworkInterface
- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:TagResource
- states:CreateStateMachine
- states>DeleteStateMachine
- states:StartExecution
- states:TagResource

- `states:DescribeStateMachine`
- `states:DescribeExecution`
- `iam:PassRole`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Note

`iam:CreateRole`、`iam>DeleteRole`、`iam:GetRole`、`iam:PutRolePolicy` 和仅 `iam>DeleteRolePolicy` 在您未使用现有 IAM 角色作为 `LambdaInvocationRoleForStepFunctions` 参数时才是必需的

该 `LambdaExecutionRole` 参数需要以下操作才能成功使用运行手册：

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Lambda 执行角色向该函数授予访问本运行手册所需的 AWS 服务和资源的权限。有关更多信息，请参阅 [Lambda 执行角色](#)。

Note

只有当您的 OpenSearch 服务集群 `ec2>DeleteNetworkInterface` 为 [亚马逊](#) 时 `ec2:DescribeNetworkInterfaces` `ec2:CreateNetworkInterface`，才需要使用、

和，VPC-based才能允许 Lambda 函数创建和管理 Amazon VPC 网络接口。有关更多信息，请参阅[将出站联网连接到 Amazon VPC 中的资源](#)和[Lambda 执行角色](#)。

LambdaInvocationRoleForStepFunctions参数授予 AWS Step Functions 状态机调用 Lambda 函数的权限。以下是一个 IAM 策略示例，该策略授予 Step Functions 调用从服务域获取诊断数据的 Lambda 函数的 OpenSearch 权限。有关更多信息，请参阅 AWS Step Functions 开发人员指南中的[创建状态机 IAM 角色](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": [
        "arn:aws:lambda:us-east-1:111122223333:function:AWSSupport-
HighCPU-*"
      ]
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. 在 AWS Systems Manager 控制台[AWSSupport-TroubleshootOpenSearchHighCPU](#)中导航到。
2. 选择 Execute automation (执行自动化)。
3. 要输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DomainName (必填)：

您要针对高 CPU 问题进行故障排除的 Amazon OpenSearch 服务域的名称。

- LambdaExecutionRoleForOpenSearch (必填) :

要附加到 Lambda 函数的 IAM 角色的 ARN。Lambda 函数使用此角色的证书签署对亚马逊 OpenSearch 服务域的请求。如果在 Amazon Ser OpenSearch vice 域上启用了精细访问控制，则必须将此角色映射到至少具有“cluster_monitor”权限的 OpenSearch 服务控制面板后端角色。

- LambdaInvocationRoleForStepFunctions (可选) :

(可选) 要附加到 Step Functions 工作流程的 IAM 角色的 ARN。状态机使用此角色的凭证来调用从服务域获取诊断数据的 Lambda 函数。OpenSearch 如果未指定任何角色，则此自动化将在您的账户中为 Step Functions 创建一个 IAM 角色。

- DataRetentionDays (可选) :

保留从 Amazon OpenSearch 服务域收集的诊断数据的天数。默认情况下，数据保留 24 小时 (一天)。您可以选择将数据最多保留 30 天。

- NumberOfDataSamples (可选) :

要从 Amazon OpenSearch 服务域中收集的数据样本数量。默认情况下，会收集 5 个数据样本。您最多可以收集 10 个样本，并且将为每个样本集合调用 Lambda 函数。

4. 如果您已在 S OpenSearch ervice 集群上启用了[精细访问控制](#)，请确保将LambdaExecutionRole角色 arn 映射到至少具有权限的角色。cluster_monitor

The screenshot shows the 'Mapped users' configuration page in the AWS IAM console. The 'Permissions' tab is active. In the 'Cluster permissions (1)' section, the 'cluster_monitor' permission is selected. In the 'Backend roles' section, a role with the ARN 'arn:aws:iam::[redacted]:role/LambdaExecutionRole' is listed. The 'Map' button at the bottom right is highlighted with a red box.

5. 选择执行。
6. 自动化启动。
7. 自动化运行手册执行以下步骤：

- 检查并发性：

确保只有一次针对指定的 Amazon S OpenSearch ervice 域名执行此操作手册。如果 runbook 发现另一次针对相同域名的执行，则会返回错误并结束。

- 得到DomainConfig：

获取目标 OpenSearch 服务域的配置详细信息。

- 配置资源：

使用配置用于数据收集的资源 CloudFormation。

- 等等ForStackCreation：

等待 CloudFormation 堆栈完成。

- 描述StackResources：

描述 CloudFormation 堆栈并获取状态机的 ARN。

- 运行StateMachine：

通过运行 Step Functions 状态机来调用数据收集器 Lambda 函数一次或多次。

- 描述ErrorsFromStackEvents：

描述 CloudFormation 堆栈中的错误是否存在错误。

- 取消舞台OpenSearchHighCPUAutomation：

删除AWSSupport-TroubleshootOpenSearchHighCPU CloudFormation 堆栈。

- 描述ErrorsFromStackDeletion：

描述删除 CloudFormation 堆栈时遇到的错误。

- 最终状态：

返回AWSSupport-TroubleshootOpenSearchHighCPU运行手册的最终输出。

8. 完成后，查看“输出”部分以了解执行的详细结果。

- 决赛Status.FinalOutput：

提供存储诊断数据的 CloudWatch 日志组。

▼ Outputs

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流登录页面](#)

AWS 服务文档

- 有关更多信息，请参阅 [Amazon OpenSearch 服务疑难解答](#)

EventBridge

AWS Systems Manager 自动化为 Amazon EventBridge 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

AWS-AddOpsItemDedupStringToEventBridgeRule

描述

该AWS-AddOpsItemDedupStringToEventBridgeRule运行手册为所有 AWS Systems Manager OpsItems 与 Amazon EventBridge 规则关联的内容添加了重复数据删除字符串。如果已应用重复数据删除字符串，则此运行手册不会添加该字符串至规则中。要了解更多重复数据删除字符串和 OpsItems，请参阅《AWS Systems Manager 用户指南》OpsItems中的[减少重复](#)内容。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DedupString

类型：字符串

描述：(必需) 要添加到规则的重复删除字符串。

- RuleName

类型：字符串

描述：(必需) 要将重复删除字符串添加到的规则的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:ListTargetsByRule
- events:PutTargets

文档步骤

- aws:executeScript-在RuleName参数中指定的 EventBridge规则中添加重复数据删除字符串。

AWS-DisableEventBridgeRule

描述

AWS-DisableEventBridgeRule运行手册禁用您指定的亚马逊 EventBridge 规则。要了解有关规则的更多信息 EventBridge ，请参阅亚马逊用户指南 [EventBridge 中的亚马逊](#)规则。 EventBridge

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EventBusName

类型：字符串

默认：default

描述：(可选) 与要禁用的规则关联的事件总线。

- RuleName

类型：字符串

描述：(必选) 要禁用的规则的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:DisableRule

文档步骤

- aws:executeAwsApi-禁用您在RuleName参数中指定的 EventBridge 规则。

AWS Glue

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Glue有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWSSupport-TroubleshootGlueConnection](#)

AWSSupport-TroubleshootGlueConnection

描述

该AWSSupport-TroubleshootGlueConnections运行手册有助于解决 AWS Glue 连接问题。测试连接的目标必须通过 JDBC 连接到达，可以是亚马逊关系数据库服务 (Amazon RDS) cluster/instance、Amazon Redshift 集群，也可以是可通过 JDBC 访问的任何其他目标。在前两种情况下，Reachability Analyzer 工具用于确定源 (AWS Glue) 和目标 (Amazon RDS 或 Amazon Redshift) 之间的连接是否获得授权。

如果连接的目标不是 Amazon RDS 或 Amazon Redshift，则仍要通过在与 AWS Glue 连接相同的子网（网络接入点）中创建一个 AWS Lambda 函数，然后检查目标名称是否可解析以及目标端口是否可以访问来测试连接。

⚠ Important

为了运行 [Reachability Analyzer](#) 检查，将在连接的每个数据源子网中创建弹性网络接口。在运行此自动化之前，请确保这些子网上有足够的免费 IP，并且使用一个 IP 不会影响您的工作负载。

⚠ Important

此自动化创建的所有资源都已标记，因此可以轻松找到它们。使用的标签是：

- `AWSSupport-TroubleshootGlueConnection` : true
- `AutomationExecutionId`: *Amazon EC2 Systems Manager Execution Id*

如何工作？

运行手册执行以下步骤：

- 描述用于获取 AWS Glue 连接检查的源信息（子网和安全组）的连接。
- 从 JDBC URL 中引用的数据源或和 `DatasourceSubnets` 参数（如果存在）中获取目标信息（子网 `DatasourceSecurityGroups` 和安全组）。
- 如果 JDBC URL 中存在的数据源是 Amazon RDS 实例或集群或 Amazon Redshift 集群，则此自动使用在前面步骤中收集的源和目标信息创建 ENI，并使用 Reachability Analyzer 在它们之间执行连接检查。
- Lambda 函数（此自动化环境中的网络接入点）用于执行 L4 连接和名称解析检查。
- 使用相同的 Lambda 函数对亚马逊 S3 终端节点执行检查。
- 策略模拟器用于确定连接中使用的 IAM 角色是否具有所需的权限。
- 自动化会检查连接使用的安全组是否具有预期的配置。
- 将生成一份报告，其中包含测试连接操作失败的可能原因 and/or 以及已执行的成功测试。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack
- ec2:CreateNetworkInsightsPath
- ec2:CreateNetworkInterface
- ec2:CreateTags
- ec2>DeleteNetworkInsightsAnalysis
- ec2>DeleteNetworkInsightsPath
- ec2>DeleteNetworkInterface
- ec2:StartNetworkInsightsAnalysis
- iam:AttachRolePolicy
- iam:CreateRole
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:DetachRolePolicy
- iam:PutRolePolicy
- iam:TagRole
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:TagResource
- logs:CreateLogGroup
- logs>DeleteLogGroup

- logs:PutRetentionPolicy
- logs:TagResource
- glue:GetConnection
- glue:GetDataCatalogEncryptionSettings
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- ec2:DescribeDhcpOptions
- ec2:DescribeNetworkInsightsPaths
- ec2:DescribeNetworkInsightsAnalyses
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeVpcAttribute
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:InvokeFunction
- lambda:GetFunction
- s3:GetEncryptionConfiguration
- iam:PassRole

 Important

除了上述操作外，还AutomationAssumeRole应将[AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)作为附加的托管策略，以便成功执行[Reachability Analyzer](#) 测试。

以下是可以为以下各项授予的政策示例AutomationAssumeRole：

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "TaggedAWSResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
      }
    },
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:TagRole",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:TagResource",
      "logs>DeleteLogGroup",
      "logs>CreateLogGroup",
      "logs:PutRetentionPolicy",
      "logs:TagResource",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack"
    ],
    "Resource": "*"
  },
  {
    "Sid": "TaggedEC2ResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
      }
    },
    "Action": [

```

```

        "ec2:DeleteNetworkInterface"
    ],
    "Resource": "*"
},
{
    "Sid": "PutRolePolicy",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "iam:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
    },
    "Action": [
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "InvokeFunction",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn*:lambda:*:*:function:point-of-presence-*"
},
{
    "Sid": "UnTaggedActions",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInsightsPath",
        "ec2>DeleteNetworkInsightsAnalysis",
        "ec2>DeleteNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:StartNetworkInsightsAnalysis",
        "glue:GetConnection",
        "glue:GetDataCatalogEncryptionSettings",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInsightsAnalyses",

```

```

        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:SimulatePrincipalPolicy",
        "kms:DescribeKey",
        "lambda:GetFunction",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn:*:iam:*:role/point-of-presence-*",
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": "lambda.amazonaws.com"
      }
    }
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSsupport-TroubleshootGlueConnection](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- TestConnectionRole (必填)

连接测试期间使用的 IAM 角色的亚马逊资源名称 (ARN)。

- ConnectionName (必填)

AWS Glue 您要排除故障的测试连接名称失败。

- PersistReachabilityAnalyzerResults (可选)

指示是否应保留 Reachability Analyzer 执行结果的标志。默认值：false。

- PointOfPresenceLogRetentionPeriod (可选)

Lambda 接入点日志的存储天数。默认值：7。

- DatasourceSubnets (可选)

如果原始数据源不可用，请使用此参数提供其使用的子网，以便仍然可以进行连通性测试。必须搭配使用 DatasourceSecurityGroups。示例：subnet-1, subnet-2。

- DatasourceSecurityGroups (可选)

如果原始数据源不可用，请使用此参数提供其使用的安全组，以便仍然执行连接测试。必须搭配使用 DatasourceSubnets。示例：sg-1, sg-2。

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

TestConnectionRole
(Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.

PointOfPresenceLogRetentionPeriod
(Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7.

DatasourceSecurityGroups
(Optional) If the original datasource is not available, use this parameter to provide the security groups it used so that the connectivity tests are still performed. ****Must**** be used with `DatasourceSubnets`. Example: sg-1,sg-2.

ConnectionString
(Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt.

PersistReachabilityAnalyzerResults
(Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false.

DatasourceSubnets
(Optional) If the original datasource is not available, use this parameter to provide the subnets that it used so that the connectivity tests are still performed. ****Must**** be used with `DatasourceSecurityGroups`. Example: subnet-1,subnet-2.

4. 选择执行。

5. 自动化启动。

6. 自动化运行手册执行以下步骤：

- ParseInputs:

此步骤验证输入的组合。如果同时提

供DatasourceSecurityGroups和DatasourceSubnets，则它们有效并按原样返回。如果未提供任何列表，则返回两个空列表。如果只提供了其中一个，则该步骤会引发ValueException。

- GetConnectionDetails:

此步骤将返回所提供 AWS Glue 连接的详细信息。

- ParseSecurityGroupList:

此步骤用于连接 a SecurityGroupIdList 中的，以备String将来在此自动化中使用。

- GetConnectionData:

根据 JDBC 网址确定:RedShiftRdsInstance、RdsCluster和之间的连接类型。Other此外，还会返回 JDBC 连接中使用的域和端口、连接的 Amazon VPC 及其域名服务器。

- GetNetworkDetails:

从 Amazon RDS 或 Amazon Redshift 目标获取子网和安全组信息。

- 创建 eniTemplate :

生成用于创建用于测试连通性的网络接口的 AWS CloudFormation 模板。这是运行 Reachability Analyzer 工具所必需的。

- createeniStack :

根据上一步中创建的模板创建 CloudFormation 堆栈。

- GetStackDetails:

描述在前SourceNetworkInterface一个 CloudFormation 堆栈中创建的堆栈并检索TargetNetworkInterfaces信息。

- RunSourceToTargetCheck:

使用 Reachability Analyzer 工具在上一步中创建的源网卡和目标 ENI 之间运行检查。

- DeleteeniStack :

删除创建网络接口的 CloudFormation 堆栈

- CreateNetworkPointOfPresence:

CloudFormation 创建用作网络接入点的 Lambda 函数。

- GetFunctionName:

执行 CloudFormation 描述堆栈 API 调用，以检索在上一步中创建的 Lambda 函数的名称。

- RunEndpointChecks:

使用网络接入点来确定 JDBC 连接中存在的端点是否可解析且可在声明的端口中访问。

- 检查 3Connectivity :

检查与 Amazon S3 服务的 AWS Glue 连接之间的网络连接。

- DeletePointOfPresence:

删除创建网络接入点 Lambda 的 CloudFormation 堆栈。

- TestIAMRolePermissions:

检查用于测试的 IAM 角色是否具有执行测试所需的权限。

- CheckConnectionSecurityGroupReferencingRule:

检查 AWS Glue 连接中使用的安全组是否允许来自其自身的所有入口流量。它将返回没有此规则的安全组列表（如果有）。

- **GenerateReport:**

生成一份报告，其中包含发现的列表（连接测试失败的可能原因）和后续步骤（尝试解决连接测试失败的问题）。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- **自动化结果**

在本节中，您将找到描述测试连接操作失败的可能原因（发现）以及如何修复这些情况（后续步骤）的场景。如果自动化无法找到测试失败的原因，也将在本节中告知这一点。

- **成功的测试**

在本节中，您将找到一些场景，告知此自动化已成功测试的内容。如果自动化无法确定测试连接失败的原因，成功的测试非常有用，因为它们会通过告知没有导致问题的因素来缩小调查范围。

- **自动化错误**

在本节中，您将找到描述自动化过程中发生的问题的场景，这些问题可能限制了自动化可以执行的测试数量。场景描述将告知哪个步骤失败。


```

TroubleshootGlueConnection

Automation Results
Below are possible causes for the issue being troubleshoot and their fixes.

-----

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
- The JDBC URL's endpoint dummy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue connection's subnet subnet-
- Glue connection's VPC (vpc-██████████) is using AWS DNS Resolver but no issue could be found.
➔ Next steps:
- Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries.
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support

# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
- The IAM role arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi used for the AWS Glue connection test has no trust relationship with the AWS Glue service.
➔ Next steps:
- Please add the AWS Glue service to the arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi trust relationship. More details on the following link:
- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/edit_trust.html

# Scenario: Glue test connection role IAM check
🔍 Findings:
- The IAM role (arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi) used to test the connection is not allowed to perform 'glue:TestConnection'.
➔ Next steps:
- Please add the 'glue:TestConnection' action to the role used for the AWS Glue connection test:
arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi.

-----

✓ Successful Tests
Below are the successful tests performed by the automation, for further troubleshooting.

-----

# Scenario: Datasource security group
✓ The target's security group(s) allow(s) inbound connections from the Glue connection.

# Scenario: Checking connection security group self referencing rule
✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.

```

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

Amazon FSx

AWS Systems Manager 自动化为 Amazon FSx 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-ValidateFSxWindowsADConfig](#)

AWSSupport-ValidateFSxWindowsADConfig

描述

该AWSSupport-ValidateFSxWindowsADConfig运行手册用于验证适用于 Windows File Server 的亚马逊 FSx 的自我管理活动目录 (AD) 配置

如何工作？

该运行手册在亚马逊 FSx 子网上启动的临时亚马逊弹性计算云 (Amazon EC2) Windows 实例上AWSSupport-ValidateFSxWindowsADConfig执行亚马逊 FSx 验证脚本。该脚本会执行多项检查，以验证与自管 AD/DNS 服务器的网络连接以及 Amazon FSx 服务账户的权限。运行手册可以验证失败或配置错误的适用于 Windows File Server 的 Amazon FSx，或者使用自我管理 AD 创建适用于 Windows 文件服务器的新 Amazon FSx。

默认情况下，运行手册使用 CloudFormation Amazon FSx 子网创建 Amazon EC2 Windows 实例、AWS Systems Manager AWS Identity and Access Management (SSM) 访问安全组、(IAM) 角色和策略。如果您想在现有 Amazon EC2 实例上运行脚本，请在参数中提供 ID InstanceId。成功执行后，它会删除 CloudFormation 资源。但是，要保留资源，请将RetainCloudFormationStack参数设置为true。

该 CloudFormation 模板代表您创建一个 IAM 角色，该角色具有附加到 Amazon EC2 实例以运行 Amazon FSx 验证脚本所需的权限。要为临时实例指定现有 IAM 实例配置文件，请使用InstanceProfileName参数。关联的 IAM 角色必须包含以下权限：

- ec2:DescribeSubnets以及ec2:DescribeVpcs权限和 Amazon 托管政策AmazonSSManagedInstanceCore。
- 通过调用 API 从 Systems Manager 获取亚马逊 FSx 服务账户用户名和密码的GetSecretValue权限。
- 将对象放入亚马逊简单存储服务 (Amazon S3) 存储桶中以获取脚本输出的权限。

先决条件

创建临时 Amazon EC2 实例（或InstanceId参数中提供的现有实例）的子网必须允许访问 AWS Systems Manager AWS Secrets Manager、和 Amazon S3 终端节点，才能使用 SSM 运行命令运行AmazonFSxADValidation脚本。

AWS Secrets Manager 设置

验证脚本通过运行时调用 Secrets Manager 来检索亚马逊 FSx 服务账户的用户名和密码，从而连接到 Microsoft AD 域。按照创建密钥中的步骤[创建新的 S AWS Secrets Manager ecr ets](#) Manager 密钥。确保用户名和密码使用一 key/value 对格式存储{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}。有关保护对机密[的访问的信息 AWS Secrets Manager](#)，请参阅[身份验证和访问控制](#)。

有关该工具的更多信息，请参阅README.md文件中的TROUBLESHOOTING.md和[AmazonFSxADValidation](#)文件。

运行手册执行

使用 Amazon FSx ID 或 AD 参数执行运行手册。以下是运行手册的工作流程：

- 从 Amazon FSx ID 获取参数或使用输入的 AD 参数。
- 使用在 Amazon FSx 子网上创建临时验证 Amazon EC2 Windows 实例、SSM 访问安全组、IAM 角色和策略（有条件的）。CloudFormation如果指定了InstanceId参数，则使用该参数。
- 在 Amazon FSx 主子网中的目标 Amazon EC2 实例上下载并执行验证脚本。
- 在自动化输出中提供 AD 验证结果代码。此外，完整的脚本输出将上传到 Amazon S3 存储桶。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack

- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackResources`
- `cloudformation:DescribeStackEvents`
- `ec2:CreateTags`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `ec2:CreateLaunchTemplate`
- `ec2>DeleteLaunchTemplate`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:CreateSecurityGroup`
- `ec2>DeleteSecurityGroup`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupEgress`
- `iam:CreateRole`
- `iam:CreateInstanceProfile`
- `iam:GetInstanceProfile`
- `iam:getRolePolicy`
- `iam>DeleteRole`
- `iam>DeleteInstanceProfile`
- `iam:AddRoleToInstanceProfile`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`

- iam:GetRole
- iam:PassRole
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:DescribeAutomationExecutions
- ssm:GetDocument
- ssm:GetAutomationExecution
- ssm:DescribeAutomationStepExecutions
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:ListCommands
- ssm:GetCommandInvocation
- fsx:DescribeFileSystems
- ds:DescribeDirectories
- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetAccountPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetBucketLocation

自动化承担角色的 IAM policy 示例

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribe",
      "Effect": "Allow",
```

```

        "Action": [
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeImages",
            "ec2:DescribeInstances",
            "ec2:DescribeLaunchTemplates",
            "ec2:DescribeLaunchTemplateVersions",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeAutomationExecutions",
            "ssm:DescribeAutomationStepExecutions",
            "fsx:DescribeFileSystems",
            "ds:DescribeDirectories"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CloudFormation",
        "Effect": "Allow",
        "Action": [
            "cloudformation:DescribeStacks",
            "cloudformation:DescribeStackResources",
            "cloudformation:DescribeStackEvents",
            "cloudformation:CreateStack",
            "cloudformation>DeleteStack"
        ],
        "Resource": "arn*:cloudformation:*:*:stack/
AWSsupport-ValidateFSxWindowsADConfig-*"
    },
    {
        "Sid": "AllowCreateLaunchTemplate",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateLaunchTemplate",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:launch-template/*"
        ]
    },
    {
        "Sid": "AllowEC2RunInstances",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances",

```

```

        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:::image/*",
        "arn:aws:ec2:::snapshot/*",
        "arn:aws:ec2:::subnet/*",
        "arn:aws:ec2:::network-interface/*",
        "arn:aws:ec2:::security-group/*",
        "arn:aws:ec2:::key-pair/*",
        "arn:aws:ec2:::launch-template/*"
    ]
},
{
    "Sid": "AllowEC2RunInstancesWithTags",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:::instance/*",
        "arn:aws:ec2:::volume/*"
    ]
},
{
    "Sid": "EC2SecurityGroup",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn*:ec2:::security-group/*",
        "arn*:ec2:::vpc/*"
    ]
},
{
    "Sid": "EC2Remove",
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances",
        "ec2>DeleteLaunchTemplate",

```

```

        "ec2:DeleteSecurityGroup"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:*:ec2:*:*:security-group/*"
    ]
},
{
    "Sid": "IAMInstanceProfile",
    "Effect": "Allow",
    "Action": [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": "arn:*:iam:*:*:instance-profile/*"
},
{
    "Sid": "IAM",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:getRolePolicy",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
    ],
    "Resource": "arn:*:iam:*:*:role/*"
},
{
    "Sid": "SSM",
    "Effect": "Allow",
    "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",

```



```

        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:GetCommandInvocation"
    ],
    "Resource": "*"
},
{
    "Sid": "SSMSendCommand",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript"
},
{
    "Sid": "SSMSendCommandOnlyFsxInstance",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringLike": {
            "ssm:resourceTag/CreatedBy": [
                "AWSSupport-ValidateFSxWindowsADConfig"
            ]
        }
    }
},
{
    "Sid": "AllowPassRoleToEC2",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:*:iam:*:*:role/AWSSupport-ValidateFSxWindowsADConfig-*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ec2.amazonaws.com"
            ]
        }
    }
}

```

```

    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetAccountPublicAccessBlock",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketAcl",
      "s3:GetBucketLocation"
    ],
    "Resource": "*"
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-ValidateFSxWindowsADConfig](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 要使用现有失败或配置错误的 Amazon FSx 验证自我管理的 AD，请输入以下参数：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- FSxId (视情况而定)：

适用于 Windows 的亚马逊 FSx 文件服务器 ID。这是验证现有失败或配置错误的 Amazon FSx 所必需的。

- SecretArn (必填)：

你的 Secrets Manager 密钥的 ARN，其中包含亚马逊 FSx 服务账户的用户名和密码。确保用户名和密码使用一 key/value 对格式存储{"username":"EXAMPLE-

USER", "password": "EXAMPLE-PASSWORD"}。CloudFormation 堆栈创建具有对此 ARN 执行权限 `GetSecretValue` 的验证实例。

- **FSxSecurityGroupId** (必填) :

适用于 Windows File Server 的亚马逊 FSx 的安全组 ID。

- **BucketName** (必填) :

要将验证结果上传到的 Amazon S3 存储桶。确保存储桶配置了服务器端加密 (SSE)，并且存储桶策略不会向不需要访问日志的各方授予不必要的 read/write 权限。此外，请确保亚马逊 EC2 Windows 实例拥有对亚马逊 S3 存储桶的必要访问权限。

Input parameters

InstanceId
 (Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. ****Caution****: The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, ****do not use a production instance****. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

☒ Show interactive instance picker

AWS::EC2::Instance::Id

AutomationAssumeRole
 (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

fsx-test

BucketName
 (Required) The Amazon S3 bucket to upload the validation results to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

test-for-customer

RetainCloudFormationStack
 (Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

SecretArn
 (Required) The ARN of your AWS Secrets Manager secret containing the FSx service account username and password. Make sure that the username and password are stored using a key/value pair in the format {"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"} .

arn:aws:secretsmanager:us-west-2:123456789012:secret:fsx-test

FSxSecurityGroupId
 (Required) The security group ID of the Amazon FSx for Windows File Server.

sg-examplesg1234

FSxId
 (Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

fs-abcdef123456789

4. 要验证用于创建新的 Amazon FSx 的自管理 AD 配置，请输入以下参数：

- **AutomationAssumeRole** (可选) :

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- **SecretArn** (必填) :

你的 Secrets Manager 密钥的 ARN，其中包含亚马逊 FSx 服务账户的用户名和密码。确保用户名和密码使用一 key/value 对格式存储 {"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}。CloudFormation 堆栈创建具有对此 ARN 执行权限 `GetSecretValue` 的验证实例。

- FSxSecurityGroupId (必填) :

适用于 Windows File Server 的亚马逊 FSx 的安全组 ID。

- BucketName (必填) :

要将验证结果上传到的 Amazon S3 存储桶。确保存储桶配置了服务器端加密 (SSE)，并且存储桶策略不会向不需要访问日志的各方授予不必要的 read/write 权限。此外，请确保亚马逊 EC2 Windows 实例拥有对亚马逊 S3 存储桶的必要访问权限。

- FSxPreferredSubnetId (视情况而定) :

适用于 Windows File Server 的 Amazon FSx 首选子网。

- DomainName (视情况而定) :

你自行管理的 Microsoft AD 域的完全限定域名。

- DnsIpAddresses (视情况而定) :

您的自管理 AD 域中最多两个 DNS 服务器或域控制器 IP 地址的列表。对于最多两个 IP，请用逗号分隔输入。

- FSxAdminsGroup (视情况而定) :

适用于 Windows File Server 的 Amazon FSx 委派了文件系统管理员组。默认情况下，该名称为 Domain Admins。

- FSxOrganizationalUnit (视情况而定) :

您要加入文件系统的组织单位 (OU)。提供 OU 的可分辨路径名。示例：OU=org,DC=example,DC=com。

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

TestServiceAccountPermissions

(Optional) Enable service account permission validation. This validation will create test Active Directory computer objects in the Microsoft Active Directory Organizational Unit. The resources are cleaned up by the script unless delete permissions are not properly configured on the provided service account in which case manual cleanup may be necessary.

DnsIpAddresses

(Conditional) A list of up to two DNS server or domain controller IP addresses in your self-managed AD domain. Required if the `FSxId` parameter is not specified. For up to two IPs, enter them separated by a comma.

FSxSecondarySubnetId

(Conditional) The Amazon FSx for Windows File Server secondary subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Optional if the `FSxId` parameter is not specified.

FSxOrganizationalUnit

(Conditional) The Organizational Unit (OU) within which you want to join your file system. Provide the distinguished path name of the OU. Example: `OU=org,DC=example,DC=com`. Optional if the `FSxId` parameter is not specified.

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

DomainName

(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.

FSxPreferredSubnetId

(Conditional) The Amazon FSx for Windows File Server preferred subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Required if the `FSxId` parameter is not specified.

FSxAdminsGroup

(Conditional) The Amazon FSx for Windows File Server delegated file system administrators group. Optional if the `FSxId` parameter is not specified. By default, this is `Domain Admins`.

InstanceKeyPairName

(Conditional) An existing Amazon EC2 key pair you want to associate to the temporary Amazon EC2 instance. Optional when the `InstanceId` parameter is not specified.

5. 选择执行。

6. 自动化启动。

7. 文档将执行以下步骤：

- **CheckBucketPublicStatus** (aws: ExecuteScript)：

检查目标 Amazon S3 存储桶是否有可能授予对其对象的读 and/or 写公共访问权限。

- **BranchOnInputParameters** (aws: branch)：

在提供的输入参数上进行分支，例如亚马逊 FSx ID 或亚马逊 FSx 参数。

- **AssertFileSystemTypeIsWindows** (aws: assertAwsResourceProperty)：

如果提供了亚马逊 FSx ID，则验证文件系统类型是否为适用于 Windows File Server 的 Amazon FSx。

- **GetValidationInputs** (aws: ExecuteScript)：

返回 CloudFormation 模板创建亚马逊 EC2 实例所需的自行管理的 Microsoft AD 配置。

- **BranchOnInstanceId** (aws: branch)：

在提供的输入上进行分支InstanceId。如果提供，InstanceId则验证脚本将通过自动化在目标 Amazon EC2 实例上运行step:RunValidationScript。

- **CreateEC2InstanceStack** (aws: createStack)：

使用该AmazonFSxADValidation工具的执行 CloudFormation 位置在首选子网中创建 Amazon EC2 实例

- DescribeStackResources (aws: execute) : AwsApi

描述用于获取临时 Amazon EC2 实例 ID 的 CloudFormation 堆栈。

- WaitForEC2InstanceToBeManaged (aws: waitForAwsResourceProperty) :

等待 Amazon EC2 实例由 Systems Manager 管理，以便使用 SSM 运行命令运行验证脚本。

- GetAmazonFSxADValidationAttachment (aws: execute) : AwsApi

从运行手册附件中获取AmazonFSxADValidation工具 URL。

- RunValidationScript (aws: runCommand) :

在临时 Amazon EC2 实例上运行该AmazonFSxADValidation工具，并将结果存储在BucketName参数中指定的 Amazon S3 存储桶中。

- DescribeErrorsFromStackEvents (aws: ExecuteScript) :

描述运行手册无法创建 CloudFormation 堆栈时的堆栈事件。

- BranchOnRetainCloudFormationStack (aws: branch) :

对RetainCloudFormationStack和InstanceId参数进行分支，用于确定是否应删除 CloudFormation 堆栈。

- DeleteCloudFormationStack (aws: deleteStack) :

删除 CloudFormation 堆栈。

8. 完成后，请查看“输出”部分以了解执行结果：

▼ Outputs

```
DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:[REDACTED]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msfc.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-[REDACTED]
TestServiceAccountPermissions: True
TranscriptDirectory: C:\ProgramData\Amazon\AmazonFSxADValidation\3428bd96-f8ca-4c8d-9b02-57d81560bac8
AdminGroup: Domain Admins
OrganizationalUnit:

=====
The validation details and logs can be found in the bucket test-for-customer.

ERRORS: 1
- InvalidCredentials

WARNINGS: 0

For detailed information about a given warning or error, see C:\ProgramData\Amazon\AmazonFSxADValidation\AmazonFSxADValidation\TROUBLESHOOTING.md.

=====
The local DNS configuration has been reset successfully.
```

运行手册会将验证脚本的执行结果上传到 Amazon S3 存储桶。

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWS 服务文档

- [What is Amazon FSx for Windows File Server?](#)
- [正在验证适用于 Windows File Server 的 Amazon FSx 的自管理 AD 配置](#)

GuardDuty

AWS Systems Manager 自动化为 Amazon GuardDuty 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

AWSConfigRemediation-CreateGuardDutyDetector

描述

AWSConfigRemediation-CreateGuardDutyDetector 运行手册会在您运行自动化的 AWS 区域位置创建一个 Amazon GuardDuty (GuardDuty) 检测器。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector
- guardduty:GetDetector

文档步骤

- `aws:executeAwsApi`-创建 GuardDuty 探测器。
- `aws:assertAwsResourceProperty` - 验证检测器的 Status 是否为 ENABLED。

IAM

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Identity and Access Management有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)
- [AWS-AttachIAMToInstance](#)
- [AWS-DeleteIAMInlinePolicy](#)
- [AWSConfigRemediation-DeleteIAMRole](#)
- [AWSConfigRemediation-DeleteIAMUser](#)
- [AWSConfigRemediation-DeleteUnusedIAMGroup](#)
- [AWSConfigRemediation-DeleteUnusedIAMPolicy](#)
- [AWSConfigRemediation-DetachIAMPolicy](#)
- [AWSConfigRemediation-EnableAccountAccessAnalyzer](#)
- [AWSSupport-GrantPermissionsToIAMUser](#)
- [AWSConfigRemediation-RemoveUserPolicies](#)
- [AWSConfigRemediation-ReplaceIAMInlinePolicy](#)
- [AWSConfigRemediation-RevokeUnusedIAMUserCredentials](#)
- [AWSConfigRemediation-SetIAMPasswordPolicy](#)
- [AWSSupport-ContainIAMPrincipal](#)
- [AWSSupport-TroubleshootSAMLIssues](#)

AWSSupport - TroubleshootIAMAccessDeniedEvents

描述

AWSsupport-TroubleshootIAMAccessDeniedEvents 自动化运行手册可帮助排除 AWS Identity and Access Management (IAM) 访问被拒绝的问题。运行手册会查询 CloudTrail 与指定 IAM 实体和 AWS 服务事件源相关的最近访问被拒绝事件。它可以在长达 24 小时的可配置时间窗口内分析事件，每次执行最多处理 10 个事件。对每个已识别的访问被拒绝事件进行检查，以帮助了解拒绝和尝试操作的背景。自动化同时分析基于身份和基于资源的 IAM 策略。对于基于身份的策略，它会检查附加到 IAM 实体的内联和托管策略。对于基于资源的策略，它会评估多种 AWS 服务的策略，包括亚马逊简单存储服务 (Amazon S3)、()、AWS Key Management Service 亚马逊简单通知服务 (Amazon SNS) Simple Notification Service、AWS Lambda 亚马逊弹性容器注册表 (Amazon ECR)、Amazon API Gateway、亚马逊弹性文件系统 (Amazon EFS)、CodeArtifact 亚马逊简单队列服务 (亚马逊 SQS) Simple Service、Amazon AWS Cloud9 服务、Signer 和 AWS KMS OpenSearch AWS Serverless Application Repository AWS Secrets Manager

该运行手册利用 IAM 策略模拟功能根据事件中发现的被拒绝操作来评估这些策略。CloudTrail 该运行手册通过针对 IAM 用户和 IAM 角色利用 [SimulatePrincipalPolicy](#) 用 IAM [SimulateCustomPolicy](#) 的策略模拟功能，根据事件中发现的被拒绝的操作来评估这些策略。CloudTrail 自动化会输出一份报告，该报告可帮助识别被拒绝的具体操作，区分隐式拒绝和显式拒绝，列出导致拒绝访问的策略，并为每一次拒绝提供解释。该报告还提出了可能的解决方案，例如识别缺失的允许声明或相互矛盾的拒绝声明

如何工作？

运行手册执行以下步骤：

- 描述和验证 RequesterARN (角色或用户) 以获取诸如 IAM 实体类型和 IAM ID 之类的信息。
- 获取与 RequesterARNEventSource、和关联 CloudTrail 的事件 (ResourceARN 如果提供)。
- 分析 CloudTrail 事件以获取返回“访问被拒绝”错误时执行的操作，然后检查所有 IAM 策略，例如附加到 IAM 实体的内联和托管策略，以及基于资源的策略。然后，它会根据相关 CloudTrail 事件的“Access Denied”错误中发现的操作来模拟这些策略，以确定错误的原因。
- 输出一份报告，确定 Access Denied 错误的类型、导致错误的策略，并就错误的可能解决方案提供建议。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- apigateway:GetRestApis
- cloudtrail:LookupEvents
- cloud9:GetEnvironment
- codeartifact:GetRepositoryPermissionsPolicy
- ecr:GetRepositoryPolicy
- elasticfilesystem:GetFileSystemPolicy
- es:DescribeDomain
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRole
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies
- iam:SimulatePrincipalPolicy
- iam:SimulateCustomPolicy
- kms:GetKeyPolicy
- lambda:GetPolicy
- secretsmanager:GetResourcePolicy
- serverlessrepo:GetApplication

- signer:GetSigningProfile
- sns:GetTopicAttributes
- ssm:StartAutomationExecution
- ssm:StopAutomationExecution
- sqs:GetQueueAttributes
- s3:GetBucketPolicy

策略示例：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:ListUserPolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetUserPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedUserPolicies",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "cloudtrail:LookupEvents",
        "iam:SimulateCustomPolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketPolicy",
        "kms:GetKeyPolicy",
```

```

        "lambda:GetPolicy",
        "sns:GetTopicAttributes",
        "ecr:GetRepositoryPolicy",
        "apigateway:GET",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:DescribeEnvironmentStatus",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
    ]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。需要将该角色添加到您的 Amazon EKS 集群访问条目或 RBAC 权限中，才能允许 Kubernetes API 调用。
 - 类型：AWS::IAM::Role::Arn
 - requesterArn (必填)：
 - 描述：(必填) 您要调查其对特定 AWS 资源的访问权限的 IAM 用户或角色的 ARN。
 - 类型：String
 - 允许模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`

- resourceArn (可选) :
 - 描述 : (可选) 评估访问被拒绝 AWS 的资源的 ARN。AWS 目标资源应位于执行自动化 Runbook 的同一区域。
 - 类型 : String
 - 允许模式 : `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:([a-zA-Z0-9\\-]{1,63}):([a-z0-9\\-]{0,63})?:((\\d{12})?:([a-zA-Z0-9\\-_/:.]{1,1024}))$`
- EventSource (必填) :
 - 描述 : (必填) CloudTrail事件起源的 Amazon API 终端节点。例如 : `s3.amazonaws.com`。
 - 类型 : String
 - 允许模式 : `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (可选) :
 - 描述 : (可选) 与 CloudTrail 事件关联的 Amazon API 操作名称。例如 : `s3:CreateBucket`。
 - 类型 : String
 - 允许模式 : `^$|^([a-z0-9]+:[A-Za-z0-9])+$`
- LookBackHours (可选) :
 - 描述 : (可选) 搜索 CloudTrail 事件时要回顾 Access Denied事件的小时数。有效范围 : 1到24小时。
 - 类型 : 整数
 - 允许模式 : `^([1-9]|1[0-9]|2[0-4])$`
 - 默认值 : 12
- MaxEvents (可选) :
 - 描述 : (可选) 搜索 CloudTrail Access Denied事件时返回的最大事件数。有效范围 : 1至5事件。
 - 类型 : 整数
 - 允许模式 : `^([1-9]|1[0-9]|2[0-4])$`
 - 原定设置值 : 3
- UseContextEntries (可选) :
 - 描述 : (可选) 如果您指定 `true` , 则自动化会从 CloudTrail 事件中提取有关 API 请求上下文的

- 类型：布尔值
- 允许模式：`^([1-9]|1[0-9]|2[0-4])$`
- 原定设置值：3

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- `ValidateRequesterArn`

验证和解构 `RequesterArn` ARN，检索有关目标 IAM 用户或角色的信息。

- `GetCloudTrailEventsWithAccessDeniedError`

查询与指定 IAM 实体和 AWS 服务相关的最新 `Access Denied` 事件 `EventSource`。CloudTrail

- 评估 `IAMRequester` 政策

根据事件产生的操作评估请求者 IAM 实体的 IAM 权限。CloudTrail 此评估包括分析与请求者相关的基于身份和基于资源的策略。自动化利用 IAM 的策略模拟功能，在 CloudTrail 事件中发现的被拒绝操作的背景下评估这些策略。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- `PermissionEvaluationResults`

输出一份报告，该报告有助于识别被拒绝的具体操作，区分隐含拒绝和显式拒绝。它还列出了导致拒绝访问的政策，并对每一次拒绝都提供了解释。该报告还提出了可能的解决方案，例如识别缺失的允许声明或相互矛盾的拒绝声明

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

AWS-AttachIAMToInstance

描述

将 AWS Identity and Access Management (IAM) 角色附加到托管实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ForceReplace

类型：布尔值

描述：(可选) 指定是否替换现有 IAM 配置文件的标志。

默认：True

- InstanceId

类型：字符串

描述：(必需) 要为其分配 IAM 角色的实例 ID。

- RoleName

类型：字符串

描述：(必需) 要添加到托管实例的 IAM 角色名称。

文档步骤

1. `aws:executeAwsApi- DescribeInstanceProfile` -查找附加到 EC2 实例的 IAM 实例配置文件。
2. `aws:branch- CheckInstanceProfileAssociations` -检查附加到 EC2 实例的 IAM 实例配置文件。
 - a. 如果附加了 `ForceReplace` IAM 实例配置文件并将 `设置为 true` :
 - i. `aws:executeAwsApi- DisassociateIamInstanceProfile` -解除 IAM 实例配置文件与 EC2 实例的关联。
 - b. `aws:executeAwsApi- ListInstanceProfilesForRole` -列出所提供的 IAM 角色的实例配置文件。
 - c. `aws:branch- CheckInstanceProfileCreated` -检查提供的 IAM 角色是否有关联的实例配置文件。
 - i. 如果 IAM 角色具有关联的实例配置文件 :
 - A. `aws:executeAwsApi- AttachIAMProfileToInstance` -将 IAM 实例配置文件角色附加到 EC2 实例。
 - i. 如果 IAM 角色没有关联的实例配置文件 :
 - A. `aws:executeAwsApi- CreateInstanceProfileForRole` -为指定的 IAM 角色创建实例配置文件角色。
 - B. `aws:executeAwsApi- AddRoleToInstanceProfile` -将实例配置文件角色附加到指定的 IAM 角色。
 - C. `aws:executeAwsApi- GetInstanceProfile`-获取指定 IAM 角色的实例配置文件数据。
 - D. `aws:executeAwsApi- AttachIAMProfileToInstanceWithRetry` -将 IAM 实例配置文件角色附加到 EC2 实例。

输出

`AttachIAMProfileToInstanceWithRetry.AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`AttachIAMProfileToInstance.AssociationId`

`ListInstanceProfilesForRole.InstanceProfileName`

`ListInstanceProfilesForRole.InstanceProfileArn`

AWS-DeleteIAMInlinePolicy

描述

AWS-DeleteIAMInlinePolicy运行手册会删除附加到您指定的 IAM 身份的所有 AWS Identity and Access Management (IAM) 内联策略。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- IamArns

类型：字符串

描述：(必填) 要从中删除内联策略的 IAM 身份的 ARN 列表，以逗号分隔。此列表可以包括 IAM 用户、群组或角色。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- iam:DeleteGroupPolicy

- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

文档步骤

- aws:executeScript-删除附加到目标 IAM 身份的 IAM 内联策略。

AWSConfigRemediation-DeleteIAMRole

描述

AWSConfigRemediation-DeleteIAMRole 运行手册可删除您指定的 AWS Identity and Access Management (IAM) 角色。此自动化并不删除与 IAM 角色或服务相关角色关联的实例配置文件。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- IAMRoleID

类型：字符串

描述：(必选) 要删除的 IAM 角色的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam>ListInstanceProfilesForRole`
- `iam>ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

文档步骤

- `aws:executeScript` - 收集您在 IAMRoleID 参数中指定的 IAM 角色的名称。
- `aws:executeScript` - 收集与 IAM 角色关联的策略和实例配置文件。
- `aws:executeScript` - 删除附加的策略。
- `aws:executeScript` - 删除 IAM 角色并验证该角色已被删除。

AWSConfigRemediation-DeleteIAMUser

描述

AWSConfigRemediation-DeleteIAMUser 运行手册可删除您指定的 AWS Identity and Access Management (IAM) 用户。此自动化可删除或分离与 IAM 用户关联的以下资源：

- 访问密钥

- 附加的托管策略
- Git 凭证
- IAM 群组成员资格
- IAM 用户密码
- 内联策略
- Multi-factor 身份验证 (MFA) 设备
- 签名证书
- SSH 公约

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- IAMUserId

类型：字符串

描述：(必选) 要删除的 IAM 用户的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeactivateMFADevice
- iam>DeleteAccessKey
- iam>DeleteLoginProfile
- iam>DeleteServiceSpecificCredential
- iam>DeleteSigningCertificate
- iam>DeleteSSHPublicKey
- iam>DeleteVirtualMFADevice
- iam>DeleteUser
- iam>DeleteUserPolicy
- iam:DetachUserPolicy
- iam:GetUser
- iam:ListAttachedUserPolicies
- iam:ListAccessKeys
- iam:ListGroupsForUser
- iam:ListMFADevices
- iam:ListServiceSpecificCredentials
- iam:ListSigningCertificates
- iam:ListSSHPublicKeys
- iam:ListUserPolicies
- iam:ListUsers
- iam:RemoveUserFromGroup

文档步骤

- aws:executeScript - 收集您在 IAMUserId 参数中指定的 IAM 用户的用户名。
- aws:executeScript - 收集与 IAM 用户关联的访问密钥、证书、凭证、MFA 设备和 SSH 密钥。
- aws:executeScript - 收集 IAM 用户的群组成员资格和策略。
- aws:executeScript - 删除与 IAM 用户关联的访问密钥、证书、凭证、MFA 设备和 SSH 密钥。

- `aws:executeScript` - 删除 IAM 用户的群组成员资格和策略。
- `aws:executeScript` - 删除 IAM 用户并验证该用户已被删除。

AWSConfigRemediation-DeleteUnusedIAMGroup

描述

AWSConfigRemediation-DeleteUnusedIAMGroup 运行手册将删除不包含任何用户的 IAM 群组。

AWSConfigRemediation-DeleteUnusedIAMGroup 运行手册将删除不包含任何用户的 IAM 群组。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- GroupName

类型：字符串

描述：(必需) 要删除的 IAM 群组的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteGroup
- iam>DeleteGroupPolicy
- iam:DetachGroupPolicy

文档步骤

- aws:executeScript - 移除附加到目标 IAM 群组的托管和内联 IAM 策略，然后删除该 IAM 组。

AWSConfigRemediation-DeleteUnusedIAMPolicy

描述

AWSConfigRemediation-DeleteUnusedIAMPolicy 运行手册将删除未附加到任何用户、群组或角色的 AWS Identity and Access Management (IAM) 策略。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- **IAMResourceId**

类型：字符串

描述：(必需) 要删除的 IAM policy 的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DeletePolicy
- iam:DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

文档步骤

- `aws:executeScript` - 删除您在 IAMResourceId 参数中指定的策略，并验证该策略是否已删除。

AWSConfigRemediation-DetachIAMPolicy

描述

AWSConfigRemediation-DetachIAMPolicy 运行手册将分离您指定的 AWS Identity and Access Management (IAM) 策略。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- IAMResourceId

类型：字符串

描述：(必选) 要分离的 IAM policy 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy
- iam:DetachUserPolicy
- iam:GetPolicy
- iam:ListEntitiesForPolicy

文档步骤

- aws:executeScript - 将 IAM policy 与所有资源分离。

AWSConfigRemediation-EnableAccountAccessAnalyzer

描述

AWSConfigRemediation-EnableAccountAccessAnalyzer运行手册将在您的 AWS 账户中创建一个 AWS Identity and Access Management (IAM) 访问分析器。有关 Access Analyzer 的信息，请参阅《IAM 用户指南》中的[使用 AWS IAM Access Analyzer](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AnalyzerName

类型：字符串

描述：(必需) 要创建的分析器名称。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

文档步骤

- `aws:executeAwsApi` - 为您的账户创建一个访问分析器。
- `aws:waitForAwsResourceProperty` - 等待访问分析器的状态变为 ACTIVE。
- `aws:assertAwsResourceProperty` - 确认访问分析器的状态为 ACTIVE。

AWSsupport-GrantPermissionsToIAMUser

描述

此运行手册将指定的权限授予 IAM 组（新建组或现有组），并将现有的 IAM 用户添加到此组。您可以选择的策略：[账单](#)或[支持](#)。要为 IAM 启用账单访问权限，请注意还需要激活 [IAM 用户和联合用户对“账单和成本管理”页面的访问权限](#)。

Important

如果提供的是现有 IAM 组，则此组中的所有当前 IAM 用户都将收到新权限。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- IAMGroupName

类型：字符串

默认：ExampleSupportAndBillingGroup

描述：(必需) 可以是新组或现有组。必须符合 [IAM 实体名称限制](#)。

- IAMUserName

类型：字符串

默认：ExampleUser

描述：(必需) 必须是现有用户。

- LambdaAssumeRole

类型：字符串

描述：(可选) Lambda担任的角色的 ARN。

- Permissions

类型：字符串

有效值：SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

默认：SupportAndBillingFullAccess

描述：(必需) 选择以下值之一：SupportFullAccess 授予支持中心的完全访问权限。BillingFullAccess 授予“账单”控制面板的完全访问权限。SupportAndBillingFullAccess 授予支持中心和“账单”控制面板的完全访问权限。有关策略的更多信息，请参阅文档详细信息。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

所需的权限取决于 AWSSupport-GrantPermissionsToIAMUser 的运行方式。

以当前登录的用户或角色运行

建议附加 AmazonSSMAutomationRole Amazon 托管策略以及以下额外权限，以便创建 Lambda 函数和将 IAM 角色传递给 Lambda：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource": [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
```

```

        "arn:aws:iam::aws:policy/job-function/Billing",
        "arn:aws:iam::aws:policy/AWSSupportAccess"
    ]
}
},
{
    "Effect": "Allow",
    "Action": [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
    ],
    "Resource": "*"
}
]
}

```

使用 AutomationAssumeRole 和 LambdaAssumeRole

用户在运行手册上必须具有 `ssm: StartAutomationExecution` 权限，对作为 `AutomationAssumeRole` 和传递的 IAM 角色必须具有 `iam: PassRole` 权限。LambdaAssumeRole 以下是每个 IAM 角色所需的权限：

AutomationAssumeRole

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda>DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
"arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
            "Effect": "Allow"
        }
    ]
}

```

LambdaAssumeRole

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
            "arn:aws:iam::aws:policy/job-function/Billing",
            "arn:aws:iam::aws:policy/AWSSupportAccess"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}

```



```
}
```

文档步骤

1. `aws:createStack`-运行 CloudFormation 模板创建 Lambda 函数。
2. `aws:invokeLambdaFunction` - 运行 Lambda 以设置 IAM 权限。
3. `aws:deleteStack`-删除 CloudFormation 模板。

输出

配置 IAM.Payload

AWSConfigRemediation-RemoveUserPolicies

描述

AWSConfigRemediation-RemoveUserPolicies 运行手册将删除 AWS Identity and Access Management (IAM) 内联策略，并分离附加到指定用户的所有托管策略。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- **IAMUserID**

类型：字符串

描述：(必需) 要从其移除策略的用户的 ID。

- **PolicyType**

类型：字符串

有效值：全部 | 内联 | 托管

默认：全部

描述：(必需) 要从用户移除的 IAM 策略的类型。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteUserPolicy
- iam:DetachUserPolicy
- iam>ListAttachedUserPolicies
- iam:ListUserPolicies
- iam:ListUsers

文档步骤

- `aws:executeScript` - 删除您在 IAMUserID 参数中指定的用户的 IAM 策略并将其与该用户分离。

AWSConfigRemediation-ReplaceIAMInlinePolicy

描述

AWSConfigRemediation-ReplaceIAMInlinePolicy 运行手册将内联 AWS Identity and Access Management (IAM) 策略替换为复制的托管 IAM 策略。对于附加到用户、群组或角色的内联策略，内

联策略权限会克隆到托管 IAM policy。托管 IAM 策略已添加到资源中，并删除内联策略。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- InlinePolicyName

类型：StringList

描述：(必需) 要替换的内联 IAM policy。

- ResourceId

类型：字符串

描述：(必需) 要替换其内联策略的 IAM 用户、群组或角色的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `iam:AttachGroupPolicy`
- `iam:AttachRolePolicy`
- `iam:AttachUserPolicy`
- `iam:CreatePolicy`
- `iam:CreatePolicyVersion`
- `iam>DeleteGroupPolicy`
- `iam>DeleteRolePolicy`
- `iam>DeleteUserPolicy`
- `iam:GetGroupPolicy`
- `iam:GetRolePolicy`
- `iam:GetUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

文档步骤

- `aws:executeScript` - 将内联 IAM policy 替换为指定资源的 AWS 复制策略。

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

描述

AWSConfigRemediation-RevokeUnusedIAMUserCredentials运行手册会撤销未使用的 AWS Identity and Access Management (IAM) 密码和有效的访问密钥。此运行手册还会停用过期的访问密钥，并删除过期的登录配置文件。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- IAMResourceId

类型：字符串

描述：(必需) 要从其撤销未使用的凭证的 IAM 资源的 ID。

- MaxCredentialUsageAge

类型：字符串

默认：90

描述：(必需) 凭证必须已使用的天数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam>DeleteAccessKey
- iam>DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile

- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

文档步骤

- aws:executeScript - 撤销您在 IAMResourceId 参数中指定的用户的 IAM 凭证。过期的访问密钥将被停用，过期的登录配置文件将被删除。

Note

确保将此修复操作的MaxCredentialUsageAge参数配置为与用于触发此操作的 AWS Config 规则的maxAccessKeyAge参数相匹配：[access-keys-](#) rotated。

AWSConfigRemediation-SetIAMPasswordPolicy

描述

AWSConfigRemediation-SetIAMPasswordPolicy运行手册将为您的 AWS 账户设置 AWS Identity and Access Management (IAM) 用户密码策略。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- AllowUsersToChangePassword

类型：布尔值

默认：false

描述：(可选) 如果设置为true，则您的所有 IAM 用户都 AWS 账户 可以使用 AWS 管理控制台 来更改其密码。

- HardExpiry

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true，IAM 用户将无法在密码到期后重置密码。

- MaxPasswordAge

类型：整数

默认值：0

描述：(可选) IAM 用户密码的有效天数。

- MinimumPasswordLength

类型：整数

默认：6

描述：(可选) IAM 用户的密码可以包含的最少字符数。

- PasswordReusePrevention

类型：整数

默认值：0

描述：(可选) 阻止 IAM 用户再次使用的先前密码的数量。

- **RequireLowercaseCharacters**

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true , 则 IAM 用户的密码必须包含 ISO 基本拉丁字母 (a 到 z) 中的小写字符。

- **RequireNumbers**

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true , 则 IAM 用户的密码必须包含数字字符 (0-9)。

- **RequireSymbols**

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true , 则 IAM 用户的密码必须包含非字母数字字符 (! @ # \$ % ^ * () _ + - = [] { } | ')。

- **RequireUppercaseCharacters**

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true , 则 IAM 用户的密码必须包含 ISO 基本拉丁字母 (A 到 Z) 中的大写字符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:GetAccountPasswordPolicy
- iam:UpdateAccountPasswordPolicy

文档步骤

- `aws:executeScript` - 根据您为 AWS 账户的运行手册参数指定的值设置 IAM 用户密码策略。

AWSSupport-ContainIAMPrincipal

描述

如果发生安全事件或涉嫌泄露 AWS Identity and Access Management (IAM) 用户/角色或 AWS 身份中心 (IDC) 用户，在保留其配置以供调查的同时，迅速隔离受影响的身份至关重要。该操作 `AWSSupport-ContainIAMPrincipal` 手册提供了一种结构化、可逆的方法来遏制受损的 IAM 或 IDC 身份，从而有效地阻止他们访问 AWS 资源并防止漏洞的潜在传播。

这种自动化过程允许在不永久更改身份配置的情况下进行调查，从而允许在认为适当时恢复正常访问权限。遏制过程可以维护 IAM 中的用户或角色或 IDC 中的用户，同时有效地将其与所有网络活动隔离开来。这种隔离可防止所包含的身份资源与您的 Amazon Virtual Private Cloud 内的资源通信或访问互联网资源。封闭装置的设计是可逆的，允许在认为适当时恢复正常进入。

如何工作？

该 `AWSSupport-ContainIAMPrincipal` 运行手册对 IAM 用户、角色和身份中心用户实施了全面的控制流程。在 `Contain` 模式下执行时，它会首先验证所有输入参数，然后对指定的 Amazon S3 存储桶执行安全检查。然后，它收集有关目标 IAM 委托人的详细信息，并根据委托人类型应用适当的遏制措施。对于 IAM 用户，它会禁用访问密钥、移除控制台访问权限并附加拒绝策略。对于 IAM 角色，它会附加一个拒绝策略，该策略可撤消在包含之前创建的会话的权限。对于 Identity Center 用户，它会删除权限集、群组成员资格，并应用拒绝策略。在整个过程中，运行手册会将原始配置备份到 Amazon S3 存储桶，以便进行恢复。在 `Restore` 模式下执行时，它会尝试使用备份的配置将主体恢复到其预先包含的状态。运行手册包括一个无需应用更改即可预览变更的 `DryRun` 选项，并提供有关成功操作和失败场景的全面报告。

Important

- **使用提升权限：**此 SSM 文档执行各种需要提升权限的操作，例如修改 IAM 和 IDC 身份策略以及应用隔离配置。这些操作可能会导致权限升级或影响依赖目标身份的其他工作负载。您应查看向 `AutomationAssumeRole` 参数指定的角色授予的权限，并确保这些权限适用于预期用例。有关 IAM 权限的更多信息，您可以参考以下 AWS 文档：
 - [身份和访问管理 \(IAM\) Access Management 权限](#)
 - [AWS Systems Manager 自动化权限](#)

- **工作负载不可用风险**：本 Systems Manager 文档执行的隔离操作可能会导致工作负载不可用或中断。在安全事件期间执行时，它将通过撤消指定 IAM 和 IDC 身份的 AWS API 权限来限制对受影响资源的访问，阻止他们进行任何 AWS API 调用或操作。这可能会影响依赖这些身份的任何应用程序或服务。
- **创建其他资源**：自动化文档可能会有条件地创建其他资源，例如亚马逊简单存储服务 (Amazon S3) 存储桶和存储在其中的 Amazon S3 对象，具体取决于执行参数。这些资源将根据您的 AWS 使用情况产生额外费用。
- **恢复风险**：如果操作参数设置为 Restore，则此 SSM 文档会尝试将 IAM 或 IDC 身份配置恢复到其原始状态。但是，恢复过程可能会失败，从而导致 IAM 或 IDC 身份处于不一致的状态。本文档提供了在出现此类故障时手动恢复的说明，但您应该做好在恢复过程中处理潜在问题的准备。

建议在生产环境中执行运行手册之前，请仔细阅读运行手册，了解其潜在影响，并在非生产环境中对其进行测试。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

该 AutomationAssumeRole 参数需要以下权限才能成功使用运行手册：

- s3 : GetBucketLocation
- s3 : GetBucket
- s3 : ListBucket
- s3 : GetBucketPublicAccessBlocks

- s3 : GetAccountPublicAccessBlocks
- s3 : GetBucketPolicyStatus
- s3 : GetBucketAcl
- s3 : GetObject
- s3 : CreateBucket
- s3 : PutObject
- 我是 : GetUser
- 我是 : GetUserPolicy
- 我是 : GetRole
- 我是 : ListUserPolicies
- 我是 : ListAttachedUserPolicies
- 我是 : ListAccessKeys
- 我是 : ListMfaDevices
- 我是 : ListVirtualMFADevices
- 我是 : GetLoginProfile
- 我是 : GetPolicy
- 我是 : GetRolePolicy
- 我是 : ListPolicies
- 我是 : ListAttachedRolePolicies
- 我是 : ListRolePolicies
- 我是 : UpdateAccessKey
- 我是 : CreateAccessKey
- 我是 : DeleteLoginProfile
- 我是 : DeleteAccessKey
- 我是 : PutUserPolicy
- 我是 : DeleteUserPolicy
- 我是 : 停用 MFADevice
- 我是 : AttachRolePolicy
- 我是 : AttachUserPolicy
- 我是 : DeleteRolePolicy

- 我是:Tag MFADevice
- 我是 : PutRolePolicy
- 我是 : TagPolicy
- 我是 : TagRole
- 我是 : TagUser
- 我是 : UntagUser
- 我是 : UntagRole
- 组织 : ListAccounts
- sso : ListPermissionSetsProvisionedToAccount
- sso : GetInlinePolicyForPermissionSet
- sso : ListInstances
- sso 目录 : SearchUsers
- sso : ListPermissionSets
- sso : ListAccountAssignments
- sso 目录 : DescribeUser
- identitystore : ListUsers
- identitystore : ListGroups
- identitystore : IsMemberInGroups
- identitystore : ListGroupMemberships
- 秘密管理器 : CreateSecret
- 秘密管理器 : DeleteSecret
- sso : DeleteAccountAssignment
- sso : PutInlinePolicyToPermissionSet
- sso : CreateAccountAssignment
- sso : DeleteInlinePolicyFromPermissionSet
- sso : TagResource
- sso : UntagResource
- identitystore : DeleteGroupMembership
- identitystore : CreateGroupMembership

以下是 IAM 策略的示例，该策略为以下各项授予必要权限AutomationAssumeRole：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetRole",
        "iam:ListUserPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListAccessKeys",
        "iam:ListMfaDevices",
        "iam:ListVirtualMFADevices",
        "iam:GetLoginProfile",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:ListPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:UpdateAccessKey",
        "iam:CreateAccessKey",
        "iam>DeleteLoginProfile",

```

```

        "iam:DeleteAccessKey",
        "iam:PutUserPolicy",
        "iam:DeleteUserPolicy",
        "iam:DeactivateMFADevice",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DeleteRolePolicy",
        "iam:TagMFADevice",
        "iam:PutRolePolicy",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagUser",
        "iam:UntagUser",
        "iam:UntagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "OrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Sid": "SSOPermissions",
    "Effect": "Allow",
    "Action": [
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListInstances",
        "sso-directory:SearchUsers",
        "sso:ListPermissionSets",
        "sso:ListAccountAssignments",
        "sso-directory:DescribeUser",
        "sso:DeleteAccountAssignment",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:TagResource",
        "sso:UntagResource"
    ],
    "Resource": "*"
}

```

```

    },
    {
      "Sid": "IdentityStorePermissions",
      "Effect": "Allow",
      "Action": [
        "identitystore:ListUsers",
        "identitystore:ListGroups",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore>DeleteGroupMembership",
        "identitystore>CreateGroupMembership"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecretsManagerPermissions",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager>DeleteSecret"
      ],
      "Resource": "*"
    }
  ]
}

```

说明

按照这些步骤对自动化进行配置：

1. 在 S AWS ystems Manager 控制台[AWSSupport-ContainIAMPrincipal](#)中导航到。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) AWS 身份和访问管理 (IAM) Access Management 角色的亚马逊资源名称 (ARN)，允许系统管理员自动化代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - PrincipalType (必填)：

- 描述：(必填) AWS IAM 委托人类型：IAM 用户、IAM 角色或身份中心用户。
- 类型：字符串
- 允许的值：IAM user|IAM role|Identity Center user
- PrincipalName (必填)：
 - 描述：(必填) IAM 委托人的名称。对于身份中心用户，请提供用户名。
 - 类型：字符串
 - 允许的模式：`^[a-zA-Z0-9\\.\-_\!\*'()/+=,@]{1,1024}$`
- 操作 (必填)：
 - 描述：(必填) 选择Contain隔离目标 IAM 委托人或Restore尝试将 IAM 委托人恢复到之前备份的原始配置。
 - 类型：字符串
 - 允许的值：Contain|Restore
- DryRun (可选)：
 - 描述：(可选) 如果设置为true，自动化将不会对目标 IAM 委托人进行任何更改，而是输出它本来会尝试更改的内容，详细说明每个步骤。默认值：true。
 - 类型：布尔值
 - 允许的值：true|false
- ActivateDisabledKeys (视情况而定)：
 - 描述：(视情况而定) 如果输入参数“操作”设置为，Restore且设置 PrincipalType 为 IAM 用户，则此选项决定在停用后，此自动化是否应尝试激活关联的访问密钥。请注意，无法验证泄露的访问密钥的完整性。AWS 强烈建议不要重新激活被盗的密钥。相反，建议生成新密钥。默认值：false。
 - 类型：布尔值
 - 允许的值：true|false
- BackupS3BucketName (视情况而定)：
 - 描述：(视情况而定) Amazon Amazon S3 存储桶，用于在操作设置为时备份 IAM 主体配置Contain或从操作设置为时恢复配置Restore。请注意，如果指定的 Acti Contain on 是，而 runbook 无法访问该存储桶或未提供值，则会在您的账户中创建一个名awssupport-containiamprincipal-`<random-string>`为的新存储桶。如果设置 DryRun 为，则需要true此参数。
 - 类型：AWS::S3::Bucket::Name

- 描述：（视情况而定）如果将操作设置为Restore，则指定自动化用于尝试恢复 IAM 委托人配置的 Amazon Amazon S3 密钥。亚马逊 Amazon S3 密钥通常遵循以下格式:{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json。密钥可以从之前的控制自动化执行的输出中获得。
- 类型：字符串
- 允许的模式：`^[a-zA-Z0-9\\.\_-\\!*'()/]{0,1024}$`
- BackupS3BucketAccess（视情况而定）：
 - 描述：（视情况而定）在运行控制操作后将被允许访问备份 Amazon Amazon S3 存储桶的 IAM 用户或角色的 ARN。当“操作”为“时，此参数是必需的Contain。自动将AutomationAssumeRole正在其上下文中运行自动化的用户添加到列表中。
 - 类型：StringList
 - 允许的模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.-]+$`
- TagIdentifier（可选）：
 - 描述：（可选）使用您选择的标签标记 IAM 委托人，格式如下：Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>。此选项允许您跟踪本运行手册所针对的 IAM 委托人。注意：标签键和值区分大小写。
 - 类型：字符串
 - 允许的模式：`^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/\\@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/\\@a-zA-Z0-9]{0,128}$`

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- ValidateRequiredInputs

根据Action指定的值验证所需的自动化输入参数。

- CheckBackupS3BucketName

检查目标 Amazon S3 存储桶是否有可能向其对象授予read或write公开访问其对象。对于容纳工作流程，如果存储桶不存在，则会创建一个新的 Amazon S3 BackupS3BucketName 存储桶。

- BranchOnAction

根据指定的值对自动化进行分支Action。

- BranchOnPrincipalTypeAndDryRun

根据 IAM 委托人的类型 (IAM 用户、IAM 角色或身份中心用户) 及其是否在DryRun模式下运行来分支自动化。

- BranchOnPrincipalTypeForContain

分支基于Contain操作和输入中指定的 IAM 委托人类型 (IAM 用户、IAM 角色或身份中心用户) 的自动化。

- 获取 IAMUser

获取目标 IAM 用户的创建时间和用户名。

- 获取IAMUser详情

获取和存储目标 IAM 用户的配置，包括内联策略、托管策略、访问密钥、MFA 设备和登录资料。

- 最新消息 3 KeyForUser

更新步骤输出中的自动化 “S3Key” 变量。GetIAMUserDetails

- 获取 IAMRole

获取目标 IAM 角色的创建时间、角色名称和路径。

- 获取IAMRole详情

获取和存储目标 IAM 角色的配置，包括内联策略和附加到该角色的托管策略。

- 最新消息 3 KeyForRole

更新步骤输出中的自动化 “S3Key” 变量。GetIAMRoleDetails

- GetIdentityStoreId

获取与 AWS 账户关联的 AWS IAM 身份中心实例的 ID。

- 获取 IDCUser

使用身份存储 ID 获取目标身份中心用户的用户 ID。

- 收集IDCUser细节

获取和存储目标 Identity Center 用户的配置，包括帐户分配、关联权限集和内联策略。

- 最新消息 3 KeyFor IDCUser

更新步骤输出中的自动化 “S3Key” 变量。GatherIDCUserDetails

根据Contain操作的值DryRun和 IAM 委托人类型对自动化进行分支。

- BranchOnDisableAccessKeys

根据 IAM 用户是否有需要禁用的访问密钥来分支自动化。

- DisableAccessKeys

禁用有效的 IAM 用户访问密钥。

- BranchOnDisableConsoleAccess

分支基于 IAM 用户是否启用了 AWS 管理控制台访问权限。

- DisableConsoleAccess

移除 IAM 用户对 AWS 管理控制台的基于密码的访问权限。

- AttachInlineDenyPolicyToUser

向 IAM 用户附加拒绝策略，以撤消对旧会话令牌的权限。

- AttachInlineDenyPolicyToRole

向 IAM 角色附加拒绝策略，以撤消对旧会话令牌的权限。

- RemovePermissionSets

移除与 Identity Center 用户关联的权限集。

- IDCUser从中删除 IDCGroups

将身份中心用户从身份中心群组中移除。

- AttachInlineDenyPolicyToPermissionSet

将拒绝策略附加到与 Identity Center 用户关联的权限集。

- BranchOnReactivateKeys

在还原过程中，根据ActivateDisabledKeys参数对自动化进行分支。

- DetachInlineDenyPolicy

移除在控制过程中附加到 IAM 角色的拒绝策略。

- DetachInlineDenyPolicyFromPermissionSet

移除在遏制过程中附加到权限集的拒绝策略。

- ReportContain

输出有关设置为时将要执行的遏制操作DryRun的详细信息。True

- ReportRestore

输出有关设置为时DryRun将要执行的恢复操作的详细信息True。

- ReportContainFailure

提供在控制工作流程失败的情况下手动恢复 IAM 委托人的原始配置的全面说明。

- ReportRestoreFailure

提供在还原工作流程失败的情况下手动完成 IAM 委托人原始配置恢复的详细说明。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果：

- 包含IAMPrincipal。输出

提供有关在“操作”设置为“包含”且 DryRun 设置为“假”时执行的遏制操作的详细信息。包括有关备份位置、已应用的拒绝策略和修改的配置的信息。

- 恢复IAMPrincipal. 输出

提供有关在“操作”设置为“还原”且 DryRun 设置为 False 时所执行的还原操作的详细信息。包括有关已恢复的配置以及恢复过程中遇到的任何问题的信息。

- ReportContain。输出

输出有关在“操作”设置为“包含”且 DryRun 设置为 True 时将执行的遏制操作的详细信息。包括当前和封闭后配置的比较。

- ReportRestore。输出

输出有关在“操作”设置为“恢复”且 DryRun 设置为 True 时将执行的还原操作的详细信息。显示当前配置和要恢复的原始配置。

- ReportContainFailure。输出

提供在控制工作流程失败的情况下手动恢复 IAM 委托人的原始配置的全面说明。

- ReportRestoreFailure。输出

提供在还原工作流程失败的情况下手动完成 IAM 委托人原始配置恢复的详细说明。

执行完成后，请查看“输出”部分以了解详细结果：

- 包含IAMPrincipal。输出

提供有关在“操作”设置为“包含”且 DryRun 设置为“假”时执行的遏制操作的详细信息。包括有关备份位置、已应用的拒绝策略和修改的配置的信息。

- 恢复IAMPrincipal。输出

提供有关在“操作”设置为“还原”且 DryRun 设置为 False 时所执行的还原操作的详细信息。包括有关已恢复的配置以及恢复过程中遇到的任何问题的信息。

- ReportContain。输出

输出有关在“操作”设置为“包含”且 DryRun 设置为 True 时将执行的遏制操作的详细信息。包括当前和封闭后配置的比较。

- ReportRestore。输出

输出有关在“操作”设置为“恢复”且 DryRun 设置为 True 时将执行的还原操作的详细信息。显示当前配置和要恢复的原始配置。

- ReportContainFailure。输出

提供在控制工作流程失败的情况下手动恢复 IAM 委托人的原始配置的全面说明。

- ReportRestoreFailure。输出

提供在还原工作流程失败的情况下手动完成 IAM 委托人原始配置恢复的详细说明。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行简单的自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSSupport-TroubleshootSAMLIssues

描述

AWSsupport-TroubleshootSAMLIssues 自动化运行手册通过分析存储在亚马逊简单存储服务 (Amazon S3) Simple S3 Service 中的 SAML 响应文件，帮助诊断与安全断言标记语言 (SAML) 相关的问题。它执行全面的验证，包括架构验证、签名验证、受众限制检查和到期时间验证。运行手册解码并从 SAML 响应中提取关键的 SAML 元素，包括发布者、断言、主题、条件、签名和属性。对于使用 SAML 通过 IAM 身份提供商访问 AWS 资源（例如 Connect Customer 或 Amazon WorkSpaces 应用程序）的环境，它会验证 SAML 响应签名中的证书是否与 IAM 身份提供商中配置的证书匹配。

如何工作？

运行手册执行以下步骤：

- 验证 SAML 响应格式和必填元素。
- 解码并提取 SAML 响应组件（发布者、断言、主题、条件、签名、属性）。
- 根据 IAM 身份提供商证书（如果提供）验证数字签名。
- 检查受众限制和时间有效性。
- 提供详细的诊断信息，显示已解析的 SAML 结构和验证结果。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- **s3:GetBucketLocation**
- **s3:ListBucket**
- **s3:GetBucketPublicAccessBlock**
- **s3:GetAccountPublicAccessBlock**
- **s3:GetObject**

- s3:GetBucketPolicyStatus
- s3:GetEncryptionConfiguration
- s3:GetBucketOwnershipControls
- s3:GetBucketAcl
- s3:GetBucketPolicy
- s3:PutObject
- iam:GetSAMLProvider
- sts:AssumeRole

策略示例：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "iam:GetSAMLProvider",
        "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. 在使用本运行手册之前，您需要捕获 Base64-encoded SAML 响应 (txt 文件) 并将其存储在 S3 存储桶中。可以在[本文档](#)中找到捕获 SAML 响应的说明
2. [AWSsupport-TroubleshootSAMLIssues](#)在 Systems Manager 的“文档”下导航至。
3. 选择 Execute automation (执行自动化)。
4. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：
 - 描述：(可选) 允许 SSM Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - InputFileS3URI (必填)：
 - 描述：(必填) 亚马逊简单存储服务 (Amazon S3) SAML Response txt 文件的 URI (例如 s3://bucket name/path-to/file /.txt)。
 - 类型：字符串
 - 允许模式：`^s3://[a-z0-9][a-z0-9.-][a-z0-9](/.)?/$`
 - S3OutputPrefix (可选)：
 - <executionID of the runbook>描述：(可选) 分析输出文件以“saml_analysis_ .json”的名义存储在输入存储桶中。如果要输出带有特定前缀的文件，则可以使用此参数。<executionID of the runbook>默认值为“output”，在这种情况下，输出结果的文件 URI 将为 's3://bucket-name/output /saml_analysis_ .json'。
 - 类型：字符串
 - 允许模式：`^[a-zA-Z0-9+ = , . @ \ - _ / ] * / $`
 - ExpectedAudience (可选)：
 - 描述：(可选) SAML 响应中的预期受众价值。如果未指定，则使用urn:amazon:webservices。如果您在 IdP 和 SP 设置中配置了特定的受众群体值，请提供确切的格式 (例如urn:amazon:webservices , https://signin.aws.amazon.com/saml)。

- 类型：字符串
- 默认：urn：亚马逊：网络服务
- IamIdProviderArn（可选）：
 - 描述：（可选）如果您使用 IAM ID 提供商实体将您的 IdP 与 AWS IAM 直接关联，请提供其 ARN（例如）。arn:aws:iam::<account-id>:saml-provider/<provider-name>
 - 类型：字符串
 - 允许模式：`^$|^arn:aws:iam::[0-9]{12}:saml-provider/[a-zA-Z0-9_-]+$`
- SAMLAuthenticationTime（可选）：
 - 描述：（可选）执行 SAML 身份验证的日期和时间。时区必须为 UTC。必须 YYYY-MM-DDThh:mm:ss 采用格式（例如，2025-02-01T10:00:00）。如果未提供此参数，则将根据当前时间戳执行过期检查。
 - 类型：字符串
 - 允许模式：`^$|^\\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[12]\\d|3[01])T(?:[01]\\d|2[0-3]):[0-5]\\d:[0-5]\\d$`
- S3BucketOwnerRoleArn（可选）：
 - 描述：（可选）用于访问 Amazon S3 存储桶的 IAM 角色 ARN。有权获取 Amazon S3 存储桶和账户封禁公开访问设置、存储桶加密配置、存储桶 ACL、存储桶策略状态以及向存储桶上传对象的 IAM 角色的 ARN。如果未指定此参数，则运行手册将使用 `AutomationAssumeRole`（如果已指定）或启动此运行手册的用户（如果未指定 `AutomationAssumeRole`）。
 - 类型：AWS::IAM::Role::Arn

5. 选择执行。

6. 自动化启动。

7. 文档将执行以下步骤：

- 验证 iamIdProvider

通过检查提供的 IAM ID 提供商 ARN 是否存在且可访问来验证该提供商 ARN。如果未提供 ARN，则会跳过验证并成功完成该步骤。

- CheckS3BucketPublicStatus

检查 Amazon S3 存储桶是否允许匿名或公开读取或写入权限。如果存储桶允许这些权限，则自动化将在此步骤停止。

- CheckS3ObjectExistence

验证对 Amazon S3 存储桶的访问权限。检查存储桶和对象是否存在，以及自动化是否具有从源读取和写入目标的必要权限。

- 分析 SAML 响应

通过执行检查（架构验证、签名验证、受众验证、到期检查）来分析 SAML 响应文件。生成详细的 JSON 报告并将其保存到指定的 Amazon S3 位置。

8. 完成后，请查看“输出”部分，了解执行的详细结果：

- 输出部分包含有关描述分析结果的 Amazon S3 对象的信息。

9. 分析结果中的 Amazon S3 对象是一个 Json 文件，其中包含以下信息：

- 验证结果：包含 SAML 响应的基本验证结果。
 - saml_info：关键的 SAML 信息，包括颁发者、签名和断言。
 - 架构验证：SAML 架构验证的结果。
- verification_result：提供更详细的诊断结果。
 - 签名：签名验证的结果。
 - 受众：受众限制验证的结果。
 - 过期：到期时间验证的结果。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflow 登录页面](#)

事件检测和响应

AWS Systems Manager 自动化为 AWS 事件检测和响应提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSPremiumSupport-OnboardWorkloadToIDR](#)

AWSPremiumSupport-OnboardWorkloadToIDR

描述

该AWSPremiumSupport-OnboardWorkloadToIDR运行手册可帮助 E AWS nterprise Support 客户使用事件检测和响应管理工作负载，进行监控和重大 AWS 事件管理。工作负载可以定义为与 AWS 资源组或 S AWS ervice Catalog AppRegistry 应用程序关联的 AWS 资源集合。如果未指定 AWS 资源组或 S AWS ervice Catalog AppRegistry 应用程序，则运行手册将使用标签筛选器或要将其资源包含在组中的 AWS CloudFormation 堆栈 ID 代表您创建一个资源组。如果您将参数设置为Yes，则自动使用CreateApplicationInsights预配置 Amazon Application Insights CloudWatch 应用程序 AWS CloudFormation。 CloudWatch Application Insights 使用 Amazon CloudWatch 指标、日志和事件为选定的应用程序资源设置推荐的指标和日志，以通知检测到的问题。

Important

此运行手册根据提供的输入参数在您的账户中执行以下操作：

- 使用 AWS CloudFormation 是否指定ResourceGroupName或AppRegistryApplication未指定来创建新的 AWS 资源组。创建堆栈后，运行手册会尝试设置终止保护。
- 标记与工作负载相关的 AWS 资源组，包括aws_idr标签。
- 如果CreateApplicationInsights输入参数设置为，则创建基于 Amazon A CloudWatch pplication Insights 资源组的Yes应用程序。创建堆栈后，运行手册会尝试为堆栈设置终止保护。
- 如果将InstallServiceLinkedRole输入参数设置为，则安装AWSServiceRoleForHealth_EventProcessor服务相关角色 (SLR)，以配置对事件检测和响应的警报摄取的访问权限。Yes
- 使用“AWS 事件检测和响应”创建 AWS 支持案例。

Important

要使用本运行手册并加入 AWS 事件检测和响应，您需要订阅 E AWS nterprise Support (需额外付费) 或统一运营订阅。有关更多信息，请参阅[比较 支持 计划](#)。

如何工作？

运行手册执行以下高级步骤：

- 检查当前的 Account AWS Support 计划是否为企业版；否则自动化将结束。
- 根据提供的参数确定是使用现有 AWS 资源组还是创建新资源组。
- 如果创建新的资源组，则生成 AWS CloudFormation 模板并使用相应标签创建堆栈。
- 使用所需 AWS 的事件检测和响应标签标记资源组。
- （可选）为 AWS 事件检测和响应安装服务相关角色。
- （可选）创建 Amazon CloudWatch 应用程序见解应用程序以增强监控。
- 创建 AWS 支持案例以完成入职流程。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateTerminationProtection`
- `iam:CreateServiceLinkedRole`
- `resource-groups:CreateGroup`
- `resource-groups:GetGroup`
- `resource-groups:TagResource`
- `servicecatalog-appregistry:GetApplication`

- support:CreateCase
- support:DescribeSeverityLevels
- support:DescribeServices
- support:DescribeSupportLevel

策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "iam:CreateServiceLinkedRole",
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:TagResource",
        "servicecatalog-appregistry:GetApplication",
        "support:CreateCase",
        "support:DescribeSeverityLevels",
        "support:DescribeServices",
        "support:DescribeSupportLevel"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSPremiumSupport-OnboardWorkloadToIDR](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

- 描述：(可选) AWS 身份和访问管理 (IAM) Access Management 角色的亚马逊资源名称 (ARN)，允许系统管理员自动化代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- 类型：AWS::IAM::Role::Arn
- WorkloadName (必填) :
 - 描述：(必填) 工作负载的名称。如果ResourceGroupName未提供，则使用工作负载名称来设置名称为的新 AWS 资源组IDR-AWS-<WorkloadName>。
 - 类型：String
 - 允许模式：^[a-zA-Z0-9_-]{1,128}\$
- WorkloadDescription (必填) :
 - 描述：(必填) 工作负载描述。输入简短描述以详细说明此工作负载的用例。请包括主要最终用户和该工作负载的功能。
 - 类型：String
 - 允许模式：^[a-zA-Z0-9.:;,-_&()]{1,1024}\$
- AppRegistryApplication (可选) :
 - 描述：(可选) S AWS service Catalog AppRegistry 应用程序的名称或 ID。如果未提供，则必须为提供输入ResourceGroupName。
 - 类型：String
 - 允许模式：^\$|^[a-zA-Z0-9.-_]{1,128}\$
 - 默认值：""
- ResourceGroupName (可选) :
 - 描述：(可选) 现有 AWS 资源组的名称 (如果AppRegistryApplication未提供)。如果要创建资源组，则必须为新资源组提供输入TagFilters，也可以选择ResourceTypeFilters创建新的 AWS 资源组。
 - 类型：String
 - 允许模式：^\$|^[a-zA-Z0-9_-]{1,128}\$
 - 默认值：""
- TagFilters (视情况而定) :
 - 描述：(视情况而定) 与附加到资源的标签进行比较的 key/values (字符串/字符串列表) 对列表 AWS。如果您未指定现有 AWS 资源组ResourceGroupName或，则此参数用于创建新的资源组AppRegistryApplication。
 - 类型：StringMap

- ResourceTypeFilters (视情况而定) :
 - 描述 : (视情况而定) Resource Groups 支持的资源类型列表。
 - 类型 : StringList
 - 最大物品数:10
 - 默认值 : AWS::AllSupported
- InstallServiceLinkedRole (可选) :
 - 描述 : (可选) 选择Yes安装AWSServiceRoleForHealth_EventProcessor服务相关角色 (SLR)。
 - 类型 : String
 - 允许的值 : [Yes,No]
 - 默认值 : No
- CreateApplicationInsights (可选) :
 - 描述 : (可选) 选择Yes创建基于 Amazon A CloudWatch pplication Insights 资源组的应用程序。
 - 类型 : String
 - 允许的值 : [Yes,No]
 - 默认值 : No
- ComplianceAndRegulatoryRequirements (必填) :
 - 描述 : (必填) 适用于此工作负载的合规性 and/or 法规要求以及事件发生 AWS 后需要采取的任何行动。
 - 类型 : String
 - 允许模式 : `^[a-zA-Z0-9.:\,\_\-\&()] {1,1024}$`
- 非AWSComponents (可选) :
 - 描述 : (可选) 详细说明此工作负载的任何本地或非AWS 组件? 如果是, 它们是什么, 它们执行什么功能。
 - 类型 : String
 - 允许模式 : `^$|^ [a-zA-Z0-9.:\,\_\-\&()] {1,1024}$`
 - 默认值 : ""
- UpstreamDownstreamDependencies (可选) :
 - 描述 : (可选) 未装载的任何 upstream/downstream 组件的详细信息, 如果出现中断, 这些组件可能会影响此工作负载。

- 类型 : String
 - 允许模式 : `^$|^[a-zA-Z0-9.:\,\-\_&()] {1,1024}$`
 - 默认值 : ""
 - FailoverDisasterRecoveryPlan (可选) :
 - 描述 : (可选) 提供可用区和区域级别的所有手动或自动 failover/disaster 恢复计划的详细信息。
 - 类型 : String
 - 允许模式 : `^$|^[a-zA-Z0-9.:\,\-\_&()] {1,1024}$`
 - 默认值 : ""
 - BridgeDetails (可选) :
 - 描述 : (可选) 贵公司建立的静态 incident/crisis 管理桥梁。如果您使用非静态网桥，请指定您的首选应用程序，并 AWS 将在事件发生期间请求这些详细信息。
 - 类型 : String
 - 允许的值 : [Amazon Chime bridge, Non-Static bridge, Static bridge]
 - 默认值 : Amazon Chime bridge
 - SubscriptionStartDate (必填) :
 - 描述 : (必填) 您要开始订阅“AWS 事件检测和响应”的日期，YYYY-MM-DD格式为。
 - 类型 : String
 - 允许模式 : `^(202[4-9]|20[3-9][0-9])-(0[1-9]|1[0-2])-(0[1-9]|12)[0-9]|3[01])$`
4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
- 查看AWSSupport套餐：

检查当前的 Account AWS t Support 计划是否为企业版；否则自动化将结束。
 - BranchOnResourceGroup:

根据是否提供了现有 AWS 资源组来分支自动化。如果未提供，则自动化会创建一个新的 AWS 资源组。
 - GetAppRegistryApplication:

- `GenerateResourceGroupTemplate`:

使用指定的标签过滤器为 AWS 资源组生成 AWS CloudFormation 模板。

- `CreateResourceGroup`:

使用创建新的 AWS 资源组 AWS CloudFormation。

- `TagResourceGroup`:

使用 AWS 事件检测和响应 (IDR) 所需的标签标记资源组。

- `InstallServiceLinkedRole`:

如果需要，安装 AWS 事件检测和响应 (IDR) 服务相关角色。

- `CreateApplicationInsightsApplication`:

根据要求创建 Amazon CloudWatch 应用程序见解应用程序。

- `CreateAwsSupportCase`:

使用“AWS 事件检测和响应”创建 AWS 支持案例。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)
- [开始使用 AWS 事件检测和响应](#)
- [事件检测和响应中的工作负载发现](#)

Amazon Kinesis Data Streams

AWS Systems Manager Automation 为 Amazon Kinesis Data Streams 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableKinesisStreamEncryption](#)

AWS-EnableKinesisStreamEncryption

描述

该AWS-EnableKinesisStreamEncryption运行手册支持对亚马逊 Kinesis Data Streams (Kinesis Data Streams) 进行加密。写入加密流的生产者应用程序如果无权访问 AWS Key Management Service (AWS KMS) 密钥，则会遇到错误。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- KinesisStreamName

类型：字符串

描述：(必填) 要启用加密的直播的名称。

- KeyId

类型：字符串

默认：alias/aws/kinesis

描述：（必填）您要用于加密的客户管理的密 AWS KMS 钥。此值可以是全局唯一标识符、别名或密钥的 ARN，也可以是以“alias/”为前缀的别名。您可以通过使用参数的默认值来使用 AWS 托管密钥。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- kinesis:DescribeStream
- kinesis:StartStreamEncryption
- kms:DescribeKey

文档步骤

- VerifyKinesisStreamStatus (aws:waitForAwsResourceProperty)-检查 Kinesis Data Streams 的状态。
- EnableKinesisStreamEncryption (aws:executeAwsApi)-为 Kinesis Data Streams 启用加密。
- VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty)-等待 Kinesis Data Streams 状态恢复为。ACTIVE
- VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty)-验证是否已为 Kinesis Data Streams 启用加密。

AWS KMS

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Key Management Service 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

AWSConfigRemediation-CancelKeyDeletion

描述

AWSConfigRemediation-CancelKeyDeletion运行手册取消删除您指定的 AWS Key Management Service (AWS KMS) 客户托管密钥。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- KeyId

类型：字符串

描述：(必需) 要为其取消删除的客户托管密钥的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion

- kms:DescribeKey

文档步骤

- aws:executeAwsApi - 取消删除您在 KeyId 参数中指定的客户托管密钥。
- aws:assertAwsResourceProperty - 确认客户托管密钥已被禁用。

AWSConfigRemediation-EnableKeyRotation

描述

该AWSConfigRemediation-EnableKeyRotation运行手册支持对 symmetric AWS Key Management Service (AWS KMS) 客户托管密钥进行自动密钥轮换。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- KeyId

类型：字符串

描述：(必需) 要对其启用自动密钥轮换的客户托管密钥的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

文档步骤

- `aws:executeAwsApi` - 对您在 KeyId 参数中指定的客户托管密钥启用自动密钥轮换。
- `aws:assertAwsResourceProperty` - 确认对客户托管密钥启用了自动密钥轮换。

Lambda

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Lambda 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

描述

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing 运行手册允许对您在 FunctionName 参数中指定的 AWS Lambda 函数进行 AWS X-Ray 实时跟踪。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- FunctionName

类型：字符串

描述：(必需) 要对其启用跟踪的 Lambda 函数的名称或 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

文档步骤

- `aws:executeAwsApi`-启用对您在参数中指定的 Lambda 函数的 X-Ray FunctionName 跟踪。
- `aws:assertAwsResourceProperty`-验证是否已在 Lambda 函数上启用 X-Ray 跟踪。

输出

UpdateLambdaConfig.UpdateFunctionConfigurationResponse -来自
UpdateFunctionConfiguration API 调用的响应。

AWSConfigRemediation-DeleteLambdaFunction

描述

AWSConfigRemediation-DeleteLambdaFunction运行手册将删除您指定的 AWS Lambda 函数。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- LambdaFunctionName

类型：字符串

描述：(必需) 要删除的 Lambda 函数的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

文档步骤

- `aws:executeAwsApi` - 删除在 `LambdaFunctionName` 参数中指定的 Lambda 函数。
- `aws:executeScript` - 验证 Lambda 函数是否已被删除。

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

描述

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK运行手册对您使用() 客户托管密钥指定的 AWS Key Management Service (AWS Lambda AWS KMS Lambda) 函数的环境变量进行静态加密。此运行手册应仅用作基准，以确保根据建议的最低安全性最佳实践对 Lambda 函数的环境变量进行加密。我们建议使用不同的客户托管密钥对多个函数进行加密。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- FunctionName

类型：字符串

描述：(必需) 要加密其环境变量的 Lambda 函数的名称或 ARN。

- KMSKeyArn

类型：字符串

描述：(必填) 您要用于加密 Lambda 函数环境变量的 AWS KMS 客户托管密钥的 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文档步骤

- aws:waitForAwsResourceProperty - 等待 LastUpdateStatus 属性变为 Successful。
- aws:executeAwsApi-使用您在参数中指定的客户托管密钥加密您在参数中FunctionName指定的 Lambda 函数 AWS KMS 的环境变量。KMSKeyArn
- aws:assertAwsResourceProperty - 确认对 Lambda 函数的环境变量启用了加密。

AWSConfigRemediation-MoveLambdaToVPC

描述

AWSConfigRemediation-MoveLambdaToVPC 运行手册将 AWS Lambda (Lambda) 函数移至 Amazon Virtual Private Cloud (Amazon VPC)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- FunctionName

类型：字符串

描述：(必需) 要移至 Amazon VPC 的 Lambda 函数的名称。

- SecurityGroupIds

类型：字符串

描述：(必需) 要分配给与 Lambda 函数关联的弹性网络接口 (ENI) 的安全组 ID。

- SubnetIds

类型：字符串

描述：(必需) 要创建与 Lambda 函数关联的弹性网络接口 (ENI) 的子网 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

文档步骤

- `aws:executeAwsApi` - 更新您在 `FunctionName` 参数中指定的 Lambda 函数的 Amazon VPC 配置。
- `aws:waitForAwsResourceProperty` - 等待 Lambda 函数 `LastUpdateStatus` 生成 `successful`。
- `aws:executeScript` - 验证 Lambda 函数 Amazon VPC 配置是否已成功更新。

AWSSupport-RemediateLambdaS3Event

描述

该AWSSupport-TroubleshootLambdaS3Event运行手册为 AWS 知识中心文章中概述的程序提供了自动解决方案[为什么我的 Amazon S3 事件通知没有触发我的 Lambda 函数？](#) 以及[为什么在创建 Amazon S3 事件通知以触发我的 Lambda 函数时会出现“无法验证以下目标配置”错误？](#) 本运行手册可帮助您识别和修复亚马逊简单存储服务 (Amazon S3) Simple Service 事件通知未能触发您指定的功能的原因。AWS Lambda 如果运行手册的输出建议验证和配置 Lambda 函数并发性，请参阅[异步调用](#)和[AWS Lambda 函数扩展](#)。

Note

由于 Amazon Simple Notification Service (Amazon SNS) 和 Amazon Simple Queue Service (Amazon SQS) Amazon S3 事件配置不正确，因此也可能出现“无法验证以下目标配置”错误。此运行手册仅检查 Lambda 函数配置。如果在使用运行手册后仍然收到“无法验证以下目标配置”错误，请查看所有现有的 Amazon SNS 和 Amazon SQS Amazon S3 事件配置。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaFunctionArn

类型：字符串

描述：(必需) Lambda 函数的 ARN。

- S3BucketName

类型：字符串

描述：(必需) 其事件通知会触发 Lambda 函数的 Amazon S3 存储桶的名称。

- 处理建议

类型：字符串

有效值：故障排除 | 纠正

描述：(必需) 要运行手册执行的操作。Troubleshoot 选项可帮助识别任何问题，但不会执行任何变更操作来解决问题。Remediate 选项有助于识别并尝试解决问题。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetDocument

- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

文档步骤

- `aws:branch`- 根据为 `Action` 参数指定的输入进行分支。

如果指定的值为 `Troubleshoot` :

- `aws:executeAutomation` - 运行 `AWSSupport-TroubleshootLambdaS3Event` 运行手册。
- `aws:executeAwsApi` - 检查在上一步运行的 `AWSSupport-TroubleshootLambdaS3Event` 运行手册的输出。

如果指定的值为 `Remediate` :

- `aws:executeScript` - 运行脚本来纠正[为什么我的 Amazon S3 事件通知没有触发 Lambda 函数？](#)以及[为什么我在创建 Amazon S3 事件通知以触发 Lambda 函数时会出现“无法验证以下目标配置”错误？](#)中概述的问题。知识中心文章。

输出

`checkoutput.Output`

`remediatelambdas3event.Output`

AWSSupport-TroubleshootLambdaInternetAccess

描述

该`AWSSupport-TroubleshootLambdaInternetAccess`运行手册可帮助您解决在亚马逊虚拟私有云 (Amazon VPC) 中启动的 AWS Lambda 功能的互联网访问问题。对子网路由、安全组规则和网络访问控制列表 (ACL) 规则等资源进行审查，以确认允许出站互联网访问。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- FunctionName

类型：字符串

描述：(必需) 要为其排除互联网访问问题的 Lambda 函数的名称。

- destinationIp

类型：字符串

描述：(必需) 要与之建立出站连接的目标 IP 地址。

- destinationPort

类型：字符串

默认值：443

描述：(可选) 要在其上建立出站连接的目标端口。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

文档步骤

- `aws:executeScript` - 验证启动 Lambda 函数的 VPC 中各种资源的配置。
- `aws:branch` - 根据指定的 Lambda 函数是否在 VPC 中进行分支。
- `aws:executeScript` - 查看其中启动 Lambda 函数的子网的路由表路由，并验证是否存在到网络地址转换 (NAT) 网关和互联网网关的路由。确认 Lambda 函数不在公有子网中。
- `aws:executeScript` - 根据为 `destinationIp` 和 `destinationPort` 参数指定的值，验证与 Lambda 函数关联的安全组是否允许出站互联网访问。
- `aws:executeScript` - 根据为 `destinationIp` 和 `destinationPort` 参数指定的值，验证与 Lambda 函数子网关联的 ACL 规则和 NAT 网关是否允许出站互联网访问。

输出

`check Vpc.vpc` - 启动您的 Lambda 函数的 VPC 的 ID。

`check Vpc.subnet` - 启动您的 Lambda 函数的子网的 ID。

`check Vpc.securityGroups` - 与 Lambda 函数关联的安全组。

`check NACL.NACL` - 带有资源名称的分析消息。 `LambdaIp` 指您的 Lambda 函数的弹性网络接口的私有 IP 地址。 `LambdaIpRules` 对象仅对具有通往 NAT 网关的路由的子网生成。以下内容为输出示例。

```
{
  "subnet-1234567890":{
    "NACL":"acl-1234567890",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule",
    "LambdaIpRules":{
      "{LambdaIp}":{
```



```

        "Egress":"notAllowed",
        "Ingress":"notAllowed",
        "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
IP in your egress and ingress NACL rules"
    }
}
},
"subnet-0987654321":{
    "NACL":"acl-0987654321",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule"
}
}

```

check SecurityGroups.secgrps -分析与您的 Lambda 函数关联的安全组。以下内容为例输出。

```

{
  "sg-123456789":{
    "Status":"Allowed",
    "Analysis":"This security group has allowed destintion IP and port in its
outbuond rule."
  }
}

```

check Subnet.subnets -分析您的 VPC 中与您的 Lambda 函数关联的子网。以下内容为例输出。

```

{
  "subnet-0c4ee6cdexample15":{
    "Route":{
      "DestinationCidrBlock":"8.8.8.0/26",
      "NatGatewayId":"nat-00f0example69fdec",
      "Origin":"CreateRoute",
      "State":"active"
    },
    "Analysis":"This Route Table has an active NAT gateway path. Also, The NAT
gateway is launched in public subnet",
    "RouteTable":"rtb-0b1fexample16961b"
  }
}

```

AWSSupport-TroubleshootLambdaS3Event

描述

该AWSSupport-TroubleshootLambdaS3Event运行手册为 AWS 知识中心文章中概述的程序提供了自动解决方案[为什么我的 Amazon S3 事件通知没有触发我的 Lambda 函数？](#) 以及[为什么在创建 Amazon S3 事件通知以触发我的 Lambda 函数时会出现“无法验证以下目标配置”错误？](#) 本运行手册可帮助您确定亚马逊简单存储服务 (Amazon S3) Simple Service 事件通知未能触发 AWS Lambda 您指定的功能的原因。如果运行手册的输出建议验证和配置 Lambda 函数并发性，请参阅[异步调用](#)和[AWS Lambda 函数扩展](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LambdaFunctionArn

类型：字符串

描述：(必需) Amazon S3 事件通知触发的 Lambda 函数的 ARN。

- S3BucketName

类型：字符串

描述：(必需) 其事件通知会触发 Lambda 函数的 Amazon S3 存储桶的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

文档步骤

- `aws:executeScript` - 运行脚本以验证 Amazon S3 事件通知的配置设置。验证您的 Lambda 函数的基于资源的 IAM 策略，并在策略中缺少所需权限时生成 AWS Command Line Interface (AWS CLI) 命令以添加所需的权限。验证其他 Lambda 函数资源策略，这些策略是同一 S3 存储桶的事件通知的一部分，如果缺少所需权限，则生成命令 AWS CLI 作为输出。

输出

lambda S3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager Automation 为适用于 Apache Airflow 的亚马逊托管工作流程提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSsupport-TroubleshootMWAAEnvironmentCreation](#)

AWSsupport-TroubleshootMWAAEnvironmentCreation

描述

该AWSsupport-TroubleshootMWAAEnvironmentCreation运行手册提供了调试适用于 Apache Airflow 的亚马逊托管工作流程 (Amazon MWAA) 环境创建问题的信息，并尽最大努力执行检查和记录在案的原因，以帮助识别故障。

如何工作？

运行手册执行以下步骤：

- 检索 Amazon MWAA 环境的详细信息。
- 验证执行角色权限。
- 检查环境是否有权使用提供的 AWS KMS 密钥进行日志记录，以及所需的 CloudWatch 日志组是否存在。
- 解析提供的日志组中的日志以查找任何错误。
- 检查网络配置以验证 Amazon MWAA 环境是否可以访问所需的终端节点。
- 生成包含调查结果的报告。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- airflow:GetEnvironment
- cloudtrail:LookupEvents
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups

- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRolePolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListRolePolicies`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`
- `kms:ListAliases`
- `logs:DescribeLogGroups`
- `logs:FilterLogEvents`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3control:GetPublicAccessBlock`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

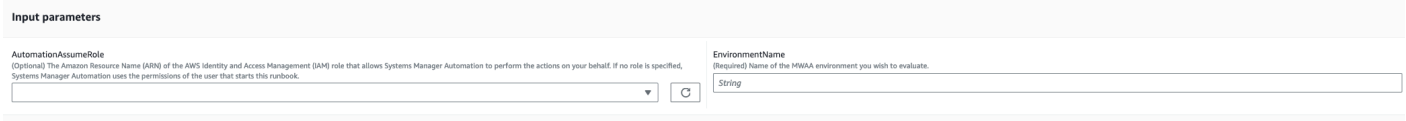
说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)在 Systems Manager 的“文档”下导航至。
2. 选择 `Execute automation` (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - `AutomationAssumeRole` (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - `EnvironmentName` (必填)：

您要评估的 Amazon MWAA 环境的名称。



Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

EnvironmentName
(Required) Name of the MWAA environment you wish to evaluate.

String

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **GetMWAAEnvironmentDetails:**

检索 Amazon MWAA 环境的详细信息。如果此步骤失败，自动化过程将停止并显示为Failed。

- **CheckIAMPermissionsOnExecutionRole:**

验证执行角色是否具有使用 Amazon MWAA、Amazon S3 CloudWatch、CloudWatch 日志和亚马逊 SQS 资源所需的权限。如果它检测到客户托管 AWS Key Management Service (AWS KMS) 密钥，则自动化会验证该密钥的所需权限。此步骤使用 iam:SimulateCustomPolicy API 来确定自动化执行角色是否满足所有必需的权限。

- **CheckKMSPolicyOnKMSKey:**

检查 AWS KMS 密钥策略是否允许 Amazon MWAA 环境使用该密钥加密 CloudWatch 日志。如果 AWS KMS 密钥是 AWS-managed，则自动化会跳过此检查。

- **CheckIfRequiredLogGroupsExists:**

检查 Amazon MWAA 环境所需的 CloudWatch 日志组是否存在。如果不是，则自动化会 CloudTrail 检查CreateLogGroup和DeleteLogGroup事件。此步骤还会检查CreateLogGroup事件。

- **BranchOnLogGroupsFindings:**

基于是否存在与 Amazon MWAA 环境相关的 CloudWatch 日志组进行分支。如果至少存在一个日志组，则自动化会对其进行解析以查找错误。如果不存在任何日志组，则自动化会跳过下一步。

- **CheckForErrorsInLogGroups:**

解析 CloudWatch 日志组以查找错误。

- **GetRequiredEndpointsDetails:**

检索 Amazon MWAA 环境使用的服务终端节点。

- **CheckNetworkConfiguration:**

验证 Amazon MWAA 环境的网络配置是否符合要求，包括检查安全组、网络 ACL、子网和路由表配置。

- **CheckEndpointsConnectivity:**

调用AWSsupport-ConnectivityTroubleshooter子级自动化来验证 Amazon MWAA 与所需终端节点的连接。

- **CheckS3BlockPublicAccess:**

检查亚马逊 MWAA 环境的 Amazon S3 存储桶是否已Block Public Access启用，并查看该账户的整体 Amazon S3 阻止公共访问设置。

- **GenerateReport:**

从自动化中收集信息并打印每个步骤的结果或输出。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- 正在检查 Amazon MWAA 环境执行角色权限：

验证执行角色是否具有 Amazon MWAA、Amazon S3 CloudWatch、CloudWatch 日志和 Amazon SQS 资源所需的权限。如果检测到客户管理的 AWS KMS 密钥，则自动化将验证该密钥的所需权限。

- 查看 Amazon MWAA 环境 AWS KMS 密钥策略：

验证执行角色是否拥有使用 Amazon MWAA、Amazon S3、CloudWatch CloudWatch日志和 Amazon SQS 资源的必要权限。此外，如果检测到客户管理的 AWS KMS 密钥，自动化系统会检查该密钥的所需权限。

- 检查 Amazon MWAA 环境 CloudWatch 日志组：

检查 Amazon MWAA 环境所需的 CloudWatch 日志组是否存在。如果没有，则自动化系统会检查 CloudTrail 定位CreateLogGroup和DeleteLogGroup事件。

- 检查 Amazon MWAA 环境路由表：

检查 Amazon MWAA 环境中的 Amazon VPC 路由表配置是否正确。

- 检查 Amazon MWAA 环境安全组：

检查 Amazon MWAA 环境 Amazon VPC 安全组的配置是否正确。

- 检查 Amazon MWAA 环境网络 ACL：

检查 Amazon MWAA 环境中的 Amazon VPC 安全组是否配置正确。

- 检查 Amazon MWAA 环境子网：

验证 Amazon MWAA 环境的子网是否为私有子网。

- 检查 Amazon MWAA 环境所需的终端节点连接：

验证 Amazon MWAA 环境是否可以访问所需的终端节点。为此，自动化会调用自动化。AWSsupport-ConnectivityTroubleshooter

- 检查亚马逊 MWAA 环境亚马逊 S3 存储桶：

检查亚马逊 MWAA 环境的 Amazon S3 存储桶是否已Block Public Access启用，并查看该账户的 Amazon S3 阻止公共访问设置。

- 检查 Amazon MWAA 环境 CloudWatch 日志组错误：

解析 Amazon MWAA 环境的现有 CloudWatch 日志组以查找错误。

▼ Outputs

GenerateReportAutomationReport

Troubleshooting report for MWAA environment

🔗

The automation found no issues with the MWAA environment configuration ✓

🔗

Checking the MWAA environment execution role permissions

All the required permissions for the MWAA environment execution role are in place ✓

🔗

Checking the MWAA environment KMS key policy

KMS key is an AWS managed key ✓

🔗

Checking the MWAA environment CloudWatch logs groups

The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment is 5. This suggests that all log groups were created successfully ✓

🔗

Checking the MWAA environment Route Tables

NAT GW has Internet route: subnet- nat- igw- ✓

NAT GW has Internet route: subnet- nat- igw- ✓

🔗

Checking the MWAA environment Security Groups

Security group has self-referencing rules for all traffic. ✓

🔗

Checking the MWAA environment Network ACLs

NACL- allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔗

Checking the MWAA environment Subnets

Subnet: subnet- is private ✓

Subnet: subnet- is private ✓

🔗

Checking the MWAA environment required endpoints connectivity

✓

Testing connectivity with sqs.eu-west-1.amazonaws.com:

Connectivity test between ENI- and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with api.ecr.eu-west-1.amazonaws.com:

Connectivity test between ENI- and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with monitoring.eu-west-1.amazonaws.com:

Connectivity test between ENI- and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with kms.eu-west-1.amazonaws.com:

Connectivity test between ENI- and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with s3.eu-west-1.amazonaws.com:

Connectivity test between ENI- and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with api.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with logs.eu-west-1.amazonaws.com:

Connectivity test between ENI- and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓

Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

🔗

Checking the MWAA environment S3 bucket

Environment's S3 bucket and/or account block public access ✓

🔗

Checking the MWAA environment CloudWatch logs groups errors

Parsed log group- DAGProcessing - no errors found ✓

Parsed log group- Scheduler - no errors found ✓

Parsed log group- Task - no errors found ✓

Parsed log group- WebServer - no errors found ✓

Parsed log group- Worker - no errors found ✓

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

Neptune

AWS Systems Manager 自动化为 Amazon Neptune 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

AWS-EnableNeptuneDbAuditLogsToCloudWatch

描述

该AWS-EnableNeptuneDbAuditLogsToCloudWatch运行手册可帮助您将 Amazon Neptune 数据库集群的审计日志发送到 Amazon Logs。 CloudWatch

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DbClusterResourceId

类型：字符串

描述：(必填) 要为其启用审核日志的 Neptune 数据库集群的资源 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文档步骤

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`)-返回 Neptune 数据库集群的 ID。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`)-验证 Neptune 数据库引擎类型为。neptune
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`)-允许向 Neptune 数据库集群发送 CloudWatch 审计日志。
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`)-验证 Neptune 数据库集群的状态为。available
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`)-验证审核日志是否已成功配置为发送到 CloudWatch 日志。

AWS-EnableNeptuneDbBackupRetentionPeriod

描述

该AWS-EnableNeptuneDbBackupRetentionPeriod运行手册可帮助您为 Amazon Neptune 数据库集群启用自动备份，备份保留期在 7 到 35 天之间。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DbClusterResourceId

类型：字符串

描述：(必填) 要为其启用备份的 Neptune 数据库集群的资源 ID。

- BackupRetentionPeriod

类型：整数

有效值：7-35

描述：(必填) 备份的保留天数。

- PreferredBackupWindow

类型：字符串

描述：(可选) 每天进行备份的时间段至少为 30 分钟。该值必须采用协调世界时 (UTC)，并使用以下格式：hh24:mm-hh24:mm。备份保留期不能与首选维护时段发生冲突。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文档步骤

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`)-返回 Neptune 数据库集群的 ID。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`)-验证 Neptune 数据库引擎类型为。neptune
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`)-验证 Neptune 数据库集群的状态为。available
- `ModifyNeptuneDbRetentionPeriod` (`aws:executeAwsApi`)-设置 Neptune 数据库集群的保留期。
- `VerifyNeptuneDbBackupsEnabled` (`aws:executeScript`)-验证是否成功设置了保留期和备份窗口。

AWS-EnableNeptuneClusterDeletionProtection

描述

AWS-EnableNeptuneClusterDeletionProtection运行手册为您指定的 Amazon Neptune 集群启用删除保护。

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DbClusterResourceId

类型：字符串

描述：(必填) 要启用删除保护的 Neptune 集群的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi)-返回 Neptune 数据库集群的 ID。
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty)-验证指定数据库集群的引擎类型为neptune。
- VerifyNeptuneStatus (aws:waitForAwsResourceProperty)-验证群集的状态是否为available。
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi)-在 Neptune 数据库集群上启用删除保护。

- `VerifyNeptuneDbDeletionProtection (aws:assertAwsResourceProperty)`-验证数据库集群上是否启用了删除保护。

输出

- `EnableNeptuneDbDeletionProtection`。 `EnableNeptuneDbDeletionProtectionResponse` -API 操作的输出。

Amazon RDS

AWS Systems Manager 自动化为 Amazon Relational Database Service 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CreateEncryptedRdsSnapshot](#)
- [AWS-CreateRdsSnapshot](#)
- [AWSConfigRemediation-DeleteRDSCluster](#)
- [AWSConfigRemediation-DeleteRDSClusterSnapshot](#)
- [AWSConfigRemediation-DeleteRDSInstance](#)
- [AWSConfigRemediation-DeleteRDSInstanceSnapshot](#)
- [AWSConfigRemediation-DisablePublicAccessToRDSInstance](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance](#)
- [AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableMultiAZOnRDSInstance](#)
- [AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance](#)
- [AWSConfigRemediation-EnableRDSClusterDeletionProtection](#)
- [AWSConfigRemediation-EnableRDSInstanceBackup](#)
- [AWSConfigRemediation-EnableRDSInstanceDeletionProtection](#)
- [AWSConfigRemediation-ModifyRDSInstancePortNumber](#)
- [AWSSupport-ModifyRDSSnapshotPermission](#)

- [AWSPremiumSupport-PostgreSQLWorkloadReview](#)
- [AWS-RebootRdsInstance](#)
- [AWSSupport-ShareRDSSnapshot](#)
- [AWS-StartRdsInstance](#)
- [AWS-StartStopAuroraCluster](#)
- [AWS-StopRdsInstance](#)
- [AWSSupport-TroubleshootConnectivityToRDS](#)
- [AWSSupport-TroubleshootRDSIAMAuthentication](#)
- [AWSSupport-ValidateRdsNetworkConfiguration](#)

AWS-CreateEncryptedRdsSnapshot

描述

AWS-CreateEncryptedRdsSnapshot运行手册从未加密的亚马逊关系数据库服务 (Amazon RDS) 实例创建加密快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBInstanceIdentifier

类型：字符串

描述：(必填)您要为其创建快照的 Amazon RDS 实例的 ID。

- DBSnapshotIdentifier

类型：字符串

描述：(可选) Amazon RDS 快照的名称模板。默认名称模板是 *DBInstanceIdentifier-yyyymmddhhmmss*。

- EncryptedDBSnapshotIdentifier

类型：字符串

描述：(可选)加密快照的名称。默认名称是您为附加的 DBSnapshotIdentifier 参数指定的值。-encrypted

- InstanceTags

类型：字符串

描述：(可选)要添加到数据库实例的标签。(例如：key=tagKey1，value=tagValue1；key=tagKey2，value=tagValue2)'

- KmsKeyId

类型：字符串

默认：alias/aws/rds

描述：(可选)您要用于加密快照的客户托管密钥的 ARN、密钥 ID 或密钥别名。

- SnapshotTags

类型：字符串

描述：(可选)要添加到快照的标签。(例如：key=tagKey1，value=tagValue1；key=tagKey2，value=tagValue2)'

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds>CreateDBSnapshot`
- `rds>DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

文档步骤

- `aws:executeScript`-创建您在`DBInstanceIdentifier`参数中指定的数据库实例的快照。
- `aws:executeScript`-验证在上一步中创建的快照是否存在。 `available`
- `aws:executeScript`-将先前创建的快照复制到加密快照。
- `aws:executeScript`-验证上一步中创建的加密快照是否存在。

输出

`CopyRdsSnapshotToEncryptedRdsSnapshot.EncryptedSnapshotId` -加密的 Amazon RDS 快照的 ID。

AWS-CreateRdsSnapshot

描述

为 Amazon RDS 实例创建 Amazon Relational Database Service (Amazon RDS) 快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBInstanceIdentifier

类型：字符串

描述：(必填) 用于创建快照的 RDS 实例的 DBInstanceID ID。

- DBSnapshotIdentifier

类型：字符串

描述：(可选) 要创建的 RDS 快照的 DBSnapshotIdentifier ID。

- InstanceTags

类型：字符串

描述：(可选) 要为实例创建的标签。

- SnapshotTags

类型：字符串

描述：(可选) 要为快照创建的标签。

文档步骤

createRDSSnapshot – 创建 RDS 快照并返回快照 ID。

verifyRDSSnapshot – 检查在上一步中创建的快照是否存在。

输出

创建 RDSSnapshot.SnapshotId -创建的快照的 ID。

AWSConfigRemediation-DeleteRDSCluster

描述

AWSConfigRemediation-DeleteRDSCluster运行手册将删除您指定的亚马逊关系数据库服务 (Amazon RDS) 集群。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- DBClusterId

类型：字符串

描述：(必需) 要对其启用删除保护的数据库集群的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds>DeleteDBCluster
- rds>DeleteDBInstance
- rds:DescribeDBClusters

文档步骤

- `aws:executeScript` - 删除您在 `DBClusterId` 参数中指定的数据库集群。

AWSConfigRemediation-DeleteRDSClusterSnapshot

描述

AWSConfigRemediation-DeleteRDSClusterSnapshot 运行手册将删除给定的 Amazon Relational Database Service (Amazon RDS) 集群快照。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DBClusterSnapshotId

类型：字符串

描述：(必需) 要删除的 Amazon RDS 集群快照标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

文档步骤

- `aws:branch` - 检查集群快照是否处于 `available` 状态。如果它不可用，则流程结束。
- `aws:executeAwsApi` - 使用数据库 (DB) 集群快照标识符删除给定的 Amazon RDS 集群快照。
- `aws:executeScript` - 验证给定的 Amazon RDS 集群快照是否已删除。

AWSConfigRemediation-DeleteRDSInstance

描述

AWSConfigRemediation-DeleteRDSInstance运行手册将删除指定的Amazon Relational Database Service (Amazon RDS) 实例。删除数据库 (DB) 实例时，会删除该实例的所有自动备份，且无法恢复。手动数据库快照不会删除。如果要删除的数据库实例处于 `failed`、`incompatible-network` 或 `incompatible-restore` 状态，则必须将 `SkipFinalSnapshot` 参数设置为 `true`。

Note

如果要删除的数据库实例位于 Amazon Aurora 数据库集群中，若该数据库实例是只读副本并且是数据库集群中唯一的实例，则运行手册不会将其删除。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DbiResourceId

类型：字符串

描述：(必需) 要删除的数据库实例的资源标识符。

- SkipFinalSnapshot

类型：布尔值

默认值：false

描述：(可选) 如果设置为 true，则在删除数据库实例之前不会创建最终快照。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBInstance
- rds:DescribeDBInstances

文档步骤

- aws:executeAwsApi - 从您在 DbiResourceId 参数中指定的值收集数据库实例名称。
- aws:branch - 根据您在 SkipFinalSnapshot 参数中指定的值进行分支。
- aws:executeAwsApi - 删除您在 DbiResourceId 参数中指定的数据库实例。
- aws:executeAwsApi - 创建最终快照后，删除您在 DbiResourceId 参数中指定的数据库实例。
- aws:assertAwsResourceProperty - 验证数据库实例是否已删除。

AWSConfigRemediation-DeleteRDSInstanceSnapshot

描述

AWSConfigRemediation-DeleteRDSInstanceSnapshot 运行手册将删除指定的 Amazon Relational Database Service (Amazon RDS) 实例快照。只有处于 available 状态的快照才会被删除。此运行手册不支持从 Amazon Aurora 数据库实例中删除快照。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DbSnapshotId

类型：字符串

描述：(必需) 要删除的快照 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

文档步骤

- `aws:executeAwsApi` - 收集在 `DbSnapshotId` 参数中指定的快照的状态。
- `aws:assertAwsResourceProperty` - 确认快照的状态为 `available`。
- `aws:executeAwsApi` - 删除在 `DbSnapshotId` 参数中指定的快照。
- `aws:executeScript` - 验证快照是否已被删除。

AWSConfigRemediation-DisablePublicAccessToRDSInstance

描述

AWSConfigRemediation-DisablePublicAccessToRDSInstance 运行手册将禁用指定的 Amazon Relational Database Service (Amazon RDS) 数据库 (DB) 实例的公共访问权限。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `DbResourceId`

类型：字符串

描述：(必需) 要为其禁用公共访问权限的数据库实例的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文档步骤

- `aws:executeAwsApi` - 从数据库实例资源标识符收集数据库实例标识符。
- `aws:assertAwsResourceProperty` - 验证数据库实例是否处于 AVAILABLE 状态。
- `aws:executeAwsApi` - 禁用数据库实例的公开可访问性。
- `aws:waitForAwsResourceProperty` - 等待数据库实例变为 MODIFYING 状态。
- `aws:waitForAwsResourceProperty` - 等待数据库实例变为 AVAILABLE 状态。
- `aws:assertAwsResourceProperty` - 确认已对数据库实例禁用公开可访问性。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

描述

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster 运行手册将对指定的 Amazon Relational Database Service (Amazon RDS) 集群启用 CopyTagsToSnapshot 设置。启用此设置可将所有标签从数据库集群复制到数据库集群的快照。默认设置是不复制它们。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- `ApplyImmediately`

类型：布尔值

默认值：`false`

描述：(可选) 如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库集群的 `PreferredMaintenanceWindow` 设置如何。

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- `DbClusterResourceId`

类型：字符串

描述：(必需) 要对其启用 `CopyTagsToSnapshot` 设置的数据库集群的资源标识符。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`

- `rds:ModifyDBCluster`

文档步骤

- `aws:executeAwsApi` - 从数据库集群资源标识符收集数据库集群标识符。
- `aws:assertAwsResourceProperty` - 确认数据库集群处于 AVAILABLE 状态。
- `aws:executeAwsApi` - 对数据库集群启用 CopyTagsToSnapshot 设置。
- `aws:assertAwsResourceProperty` - 确认已对数据库集群启用 CopyTagsToSnapshot 设置。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

描述

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance 运行手册将对指定的 Amazon Relational Database Service (Amazon RDS) 实例启用 CopyTagsToSnapshot 设置。启用此设置可将所有标签从数据库实例复制到数据库实例快照。默认设置是不复制它们。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- `ApplyImmediately`

类型：布尔值

默认值：false

描述：(可选) 如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 `PreferredMaintenanceWindow` 设置如何。

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- `DbiResourceId`

类型：字符串

描述：(必需) 要对其启用 `CopyTagsToSnapshot` 设置的数据库实例的资源标识符。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文档步骤

- `aws:executeAwsApi` - 从数据库实例资源标识符收集数据库实例标识符。
- `aws:assertAwsResourceProperty` - 确认数据库实例处于 `AVAILABLE` 状态。
- `aws:executeAwsApi` - 对数据库实例启用 `CopyTagsToSnapshot` 设置。
- `aws:assertAwsResourceProperty` - 确认已对数据库实例启用 `CopyTagsToSnapshot` 设置。

AWSConfigRemediation- EnableEnhancedMonitoringOnRDSInstance

描述

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance运行手册对指定的 Amazon RDS 数据库实例启用增强监控。有关增强监控的信息，请参阅《Amazon RDS 用户指南》中的[增强监控](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- MonitoringInterval

类型：整数

有效值：1 | 5 | 10 | 15 | 30 | 60

描述：(必需) 从数据库实例收集增强监控指标时的间隔，以秒为单位。

- MonitoringRoleArn

类型：字符串

描述：(必填) 允许 Amazon RDS 向亚马逊日志发送增强型监控指标的 IAM 角色的亚马逊资源名称 (ARN)。 CloudWatch

- ResourceId

类型：字符串

描述：(必需) 要对其启用增强监控的数据库实例的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库实例启用增强监控。
- aws:executeScript - 确认已对数据库实例启用增强监控。

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance

描述

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS运行手册将对指定的 Amazon RDS 数据库实例启用 AutoMinorVersionUpgrade 设置。启用该设置表示在维护时段期间，将对该数据库实例自动应用次要版本升级。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DbiResourceId

类型：字符串

描述：(必需) 要对其进行 AutoMinorVersionUpgrade 设置的数据库实例的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库实例启用 AutoMinorVersionUpgrade 设置。
- aws:executeScript - 确认已对数据库实例启用 AutoMinorVersionUpgrade 设置。

AWSConfigRemediation-EnableMultiAZOnRDSInstance

描述

AWSConfigRemediation-EnableMultiAZOnRDSInstance运行手册将您的亚马逊关系数据库服务 (Amazon RDS) 数据库 (DB) 实例更改为 Multi-AZ 部署。更改此设置不会导致中断。更改在下一个维护时段内应用，除非您将 ApplyImmediately 参数设置为 true。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- ApplyImmediately

类型：布尔值

默认值：false

描述：(可选) 如果您为该参数指定 true，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 PreferredMaintenanceWindow 设置如何。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DbResourceId

类型：字符串

描述：(必填) 数据库实例的 AWS 区域唯一不可变标识符，用于启用该设置。MultiAZ

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- rds:DescribeDBInstances
- rds:ModifyDBInstance
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文档步骤

- aws:executeAwsApi - 使用 DBInstanceId 参数中提供的值检索数据库实例名称。
- aws:executeAwsApi - 验证 DBInstanceStatus 是否为 available。
- aws:branch - 检查您在 DbiResourceId 参数中指定的数据库实例上的 MultiAZ 是否已设置为 true。
- aws:executeAwsApi - 将您在 DbiResourceId 参数中指定的数据库实例上的 MultiAZ 设置更改为 true。
- aws:assertAwsResourceProperty - 验证您在 DbiResourceId 参数中指定的数据库实例上 MultiAZ 是否设置为 true。

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

描述

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance 运行手册将对您指定的 Amazon RDS 数据库实例上启用 Performance Insights。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- DbiResourceId

类型：字符串

描述：(必需) 要对其启用 Performance Insights 的数据库实例的资源标识符。

- PerformanceInsightsKMSKeyId

类型：字符串

默认：alias/aws/rds

描述：(可选) 您希望 Performance Insights 用于加密所有潜在敏感数据的亚马逊资源名称 AWS Key Management Service (ARN AWS KMS)、密钥 ID 或 () 客户托管密钥的密钥别名。如果输入此参数的密钥别名，则在值前面加上 **alias/**。如果您没有为此参数指定值，AWS 托管式密钥 则使用。

- PerformanceInsightsRetentionPeriod

类型：整数

有效值：7、731

默认：7

描述：(可选) 要保留 Performance Insights 数据的天数。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- kms:CreateGrant
- kms:DescribeKey
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例的状态为 available。
- aws:executeAwsApi-收集参数中指定的客户托管密钥 AWS KMS 的 ARN。PerformanceInsightsKMSKeyId
- aws:branch - 检查是否已为数据库实例的 PerformanceInsightsKMSKeyId 属性分配了一个值。
- aws:executeAwsApi - 对您在 DbiResourceId 参数中指定的数据库实例启用 Performance Insights。
- aws:assertAwsResourceProperty - 确认为 PerformanceInsightsKMSKeyId 参数指定的值已用于对数据库实例上的 Performance Insights 启用加密。
- aws:assertAwsResourceProperty - 确认已在数据库实例上启用 Performance Insights。

AWSConfigRemediation-EnableRDSClusterDeletionProtection

描述

该AWSConfigRemediation-EnableRDSClusterDeletionProtection运行手册在您指定的亚马逊关系数据库服务 (Amazon RDS) 集群上启用删除保护。AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- ClusterId

类型：字符串

描述：(必需) 要对其启用删除保护的数据库集群的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- aws:executeAwsApi - 从数据库集群资源标识符收集数据库集群名称。
- aws:assertAwsResourceProperty - 验证数据库集群的状态为 available。
- aws:executeAwsApi - 对您在 ClusterId 参数中指定的数据库集群启用删除保护。
- aws:assertAwsResourceProperty - 验证是否已在数据库集群上启用删除保护。

AWSConfigRemediation-EnableRDSInstanceBackup

描述

AWSConfigRemediation-EnableRDSInstanceBackup运行手册将为您指定的 Amazon Relational Database Service (Amazon RDS) 数据库实例启用备份。此运行手册不支持为 Amazon Aurora 数据库实例启用备份。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

类型：布尔值

默认值：false

描述：(可选) 如果您为该参数指定 true，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 PreferredMaintenanceWindow 设置如何。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- BackupRetentionPeriod

类型：整数

有效值：1-35

描述：(必需) 备份的保留天数。

- **DbiResourceId**

类型：字符串

描述：(必需) 要为其启用备份的数据库实例的资源标识符。

- **PreferredBackupWindow**

类型：字符串

描述：(可选) 创建备份的日常时间范围 (采用 UTC 格式)。

约束：

- 必须采用 hh24:mi-hh24:mi 格式
- 必须采用协调世界时 (UTC)
- 不得与首选维护时段冲突
- 必须至少为 30 分钟

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeScript - 从数据库实例资源标识符收集数据库实例标识符。为数据库实例启用备份。确认数据库实例上已启用备份。

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

描述

AWSConfigRemediation-EnableRDSInstanceDeletionProtection运行手册将在您指定的 Amazon RDS 数据库实例上启用删除保护。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

类型：布尔值

默认值：false

描述：(可选) 如果您为该参数指定 true，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 PreferredMaintenanceWindow 设置如何。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DbInstanceResourceId

类型：字符串

描述：(必需) 要对其启用删除保护的数据库实例的资源标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文档步骤

- `aws:executeAwsApi` - 从数据库实例资源标识符收集数据库实例标识符。
- `aws:executeAwsApi` - 为您的数据库实例启用删除保护。
- `aws:assertAwsResourceProperty` - 确认已在数据库实例上启用删除保护。

AWSConfigRemediation-ModifyRDSInstancePortNumber

描述

AWSConfigRemediation-ModifyRDSInstancePortNumber 运行手册将修改 Amazon Relational Database Service (Amazon RDS) 实例接受连接所在的端口号。运行此自动化将重新启动数据库。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- PortNumber

类型：字符串

描述：(可选) 您希望数据库实例接受连接所在的端口号。

- `RDSDBInstanceResourceId`

类型：字符串

描述：(必需) 要修改其入站端口号的数据库实例的资源标识符。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文档步骤

- `aws:executeAwsApi` - 从数据库实例资源标识符收集数据库实例标识符。
- `aws:assertAwsResourceProperty` - 确认数据库实例处于 `AVAILABLE` 状态。
- `aws:executeAwsApi` - 修改数据库实例接受连接所在的入站端口号。
- `aws:waitForAwsResourceProperty` - 等待数据库实例处于 `MODIFYING` 状态。
- `aws:waitForAwsResourceProperty` - 等待数据库实例处于 `AVAILABLE` 状态。

AWSsupport-ModifyRDSSnapshotPermission

描述

`AWSsupport-ModifyRDSSnapshotPermission` 运行手册可帮助您修改多个 Amazon Relational Database Service (Amazon RDS) 快照的权限。使用此运行手册，您可以制作快照 `Public` 或 `Private` 并将其与其他 AWS 账户分享。使用默认 KMS 密钥加密的快照无法与使用此运行手册的其他账户分享。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AccountIds

类型：StringList

默认：无

描述：(可选) 要与之共享快照的账户的 ID。如果您为 Private 参数值输入 No，则此参数为必选项。

- AccountPermissionOperation

类型：字符串

有效值：添加 | 移除

默认：无

描述：(可选) 要执行的操作类型。

- 专属

类型：字符串

有效值：是 | 否

描述：(必需) 如果要与特定账户共享快照，则为该值输入 No。

- SnapshotIdentifiers

类型：StringList

描述：(必需) 要修改其权限的 Amazon RDS 快照名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBSnapshots
- rds:ModifyDBSnapshotAttribute

文档步骤

1. aws:executeScript - 验证 SnapshotIdentifiers 参数中提供的快照的 ID。验证 ID 后，脚本会检查加密快照并输出列表（若找到）。
2. aws:branch- 根据为 Private 参数输入的值对自动化进行分支。
3. aws:executeScript- 修改指定快照的权限，以便与指定账户共享快照。
4. aws:executeScript- 修改快照的权限，将其从改 Public 为 Private。

输出

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Result

MakePrivate.Result

MakePrivate.Commands

AWSPremiumSupport-PostgreSQLWorkloadReview

描述

AWSPremiumSupport-PostgreSQLWorkloadReview运行手册将捕获 Amazon Relational Database Service (Amazon RDS) PostgreSQL 数据库使用情况统计数据的多个快照。支持 [主动式服务](#) 专家需要收集到的统计数据才能进行运营审查。统计数据使用一组自定义 SQL 和 Shell 脚本进行收集。这些脚本将下载到由本运行手册创建的临时亚马逊弹性计算云 (Amazon EC2) 实例。AWS 账户运行手册要求您使用包含用户名和密码键值对的 AWS Secrets Manager 密钥提供凭证。用户名必须具有查询标准 PostgreSQL 统计视图和函数的权限。

此运行手册 AWS 账户 使用 AWS CloudFormation 堆栈自动在您中创建以下 AWS 资源。您可以使用 CloudFormation 控制台来监控堆栈的创建。

- 虚拟私有云 (VPC) 和 Amazon EC2 实例在 VPC 的私有子网中启动，可选择使用 NAT 网关连接到互联网。
- 附加到临时 Amazon EC2 实例的 AWS Identity and Access Management (IAM) 角色，有权检索 Secrets Manager 密钥值。该角色还提供将文件上传到您选择的亚马逊简单存储服务 (Amazon S3) 存储桶的权限，也可以选择上传案例。支持
- VPC 对等连接，允许在您的数据库实例和临时 Amazon EC2 实例之间建立连接。
- 附加到临时 VPC 的 Systems Manager、Secrets Manager 和 Amazon S3 VPC 端点。
- 包含已注册任务的维护时段，这些任务定期启动和停止临时 Amazon EC2 实例、运行数据收集脚本以及将文件上传到 Amazon S3 存储桶。还会为维护时段创建一个 IAM 角色，该角色提供执行已注册任务的权限。

运行手册完成后，将删除用于创建必要 AWS 资源的 CloudFormation 堆栈，并将报告上传到您选择的 Amazon S3 存储桶，也可以上传一个 支持 案例。

Note

默认情况下，将保留临时 Amazon EC2 实例的根 Amazon EBS 卷。您可以通过将 EbsVolumeDeleteOnTermination 参数设置为 true 来覆盖此设置。

先决条件

- Enterprise Support 订阅此运行手册和主动式服务工作负载诊断与审查需要订阅 Enterprise Support。在使用此运行手册之前，请联系您的技术客户经理 (TAM) 或专家 TAM (STAM) 以获取相关说明。有关更多信息，请参阅[支持 主动服务](#)。
- 账户和 AWS 区域 配额请确保您尚未达到可在账户和使用本运行手册的地区中创建的 Amazon EC2 实例或 VPC 的最大数量。如果您需要申请提高限制，请参阅[提高服务限制表](#)。

• 数据库配置

1. 您在 DatabaseName 参数中指定的数据库应配置 pg_stat_statements 扩展。如果您尚未在 shared_preload_libraries 中配置 pg_stat_statements，则必须编辑数据库参数组中的值并应用更改。更改参数 shared_preload_libraries 会要求您重启数据库实例。有关更多信息，请参阅 [Working with parameter groups](#)。将 pg_stat_statements 添加到 shared_preload_libraries 会增加一些性能开销。但这对于跟踪各个语句的表现很有用。有关 pg_stat_statements 扩展的更多信息，请参阅 [PostgreSQL 文档](#)。如果您未配置 pg_stat_statements 扩展，或者用于统计数据收集的数据库中不存在该扩展，则在操作审查中不会显示语句级别的分析。
2. 确保没有关闭 track_counts 和 track_activities 参数。如果这些参数在数据库参数组中关闭，则不会有意义的统计数据可用。更改这些参数需要重启数据库实例。有关更多信息，请参阅 [使用 Amazon RDS for PostgreSQL 数据库实例上的参数](#)。
3. 如果关闭该 track_io_timing 参数，则操作审查中将不包括 I/O 级别统计信息。更改 track_io_timing 会要求您重启数据库实例，并且会产生额外的性能开销，具体取决于数据库实例的工作负载。尽管关键工作负载会有性能开销，但此参数提供了与每次查询 I/O 时间相关的有用信息。

账单和费用 AWS 账户 将向您收取与临时的 Amazon EC2 实例、关联的 Amazon EBS 卷、NAT 网关以及此自动化运行期间传输的数据相关的费用。默认情况下，此运行手册会创建一个 t3.micro Amazon Linux 2 实例来收集统计数据。此运行手册在两个步骤之间启动和停止实例以降低成本。

数据安全和治理此运行手册通过查询 [PostgreSQL 统计视图和函数](#) 来收集统计数据。确保 SecretId 参数中提供的凭证仅允许对统计视图和函数具有只读权限。作为自动化的一部分，收集脚本将上传到 Amazon S3 存储桶，并且可以位于 `s3://amzn-s3-demo-bucket/automation execution id/queries/`。

这些脚本收集的数据供 AWS 专家用来查看对象级别的关键绩效指标。该脚本收集诸如表名、架构名和索引名之类的信息。如果此类任何信息包含收入指标、用户名、电子邮件地址或任何其他个人信息等敏感信息，则我们建议您停止此工作负载审查。请联系您的 AWS TAM，讨论工作量审核的替代方法。

确保您获得必要的批准和许可，才能与之共享此自动化收集的统计数据和元数据 AWS。

安全注意事项如果您将 UpdateRdsSecurityGroup 参数设置为 yes，则运行手册会更新与您的数据库实例关联的安全组，以允许来自临时 Amazon EC2 实例私有 IP 地址的入站流量。

如果您将 UpdateRdsRouteTable 参数设置为 yes，则运行手册会更新与您的数据库实例运行所在的子网关联的路由表，以允许通过 VPC 对等连接流向临时 Amazon EC2 实例的流量。

用户创建要允许收集脚本连接到您的 Amazon RDS 数据库，您必须设置一个具有读取统计视图权限的用户。然后您必须将这些凭证存储在 Secrets Manager 中。我们建议为此自动化创建一个新的专门用户。创建单独的用户可让您审计和跟踪此自动化执行的活动。

1. 创建新用户。

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. 确保该用户只能进行只读连接。

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. 设置用户级别限制。

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET work_mem=4096;"
```

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET statement_timeout=10000;"
```

```
psql -h <database_connection_endpoint> -p <database_port>
-U <admin_user> -c "ALTER USER <user_name> SET
idle_in_transaction_session_timeout=60000;"
```

4. 向新用户授予 pg_monitor 权限，使其能够访问数据库统计信息。（pg_monitor 角色是 pg_read_all_settings、pg_read_all_stats 和 pg_stat_scan_table 的成员。）

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

此 Systems Manager Automation 向临时 Amazon EC2 实例配置文件添加的权限以下权限已添加到与临时 Amazon EC2 实例关联的 IAM 角色。AmazonSSMManagedInstanceCore 托管策略还与 IAM 角色关联，以允许 Systems Manager 管理 Amazon EC2 实例。

JSON

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

```

    {
      "Action": [
        "ec2:DescribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation-execution-  
id/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-  
east-1:111122223333:secret:secret-id",
      "Effect": "Allow"
    },
    {
      "Action": [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:DescribeCases"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```


此 Systems Manager Automation 向临时维护时段添加的权限以下权限将自动添加到与维护时段任务关联的 IAM 角色。维护时段任务启动、停止并向临时的 Amazon EC2 实例发送命令。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:GetAutomationExecution",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation",
        "ssm:GetCalendarState",
        "ssm:CancelCommand",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ssm:SendCommand",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ssm:StartAutomationExecution"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/temporary-instance-  
id",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:111122223333:automation-execution/*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ssm.amazonaws.com"
        }
      },

```

```
        "ArnLike": {
            "iam:AssociatedResourceARN": "arn:aws:ssm:*:*:document/AWS-*"
        },
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/SSM-*",
        "Effect": "Allow"
    }
}
```

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBInstanceIdentifier

类型：字符串

描述：(必需) 您的数据库实例 ID。

- DatabaseName

类型：字符串

描述：(必需) 数据库实例上托管的数据库名称。

- SecretId

类型：字符串

描述：(必需) 包含用户名和密码键值对的 Secrets Manager 密钥的 ARN。CloudFormation 堆栈创建一个 IAM 策略，该策略具有此 ARN 的 GetSecretValue 操作权限。这些凭证用于允许临时实例收集数据库统计信息。请联系您的 TAM 或 STAM，讨论所需的最低权限。

- 确认

类型：字符串

描述：(必需) 如果您确认此运行手册将在您的账户中创建临时资源以便从数据库实例收集统计数据，请输入 **yes**。我们建议在运行此自动化之前先联系您的 TAM 或 STAM。

- SupportCase

类型：字符串

描述：(可选) 由您的 TAM 或 STAM 提供的 支持 案例编号。如果已提供，运行手册将更新此案例并附上所收集的数据。此选项要求临时 Amazon EC2 实例具有互联网连接才能访问 支持 API 终端节点。您必须将 AllowVpcInternetAccess 参数设置为 true。案例主题必须包含短语 AWSPremiumSupport-PostgreSQLWorkloadReview。

- S3BucketName

类型：字符串

描述：(必需) 您的账户中您要上传此自动化收集的数据的 Amazon S3 存储桶名称。验证存储桶策略是否向不需要访问存储桶内容的主体授予任何不必要的读取或写入权限。出于此自动化的目的，我们建议创建一个新的临时 Amazon S3 存储桶。运行手册将为附加到 Amazon EC2 实例的 IAM 角色提供 s3:PutObject API 操作的权限。上传的文件将位于 s3://*bucket name/automation execution id*/。

- InstanceType

类型：字符串

描述：(可选) 将运行自定义 SQL 和 Shell 脚本的临时 Amazon EC2 实例的类型。

有效值：t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

默认：t3.micro

- VpcCidr

类型：字符串

描述：(可选) 新 VPC 的 CIDR 表示法中的 IP 地址范围 (例如 172.31.0.0/16)。确保您选择的 CIDR 不会与任何与数据库实例相连的现有 VPC 重叠或匹配。可创建的最小 VPC 使用 /28 子网掩码，最大 VPC 使用 /16 子网掩码。

默认值：172.31.0. 0/16

- StackResourcesNamePrefix

类型：字符串

描述：(可选) CloudFormation 堆栈资源名称前缀和标签。运行手册使用此前缀作为应用于资源的名称和标签的一部分来创建 CloudFormation 堆栈资源。标签键值对的结构为 *StackResourcesNamePrefix*:{{automation:EXECUTION_ID}}。

默认：AWSPostgreSQLWorkloadReview

- Schedule

类型：字符串

描述：(可选) 维护时段计划。指定维护时段运行任务的频率。默认值为每 1 hour。

有效值：15 分钟 | 30 分钟 | 1 小时 | 2 小时 | 4 小时 | 6 小时 | 12 小时 | 1 天 | 2 天 | 4 天

默认：1 小时

- Duration

类型：整数

描述：(可选) 您希望允许自动化运行的最长持续时间 (分钟)。支持的最大持续时间为 8,640 分钟 (6 天)。默认值为 4,320 分钟 (3 天)。

有效值：30-8640

默认：4320

- UpdateRdsRouteTable

类型：字符串

描述：(可选) 如果设置为 `true`，运行手册将更新与您的数据库实例运行所在的子网关联的路由表。添加 IPv4 路由，用于通过新创建的 VPC 对等连接将流量路由到临时 Amazon EC2 实例私有 IPV4 地址。

有效值：`true` | `false`

默认：`false`

- `AllowVpcInternetAccess`

类型：字符串

描述：(可选) 如果设置为 `true`，运行手册将创建一个 NAT 网关，为临时 Amazon EC2 实例提供互联网连接，从而与 支持 API 终端节点通信。如果您只想让运行手册将输出上传到 Amazon S3 存储桶，则可以将此参数保留为 `false`。

有效值：`true` | `false`

默认：`false`

- `UpdateRdsSecurityGroup`

类型：字符串

描述：(可选) 如果设置为 `true`，运行手册将更新与您的数据库实例关联的安全组，以允许来自临时实例私有 IP 地址的流量。

有效值：`false` | `true`

默认：`false`

- `EbsVolumeDeleteOnTermination`

类型：字符串

描述：(可选) 如果设置为 `true`，则在运行手册完成并删除 CloudFormation 堆栈后，将删除临时 Amazon EC2 实例的根卷。

有效值：`false` | `true`

默认值：`false`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStackEvents
- cloudformation:DescribeStackResource
- cloudformation:DescribeStacks
- cloudformation:UpdateStack
- ec2:AcceptVpcPeeringConnection
- ec2:AllocateAddress
- ec2:AssociateRouteTable
- ec2:AssociateVpcCidrBlock
- ec2:AttachInternetGateway
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateEgressOnlyInternetGateway
- ec2:CreateInternetGateway
- ec2:CreateNatGateway
- ec2:CreateRoute
- ec2:CreateRouteTable
- ec2:CreateSecurityGroup
- ec2:CreateSubnet
- ec2:CreateTags
- ec2:CreateVpc
- ec2:CreateVpcEndpoint
- ec2:CreateVpcPeeringConnection
- ec2>DeleteEgressOnlyInternetGateway
- ec2>DeleteInternetGateway

- `ec2:DeleteNatGateway`
- `ec2:DeleteRoute`
- `ec2:DeleteRouteTable`
- `ec2:DeleteSecurityGroup`
- `ec2:DeleteSubnet`
- `ec2:DeleteTags`
- `ec2:DeleteVpc`
- `ec2:DeleteVpcEndpoints`
- `ec2:DescribeAddresses`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeNatGateways`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DetachInternetGateway`
- `ec2:DisassociateRouteTable`
- `ec2:DisassociateVpcCidrBlock`
- `ec2:ModifySubnetAttribute`
- `ec2:ModifyVpcAttribute`
- `ec2:RebootInstances`
- `ec2:ReleaseAddress`

- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam>DeleteInstanceProfile`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:TagPolicy`
- `iam:TagRole`
- `rds:DescribeDBInstances`
- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `ssm:AddTagsToResource`

- `ssm:CancelMaintenanceWindowExecution`
- `ssm:CreateDocument`
- `ssm:CreateMaintenanceWindow`
- `ssm>DeleteDocument`
- `ssm>DeleteMaintenanceWindow`
- `ssm:DeregisterTaskFromMaintenanceWindow`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeDocument`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeMaintenanceWindowExecutions`
- `ssm:GetCalendarState`
- `ssm:GetDocument`
- `ssm:GetMaintenanceWindowExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListTagsForResource`
- `ssm:RegisterTaskWithMaintenanceWindow`
- `ssm:RemoveTagsForResource`
- `ssm:SendCommand`
- `support:AddAttachmentsToSet`
- `support:AddCommunicationToCase`
- `support:DescribeCases`

文档步骤

1. `aws:assertAwsResourceProperty` - 确认数据库实例处于 `available` 状态。
2. `aws:executeAwsApi` - 收集有关数据库实例的详细信息。
3. `aws:executeScript` - 检查在 `S3BucketName` 中指定的 Amazon S3 存储桶是否允许匿名访问权限或者公开读取或写入权限。

4. `aws:executeScript`-从 Automation 运行手册附件中获取 CloudFormation 模板内容，该附件用于在中创建 AWS 账户临时 AWS 资源。
5. `aws:createStack`-创建 CloudFormation 堆栈资源。
6. `aws:waitForAwsResourceProperty`-等待 CloudFormation 模板创建的 Amazon EC2 实例开始运行。
7. `aws:executeAwsApi` - 获取 CloudFormation 创建的临时 Amazon EC2 实例和 VPC 对等连接的 ID。
8. `aws:executeAwsApi` - 获取用于配置与数据库实例连接的临时 Amazon EC2 实例的 IP 地址。
9. `aws:executeAwsApi` - 标记附加到临时 Amazon EC2 实例的 Amazon EBS 卷。
10. `aws:waitForAwsResourceProperty` - 等到临时 Amazon EC2 实例通过状态检查。
11. `aws:waitForAwsResourceProperty` - 等到临时 Amazon EC2 实例由 Systems Manager 管理。如果此步骤超时或失败，则运行手册会重启该实例。
 - a. `aws:executeAwsApi` - 如果上一步失败或超时，则重启临时 Amazon EC2 实例。
 - b. `aws:waitForAwsResourceProperty` - 等到临时 Amazon EC2 实例在重启后由 Systems Manager 管理。
12. `aws:runCommand` - 在临时 Amazon EC2 实例上安装元数据收集器应用程序要求。
13. `aws:runCommand` - 通过在临时 Amazon EC2 实例上创建配置文件来配置对数据库实例的访问权限。
14. `aws:executeAwsApi` - 创建维护时段，以便使用运行命令定期运行元数据收集器应用程序。维护时段会在命令之间启动和停止实例。
15. `aws:waitForAwsResourceProperty`-等待 CloudFormation 模板创建的维护窗口准备就绪。
16. `aws:executeAwsApi`-获取由创建的维护时段和更改日历的 ID CloudFormation。
17. `aws:sleep` - 等到维护时段的结束日期。
18. `aws:executeAwsApi` - 关闭维护时段。
19. `aws:executeScript` - 获取在维护时段期间运行的任务的结果。
20. `aws:waitForAwsResourceProperty` - 等待维护时段完成最后一项任务后再继续。
21. `aws:branch` - 根据您是否为 `SupportCase` 参数提供了值对工作流进行分支。
 - a. `aws:changeInstanceState` - 启动临时 Amazon EC2 实例，等待状态检查通过后再上传报告。
 - b. `aws:waitForAwsResourceProperty` - 等到临时 Amazon EC2 实例由 Systems Manager 管理。如果此步骤超时或失败，运行手册将重启该实例。
 - i. `aws:executeAwsApi` - 如果上一步失败或超时，则重启临时 Amazon EC2 实例。

- ii. `aws:waitForAwsResourceProperty` - 等到临时 Amazon EC2 实例在重启后由 Systems Manager 管理。
 - c. `aws:runCommand` - 如果您为 `SupportCase` 参数提供了值，则将元数据报告附加到支持案例。该脚本将报告压缩并拆分为 5 MB 的文件。该脚本附加到支持案例的最大文件数为 12。
- 22 `aws:changeInstanceState`-停止临时的 Amazon EC2 实例，以防 CloudFormation 堆栈无法删除。
- 23 `aws:executeAwsApi`-描述运行手册无法创建或更新 CloudFormation 堆栈时的 CloudFormation 堆栈事件。
- 24 `aws:waitForAwsResourceProperty`-等待 CloudFormation 堆栈处于终端状态后再删除。
- 25 `aws:executeAwsApi`-删除不包括维护时段的 CloudFormation 堆栈。如果 `EbsVolumeDeleteOnTermination` 参数值设置为 `false`，则与临时 Amazon EC2 实例关联的 Amazon EBS 根卷将保留。

AWS-RebootRdsInstance

描述

AWS-RebootRdsInstance 运行手册将在 Amazon Relational Database Service (Amazon RDS) 数据库实例未重启时将其重启。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要重启的 Amazon RDS 数据库实例 ID。

文档步骤

RebootInstance -如果数据库实例尚未重启，则重新启动该实例。

WaitForAvailableState -等待数据库实例完成重启过程。

输出

此自动化没有输出。

AWSupport-ShareRDSSnapshot

描述

AWSupport-ShareRDSSnapshot 运行手册为知识中心文章[如何与其他账户共享加密的 Amazon RDS 数据库快照？](#)概述的过程提供了自动解决方案。如果您的 Amazon Relational Database Service (Amazon RDS) 快照使用默认快照进行加密 AWS 托管式密钥，则无法共享该快照。在这种情况下，您必须使用客户托管密钥复制该快照，然后将其与目标账户共享。此自动化使用您在 SnapshotName 参数中指定的值或为所选 Amazon RDS 数据库实例或集群找到的最新快照执行这些步骤。

Note

如果您没有为 KMSKey 参数指定值，则自动化会在您的账户中创建一个用于加密快照的新 AWS KMS 客户托管密钥。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AccountIds

类型：StringList

描述：(必填) 要与之共享快照的账户列表 IDs ，以逗号分隔。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 数据库

类型：字符串

描述：(必需) 要共享其快照的 Amazon RDS 数据库实例或集群的名称。如果您为 SnapshotName 参数指定一个值，则此参数可选。

- KMSKey

类型：字符串

描述：(可选) 用于加密快照的 AWS KMS 客户托管密钥的完整 Amazon 资源名称 (ARN) 。

- SnapshotName

类型：字符串

描述：(可选) 要使用的数据库集群或实例快照的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- rds:DescribeDBInstances
- rds:DescribeDBSnapshots
- rds:CopyDBSnapshot
- rds:ModifyDBSnapshotAttribute

AutomationAssumeRole 需要执行以下操作才能成功启动数据库集群的运行手册。

- ssm:StartAutomationExecution
- rds:DescribeDBClusters
- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

必须将用于运行此自动化的 IAM 角色添加为密钥用户，才能使用 ARNKmsKey 参数中指定的 KMS 密钥。有关添加密钥用户至 KMS 密钥的信息，请参阅AWS Key Management Service 《开发人员指南》中的[更改密钥策略](#)。

如果您没有为 KMSKey 参数指定一个值，则 AutomationAssumeRole 需要执行以下额外操作才能成功启动运行手册。

- kms:CreateKey
- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

文档步骤

1. aws:executeScript - 检查是否为 KMSKey 参数提供了值，如果未找到任何值，则创建 AWS KMS 客户托管密钥。
2. aws:branch - 检查是否为 SnapshotName 参数提供了一个值，并相应地进行了分支。
3. aws:executeAwsApi - 检查提供的快照是否来自数据库实例。

4. `aws:executeScript` - 格式化将冒号替换为连字符的 `SnapshotName` 参数。
5. `aws:executeAwsApi` - 使用指定的 `KMSKey` 复制快照。
6. `aws:waitForAwsResourceProperty` - 等待复制快照操作完成。
7. `aws:executeAwsApi` - 与指定 `AccountIds` 的共享新快照。
8. `aws:executeAwsApi` - 检查提供的快照是否来自数据库集群。
9. `aws:executeScript` - 格式化将冒号替换为连字符的 `SnapshotName` 参数。
10. `aws:executeAwsApi` - 使用指定的 `KMSKey` 复制快照。
11. `aws:waitForAwsResourceProperty` - 等待复制快照操作完成。
12. `aws:executeAwsApi` - 与指定 `AccountIds` 的共享新快照。
13. `aws:executeAwsApi` - 检查为 `Database` 参数提供的值是否为数据库实例。
14. `aws:executeAwsApi` - 检查为 `Database` 参数提供的值是否为数据库集群。
15. `aws:executeAwsApi` - 检索指定 `Database` 的快照列表。
16. `aws:executeScript` - 从在上一步汇总的列表中确定可用的最新快照。
17. `aws:executeAwsApi` - 使用指定的 `KMSKey` 复制数据库实例快照。
18. `aws:waitForAwsResourceProperty` - 等待复制快照操作完成。
19. `aws:executeAwsApi` - 与指定 `AccountIds` 的共享新快照。
20. `aws:executeAwsApi` - 检索指定 `Database` 的快照列表。
21. `aws:executeScript` - 从在上一步汇总的列表中确定可用的最新快照。
22. `aws:executeAwsApi` - 使用指定的 `KMSKey` 复制数据库实例快照。
23. `aws:waitForAwsResourceProperty` - 等待复制快照操作完成。
24. `aws:executeAwsApi` - 与指定 `AccountIds` 的共享新快照。
25. `aws:executeScript` - 如果您未为 `KMSKey` 参数指定值且自动化失败，则删除由自动化创建的 AWS KMS 客户托管密钥。

AWS-StartRdsInstance

描述

启动 Amazon Relational Database Service (Amazon RDS) 实例。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要启动的 Amazon RDS 实例 ID。

AWS-StartStopAuroraCluster

描述

本运行手册启动或停止 Amazon Aurora 集群。

Note

要启动集群，它必须处于stopped状态。要停止集群，它必须处于available状态。本运行手册不能用于启动或停止 Aurora Serverless v1 集群、Aurora 多主集群、Aurora 全局数据库的一部分或使用 Aurora 并行查询的集群。运行手册可用于停止和启动 Aurora Serverless v2 集群。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ClusterName

类型：字符串

描述：(必填) 要停止或启动的 Aurora 集群的名称。

- 处理建议

类型：字符串

有效值：开始 | 停止

默认：启动

描述：(必填) 要停止或启动的 Aurora 集群的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- rds:DescribeDBClusters

- `rds:StartDBCluster`
- `rds:StopDBCluster`

文档步骤

- `aws:executeScript`-根据您为指定的值启动或停止集群。

输出

`StartStopAuroraCluster.ClusterName` -Aurora 集群的名称

`StartStopAuroraCluster.CurrentStatus` -Aurora 集群的当前状态

`StartStopAuroraCluster.Message` -自动化详情

AWS-StopRdsInstance

描述

停止亚马逊关系数据库服务 (Amazon RDS) 实例。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 要停止的 Amazon RDS 实例的 ID。

AWSsupport-TroubleshootConnectivityToRDS

描述

AWSsupport-TroubleshootConnectivityToRDS 运行手册将诊断 EC2 实例和 Amazon Relational Database Service 实例之间的连接问题。自动化可确保数据库实例可用，然后检查关联的安全组规则、网络访问控制列表 (网络 ACL) 和路由表是否存在潜在的连接问题。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBInstanceIdentifier

类型：字符串

描述：(必需) 要测试与的连接的数据库实例 ID。

- SourceInstance

类型：字符串

允许的模式：`^[a-z0-9]{8,17}$`

描述：(必需) 用于进行连接测试的 EC2 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

文档步骤

- `aws:assertAwsResourceProperty` - 确认数据库实例的状态为 `available`。
- `aws:executeAwsApi` - 获取有关数据库实例的信息。
- `aws:executeAwsApi` - 获取有关数据库实例网络 ACL 的信息。
- `aws:executeAwsApi` - 获取数据库实例子网 CIDR。
- `aws:executeAwsApi` - 获取有关 EC2 实例的信息。
- `aws:executeAwsApi` - 获取有关 EC2 实例网络 ACL 的信息。
- `aws:executeAwsApi` - 获取有关与 EC2 实例关联的安全组的信息。
- `aws:executeAwsApi` - 获取有关与数据库实例关联的安全组的信息。
- `aws:executeAwsApi` - 获取有关与 EC2 实例关联的路由表的信息。

- `aws:executeAwsApi` - 获取有关与用于 EC2 实例的 Amazon VPC 关联的主路由表信息。
- `aws:executeAwsApi` - 获取有关与数据库实例关联的路由表的信息。
- `aws:executeAwsApi` - 获取有关与用于数据库实例的 Amazon VPC 关联的主路由表信息。
- `aws:executeScript` - 评估安全组规则。
- `aws:executeScript` - 评估网络 ACL。
- `aws:executeScript` - 评估路由表。
- `aws:sleep` - 结束自动化。

输出

`get RDSInstanceProperties.DBInstanceIdentifier` - 自动化中使用的数据库实例。

`get RDSInstanceProperties.DBInstanceStatus` - 数据库实例的当前状态。

`eval SecurityGroupRules.SecurityGroupEvaluation` - 将 `SourceInstance` 安全组规则与数据库实例安全组规则进行比较的结果。

`eval NetworkAclRules.NetworkAclEvaluation` - 将 `SourceInstance` 网络 ACL 与数据库实例网络 ACL 进行比较的结果。

`eval RouteTableEntries.RouteTableEvaluation` - 比较 `SourceInstance` 路由表和数据库实例路由的结果。

AWSsupport-TroubleshootRDSIAMAuthentication

描述

`AWSsupport-TroubleshootRDSIAMAuthentication` 这有助于对适用于 PostgreSQL 的亚马逊 RDS、适用于 MySQL 的亚马逊 RDS、适用于 MariaDB 的亚马逊 RDS、亚马逊 Aurora PostgreSQL 和亚马逊 Aurora MySQL 实例进行身份验证故障排除 AWS Identity and Access Management (IAM)。使用此运行手册验证使用 Amazon RDS 实例或 Aurora 集群进行 IAM 身份验证所需的配置。它还提供了纠正与 Amazon RDS 实例或 Aurora 集群的连接问题的步骤。

Important

本运行手册不支持适用于甲骨文的亚马逊 RDS 或适用于微软 SQL Server 的亚马逊 RDS for Microsoft SQL Server。

Important

如果提供了源 Amazon EC2 实例，而目标数据库是 Amazon RDS，则会调用子自动化 `AWSSupport-TroubleshootConnectivityToRDS` 来排除 TCP 连接故障。输出还提供了您可以在 Amazon EC2 实例或源计算机上运行的命令，以便使用 IAM 身份验证连接到 Amazon RDS 实例。

如何工作？

本运行手册包含六个步骤：

- 步骤 1：验证输入：验证自动化的输入。
- 步骤 2：分支 `OnSourceEC2Provided`：验证输入参数中是否提供了源 Amazon EC2 实例 ID。
- 步骤 3： `validaterdsConnectivity`：验证来自源 Amazon EC2 实例（如果提供）的 Amazon RDS 连接。
- 第 4 步： `validaterdsiamAuthentication`：验证 IAM 身份验证功能是否已启用。
- 第 5 步： `validateiamPolicies`：验证提供的 IAM 中是否存在所需的 IAM 权限。 `user/role`
- 步骤 6：生成报告：生成先前执行步骤的结果报告。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- rdType

类型：字符串

描述：(必填)：选择要连接并进行身份验证的关系数据库的类型。

允许的值：Amazon RDS或 Amazon Aurora Cluster.

- DBInstanceIdentifier

类型：字符串

描述：(必填) 目标 Amazon RDS 数据库实例或 Aurora 数据库集群的标识符。

允许的模式：`^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

最大字符数：63

- SourceEc2InstanceIdentifier

类型：AWS::EC2::Instance::Id

描述：(可选) 如果您从在同一账户和地区运行的 Amazon EC2 实例连接到 Amazon RDS 数据库实例，则为 Amazon EC2 实例 ID。如果源不是 Amazon EC2 实例，或者目标 Amazon RDS 类型是 Aurora 数据库集群，则不要指定此参数。

默认值：""

- DBIAMRoleName

类型：字符串

描述：(可选) 用于 IAM-based身份验证的 IAM 角色名称。仅在未提供参数DBIAMUserName时提供，否则将其留空。必须提供 DBIAMRoleName 或 DBIAMUserName。

允许的模式：`^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

最大字符数：64

默认值：""

- DBIAMUserName

类型：字符串

描述：(可选) 用于 IAM-based 身份验证的 IAM 用户名。仅在未提供 DBIAMRoleName 参数时提供，否则将其留空。必须提供 DBIAMRoleName 或 DBIAMUserName。

允许的模式：`^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

最大字符数：64

默认值：""

- DBUserName

类型：字符串

描述：(可选) 映射到 IAM 的数据库用户名，role/user 用于在数据库中进行 IAM-based 身份验证。默认选项用于*评估是否允许数据库中的所有用户拥有该rds-db:connect权限。

允许的模式：`^[a-zA-Z0-9+=, .@*_]{1,64}$`

最大字符数：64

默认值：*

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- iam:GetPolicy
- iam:GetRole
- iam:GetUser
- iam:ListAttachedRolePolicies

- iam:ListAttachedUserPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies
- iam:SimulatePrincipalPolicy
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

说明

1. 导航到 AWS Systems Manager 控制台 [AWSSupport-TroubleshootRDSIAMAuthentication](#) 中的。
2. 选择 Execute automation (执行自动化)
3. 要输入参数，请输入内容：

- AutomationAssumeRole (可选)：

AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 允许 Systems Manager Automation 代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- rdSyype (必填)：

选择您要连接并进行身份验证的 Amazon RDS 的类型。从两个允许的值中进行选择：Amazon RDS 或 Amazon Aurora Cluster。

- DBInstanceIdentifier (必填)：

输入您尝试连接的目标 Amazon RDS 数据库实例或 Aurora 集群的标识符，并使用 IAM 凭证进行身份验证。

- SourceEc2InstanceIdentifier (可选)：

如果您要从同一账户和地区的 Amazon EC2 实例连接到 Amazon RDS 数据库实例，请提供 Amazon EC2 实例 ID。如果源不是亚马逊 EC2 或者目标 Amazon RDS 类型是 Aurora 集群，则留空。

- DBIAMRoleName (可选)：

输入用于 IAM-Based身份验证的 IAM 角色名称。仅在未提供DBIAMUserName时提供；否则，请留空。必须提供 DBIAMRoleName 或 DBIAMUserName。

- DBIAMUserName (可选) :

输入用于 IAM-Based身份验证的 IAM 用户。仅DBIAMRoleName在未提供时提供，否则留空。必须提供 DBIAMRoleName 或 DBIAMUserName。

- DBUserName (可选) :

输入映射到 IAM 的数据库用户，role/user以便在数据库中进行 IAM-Based 身份验证。默认选项*用于评估；此字段中未提供任何内容。

Input parameters

SourceEC2InstanceIdentifier

(Optional) The Amazon EC2 instance ID if you are connecting to the RDS DB instance from an EC2 instance running in the same account and region. Do not specify this parameter if the source is not an EC2 instance or if the target RDS type is an Aurora DB cluster.

Show interactive instance picker

Q Filter all instances

Show managed instances... ▼

< 1 ... >

Name	Instance ID	State	Availability zone	Platform
There are no managed instances in this account.				
We recommend using Quick Setup to configure your instances for Systems Manager.				
After configuring your instances for Systems Manager, the instances will be displayed here in a few minutes.				

AutomationAssumeRole

(Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

DBInstanceIdentifier

(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

String

DBIAMUserName

(Optional) The IAM user name used for IAM-based authentication. Provide only if the 'DBIAMRoleName' parameter is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

String

RDSType

(Required) The type of Relational Database.

DBIAMRoleName

(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter 'DBIAMUserName' is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

String

DBUserName

(Optional) The database user name mapped to an IAM role/user for IAM-based authentication within the database. The default option '*' evaluates if the 'rds-db:connect' permission is allowed for all users in the DB.

*

4. 选择执行。
5. 请注意，自动化已启动。
6. 文档将执行以下步骤：
- 步骤 1：验证输入：

验证自动化的输入-SourceEC2InstanceIdentifier (可选)、DBInstanceIdentifier或ClusterID、DBIAMRoleName或DBIAMUserName。它会验证您输入的输入参数是否存在于您的账户和区域中。它还会验证用户是否输入了其中一个 IAM 参数 (例如，DBIAMRoleName或DBIAMUserName)。此外，它还会执行其他验证，例如提及的数据库是否处于“可用”状态。

- 第 2 步：分支OnSourceEC2Provided：

验证输入参数中是否提供了源 Amazon EC2 以及数据库是否是 Amazon RDS。如果是，则继续执行步骤 3。否则，它将跳过步骤 3（即 Amazon EC2-Amazon RDS 连接验证），继续执行步骤 4。

- 步骤 3：验证连接：

如果输入参数中提供了源 Amazon EC2，并且数据库是 Amazon RDS，则步骤 2 将启动步骤 3。在此步骤中，将调用子自动化 `AWSSupport-TroubleshootConnectivityToRDS` 来验证来自源 Amazon EC2 的 Amazon RDS 连接。儿童自动化运行手册 `AWSSupport-TroubleshootConnectivityToRDS` 会验证所需的网络配置（Amazon Virtual Private Cloud [Amazon VPC]、安全组、网络访问控制列表 [NACL]、Amazon RDS 可用性）是否到位，以便您可以从 Amazon EC2 实例连接到 Amazon RDS 实例。

- 第 4 步：验证 dsiam 身份验证：

验证是否在 Amazon RDS 实例或 Aurora 集群上启用了 IAM 身份验证功能。

- 第 5 步：验证 IAM 政策：

验证所 `user/role` 传递的 IAM 中是否存在所需的 IAM 权限，以允许 IAM 凭证对指定数据库用户（如果有）的 Amazon RDS 实例进行身份验证。

- 步骤 6：生成报告：

获取前面步骤中的所有信息，并打印每个步骤的结果或输出。它还列出了使用 IAM 凭证连接到 Amazon RDS 实例时需要参考和执行的步骤。

7. 自动化完成后，请查看“输出”部分以了解详细结果：

- 正在检查连接数据库的 IAM User/Role 权限：

验证所 `user/role` 传递的 IAM 中是否存在所需的 IAM 权限，以使 IAM 凭证能够在指定数据库用户（如果有）的 Amazon RDS 实例中进行身份验证。

- 正在检查数据库的 IAM-Based 身份验证属性：

验证是否为指定的 Amazon RDS Database/Aurora 集群启用了 IAM 身份验证功能。

- 检查从 Amazon EC2 实例到 Amazon RDS 实例的连接：

验证所需的网络配置（亚马逊 VPC、安全组、NACL、Amazon RDS 可用性）是否已到位，以便您可以从 Amazon EC2 实例连接到 Amazon RDS 实例。

- 后续步骤：

列出了使用 IAM 凭证连接到 Amazon RDS 实例时要参考和执行的命令和步骤。

Outputs

ScriptExecutionId

Zetd[REDACTED]ba4

Output

[Troubleshooting Results]

1. Checking the IAM user/role permissions to connect to database:

✅ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[REDACTED]-db1'.

2. Checking IAM-based authentication attribute for the database:

✅ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[REDACTED]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:

✅ [SKIPPED]: No Source EC2 instance provided.

Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:

\$ telnet a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306

\$ nc -vz a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:

- Connect to DB a[REDACTED]-db1 using admin/master db user.

- Run the following query/command in your database:

SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';

- From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:

\$ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem

\$ export DBPASS=\$(aws rds generate-db-auth-token --hostname a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port 3306 --region us-[REDACTED]-2 --username <name of the DB user>)

mysql --host=a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=\$DBPASS

Reference: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>**参考****Systems Manager Automation**

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSSupport-ValidateRdsNetworkConfiguration**描述**

AWSSupport-ValidateRdsNetworkConfiguration在执行或操作之前，自动化有助于避免现有亚马逊关系数据库服务 (Amazon RDS) /Amazon Aurora/Amazon DocumentDB 实例出现不兼容的网络状态。ModifyDBInstance StartDBInstance如果实例已经处于网络不兼容状态，则运行手册将提供原因。

如何工作？

本运行手册确定您的 Amazon RDS 数据库实例是否会进入网络不兼容状态，或者如果是，则确定其处于网络不兼容状态的原因。

运行手册会对您的 Amazon RDS 数据库实例执行以下检查：

- 每个区域的 Amazon 弹性网络接口 (ENI) 配额。
- 数据库子网组中的所有子网都存在。
- 子网有足够的空闲 IP 地址可用。
- (适用于可公开访问的 Amazon RDS 实例) VPC 属性的设置 (`enableDnsSupport` 和 `enableDnsHostnames`) 。

Important

对亚马逊 Aurora/Amazon DocumentDB 集群使用本文档时，请确保使用 `DBInstanceIdentifier` 代替 `ClusterIdentifier` 否则，文档将在第一步中失败。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

示例策略：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:us-east-1:111122223333:db:db-instance-name"
      ]
    }
  ]
}
```

说明

1. 导航到 AWS Systems Manager 控制台 [AWSSupport-ValidateRdsNetworkConfiguration](#) 中的。
2. 选择 Execute automation (执行自动化)
3. 要输入参数，请输入内容：
 - AutomationAssumeRole (可选)：

AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 允许 Systems Manager Automation 代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DBInstanceIdentifier (必填)：

输入 Amazon Relational Database Service 实例标识符。

The screenshot shows the 'Input parameters' section of the AWS Systems Manager console. It contains two input fields:

- AutomationAssumeRole**: A dropdown menu with the text 'Select an existing IAM role'. Below it, a search bar shows 'AutomationAssumeRoleSSM' with a blue highlight and a close button (X). Below the search bar, the full ARN 'arn:aws:iam::111122223333:role/AutomationAssumeRoleSSM' is displayed.
- DBInstanceIdentifier**: A text input field with the value 'my-rds-instance-01'. Above the field, there is a small note: '(Required) The Amazon Aurora or Amazon DocumentDB instance identifier.'

4. 选择执行。

5. 请注意，自动化已启动。

6. 文档将执行以下步骤：

- 第 1 步：断言RdsState：

检查提供的实例标识符是否存在以及是否具有以下任何状态：`availablestopped`、`incompatible-network`。

- 第 2 步：收集RdsInformation：

收集有关 Amazon RDS 实例的必需信息，以便稍后在自动化中使用。

- 第 3 步：检查EniQuota：

检查该地区当前可用的 Amazon ENI 配额。

- 第 4 步：验证VpcAttributes：

验证 Amazon VPC 的 DNS 参数 (`enableDnsSupport` 和 `enableDnsHostnames`) 是否设置为 `true` (如果是 Amazon RDS 实例，则不是 `PubliclyAccessible`) 。

- 第 5 步：验证SubnetAttributes：

验证中是否存在子网，`DBSubnetGroup`并检查每个子网是否有可用 IP。

- 步骤 6：生成报告：

获取前面步骤中的所有信息，并打印每个步骤的结果或输出。它还列出了使用 IAM 凭证连接到 Amazon RDS 实例时需要参考和执行的步骤。

7. 自动化完成后，请查看“输出”部分以了解详细结果：

具有有效网络配置的 Amazon RDS 实例：

▼ Outputs

```
generateReport.Report
```

```
# AWS RDS Network Configuration Checks: aws-rds-01rr (available)
## ✅ No Issue(s) Found
```

```
### [Troubleshooting Results]
```

```
1. Checking ENI Quota for region the RDS Instance is in:
```

```
✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4997) is sufficient at the moment.
```

```
2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
```

```
✅ [PASSED] : [PASSED] Value for both VPC attributes ('enableDnsHostnames' and 'enableDnsSupport') is set to 'true'.
```

```
3. Checking if subnets required for RDS exists or not:
```

```
✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.
```

```
4. Checking if Available IPs are sufficient per subnets that are required:
```

```
✅ [PASSED] : There are sufficient available IPs in 'ap-south-1b' availability zone.
```

```
5. Checking if other Availability zone satisfy Check No# 3 & 4:
```

```
* Availability Zone: ap-south-1c
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
* Availability Zone: ap-south-1a
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
### [Next Steps]
```

```
✅ All the checks has passed so the RDS Network configuration is correct.
```

```
Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
```

```
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

网络配置不正确的 Amazon RDS 实例 (VPC 属性启用设置DnsHostnames 为 false) :

▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattr (stopped)
### 🚫 Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
   ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
   ❌ [FAILED] : Value for 'enableDnsHostnames' VPC Attribute is 'false'.

3. Checking if subnets required for RDS exists or not:
   ✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
   ⚠️ [WARNING] : There are sufficient available IPs in 'ap-south-1b' availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
   * Availability Zone: ap-south-1a
     i. Subnet Existence Check: ✅ [PASSED]
     ii. Available IP Check: ⚠️ [WARNING]

### [Next Steps]
o Please set the value of 'enableDnsHostnames' VPC attribute to 'true'.
  [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop operation on the instance.
  [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.

```

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

AWS 服务文档

- [如何解决处于网络不兼容状态的 Amazon RDS 数据库的问题？](#)
- [如何解决处于网络不兼容状态的 Amazon DocumentDB 实例的问题？](#)

Amazon Redshift

AWS Systems Manager 自动化为亚马逊 Redshift 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

AWSConfigRemediation-DeleteRedshiftCluster

描述

AWSConfigRemediation-DeleteRedshiftCluster 运行手册将删除您指定的 Amazon Redshift 集群。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- **ClusterIdentifier**

类型：字符串

描述：(必需) 要删除的 Amazon Redshift 集群的 ID。

- **SkipFinalClusterSnapshot**

类型：布尔值

默认值：false

描述：(可选) 如果设置为 false，则自动化会在删除 Amazon Redshift 集群之前先创建一个快照。如果设置为 true，则不会创建最终集群快照。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift>DeleteCluster
- redshift:DescribeClusters

文档步骤

- aws:branch - 根据您为 SkipFinalClusterSnapshot 参数指定的值进行分支。
- aws:executeAwsApi - 删除参数 ClusterIdentifier 中指定的 Amazon Redshift 集群。
- aws:assertAwsResourceProperty - 验证 Amazon Redshift 集群是否已删除。

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

描述

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster 运行手册将为指定的 Amazon Redshift 集群禁用公共访问权限。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- ClusterIdentifier

类型：字符串

描述：(必需) 要为其禁用公共访问权限的集群的唯一标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群禁用公开可访问性。
- aws:waitForAwsResourceProperty - 等待集群的状态变为 available。
- aws:assertAwsResourceProperty - 确认公开可访问性设置已在集群上禁用。

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

描述

AWSConfigRemediation-EnableRedshiftClusterAuditLogging运行手册将为您指定的 Amazon Redshift 集群启用审核日志记录功能。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- BucketName

类型：字符串

描述：(必需) 要将日志上传到的 Amazon Simple Storage Service (Amazon S3) 存储桶的名称。

- ClusterIdentifier

类型：字符串

描述：(必需) 要对其启用审核日志记录的集群的唯一标识符。

- S3KeyPrefix

类型：字符串

描述：(可选) 要将日志上传到的 Amazon S3 密钥前缀 (子文件夹)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeLoggingStatus
- redshift:EnableLogging
- s3:GetBucketAcl
- s3:PutObject

文档步骤

- aws:branch - 根据是否为 S3KeyPrefix 参数指定了值进行分支。
- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用审核日志记录。
- aws:assertAwsResourceProperty - 验证集群上是否启用了审核日志记录。

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

描述

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot 运行手册将为您指定的 Amazon Redshift 集群启用自动快照。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- AutomatedSnapshotRetentionPeriod

类型：整数

有效值：1-35

描述：(必需) 自动快照保留的天数。

- ClusterIdentifier

类型：字符串

描述：(必需) 要对其启用自动快照的集群的唯一标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用自动快照。
- aws:waitForAwsResourceProperty - 等待集群的状态变为 available。
- aws:executeScript - 确认已在集群上启用自动快照。

AWSConfigRemediation-EnableRedshiftClusterEncryption

描述

该AWSConfigRemediation-EnableRedshiftClusterEncryption运行手册支持使用 AWS Key Management Service AWS KMS() 客户托管密钥对您指定的 Amazon Redshift 集群进行加密。此运行手册应仅用作基准，以确保根据建议的最低的安全性最佳实践对 Amazon Redshift 集群进行加密。我们建议使用不同的客户托管密钥对多个集群进行加密。本运行手册无法更改在已加密的集群上使用的 AWS KMS 客户托管密钥。要更改用于加密集群的 AWS KMS 客户托管密钥，必须先在集群上禁用加密。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- ClusterIdentifier

类型：字符串

描述：(必需) 要对其启用加密的集群的唯一标识符。

- KMSKeyARN

类型：字符串

描述：(必需) 要用于加密集群数据的 AWS KMS 客户托管密钥的 Amazon 资源名称 (ARN) 。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的 Amazon Redshift 集群启用加密。
- aws:assertAwsResourceProperty - 验证是否已在集群上启用加密。

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

描述

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting 运行手册将为您指定的 Amazon Redshift 集群启用增强型虚拟私有云 (VPC) 路由。有关增强型 VPC 路由的信息，请参阅《Amazon Redshift 管理指南》中的[Amazon Redshift 增强型 VPC 路由](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- ClusterIdentifier

类型：字符串

描述：(必需) 对其启用增强型 VPC 路由的集群的唯一标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用增强型 VPC 路由。
- assertAwsResourceProperty - 确认已在集群上启用增强型 VPC 路由。

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

描述

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster 运行手册将要求传入连接对您指定的 Amazon Redshift 集群使用 SSL。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- ClusterIdentifier

类型：字符串

描述：(必需) 对其启用增强型 VPC 路由的集群的唯一标识符。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:DescribeClusterParameters
- redshift:ModifyClusterParameterGroup

文档步骤

- aws:executeAwsApi - 从 ClusterIdentifier 参数中指定的集群收集参数详细信息。
- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用 require_ssl 设置。
- aws:assertAwsResourceProperty - 确认已在集群上启用 require_ssl 设置。

- `aws:executeScript` - 验证集群的 `require_ssl` 设置。

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

描述

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings 运行手册将修改您指定的 Amazon Redshift 集群的维护设置。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AllowVersionUpgrade

类型：布尔值

描述：(必需) 如果设置为 `true`，将在维护时段期间将主要版本升级自动应用于该集群。

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- AutomatedSnapshotRetentionPeriod

类型：整数

有效值：1-35

描述：(必需) 自动快照保留的天数。

- ClusterIdentifier

类型：字符串

描述：(必需) 对其启用增强型 VPC 路由的集群的唯一标识符。

- PreferredMaintenanceWindow

类型：字符串

描述：(必需) 可进行系统维护的每周时间范围 (按世界协调时间计算)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 修改 ClusterIdentifier 参数中指定的集群的维护设置。
- aws:assertAwsResourceProperty - 确认已为集群配置修改后的维护设置。

AWSConfigRemediation-ModifyRedshiftClusterNodeType

描述

AWSConfigRemediation-ModifyRedshiftClusterNodeType 运行手册将修改您指定的 Amazon Redshift 集群的节点类型和节点数。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- Classic

类型：布尔值

描述：(可选) 如果设置为 true，则调整大小操作将使用经典的大小调整进程。

- ClusterIdentifier

类型：字符串

描述：(必需) 要修改其节点类型的集群的唯一标识符。

- ClusterType

类型：字符串

有效值：single-node | multi-node

描述：(必需) 要将其分配给您的集群的集群类型。

- NodeType

类型：字符串

有效值：ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

描述：(必需) 要将其分配给您的集群的节点类型。

- NumberOfNodes

类型：整数

有效值：2-100

描述：(可选) 要将其分配给集群的节点的数量。如果集群为 single-node 类型，请不要为此参数指定值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ResizeCluster

文档步骤

- aws:executeScript - 修改 ClusterIdentifier 参数中指定的集群的节点类型和节点数。

Amazon S3

AWS Systems Manager Automation 为 Amazon 简单存储服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-ArchiveS3BucketToIntelligentTiering](#)
- [AWS-ConfigureS3BucketLogging](#)
- [AWS-ConfigureS3BucketVersioning](#)
- [AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock](#)
- [AWSConfigRemediation-ConfigureS3PublicAccessBlock](#)
- [AWS-CreateS3PolicyToExpireMultipartUploads](#)
- [AWS-DisableS3BucketPublicReadWrite](#)
- [AWS-EnableS3BucketEncryption](#)

- [AWS-EnableS3BucketKeys](#)
- [AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy](#)
- [AWSConfigRemediation-RestrictBucketSSLRequestsOnly](#)
- [AWSSupport-TroubleshootS3PublicRead](#)
- [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#)
- [AWSSupport-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)
- [AWSSupport-ContainS3Resource](#)

AWS-ArchiveS3BucketToIntelligentTiering

描述

AWS-ArchiveS3BucketToIntelligentTiering运行手册为您指定的亚马逊简单存储服务 (Amazon S3) 存储桶创建或替换智能分层配置。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(必填) 您要为其创建智能分层配置的 S3 存储桶的名称。

- ConfigurationId

类型：字符串

描述：(必填) 智能分层配置的 ID。这可以是新的配置 ID，也可以是现有配置的 ID。

- NumberOfDaysToArchive

类型：字符串

有效值：90-730

描述：(必填) 存储桶中的对象有资格过渡到存档访问层之后连续经过的天数。

- NumberOfDaysToDeepArchive

类型：字符串

有效值：180-730

描述：(必填) 存储桶中的对象有资格过渡到深度存档访问权限层后的连续天数。

- S3Prefix

类型：字符串

描述：(可选) 要应用配置的对象的关键名前缀。

- 标签

类型：MapList

描述：(可选) 分配给要应用配置的对象的数据。标签由用户定义的键和值组成。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

文档步骤

- `PutBucketIntelligentTieringConfiguration` (aws: ExecuteScript)-为指定存储桶创建或更新 Amazon S3 Intelligent-Tiering 配置。
- `VerifyBucketIntelligentTieringConfiguration`(aws: assertAwsResourceProperty)-验证 S3 存储桶智能配置已应用于指定的存储桶。

AWS-ConfigureS3BucketLogging

描述

允许登录 Amazon Simple Storage Service (Amazon S3) 存储桶。

Important

请注意以下有关本运行手册使用的 Amazon S3 [PutBucketLogging](#) API 的电子邮件被授权者 ACL 的重要信息：

终止支持通知：从 2025 年 10 月 1 日起，Amazon S3 将停止支持创建新的电子邮件受让者访问控制列表 (ACL)。在此日期之前创建的电子邮件受让人 ACL 将继续起作用，并且仍可通过、(AWS CLI CLI) AWS 管理控制台、软件开发工具包和 REST API 进行访问。但是，届时您将无法再创建新的电子邮件受让者 ACL。在 2025 年 7 月 15 日至 2025 年 10 月 1 日之间，在尝试创建新的电子邮件受赠者 ACL 时，向亚马逊 S3 发出的请求 HTTP 405 错误率将开始上升。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(必需) 要为其配置日志记录的 Amazon S3 存储桶的名称。

- GrantedPermission

类型：字符串

有效值：FULL_CONTROL | READ | WRITE

描述：(必需) 分配给存储桶的被授权者的日志记录权限。

- GranteeEmailAddress

类型：字符串

(可选) 被授权者的电子邮件地址。

- GranteeId

类型：字符串

描述：(可选) 被授权者的规范用户 ID。

- GranteeType

类型：字符串

有效值：CanonicalUser | AmazonCustomerByEmail | 群组

描述：(必需) 被授权者的类型。

- GranteeUri

类型：字符串

描述：(可选) 被授权者组的 URI。

- TargetBucket

类型：字符串

描述：(必需) 指定希望 Amazon S3 存储服务器访问日志的存储桶。您可以将日志传输到您拥有的任何存储桶。您也可以配置多个存储桶，以将它们的日志传输到同一目标存储桶。在这种情况下，您应该 TargetPrefix 为每个源存储桶选择不同的存储桶，以便可以按密钥区分已交付的日志文件。

- TargetPrefix

类型：字符串

默认：/

描述：(可选) 指定用于存储日志文件的键的前缀。

AWS-ConfigureS3BucketVersioning

描述

配置 Amazon Simple Storage Service (Amazon S3) 存储桶的版本控制。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：（必需）要为其配置版本控制的 Amazon S3 存储桶的名称。

- VersioningState

类型：字符串

有效值：Enabled | Suspended

默认：Enabled

描述：（可选）应用于 VersioningConfiguration.Status。设置为“Enabled”时，此过程为存储桶中的对象启用版本控制，添加到此存储桶的所有对象都将收到唯一的版本 ID。设置为 Suspended 时，此过程将禁用存储桶中对象的版本控制。添加到存储桶的所有对象都将收到版本 ID null。

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

描述

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 运行手册根据您在运行手册参数中指定的值为 Amazon S3 存储桶配置 Amazon Simple Storage Service (Amazon S3) 公共访问屏蔽设置。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- BlockPublicAcls

类型：布尔值

默认：True

描述：(可选) 如果设置为 true，Amazon S3 会屏蔽 S3 存储桶的公共访问控制列表 (ACL) 以及您在 BucketName 参数中指定的 S3 存储桶中存储的对象。

- BlockPublicPolicy

类型：布尔值

默认：True

描述：(可选) 如果设置为 true，Amazon S3 会阻止您在 BucketName 参数中指定的 S3 存储桶的公有存储桶策略。

- BucketName

类型：字符串

描述：(必需) 要配置的 S3 存储桶的名称。

- IgnorePublicAcls

类型：布尔值

默认：True

描述：(可选) 如果设置为 true，Amazon S3 会忽略您在 BucketName 参数中指定的 S3 存储桶的所有公有 ACL。

- RestrictPublicBuckets

类型：布尔值

默认：True

描述：(可选) 如果设置为 true , Amazon S3 会限制您在 BucketName 参数中指定的 S3 存储桶的公有存储桶策略。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

文档步骤

- aws:executeAwsApi - 创建或修改在 BucketName 参数中指定的 S3 存储桶的 PublicAccessBlock 配置。
- aws:executeScript - 返回在 BucketName 参数中指定的 S3 存储桶的 PublicAccessBlock 配置，并验证是否根据在运行手册参数中指定的值成功进行了更改。

AWSConfigRemediation-ConfigureS3PublicAccessBlock

描述

该AWSConfigRemediation-ConfigureS3PublicAccessBlock运行手册根据你在运行手册参数中指定的值来配置的 AWS 账户亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的公共访问封锁设置。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AccountId

类型：字符串

描述：(必填) 拥有您正在配置的 S3 存储桶的 ID。AWS 账户

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- BlockPublicAcls

类型：布尔值

默认：True

描述：(可选) 如果设置为true，Amazon S3 会阻止 AWS 账户 您在参数中指定的 S3 存储桶的公共访问控制列表 (ACL)。AccountId

- BlockPublicPolicy

类型：布尔值

默认：True

描述：(可选) 如果设置为true，Amazon S3 将阻止 AWS 账户 您在AccountId参数中指定的拥有的 S3 存储桶的公有存储桶策略。

- IgnorePublicAcls

类型：布尔值

默认：True

描述：(可选) 如果设置为true，Amazon S3 将忽略 AWS 账户 您在参数中指定的拥有的 S3 存储桶的所有公有 ACL。AccountId

- RestrictPublicBuckets

类型：布尔值

默认：True

描述：(可选) 如果设置为true，Amazon S3 会限制 AWS 账户 您在参数中指定的拥有的 S3 存储桶的公有存储桶策略。AccountId

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock

文档步骤

- aws:executeAwsApi - 为在 AccountId 参数中指定的 AWS 账户 创建或修改 PublicAccessBlock 配置。
- aws:executeScript-返回AccountId参数中 AWS 账户 指定的PublicAccessBlock配置，并根据 runbook 参数中指定的值验证更改是否成功完成。

AWS-CreateS3PolicyToExpireMultipartUploads

描述

AWS-CreateS3PolicyToExpireMultipartUploads运行手册为指定的存储桶创建生命周期策略，该策略将在规定的天数后过期未完成的分段上传。本运行手册将新的生命周期策略与任何已存在的现有生命周期存储桶策略合并。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(必需) 要配置的 S3 存储桶的名称。

- DaysUntilExpire

类型：整数

描述：(必填) Amazon S3 在永久删除所有上传部分之前等待的天数。

- RuleId

类型：字符串

描述：(必填) 用于标识生命周期存储桶规则的 ID。这必须是唯一的值。

- S3Prefix

类型：字符串

描述：(可选) 要应用配置的对象的关键名前缀。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

文档步骤

- `ConfigureExpireMultipartUploads (aws: ExecuteScript)`-为存储桶配置生命周期策略。
- `VerifyExpireMultipartUploads (aws: ExecuteScript)`-验证是否已为存储桶配置生命周期策略。

输出

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

描述

使用 Amazon Simple Storage Service (Amazon S3) Block Public Access 禁用公有 S3 存储桶的读写权限。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的[使用 Amazon S3 阻止公有访问](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3BucketName

类型：字符串

描述：(必需) 要限制对其的访问的 S3 存储桶。

AWS-EnableS3BucketEncryption

描述

为 Amazon Simple Storage Service (Amazon S3) 存储桶配置默认加密。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(必需) 要加密其内容的 S3 存储桶的名称。

- SSEAlgorithm

类型：字符串

默认值：AES256

描述：(可选) 用于默认 Server-side 加密的加密算法。

AWS-EnableS3BucketKeys

描述

AWS-EnableS3BucketKeys运行手册在您指定的亚马逊简单存储服务 (Amazon S3) 存储桶上启用存储桶密钥。此存储桶级密钥在新对象的生命周期中为其创建数据密钥。如果您未为KmsKeyId参数指定值，则默认加密配置将使用使用 Amazon S3 托管密钥 (SSE-S3) 的服务器端加密。

Note

使用 () 密钥 () 进行双层服务器端加密不支持 Amazon S3 存储桶密钥 AWS Key Management Service (AWS KMS DSSE-KMS)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BucketName

类型：字符串

描述：(必填) 您要为其启用存储桶密钥的 S3 存储桶的名称。

- KMSKeyId

类型：字符串

描述：(可选) 您要用于服务器端加密的 Amazon 资源名称 (ARN)、密钥 ID 或 AWS Key Management Service (AWS KMS) 客户托管密钥的密钥别名。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetEncryptionConfiguration
- s3:PutEncryptionConfiguration

文档步骤

- ChooseEncryptionType (aws: branch)-评估为KmsKeyId参数提供的值以确定是使用 SSE-S3 (AES256) 还是 SSE-KMS 将使用。

- PutBucketKeysKMS (aws: executeAwsApi)-使用指定的将true指定 S3 存储桶的BucketKeyEnabled属性设置为。KmsKeyId
- PutBucketKeysAES256 (aws: executeAwsApi)-将具有 AES256 加密true的指定 S3 存储桶的BucketKeyEnabled属性设置为。
- VerifyS3BucketKeysEnabled (aws: assertAwsResourceProperty)-验证目标 S3 存储桶上是否启用了存储桶密钥。

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

描述

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 运行手册将从您的 Amazon Simple Storage Service (Amazon S3) 存储桶策略中移除带有通配符 (Principal: * 或 Principal: "AWS": *) 的用于 Allow 操作的主体策略语句。带有条件的策略语句也会被删除。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- BucketName

类型：字符串

描述：(必需) 要修改其策略的 Amazon S3 存储桶的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutBucketPolicy

文档步骤

- aws:executeScript - 修改存储桶策略并验证带有通配符的主体策略语句已从您在 BucketName 参数中指定的 Amazon S3 存储桶中移除。

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

描述

AWSConfigRemediation-RestrictBucketSSLRequestsOnly 运行手册将创建一个 Amazon Simple Storage Service (Amazon S3) 存储桶策略语句，明确拒绝对您指定的 Amazon S3 存储桶的 HTTP 请求。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- BucketName

类型：字符串

描述：(必需) 要拒绝 HTTP 请求的 S3 存储桶的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

文档步骤

- aws:executeScript - 为在 BucketName 参数中指定的 S3 存储桶创建一个明确拒绝 HTTP 请求的存储桶策略。

AWSSupport-TroubleshootS3PublicRead

描述

AWSSupport-TroubleshootS3PublicRead 运行手册将诊断从您在 S3BucketName 参数中指定的公有 Amazon Simple Storage Service (Amazon S3) 存储桶读取对象时遇到的问题。还会分析 S3 存储桶中对象的设置子集。

[运行此自动化 \(控制台 \)](#)

限制

- 此自动化不会检查是否存在允许对对象进行公共访问的接入点。
- 此自动化不会评估 S3 存储桶策略中的条件密钥。
- 如果您使用的是 AWS Organizations，此自动化不会评估服务控制策略以确认是否允许访问 Amazon S3。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CloudWatchLogGroupName

类型：字符串

描述：(可选) 您要向其中发送自动化输出的 Amazon CloudWatch 日志组。如果找不到与您指定的值匹配的日志组，此自动化将使用该参数值创建一个日志组。此自动化创建的日志组的保留期为 14 天。

- CloudWatchLogStreamName

类型：字符串

描述：(可选) 您要将自动化输出发送到的 CloudWatch 日志流。如果找不到与您指定的值匹配的日志流，此自动化将使用该参数值创建一个日志流。如果您未为该参数指定一个值，此自动化将使用 ExecutionId 作为日志流的名称。

- HttpGet

类型：布尔值

有效值：true | false

默认：True

描述：(可选) 如果此参数设置为 true，此自动化将对您在 S3BucketName 中指定的对象发出部分 HTTP 请求。使用 Range HTTP 标头仅返回对象的第一个字节。

- IgnoreBlockPublicAccess

类型：布尔值

有效值：true | false

默认值：false

描述：(可选) 如果此参数设置为 true，则此自动化将忽略您在 S3BucketName 参数中指定的 S3 存储桶的公共访问屏蔽设置。不建议更改该参数的默认值。

- MaxObjects

类型：整数

有效值：1-25

默认：5

描述：(可选) 您在 S3BucketName 参数中指定的 S3 存储桶中要分析的对象数量。

- S3BucketName

类型：字符串

描述：(必需) 要排查问题的 S3 存储桶的名称。

- S3PrefixName

类型：字符串

描述：(可选) 要在 S3 存储桶中分析的对象的关键名称前缀。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的[对象密钥](#)。

- StartAfter

类型：字符串

描述：(可选) 您希望此自动化开始分析 S3 存储桶中对象的对象密钥名称。

- ResourcePartition

类型：字符串

有效值：aws |aws-us-gov |aws-cn

默认值：aws

描述：(必需) 您的 S3 存储桶所在的分区。

- 详细

类型：布尔值

有效值：true | false

默认值：false

描述：(可选) 要在自动化期间返回更多详细信息，请将此参数设置为 true。如果将此参数设置为 false，则只会返回警告和错误消息。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

仅当您希望自动化将日志数据发送到日志时，才需要logs:CreateLogStream、和logs:PutLogEvents权限。logs:CreateLogGroup CloudWatch

JSON

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

```

        "Action": [
            "iam:SimulateCustomPolicy",
            "iam:GetContextKeysForCustomPolicy",
            "s3:ListAllMyBuckets",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:PutRetentionPolicy",
            "s3:GetAccountPublicAccessBlock"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:GetObjectTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketRequestPayment",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPolicy",
            "s3:GetBucketAcl"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
        "Effect": "Allow"
    }
]
}

```

文档步骤

- `aws:assertAwsResourceProperty` - 确认 S3 存储桶存在并且可以访问。
- `aws:executeScript` - 返回 S3 存储桶位置和您的规范用户 ID。

- `aws:executeScript` - 返回对您的账户和 S3 存储桶的公共访问屏蔽设置。
- `aws:assertAwsResourceProperty` - 确认 S3 存储桶付款方被设置为 `BucketOwner`。如果在 S3 存储桶上启用 `Requester Pays`，此自动化将结束。
- `aws:executeScript` - 返回 S3 存储桶策略状态并确定其是否被视为公开。有关公有 S3 存储桶的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中[“公有”的含义](#)。
- `aws:executeAwsApi` - 返回 S3 存储桶策略。
- `aws:executeAwsApi` - 返回在 S3 存储桶策略中找到的所有上下文键。
- `aws:assertAwsResourceProperty` - 确认 S3 存储桶策略中是否有对 `GetObject` API 操作的明确拒绝。
- `aws:executeAwsApi` - 返回 S3 桶的访问控制列表 (ACL)。
- `aws:executeScript` - 如果您为 `CloudWatchLogGroupName` 参数指定值，则创建 CloudWatch 日志组和日志流。
- `aws:executeScript` - 根据您在运行手册输入参数中指定的值，评估自动化期间收集的任何 S3 存储桶设置是否阻止对象被公众访问。此脚本执行以下功能：
 - 评估公共访问屏蔽设置
 - 根据您在 `MaxObjects`、`S3PrefixName` 和 `StartAfter` 参数中指定的值返回 S3 存储桶中的对象。
 - 返回 S3 存储桶策略，以模拟从 S3 存储桶返回的对象的自定义 IAM policy。
 - 如果 `HttpGet` 参数设置为 `true`，则对返回的对象执行部分 HTTP 请求。使用 `Range` HTTP 标头仅返回对象的第一个字节。
 - 检查返回的对象的键名以确认它是以一个还是两个句点结尾。无法从 Amazon S3 控制台下载以句点结尾的对象键名。
 - 检查返回的对象的所有者是否匹配 S3 存储桶的所有者。
 - 检查对象的 ACL 是否向匿名用户授予 `READ` 或 `FULL_CONTROL` 权限。
 - 返回与对象关联的标签。
 - 使用模拟的 IAM policy 确认 `GetObject` API 操作的 S3 存储桶策略中是否明确拒绝此对象。
 - 返回对象的元数据以确认是否支持该存储类别。
 - 检查对象的服务器端加密设置，以确认是否使用 AWS Key Management Service (AWS KMS) 客户管理的密钥对对象进行加密。

输出

AnalyzeObjects.bucket

AnalyzeObjects.object

AWSsupport-ConfigureS3ReplicationSameAndCrossAccount

描述

AWSsupport-ConfigureS3ReplicationSameAndCrossAccount 自动化运行手册为相同账户或跨账户配置亚马逊简单存储服务 (Amazon S3) Simple Storage Service 在源存储桶和目标存储桶之间复制。此自动化支持复制使用服务器端加密、使用 Amazon S3 托管密钥 (SSE-S3) 和使用 (SSE-KMS) 进行服务器端加密 (SSE-KMS) 加密的存储桶。AWS Key Management Service 它还支持基于前缀和标签的选择性复制筛选、具有 15 分钟 SLA 的 Amazon S3 复制时间控制 (Amazon S3 RTC) 以及删除标记复制。自动化会执行以下操作：

- 验证输入参数和存储桶配置的兼容性。
- 检查源存储桶和目标存储桶的加密设置。
- 如果未作为输入提供，则创建一个具有相应复制权限的新 AWS Identity and Access Management (IAM) 角色。
- 根据指定的参数（前缀、标签或整个存储桶）配置复制规则。
- 如果尚未启用，则启用存储桶版本控制。
- 使用复制时间控制 (RTC) 和删除标记复制等可选功能设置复制配置。

Important

- 这种自动化不支持具有现有复制规则的存储桶。源存储桶不得有任何现有的复制配置。
- 如果未提供 S3 ReplicationRole 输入，此自动化会创建一个具有相应复制权限的新 IAM 角色。
- 这种自动化不会复制现有对象。Amazon S3 复制仅适用于启用复制配置 uploaded/created 后的对象。
- 要进行跨账户复制，您必须在目标账户中为一个 IAM 角色提供相应的 Amazon S3 操作和 AWS KMS 操作权限（如果存储桶使用 AWS KMS 加密）。
- 此自动化使用aws:approve操作，该操作会暂时暂停执行，直到指定的委托人批准配置更改。有关更多信息，[请参阅与批准者一起运行自动化](#)。

如何工作？

运行手册执行以下步骤：

- `ValidateInputParameters`：验证所有输入参数的正确性和兼容性，以确保复制配置正确。
- `PrepareApprovalMessage`：准备包含所有复制配置参数的批准消息，以供用户查看。
- `RequestApproval`：在源存储桶上添加 Amazon S3 复制配置之前，请先请求授权用户的批准。
- `CheckBucketEncryption`：检查源和目标 Amazon S3 存储桶的加密配置，以确定兼容的复制设置。
- `BranchOnEncryptionType`：基于 Amazon S3 存储桶加密类型分支执行，以便为 SSE-S3 或 SSE-KMS 加密存储桶应用适当的复制配置。
- `配置SSES3复制`：为使用服务器端加密和 Amazon S3 托管密钥 (SSE-S3) 加密的存储桶配置 Amazon S3 复制，包括 IAM 角色和复制规则。
- `配置 SSEKMSReplication`：为使用服务器端加密 AWS KMS (SSE-KMS) 加密的存储桶配置 Amazon S3 复制，包括 IAM 角色、KMS 密钥权限和复制规则。
- `CleanupResources`：如果未提供 S3 作为输入，则清理在复制配置失败期间创建 `ReplicationRole` 的 IAM 角色。

[运行此自动化 \(控制台 \)](#)

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `s3` : `ListBucket`
- `s3` : `GetBucketVersioning`
- `s3` : `GetEncryptionConfiguration`
- `s3` : `GetBucketLocation`
- `s3` : `GetReplicationConfiguration`
- `s3` : `PutBucketVersioning`
- `s3` : `PutReplicationConfiguration`
- `我是` : `ListRoles`
- `我是` : `GetRole`
- `我是` : `GetRolePolicy`
- `我是` : `ListRoleTags`
- `我是` : `ListAttachedRolePolicies`
- `我是` : `ListRolePolicies`

- 我是 : SimulatePrincipalPolicy
- 我是 : CreateRole
- 我是 : TagRole
- 我是 : PassRole
- 我是 : DeleteRole
- 我是 : DeleteRolePolicy
- 我是 : DetachRolePolicy
- 我是 : PutRolePolicy
- sts: GetCallerIdentity
- sns: Publish
- kms: GetKeyPolicy (当存储桶使用 SSE-KMS 时 , 同账号复制)
- kms: DescribeKey (当存储桶使用 SSE-KMS 时 , 同账号复制)
- kms: PutKeyPolicy (当存储桶使用 SSE-KMS 时 , 同账号复制)
- sts: AssumeRole (用于跨账户复制)

CrossAccountReplicationRole (适用于跨账户场景) :

要进行跨账户复制 , 您必须为 CrossAccountReplicationRole 目标账户提供以下权限 :

- s3 : ListBucket
- s3 : GetBucketVersioning
- s3 : GetBucketLocation
- s3 : GetBucketPolicy
- s3 : GetEncryptionConfiguration
- s3 : PutBucketVersioning
- s3 : PutBucketPolicy
- kms: GetKeyPolicy (当跨账户目标存储桶使用 SSE-KMS 时)
- kms: DescribeKey (当跨账户目标存储桶使用 SSE-KMS 时)
- kms: PutKeyPolicy (当跨账户目标存储桶使用 SSE-KMS 时)

S3ReplicationRole (客户提供的角色) :

如果您提供现有 S3ReplicationRole , 则它必须具有以下权限 :

- s3 : ListBucket
- s3 : GetBucketLocation
- s3 : GetReplicationConfiguration
- s3 : GetObjectVersionAcl
- s3 : GetObjectVersionTagging
- s3 : GetObjectVersionForReplication
- s3 : GetObjectTagging
- s3 : ReplicateObject
- s3 : ReplicateDelete
- s3 : ReplicateTags
- s3 : ObjectOwnerOverrideToBucketOwner
- kms: decrypt (对于 SSE-KMS 场景，来源 KMS 密钥)
- KMS: 加密 (对于 SSE-KMS 方案，使用目标 KMS 密钥)
- kms:GenerateDataKey (对于 SSE-KMS 场景，请使用目标 KMS 密钥)
- kms: ReEncrypt * (对于 SSE-KMS 方案，目标 KMS 密钥)

同账号复制AutomationAssumeRole策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::DESTINATION_BUCKET"
      ]
    }
  ]
}
```

```

    ],
  },
  {
    "Sid": "IAMReadOperations",
    "Effect": "Allow",
    "Action": [
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListRoleTags",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:SimulatePrincipalPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IAMListRolesForCleanup",
    "Effect": "Allow",
    "Action": "iam:ListRoles",
    "Resource": "*"
  },
  {
    "Sid": "IAMCreateAndTagRole",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:TagRole"
    ],
    "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {
      "StringLike": {
        "aws:RequestTag/AWSSupport-ConfigureS3ReplicationSameAndCrossAccount": "*"
      }
    }
  },
  {
    "Sid": "IAMPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      }
    }
  }
}

```

```

        }
    },
    {
        "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "STSGetCallerIdentity",
        "Effect": "Allow",
        "Action": "sts:GetCallerIdentity",
        "Resource": "*"
    },
    {
        "Sid": "SNSPublish",
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "SNS_TOPIC_ARN"
    },
    {
        "Sid": "KMSKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": [
            "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
            "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
        ]
    },
},

```

```

    {
      "Sid": "KMSKeyMutatingOperations",
      "Effect": "Allow",
      "Action": "kms:PutKeyPolicy",
      "Resource": [
        "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
        "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
      ],
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "ACCOUNT_ID"
        }
      }
    }
  ]
}

```

Note

只有当存储桶使用 SSE-KMS 加密时，才需要策略声明 (KMSKeyReadOperations 和 KMSKeyMutatingOperations)。

跨账户复制AutomationAssumeRole策略示例：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration"
      ],
    }
  ],
}

```

```

        "Resource": "arn:aws:s3:::SOURCE_BUCKET"
    },
    {
        "Sid": "IAMReadOperations",
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:ListRoleTags",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "IAMListRolesForCleanup",
        "Effect": "Allow",
        "Action": "iam:ListRoles",
        "Resource": "*"
    },
    {
        "Sid": "IAMCreateAndTagRole",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:TagRole"
        ],
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:RequestTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "IAMPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "s3.amazonaws.com"
            }
        }
    }
}

```

```

    }
  },
  {
    "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
      }
    }
  },
  {
    "Sid": "CrossAccountRoleAssumption",
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "CROSS_ACCOUNT_REPLICATION_ROLE_ARN"
  },
  {
    "Sid": "STSGetCallerIdentity",
    "Effect": "Allow",
    "Action": "sts:GetCallerIdentity",
    "Resource": "*"
  },
  {
    "Sid": "SNSPublish",
    "Effect": "Allow",
    "Action": "sns:Publish",
    "Resource": "SNS_TOPIC_ARN"
  },
  {
    "Sid": "KMSSourceKeyReadOperations",
    "Effect": "Allow",
    "Action": [
      "kms:GetKeyPolicy",
      "kms:DescribeKey"
    ]
  }
}

```

```

    ],
    "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
  },
  {
    "Sid": "KMSSourceKeyMutatingOperations",
    "Effect": "Allow",
    "Action": "kms:PutKeyPolicy",
    "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID",
    "Condition": {
      "StringEquals": {
        "kms:CallerAccount": "SOURCE_ACCOUNT_ID"
      }
    }
  }
]
}

```

Note

- 只有当源存储桶使用 SSE-KMS 加密时，才需要策略声明 (KMSSourceKeyReadOperations 和 KMSSourceKeyMutatingOperations)。
- 将 CROSS_ACCOUNT_REPLICATION_ROLE_ARN 替换为您向自动化提供的实际参数值。CrossAccountReplicationRole

CrossAccountReplicationRole策略示例：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3DestinationBucketReadOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",

```



```

        "s3:GetEncryptionConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET"
},
{
    "Sid": "KMSDestinationKeyReadOperations",
    "Effect": "Allow",
    "Action": [
        "kms:GetKeyPolicy",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
},
{
    "Sid": "KMSDestinationKeyMutatingOperations",
    "Effect": "Allow",
    "Action": "kms:PutKeyPolicy",
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "DESTINATION_ACCOUNT_ID"
        }
    }
}
]
}

```

Note

仅当目标存储桶使用 SSE-KMS 加密时，才需要 KMS 语句（KMSDestinationKeyReadOperations 和 KMSDestinationKeyMutatingOperations）。对于 SSE-S3 场景，请删除这些语句。

CrossAccountReplicationRole 信任策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "AUTOMATION_ASSUME_ROLE_ARN"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Note

将 AUTOMATION_ASSUME_ROLE_ARN 替换为您提供的实际参数值。
AutomationAssumeRole

S3 ReplicationRole 策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::SOURCE_BUCKET/*"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Sid": "S3DestinationBucketPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:ReplicateObject",
      "s3:ReplicateDelete",
      "s3:ReplicateTags"
    ],
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
  },
  {
    "Sid": "S3CrossAccountPermissions",
    "Effect": "Allow",
    "Action": "s3:ObjectOwnerOverrideToBucketOwner",
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
  },
  {
    "Sid": "KMSSourceKeyPermissions",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
  },
  {
    "Sid": "KMSDestinationKeyPermissions",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:GenerateDataKey",
      "kms:ReEncrypt*"
    ],
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/
DESTINATION_KMS_KEY_ID"
  }
]
}

```

Note

- 仅当存储桶使用 SSE-KMS 加密时，才需要 KMS 语句 (KMSSourceKeyPermissions 和 KMSTDestinationKeyPermissions)。
- 只有跨账户存储桶复制才需要 S3 CrossAccountPermissions 语句。

S3 ReplicationRole 信任策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (必填)：
 - 描述：(必填) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - SourceBucket (必填)：

- 描述：(必填) 将在其中创建或更新复制规则的源 Amazon S3 存储桶的名称。
- 类型：AWS::S3::Bucket::Name
- DestinationBucket (必填)：
 - 描述：(必填) 将对象复制到的目标 Amazon S3 存储桶的名称。
 - 类型：String
 - 允许的模式：`^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- SourceAccountId (必填)：
 - 描述：(必填) 源存储桶所在的 AWS 账户 ID。
 - 类型：String
 - 允许的模式：`^[0-9]{12,13}$`
- DestinationAccountId (必填)：
 - 描述：(必填) 目标存储桶所在的 AWS 账户 ID。
 - 类型：String
 - 允许的模式：`^[0-9]{12,13}$`
- SnsNotificationArn (必填)：
 - 描述：(必填) 用于自动化批准的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 的 ARN 主题。
 - 类型：String
 - 允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:sns:[a-z]{2}(-gov)?(-iso[a-z])?-[a-z]{2,10}-[0-9]{1,2}:\d{12}:[0-9a-zA-Z-_{1,256}](.fifo)?$`
- 批准者 (必填)：
 - 描述：(必填) user/role ARNs 授权批准自动化执行的 IAM 列表。
 - 类型：StringList
 - 允许的模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:.\d{12}:(user|role)/[\w+=,.\@\\-/+]+$`
- S3ReplicationRole (可选)：
 - 描述：(可选) 用于 Amazon S3 复制操作的现有 IAM 角色的 ARN。此角色必须具有从源存储桶读取和写入目标存储桶的权限，如果存储桶使用 SSE-KMS 加密，则包括 KMS 权限。如果未提供，则自动化将创建一个具有适当权限的新角色。

- 允许的模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::\d{12}:role/[\\w+=,.\@\\-/+]+$`
- 默认值：`""`
- `CrossAccountReplicationRole`（可选）：
 - 描述：（可选）自动化可以代入的目标账户中 IAM 角色的 ARN。这是跨账户复制所必需的。对于同账号复制，请将其留空。
 - 类型：`String`
 - 允许的模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::\d{12}:role/[\\w+=,.\@\\-/+]+$`
 - 默认值：`""`
- `ReplicateEntireBucket`（可选）：
 - 描述：（可选）如果设置为`true`，则将复制整个存储桶，并且前缀和标签必须为空。如果为`false`，则复制将基于指定的前缀或标记。
 - 类型：`Boolean`
 - 允许的值：`[true, false]`
 - 默认值：`true`
- `ReplicationRuleStatus`（可选）：
 - 描述：（可选）如果设置为`true`，则将启用创建的复制规则。如果设置为`false`，则创建的复制规则将设置为“已禁用”。
 - 类型：`Boolean`
 - 允许的值：`[true, false]`
 - 默认值：`true`
- `DeleteMarkerReplicationStatus`（可选）：
 - 描述：（可选）如果设置为`true`，则自动化将启用删除标记复制。
 - 类型：`Boolean`
 - 允许的值：`[true, false]`
 - 默认值：`false`
- `ReplicationTimeControl`（可选）：
 - 描述：（可选）如果设置为`true`，则启用具有 15 分钟 SLA 的 Amazon S3 复制时间控制 (Amazon S3 RTC)，以实现可预测的复制时间。

- 允许的值：[true, false]
- 默认值：false
- ReplicaModifications (可选) :
 - 描述：(可选) 如果设置为true，则允许复制对副本对象所做的元数据更改，从而允许将对复制对象的修改同步回源中。
 - 类型：Boolean
 - 允许的值：[true, false]
 - 默认值：false
- 前缀 (可选) :
 - 描述：(可选) 前缀过滤器，用于选择性复制具有特定键前缀的对象。前缀必须以尾部斜杠 (/) 结尾，才能正确筛选 Amazon S3 前缀。
 - 类型：String
 - 允许的模式：`^$|^([a-zA-Z0-9!_'\(\)\-\-])*\/+$`
 - 默认值：""
- 标签 (可选) :
 - 描述：(可选) JSON 标签数组，用于筛选要复制的对象。单个标签的格式：[{"Key": "TagKey", "Value": "TagValue"}]，多个标签的格式：[{"Key": "TagKey 1", "Value": "TagValue 1"}, {"Key": "TagKey 2", "Value": "TagValue 2"}]。
 - 类型：String
 - 允许的模式：`^\\[\\(\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\",\\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{0,256}\\\"\\}\\}\\(\\,\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\",\\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{0,256}\\\"\\}\\}\\)*\\)?\\$`
 - 默认值：[]

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- ValidateInputParameters:

验证所有输入参数的正确性和兼容性，以确保复制配置正确。

- PrepareApprovalMessage:

准备带有所有复制配置参数的批准消息，以供用户查看。

- RequestApproval:

在继续进行 Amazon S3 复制配置更改之前，请先请求授权用户的批准。

- CheckBucketEncryption:

检查源和目标 Amazon S3 存储桶的加密配置，以确定兼容的复制设置。

- BranchOnEncryptionType:

基于 Amazon S3 存储桶加密类型分支执行，以便为 SSE-S3 或 SSE-KMS 加密存储桶应用适当的复制配置。

- 配置SSES3复制：

为使用服务器端加密、使用 Amazon S3 托管密钥 (SSE-S3) 加密的存储桶配置 Amazon S3 复制，包括 IAM 角色和复制规则。

- 配置 SSEKMSReplication：

为使用服务器端加密 AWS KMS (SSE-KMS) 加密的存储桶配置 Amazon S3 复制，包括 IAM 角色、KMS 密钥权限和复制规则。

- CleanupResources:

当客户未提供 S3 时，清理在复制配置失败期间创建ReplicationRole 的 IAM 角色。

7. 完成后，查看配置SSES3复制步骤（对于 SSE-S3 加密存储桶）或配置SSEKMSReplication步骤（对于 SSE-KMS 加密存储桶）的输出，以了解执行结果，包括复制配置状态以及用于复制的 IAM 角色。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

AWSsupport-EmptyS3Bucket

描述

AWSSupport-EmptyS3Bucket 自动化运行手册使用生命周期过期配置规则清空现有的亚马逊简单存储服务 (Amazon S3) 存储桶。

Important

- 不支持启用了多重身份验证 (MFA) 的 Amazon S3 存储桶。
- 本运行手册修改的生命周期规则将永久删除指定 Amazon S3 存储桶中的所有对象及其版本。您无法恢复永久删除的对象。有关更多信息，请查看[过期对象](#)。

如何工作？

运行手册AWSSupport-EmptyS3Bucket执行以下高级步骤：

- 如果启用，则暂停存储桶版本控制。
- 更新存储桶策略以拒绝任何 s3:PutObject API 调用（以防止在清空时上传新的内容）。
- 更新生命周期规则以根据输入参数中指定的过期天数删除所有对象。

Note

- 使用 Amazon S3 对象锁定保护的版本不会被生命周期配置删除或覆盖。
- 删除过程是异步的，运行手册执行完成后可能需要一段时间才能完成。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

该 AutomationAssumeRole 参数需要以下操作才能成功使用运行手册：

- ssm : DescribeAutomationExecutions
- ssm : GetAutomationExecution
- s3 : GetBucketVersioning
- s3 : PutBucketVersioning
- s3 : GetBucketPolicy
- s3 : GetBucketLifecycleConfiguration
- s3 : GetLifecycleConfiguration
- s3 : PutBucketPolicy
- s3 : PutBucketLifecycleConfiguration
- s3 : PutLifecycleConfiguration
- s3 : DeleteBucketPolicy
- s3 : DeleteBucketLifecycle

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-EmptyS3Bucket](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3BucketName：

您要清空的 Amazon S3 存储桶的名称。

- SNSTopicArn：

提供亚马逊 SNS 主题的 ARN 以获得批准通知。此 Amazon SNS 主题用于在自动化执行期间按要求发送批准通知。

- ApproverIAM :

提供能够批准或拒绝操作的 AWS 经过身份验证的委托人列表。批准者的最大数量为 10。您可以使用以下任何一种格式来指定委托人：AWS Identity and Access Management (IAM) 用户名、IAM 用户 ARN、IAM 角色 ARN 或 IAM 代入角色用户 ARN。

- MinimumRequiredApprovals (可选) :

恢复自动化所需的最小批准数。如果未指定值，则系统默认为 1。此参数的值必须为正数。此参数的值不能超过 approverIAM 参数定义的批准者数量。

- NoncurrentVersionExpirationDays (可选) :

指定非当前对象版本过期的天数。到期后，Amazon S3 将永久删除非当前对象版本。

- 默认值：1

- 最大值：365

- ExpirationDays (可选) :

以天数形式指定对象生命周期的到期时间。

- 默认值：1

- 最大值：365

- AbortIncompleteMultipartUpload (可选) :

指定 Amazon S3 在未完成的分段上传开始后等待的天数，然后才会永久删除上传的所有部分。

- 默认值：1

- 最大值：365

- 致谢 :

请阅读本自动化操作手册所执行操作的完整详细信息，Yes, I understand and acknowledge如果您确认这些步骤，请表示同意。

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

SNSTopicArn
(Required) The ARN of the Amazon Simple Notification Service (Amazon SNS) Topic for approval notification. This SNS topic is used to send the approval notifications required during the automation execution.

MinimumRequiredApprovals
(Optional) The minimum number of approvals required to resume the automation. If you don't specify a value, the system defaults to one. The value for this parameter must be a positive number. The value for this parameter can't exceed the number of approvers defined in the 'ApproverIAM' parameter.

ExpirationDays
(Optional) Specify the expiration for the lifecycle of the object in days. Default value is 1 and max value is 365.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps. ****Important:**** You cannot recover permanently removed objects. For more information please review [Expiring objects] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-expire-general-considerations.html>).

S3BucketName
(Required) The name of the Amazon S3 bucket you want to empty.

ApproverIAM
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

NoncurrentVersionExpirationDays
(Optional) Specify the number of days when noncurrent object versions expire. Upon expiration, Amazon S3 permanently deletes the noncurrent object versions. Default value is 1 and max value is 365.

AbortIncompleteMultipartUpload
(Optional) Specify the days since the initiation of an incomplete multipart upload that Amazon S3 will wait before permanently removing all parts of the upload. Default value is 1 and max value is 365.

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- **checkConcurrency:**

确保只有一次针对指定的 Amazon S3 存储桶执行此运行手册。如果 runbook 发现另一个针对相同存储桶名称的正在执行的执行，则会返回错误并结束。

- **getBucketVersioningConfiguration:**

获取指定 Amazon S3 存储桶的版本控制状态。

- **branchOnStoppingIfMFADeleteEnabled** (有条件的)：

如果在指定的 Amazon S3 存储桶上启用了多重身份验证 (MFA)，则停止自动化。

- **approvalToMakeChangesToTheProvidedS3Bucket:**

等待指定委托人批准后才能禁用存储桶版本控制并更新指定 Amazon S3 存储桶的存储桶策略和生命周期规则配置。

- **branchOnBucketVersioningStatus** (有条件的)：

如果在指定的 Amazon S3 存储桶上启用了版本控制，请将其禁用，否则请继续更新存储桶策略和生命周期配置。

- **suspendBucketVersioning:**

暂停指定 Amazon S3 存储桶的版本控制状态。

- **updateBucketPolicyAndLifeCycleConfiguration:**

添加或更新存储桶策略以拒绝所有 `s3:PutObject` 请求，并根据用户提供的输入参数更新生命周期配置以使对象过期。

- **branchOnFailingIfBucketPropertiesNotUpdated** (有条件的) :

检查 `updateBucketPolicyAndLifeCycleConfiguration` 步骤的状态，如果自动更改了原始存储桶版本控制状态，则尝试恢复原始存储桶版本控制状态。

- **branchOnFailureOriginalVersioningStatus** (有条件的) :

失败时，分支以确定原始版本控制状态。如果此自动化已启用并暂停，请尝试再次启用。

- **onFailureRestoreBucketVersioning**

恢复指定 Amazon S3 存储桶的启用版本控制状态。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

Execution has been initiated.

Execution detail: AWSSupport-EmptyS3Bucket

Cancel execution

Actions

▶ Execution description

▼ Outputs

updateBucketPolicyAndLifecycleConfiguration.Message

===== Execution Result =====

INFO: Getting the configured lifecycle rules for the S3 Bucket: sample-not-empty-bucket
INFO: Getting bucket policy for S3 Bucket: sample-not-empty-bucket
INFO: Creating new bucket policy to deny any s3:PutObject API calls (to prevent new uploads while it is being emptied).
INFO: Creating a new lifecycle rule to delete all the objects according to the expiration days specified in the input parameters
INFO: The bucket updates have been successfully completed.
Upon the expiration of items, as specified in the parameters, the bucket will be emptied.
Meanwhile, S3 'put object' requests are denied by the bucket policy to prevent the upload of new items.

Execution status

Overall status

Success

Failed

0

All executed steps

7

Cancelled

0

Succeeded

7

TimedOut

0

Executed steps (10)

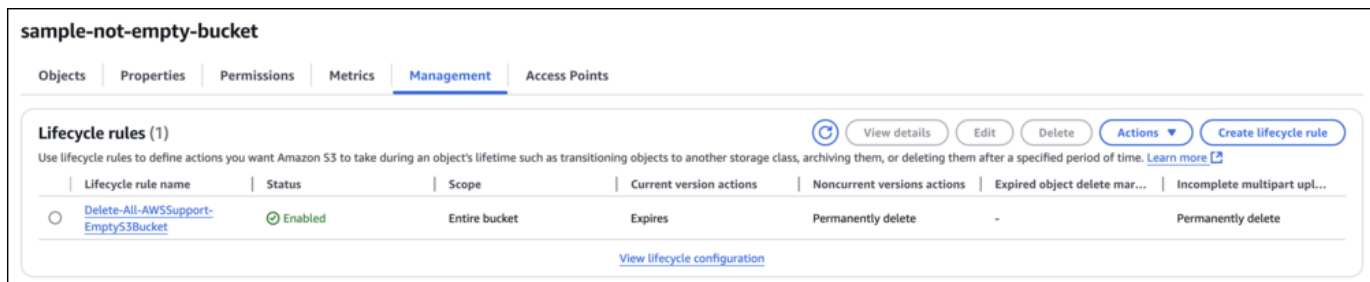
Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time
17e09354-6a90-4216-9797-a9d6fa18d57c	1	checkConcurrency	aws:executeScript	Success	Wed, 18 Dec 2024 08:01:54 GM
44bc75db-0bd9-44c1-9537-0b9ff9eea87a	2	getBucketVersioningConfiguration	aws:executeAwsApi	Success	Wed, 18 Dec 2024 08:02:08 GM
1e942013-e886-4fce-b685-bc8e578bcb2a	3	branchOnStoppingIfMFADeleteEnabled	aws:branch	Success	Wed, 18 Dec 2024 08:02:09 GM
742066ac-39a8-4699-8aa4-13a7a8b0239f	4	approvalToMakeChangesToTheProvidedS3Bucket	aws:approve	Success	Wed, 18 Dec 2024 08:02:09 GM
34c276bb-f7e3-43f8-a89f-8d457040cc31	5	branchOnBucketVersioningStatus	aws:branch	Success	Wed, 18 Dec 2024 08:03:24 GM
5f3efb16-d6f8-441e-b090-ab6c88ab2a9d	6	updateBucketPolicyAndLifecycleConfiguration	aws:executeScript	Success	Wed, 18 Dec 2024 08:03:25 GM
739dd72a-e7de-42d9-900a-7a0aa5e826d0	7	branchOnFailingIfBucketPropertiesNotUpdated	aws:branch	Success	Wed, 18 Dec 2024 08:03:29 GM
f97fc493-3d62-4884-901f-dcc2a2a3bcd0	8	suspendBucketVersioning	aws:executeAwsApi	Pending	-
4b02a204-8de7-49c8-b079-e94741c40a37	9	branchOnFailureOriginalVersioningStatus	aws:branch	Pending	-
92645daf-8587-4947-bc53-b4c440d07f84	10	onFailureRestoreBucketVersioning	aws:executeAwsApi	Pending	-

成功执行

此工作流程更新了存储桶的生命周期规则。将根据Delete-All-AWSSupport-EmptyS3-Bucket生命周期策略删除对象。



- 失败执行

将不执行部分删除。如果执行失败，则会回滚生命周期和其他存储桶设置。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [Support 自动化工作流程](#)

有关管理 Amazon S3 存储桶和对象的更多信息，请参阅[清空存储桶](#)。

AWSSupport-TroubleshootS3EventNotifications

描述

AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager 自动化运行手册可帮助对配置了 AWS Lambda 函数、亚马逊简单通知服务 (Amazon SNS) 主题或亚马逊简单队列服务 (Amazon SQS) Simple Queue Service 队列的亚马逊简单存储服务 (Amazon S3) 存储桶事件通知进行故障排除。它提供了配置设置报告，其中包含使用 Amazon S3 存储桶作为目标事件通知配置的不同资源。

如何工作？

运行手册执行以下步骤：

- 检查 Amazon S3 存储桶是否存在于执行所在AWSSupport-TroubleshootS3EventNotifications的同一个账户中。
- 使用 API 获取配置为 Amazon S3 存储桶事件通知的目标资源（AWS Lambda 函数、Amazon SNS 主题或亚马逊 SQS 队列）。[GetBucketNotificationConfiguration](#)

- 验证目标资源是否存在，然后查看目标资源的基于资源的策略，以确定是否允许 Amazon S3 向目标发布内容。
- 如果您使用 AWS Key Management Service (AWS KMS) 密钥加密了目标，则会检查密钥策略以确定是否允许 Amazon S3 访问。
- 生成所有目标资源检查的报告。

Important

- 只有当 Amazon S3 存储桶拥有者与执行自动化运行手册的所有者相同时 AWS 账户，此运行手册才能评估事件通知配置。
- 此外，本运行手册无法评估托管在其他 AWS 账户资源中的目标资源的策略。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3 BucketName

类型：AWS::S3::Bucket::Name

描述：(必填) 配置了事件通知的 Amazon S3 存储桶的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:GetBucketNotification
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sns:GetTopicAttributes
- kms:GetKeyPolicy
- kms:DescribeKey
- kms:ListAliases
- lambda:GetPolicy
- lambda:GetFunction
- iam:GetContextKeysForCustomPolicy
- iam:SimulateCustomPolicy
- iam:ListRoles
- ssm:DescribeAutomationStepExecutions

自动化承担角色的 IAM policy 示例

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permission",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
},
{
    "Sid": "S3PermissionGetBucketNotification",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketNotification"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
},
{
    "Sid": "SQSPermission",
    "Effect": "Allow",
    "Action": [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
    ],
    "Resource": "arn:aws:sqs:us-
east-1:111122223333:*"
},
{
    "Sid": "SNSPermission",
    "Effect": "Allow",
    "Action": [
        "sns:GetTopicAttributes"
    ],
    "Resource": "arn:aws:sns:us-
east-1:111122223333:*"
},
{
    "Sid": "KMSPermission",
    "Effect": "Allow",
    "Action": [
        "kms:GetKeyPolicy",
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource": "arn:aws:kms:us-
east-1:111122223333:key/key-id"
},
{

```

```

        "Sid": "LambdaPermission",
        "Effect": "Allow",
        "Action": [
            "lambda:GetPolicy",
            "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:us-  
east-1:111122223333:function:*"
    },
    {
        "Sid": "IAMPermission",
        "Effect": "Allow",
        "Action": [
            "iam:GetContextKeysForCustomPolicy",
            "iam:SimulateCustomPolicy",
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermission",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationStepExecutions"
        ],
        "Resource": "*"
    }
]
}

```

说明

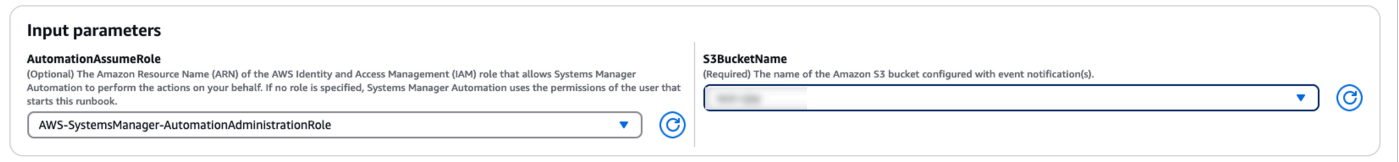
按照这些步骤对自动化进行配置：

1. [AWSsupport-TroubleshootS3EventNotifications](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- S3BucketName (必填) :

配置了事件通知的 Amazon S3 存储桶的名称。



Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

S3BucketName
(Required) The name of the Amazon S3 bucket configured with event notification(s).

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- ValidateInputs

验证提供的 Amazon S3 存储桶属于执行自动化的同一个账户，并获取存储桶托管的区域。

- GetBucketNotificationConfiguration

调用 GetBucketNotificationConfiguration API 来查看使用 Amazon S3 存储桶配置的事件通知并格式化输出。

- BranchOnSQSResourcePolicy

关于事件通知中是否有 Amazon SQS 资源的分支。

- 验证SQSResource策略

验证有关亚马逊 SQS 队列属性的资源策略是否具有 `sqs:SendMessage` 具有 Amazon S3 的权限。如果 Amazon SQS 资源已加密，则会检查加密是否使用默认 AWS KMS 密钥，即 `aws/sqs` 检查密 AWS KMS 策略是否具有对 Amazon S3 的权限。

- BranchOnSNSResourcePolicy

关于事件通知中是否有 Amazon SNS 资源的分支。

- 验证SNSResource策略

验证 Amazon SNS 上的资源策略主题属性是否具有 `sns:Publish` 具有 Amazon S3 的权限。如果 Amazon SNS 资源已加密，则会检查加密是否使用默认 AWS KMS 密钥，即 `aws/sns` 检查密 AWS KMS 策略是否具有 Amazon S3 的权限。

- BranchOnLambdaFunctionResourcePolicy

关于事件通知中是否有 AWS Lambda 功能的分支。

- ValidateLambdaFunctionResourcePolicy

验证 AWS Lambda 函数上的资源策略是否具有 Amazon S3 的 `lambda:InvokeFunction` 权限。

- GenerateReport

返回运行手册步骤、输出的详细信息以及解决使用 Amazon S3 存储桶配置的事件通知的任何问题的建议。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- 亚马逊 SQS 事件通知

如果使用 Amazon S3 存储桶配置了 Amazon SQS 目标通知，则在检查结果旁边会显示亚马逊 SQS 队列列表。该报告包括 Amazon SQS 资源检查、Amazon SQS 访问策略检查 AWS KMS、密钥检查、密钥状态检查 AWS KMS AWS KMS 和密钥策略检查。

- 亚马逊 SNS 事件通知

如果使用 Amazon S3 存储桶配置了 Amazon SNS 目标通知，则在检查结果旁边会显示亚马逊 SNS 主题列表。该报告包括 Amazon SNS 资源检查、Amazon SNS 访问策略检查 AWS KMS、密钥检查、密钥状态检查 AWS KMS AWS KMS 和密钥策略检查。

- AWS Lambda 活动通知

如果使用 Amazon S3 存储桶配置了 AWS Lambda 目标通知，则会在检查结果旁边显示 Lambda 函数列表。该报告包括 Lambda 资源检查和 Lambda 访问策略检查。

```

▼ Outputs
generateReport.Output
-----
| Amazon S3 Event Notification Troubleshooting Results for S3 Bucket |
|-----|
| Amazon SQS Event Notifications |
|-----|
| SQS Queue: 1. arn:aws:sqs:us-east-1:123456789012:SAW-Core-TroubleshootS3EventNotification-EncryptedQueue | KMS Key: |
| SQS resource check | ✓[PASSED]: The resource exists in the S3 Bucket Region. |
| SQS access policy check | ✓[PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓[PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✗[FAILED]: The KMS key is disabled. |
| KMS key policy check | ✓[PASSED]: The resource policy is properly configured for use with S3 Bucket. |
|-----|
| Amazon SNS Event Notifications |
|-----|
| SNS Topic: 1. arn:aws:sns:us-east-1:123456789012:3CoreInfra-TestSNSTopic-1dW0EaySLdmr | KMS Key: alias/aws/sns |
| SNS resource check | ✓[PASSED]: The resource exists in the S3 Bucket Region. |
| SNS access policy check | ✓[PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓[PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✓[INFO]: Not Applicable. |
| KMS key policy check | ✗[FAILED]: Amazon S3 Event Notifications does not support using SQS or SNS targets encrypted using AWS managed keys, i.e., aws/sns or aws/sqs respectively. |
|-----|
| AWS Lambda Event Notifications |
|-----|
| Lambda Function: 1. arn:aws:lambda:us-east-1:123456789012:function:SAW-Core-TroubleshootS3EventNotification-LambdaFunction |
| Lambda resource check | ✓[PASSED]: The resource exists in the S3 Bucket Region. |
| Lambda access policy check | ✗[FAILED]: No resource policies found on the resource. Please update the resource with a valid policy using this guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/grant-destin

```

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

AWSSupport-ContainS3Resource

描述

该AWSSupport-ContainS3Resource运行手册为文章《[支持自动化工作流程 \(SAW\) 运行手册：包含受损的 AWS Amazon S3 存储桶](#)》中概述的程序提供了自动解决方案

Important

- 本运行手册执行各种需要提升权限的操作，例如修改 Amazon S3 存储桶策略、标签和公共访问配置。这些操作可能会导致权限提升或影响依赖目标 Amazon S3 存储桶的其他工作负载。您应查看向AutomationAssumeRole参数指定的角色授予的权限，并确保这些权限适用于预期用例。您可以参考以下 AWS 文档，了解有关 IAM 权限的更多信息：[Identity and Access Management \(IAM\) PermissionsAWS AWS Systems Manager Automation Permissions](#)。
- 此运行手册执行的变异操作可能会导致您的工作负载不可用或中断。具体而言，该Contain操作会阻止对指定 Amazon S3 存储桶的所有访问权限，但SecureRoles参数中指定的角色除外。这可能会影响依赖目标 Amazon S3 存储桶的任何应用程序或服务。
- 在Contain操作期间，此运行手册可能会额外创建一个 Amazon S3 存储桶（由BackupS3BucketName参数指定）来存储原始存储桶配置的备份（如果尚不存在）。
- 如果将Action参数设置为Restore，则本运行手册会尝试根据存储在存储桶中的备份将 Amazon S3 存储BackupS3BucketName桶的配置恢复到其原始状态。但是，还原过程可能会失败，从而使 Amazon S3 存储桶处于不一致的状态。运行手册提供了在出现此类故障时手动恢复的说明，但您应该做好在恢复过程中处理潜在问题的准备。

建议在生产环境中执行运行手册之前，请仔细阅读运行手册，了解其潜在影响，并在非生产环境中对其进行测试。

如何工作？

根据资源类型和操作，此运行手册的操作方式有所不同：

- 对于 Amazon S3 通用存储桶Containment：自动化会阻止对存储桶的公开访问，禁用 ACL 配置，强制执行存储桶所有者对象所有权，并设置限制性存储桶策略，除了允许列出的 IAM 角色外，拒绝对存储桶执行所有 Amazon S3 操作。
- 对于 Amazon S3 通用对象Containment：自动化会阻止对存储桶的公开访问，禁用 ACL 配置，强制执行存储桶所有者对象所有权，并设置限制性存储桶策略，除了允许列出的 IAM 角色外，拒绝对该对象执行所有 Amazon S3 操作。
- 对于 Amazon S3 目录存储桶Containment：自动化设置了限制性存储桶策略，除了允许列出的 IAM 角色外，拒绝对该存储桶执行所有 Amazon S3 操作。
- 对于 Amazon S3 通用存储桶Restore：自动化会将封锁公共访问配置、存储桶 ACL 配置、存储桶所有者对象所有权和存储桶策略恢复到包含之前的初始配置。
- 对于 Amazon S3 通用对象Restore：自动化会将阻止公共访问配置、存储桶 ACL 配置、对象 ACL 配置、存储桶所有者对象所有权和存储桶策略恢复到包含之前的初始配置。
- 对于 Amazon S3 目录存储桶Restore：自动化会将存储桶策略恢复到包含之前的初始配置。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- s3 : CreateBucket
- s3 : DeleteBucketPolicy

- s3 : DeleteObjectTagging
- s3 : GetAccountPublicAccessBlock
- s3 : GetBucketAcl
- s3 : GetBucketLocation
- s3 : GetBucketOwnershipControls
- s3 : GetBucketPolicy
- s3 : GetBucketPolicyStatus
- s3 : GetBucketTagging
- s3 : GetEncryptionConfiguration
- s3 : GetObject
- s3 : GetObjectAcl
- s3 : GetObjectTagging
- s3 : GetReplicationConfiguration
- s3 : ListBucket
- s3 : PutAccountPublicAccessBlock
- s3 : PutBucketACL
- s3 : PutBucketOwnershipControls
- s3 : PutBucketPolicy
- s3 : PutBucketPublicAccessBlock
- s3 : PutBucketTagging
- s3 : PutBucketVersioning
- s3 : PutObject
- s3 : PutObjectAcl
- s3express : CreateSession
- s3express : DeleteBucketPolicy
- s3express : GetBucketPolicy
- s3express : PutBucketPolicy
- ssm : DescribeAutomationExecutions

以下是 IAM 策略的示例，该策略为以下各项授予必要权限AutomationAssumeRole：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketACL",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ExpressPermissions",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateSession",
        "s3express:DeleteBucketPolicy",

```

```

        "s3express:GetBucketPolicy",
        "s3express:PutBucketPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SSMPermissions",
    "Effect": "Allow",
    "Action": [
      "ssm:DescribeAutomationExecutions"
    ],
    "Resource": "*"
  }
]
}

```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-ContainS3Resource](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - BucketName (必填)：
 - 描述：(必填) Amazon S3 存储桶的名称。
 - 类型：AWS::S3::Bucket::Name
 - 操作 (必填)：
 - 描述：(必填) 选择Contain隔离 Amazon S3 资源或Restore尝试将资源配置从先前备份恢复到其原始状态。
 - 类型：字符串
 - 允许的值：Contain|Restore
 - DryRun (可选)：
 - 描述：(可选) 当设置为 true 时，自动化不会对目标 Amazon S3 资源进行任何更改，而是输出它本来会尝试更改的内容。默认值：真。
 - 类型：布尔值
 - 允许的值：true|false

- BucketKeyName (可选) :
 - 描述 : (可选) 您要包含或恢复的 Amazon S3 对象的密钥。在对象级收容期间使用。
 - 类型 : 字符串
 - 允许的模式 : `^[a-zA-Z0-9\\.\_-\\!*'()/]{0,1024}$`
- BucketRestrictAccess (视情况而定) :
 - 描述 : (视情况而定) 在运行控制操作后将被允许访问目标 Amazon S3 资源的 IAM 用户或角色的 ARN。Action 设置为 Contain 时需要此参数。
 - 类型 : StringList
 - 允许的模式 : `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- TagIdentifier (可选) :
 - 描述 : (可选) 格式为 Key=BatchId, Value=78925 的标签, 该标签将添加到此运行手册在包含工作流程中创建或修改的资源中。
 - 类型 : 字符串
 - 允许的模式 : `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{0,128}$`
- BackupS3BucketName (视情况而定) :
 - 描述 : (视情况而定) Amazon S3 存储桶, 用于在设置Action为时备份目标资源配置, Contain或从设置Action为时恢复配置Restore。
 - 类型 : AWS::S3::Bucket::Name
- BackupS3KeyName (视情况而定) :
 - 描述 : (视情况而定) 如果设置Action为Restore, 则指定自动化用于尝试恢复目标资源配置的 Amazon S3 密钥。
 - 类型 : 字符串
 - 允许的模式 : `^[a-zA-Z0-9\\.\_-\\!*'()/]{0,1024}$`
- BackupS3BucketAccess (视情况而定) :
 - 描述 : (视情况而定) 在运行控制操作后将被允许访问备份 Amazon S3 存储桶的 IAM 用户或角色的 ARN。当是时, 此参数是必需Action的Contain。
 - 类型 : StringList
 - 允许的模式 : `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`

- AutomationAssumeRole (可选) :
 - 描述 : (可选) 允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。
 - 类型 : AWS::IAM::Role::Arn

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤 :

- validateRequiredInputs

根据指定的操作验证所需的自动化输入参数。

- assertBucketExists

检查目标 Amazon S3 存储桶是否存在并且可以访问。

- backupBucketPre支票

检查备份 Amazon S3 存储桶是否有可能向公众授予对其对象的读取或写入权限。

- backupTargetBucket元数据

描述目标 Amazon S3 存储桶的当前配置 , 并将备份上传到指定的备份 Amazon S3 存储桶。

- 容器桶

执行存储桶级别的操作以包含目标 Amazon S3 存储桶。

- BranchOnActionAndMode

根据输入参数 “操作” 和 “分支自动化” DryRun。

- RestoreInstanceConfiguration

从备份中恢复 Amazon S3 存储桶配置。

- containFinalOutput

以可读的格式整合控制活动。

- ReportContain

输出遏制操作的试运行详细信息。

- ReportRestore

输出恢复操作的试运行详细信息。

- ReportRestoreFailure

提供在恢复工作流程失败的情况下恢复 Amazon S3 存储桶原始配置的说明。

- ReportContainmentFailure

提供在控制工作流程失败的情况下恢复 Amazon S3 存储桶原始配置的说明。

- FinalOutput

输出遏制操作的详细信息。

7. 执行完成后，请查看“输出”部分，了解执行的详细结果：

- ContainFinalOutput. 输出

当设置为 False 时DryRun，输出此运行手册执行的遏制操作的详细信息。

- RestoreFinalOutput. 输出

当设置为 False 时DryRun，输出此运行手册执行的还原操作的详细信息。

- 包含 3ResourceDryRun. 输出

设置为 Tr DryRun ue 时，输出此运行手册执行的遏制操作的详细信息。

- 恢复 3ResourceDryRun. 输出

设置为 True 时DryRun，输出此运行手册执行的还原操作的详细信息。

- ReportContainmentFailure. 输出

提供在控制工作流程失败的情况下恢复目标 Amazon S3 资源原始配置的说明。

- ReportRestoreFailure. 输出

提供在恢复工作流程失败的情况下恢复目标 Amazon S3 资源原始配置的说明。

参考

Systems Manager Automation

- [运行此自动化 \(控制台 \)](#)

- [运行自动化](#)

- [设置自动化](#)

- [Support 自动化工作流程](#)

Amazon SES

AWS Systems Manager Automation 为 Amazon 简单电子邮件服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSSupport-AnalyzeSESMessageSendingStatus](#)
- [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#)

AWSSupport-AnalyzeSESMessageSendingStatus

说明

AWSSupport-AnalyzeSESMessageSendingStatus 自动化运行手册汇总了未送达电子邮件的电子邮件发送状态，并为您提供解决未送达原因的建议。该运行手册检索存储在亚马逊 SES 发布的亚马逊 CloudWatch 日志组中的亚马逊简单电子邮件服务 (Amazon SES) Simple Email SES 电子邮件发送事件。有关 Amazon SES 事件发布的详细信息，请参阅[使用亚马逊简单电子邮件服务监控事件发布](#)。该运行手册还提供了电子邮件发送的摘要和时间表，以及可能影响未送达电子邮件的建议。你可以在每次执行的输出部分找到这些消息。请注意，此运行手册只能在部署事件存储之后对事件进行故障排除。

如何工作？

运行手册执行以下步骤：

- 检查同一 CloudWatch logs 组的并发自动化执行情况。
- 分析与自动化参数 IDs 给出的消息对应的 Amazon SES 事件。
- 将交付摘要输出到自动化执行的输出部分。

Important

- 在执行本运行手册之前，您必须将已发布的 Amazon SES 事件存储到由自动化参数指定的 CloudWatch 日志组中。本运行手册仅分析存储在日志组中的 Amazon SES 事件。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- logs:StartQuery
- logs:GetQueryResults
- ses:GetIdentityMailFromDomainAttributes
- ses:GetSendQuota
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-AnalyzeSESMessagesSendingStatus](#)在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化)。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - MessageIds (必填)

以逗号分隔您要分析 IDs 的亚马逊简单电子邮件服务事件的亚马逊简单电子邮件服务消息。

- CloudWatchLogsGroup （可选）

存储亚马逊简单电子邮件服务事件的 Amazon L CloudWatch ogs 组。默认日志组名称为 ``/ses/sending_event_logs``。如果您想使用默认日志组以外的其他日志组，请在此字段中输入您的日志组名称。“，

- QueryStartTime （可选）

事件分析的时间范围的开始时间。有效的时间格式为 ISO8601 （例如 ``yyyy-mm-ddthh: mm:ss``、``1970-01-01T 00:00:00``）。默认日期时间为 30 天前。

- QueryEndTime （可选）

事件分析的时间范围的结束时间。有效的时间格式为 ISO8601 （例如 ``yyyy-mm-ddthh: mm:ss``、``1970-01-01T 00:00:00``）。默认日期时间为当前时间。

Input parameters

AutomationAssumeRole

(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

CloudWatchLogsGroup

(Optional) The Amazon CloudWatch Logs group which stores Amazon SES events. The default log group name is ``/ses/sending_event_logs``. If you would like to utilize another log group than the default log group, please enter your log group name in this field.

/ses/sending_event_logs

QueryEndTime

(Optional) The end time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is the current time.

String

MessageIds

(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

StringList

QueryStartTime

(Optional) The start time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is 30 days ago.

String

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- CheckConcurrency:

确保此运行手册只执行一次针对 Amazon CloudWatch Logs 组。如果 runbook 发现另一个针对同一日志组的执行，则会返回错误并结束。

- AnalyzeSesEvents:

分析存储在由自动化参数指定的亚马逊 CloudWatch 日志组中的亚马逊简单电子邮件服务事件。

- **OutputFailureReason:**

步骤失败时输出执行AnalyzeSESMessagesSendingStatus步骤失败消息。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

- 对因退信而未送达的电子邮件进行分析的输出

由于退信而未到达目标邮箱的电子邮件的自动化执行输出。

```
▼ Outputs

OutputFailureReason.FailureReason
No output available yet because the step is not successfully executed

AnalyzeSesEvents.ResultMessage
==== Delivery summary of the message ID [REDACTED] ====
SES received bounces or complaints.

==== Timeline of [REDACTED] =====
[2024-08-21 06:22:58.193000+00:00] Your email message was sent from SES.
[2024-08-21 06:22:58.193000+00:00] SES received a bounce from [REDACTED].
Bounce type: Permanent(General)
Bounce sources:
- email address: [REDACTED] diagnostic code: "smtp; 550 5.1.1 user unknown"

==== Next Action ====
Please fix the issues described in the delivery error messages returned from the destination email servers in the Timeline section. In the case you received s

==== Recommendations for arn:aws:ses:[REDACTED] =====
- The SES account in this region seems to be in the sandbox environment. If you haven't requested the production access, please consider to move out of the san
```

参考

Systems Manager Automation

- [运行此自动化 \(控制台\)](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流登录页面](#)

AWSsupport-DeploySESSendingLogsToCloudWatchLogs

描述

AWSsupport-DeploySESSendingLogsToCloudWatchLogs 自动化运行手册可帮助配置亚马逊简单电子邮件服务 (Amazon SES) Service 将事件发布到 CloudWatch 亚马逊日志CloudWatch (日志) 所需

的基础设施。本运行手册设置了捕获电子邮件发送事件并将其存储在 CloudWatch 日志中以进行监控和分析所需的组件。有关 Amazon SES 事件发布的更多信息，请参阅[使用 Amazon SES 事件发布监控电子邮件发送](#)。

当 `ApproveDeployAnalyticEnvironment` 参数设置为 `approve`，此运行手册会在您的 AWS 账户中创建新 AWS 资源。除非设置为 `no`，否则 CloudFormation 堆栈将在 `SleepTime` 参数中指定的时间之后自动删除。

如何工作？

此运行手册执行以下操作：

- 列出已为亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题或传送流配置了事件目标的现有配置集。
- 当 `ApproveDeployAnalyticEnvironment` 参数设置为 `approve` 时，创建 Amazon SES 事件发布到 CloudWatch 日志所需的基础设施。

当 `ApproveDeployAnalyticEnvironment` 参数设置为 `approve`，运行手册将创建以下资源：

- 一个名为 `AWSSupport-SESSendingLogsToCloudWatchLogs` 的 CloudFormation 堆栈，其中包括：
 - 使用 AWS Key Management Service (AWS KMS) 加密的 Amazon SNS 主题
 - Amazon Simple Queue Service (Amazon SQS) 队列
 - AWS Lambda 用于处理电子邮件发送事件的函数
 - AWS Identity and Access Management (IAM) 执行角色，具有 Amazon SQS 和日志权限 CloudWatch
 - CloudWatch 日志组
 - AWS KMS 加密密钥
 - 带有事件目标的 Amazon SES 配置集
- 基础设施按以下流程处理电子邮件发送事件：Amazon SES 电子邮件发送事件 → Amazon SES 配置集 → 亚马逊 SNS 主题 → 亚马逊 SQS 队列 → Lambda 函数 → 日志 CloudWatch
- 提供 `SesIdentity` 参数时，将创建的配置集关联为指定 Amazon SES 身份的默认配置集。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStackEvents
- cloudformation:DescribeStacks
- iam:CreateRole
- iam:AttachRolePolicy
- iam:PassRole
- kms:CreateKey
- kms:CreateAlias
- lambda:CreateFunction
- lambda:AddPermission
- logs:CreateLogGroup
- logs:PutRetentionPolicy
- ses:CreateConfigurationSet
- ses:CreateConfigurationSetEventDestination
- ses:ListConfigurationSets
- ses:PutEmailIdentityConfigurationSetAttributes
- sns:CreateTopic
- sns:Subscribe
- sqs:CreateQueue

- sqs:SetQueueAttributes
- ssm:DescribeAutomationExecutions

策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "kms:CreateKey",
        "kms:CreateAlias",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "ses:CreateConfigurationSet",
        "ses:CreateConfigurationSetEventDestination",
        "ses:ListConfigurationSets",
        "ses:PutEmailIdentityConfigurationSetAttributes",
        "sns:CreateTopic",
        "sns:Subscribe",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    }
  ]
}
```

说明

按照这些步骤对自动化进行配置：

1. [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#) 在 Systems Manager 的“文档”下导航至。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：
 - AutomationAssumeRole (可选) :
 - 描述：(可选) 允许 Systems Manager Automation 代表您执行操作的 IAM 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
 - 类型：AWS::IAM::Role::Arn
 - ApproveDeployAnalyticEnvironment (可选) :
 - 描述：(可选) 批准部署 Amazon SES 事件发布基础设施。输入approve以创建 CloudFormation 堆栈和相关资源。如果留空，则运行手册仅显示当前区域中包含或 Amazon SNS 事件目标的现有配置集。
 - 类型：String
 - 允许模式：^\$|^approve\$
 - 默认值：""
 - SesIdentity (可选) :
 - 描述：(可选) Amazon SES 身份 (电子邮件地址或域)，用于与新创建的配置集关联为默认配置集。这将覆盖为指定身份设置的任何现有默认配置。
 - 类型：String
 - 默认值：""
 - CloudWatchLogGroupName (可选) :
 - 描述：(可选) 为存储 Amazon SES 电子邮件发送事件而创建的 CloudWatch 日志日志组的名称。
 - 类型：String
 - 允许模式：^[0-9a-zA-Z_.#/\-]{1,512}\$
 - 默认值：/ses/sending_event_logs
 - 口罩PIIData (可选) :
 - 描述：(可选) 指定是否在 CloudWatch 日志中屏蔽个人身份信息 (PII) 数据，例如目标电子邮件地址和电子邮件主题。设置False为可将此信息包含在日志中。
 - 类型：String
 - 允许的值：[True, False]

- 默认值：True
- SleepTime（可选）：
 - 描述：（可选）在自动删除 CloudFormation 堆栈之前等待的分钟数。默认值为 24 小时（1,440 分钟），最长为 7 天（10,080 分钟）。设置为 0 可防止自动删除。
 - 类型：String
 - 允许模式：`^(?:[0-9]|[1-9]\d{1,3}|100[0-7][0-9])$`
 - 默认值：1440
- RetainCloudWatchLogsOnDeletion（可选）：
 - 描述：（可选）指定在删除 CloudFormation 堆栈时是否保留 CloudWatch 日志日志组。设置 False 为可删除日志组和堆栈。
 - 类型：String
 - 允许的值：`[True, False]`
 - 默认值：True
- UniqueId（可选）：
 - 说明：（可选）工作流程的唯一标识符。
 - 类型：String
 - 允许模式：`\\{\\{ automation:EXECUTION_ID \\}\\}\\{[a-zA-Z0-9-]+`
 - 默认值：`{{ automation:EXECUTION_ID }}`
 - ax 字符：64

4. 选择执行。

5. 自动化启动。

6. 文档将执行以下步骤：

- BranchOnValueOfParameterApproveDeployAnalyticEnvironment

根据 ApproveDeployAnalyticEnvironment 参数值确定是否部署 Amazon SES 事件发布基础设施。

- GetEligibleConfigurationSets

检索现有 Amazon SES 配置集，并识别那些为传送流或 Amazon SNS 主题配置了事件目标的配置集。

- CheckConcurrency

验证是否不存在任何现有堆栈，以及此 runbook 的其他并发执行是否正在创建相同的堆栈。

- `DeploySesEventDestinations`

创建包含 Amazon SES 事件发布基础设施的 CloudFormation 堆栈，包括亚马逊 SNS 主题、亚马逊 SQS 队列、Lambda 函数和日志组。CloudWatch

- `RelateConfigurationSetAsDefaultConfigurationSet`

将新创建的 Amazon SES 配置集关联为指定 Amazon SES 身份的默认配置集（如果提供）。

- `SleepBeforeDeleteCloudFormationStack`

等待 `SleepTime` 参数中指定的持续时间后再继续删除 CloudFormation 堆栈。

- `DeleteCloudFormationStack`

在指定的时间段后删除 CloudFormation 堆栈。

7. 完成后，请查看“输出”部分，了解执行的详细结果。

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化工作流程登录页面](#)

SageMaker AI

AWS Systems Manager 自动化为 Amazon SageMaker AI 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-DisableSageMakerNotebookRootAccess](#)
- [AWSSupport-RequestSageMakerLimitIncrease](#)

AWS-DisableSageMakerNotebookRootAccess

描述

AWS-DisableSageMakerNotebookRootAccess运行手册禁用 Amazon A SageMaker I 笔记本实例的根访问权限。在自动化过程中，notebook 实例将停止以进行所需的更改。SageMaker 不支持 AI Studio 笔记本实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- NotebookInstanceName

类型：字符串

描述：(必填) 要禁用根访问权限的 SageMaker AI 笔记本实例的名称。

- StartInstanceAfterUpdate

类型：布尔值

默认：True

描述：(可选) 确定禁用 root 访问权限后是否启动笔记本实例。此参数的默认设置为true。如果设置为true，则实例将在禁用 root 访问权限后启动。如果设置为false，则禁用 root 访问权限后，实例将保持stopped状态。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

文档步骤

- `CheckNotebookInstanceStatus` (aws: executeAwsApi) : 检查笔记本实例的当前状态。
- `StopOrUpdateNotebookInstance` (aws: branch) : 基于笔记本实例状态的分支。
- `StopNotebookInstance` (aws: executeAwsApi) : 如果状态为 `stopped`，则启动实例。
- `WaitForInstanceToStop` (aws: wait ForAwsResourceProperty t) : 验证实例是否为 `stopped`。
- `UpdateNotebookInstance` (aws: executeAwsApi) : 禁用笔记本实例的根访问权限。
- `WaitForNotebookUpdate` (aws: wait ForAwsResourceProperty) : 验证是否已禁用根访问权限以及实例是否处于状态 `stopped`。
- `ChooseInstanceStart` (aws: branch) : 根据是否应启动实例进行分支。
- `StartNotebookInstance` (aws: executeAwsApi) : 启动笔记本实例。
- `VerifyNotebookInstanceStatus` (aws: wait ForAwsResourceProperty) : `available` 在禁用 root 访问权限之前验证实例是否已启用。
- `VerifyNotebookInstanceRootAccess` (aws: assertAwsResourceProperty) : 验证笔记本实例根访问权限设置是否已成功禁用。

AWSSupport-RequestSageMakerLimitIncrease

描述

该AWSSupport-RequestSageMakerLimitIncrease运行手册支持在单个操作中批量提交多个SageMaker Amazon SageMaker AI (AI) 配额增加请求，从而简化了大规模机器学习工作负载的配额管理。运行手册根据可调整的 SageMaker AI 服务配额验证每个请求，在自动批准阈值内路由请求以便

立即处理，并为需要手动审核的请求创建 Support 案例。AWS 配额增加适用于执行运行手册的同一 AWS 区域。

Important

本运行手册不支持对特殊计算实例（包括 P4、P5 和 Trainium 实例类型）的配额增加请求。对于这些实例类型，请通过 `S AWS service Quotas` 控制台或 `Su AWS pport` 提交单独的配额增加请求。

在等待指定负责人通过亚马逊简单通知服务 (Amazon SNS) Service 通知获得批准时，运行手册最多会暂停一小时。批准前请仔细查看 `ApproveQuotaCodeLimitMapping` 步骤输出，因为批准的配额增加无法逆转。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型:: `AWS::IAM::Role`: Arn

描述：（可选）允许（Systems Manager）自动化代表您执行操作的 AWS Identity and Access Management AWS Systems Manager（IAM）角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- ResourcesMapping

类型：StringList

描述：（必填）要增加的 SageMaker AI 服务配额，指定为冒号分隔的值。支持三种格式：

- `Category:Resource:NewValue`— 当类别和资源名称都可用时。示例：`spot-training-job:ml.c4.xlarge:25`
- `Resource:NewValue`— 当只有资源名称可用时。示例：`max_number_of_experiment_trial_associations:501`
- `QuotaCode:NewValue`— 使用直接配额代码时。示例：`L-9xAxx23x:25`

你可以在同一个请求中混合格式，用逗号分隔。最多 50 件物品。示例：`studio:CodeEditor-ml.r6id.large:787,spot-training-job:ml.c4.xlarge:34,L-99AEC235:2`

- `SNSTopicArn`

类型：字符串

描述：(必填) 用于在自动化执行期间发送批准通知的 Amazon SNS 主题的 ARN。

- `ApproverIAM`

类型：StringList

描述：(必填) AWS 经过身份验证的委托人列表，他们可以批准或拒绝增加配额的请求。最多 10 个批准者。可接受的格式：IAM 用户名、IAM 用户 ARN、IAM 角色 ARN 或 IAM 代入角色用户 ARN。

- `MinimumRequiredApprovals`

类型：整数

有效值：1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

默认：1

描述：(可选) 恢复自动化所需的最低批准数量。不能超过中定义的批准者人数。ApproverIAM

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `servicequotas:ListServiceQuotas`
- `servicequotas:RequestServiceQuotaIncrease`
- `servicequotas:GetRequestedServiceQuotaChange`
- `sns:Publish`

- `ssm:SendAutomationSignal`

文档步骤

1. `VerifyCategoriesAndResources`-使用 Service Quotas API 根据可调整的 SageMaker AI 服务配额验证所有指定的类别和资源。AWS 确认每个类别和资源名称都存在且可修改，并识别新限制低于当前值的请求。
2. `BranchOnValidCategoriesFound`-检查是否找到了任何有效的配额映射。如果存在有效的映射，则继续执行。`ApproveQuotaCodeLimitMapping`否则，直接跳到。`GenerateSummaryReport`
3. `ApproveQuotaCodeLimitMapping`-准备一份详细的批准消息，显示可供处理的有效申请、带有解释的无效请求（例如限制低于当前值或不支持的配额代码），以及所有配额增加请求的完整明细，以供批准前审查。
4. `WaitingForApproval`-暂停自动操作并向指定的 Amazon SNS 主题发送批准通知。指定的批准者必须查看`ApproveQuotaCodeLimitMapping`步骤输出并批准或拒绝申请。如果未采取任何操作，则此步骤将在 3600 秒（一小时）后超时。
5. `RequestQuotaIncreases`-通过 Service Quotas API 为每个有效资源提交单独的配 AWS 额增加请求。请求的节奏为每秒一个，以防止 API 限制。通过指数重试处理 API 异常。
6. `WaitForRequestQuotaIncreaseResults`-轮询所有已提交的配额增加请求的状态，直到没有任何请求保持PENDING状态。可接受的终端状态为CASE_OPENEDAPPROVED、DENIED、、NOT_APPROVEDCASE_CLOSED、和。INVALID_REQUEST
7. `GetRequestQuotaIncreaseResults`-从 Serv AWS ice Quotas API 检索所有已提交的配额增加请求的最终状态，并将支持案例映射 IDs 到相应的资源和报告请求 IDs 。
8. `GenerateSummaryReport`-汇编所有配额增加请求及其结果的全面摘要，包括请求总数、每个请求的详细信息、需要手动审核 IDs 的请求的支持案例以及可行的后续步骤。

输出

`GenerateSummaryReport.SummaryReport`-所有配额增加请求、其状态以及为手动审查而 IDs 创建的任何支持案例的全面摘要。

Secrets Manager

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Secrets Manager 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

AWSConfigRemediation-DeleteSecret

描述

AWSConfigRemediation-DeleteSecret 运行手册会删除一个密钥和存储在其中的 AWS Secrets Manager 所有版本。您可以选择指定恢复时段，在此期间您可以恢复密钥。如果您没有为 RecoveryWindowInDays 参数指定一个值，则操作将默认为 30 天。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- **RecoveryWindowInDays**

类型：整数

有效值：7-30

默认：30

描述：(可选) 您可以恢复密钥的天数。

- **SecretId**

类型：字符串

描述：(必需) 要删除的密钥的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

文档步骤

- `aws:executeAwsApi` - 删除您在 SecretId 参数中指定的密钥。
- `aws:executeScript` - 验证密钥已计划进行删除。

AWSConfigRemediation-RotateSecret

描述

AWSConfigRemediation-RotateSecret 运行手册会轮换存储在中的密钥。AWS Secrets Manager

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- RotationInterval

类型：间隔

有效值：1-365

描述：(必需) 密钥两次轮换之间的天数。

- RotationLambdaArn

类型：字符串

描述：(必需) 可以轮换密钥的 AWS Lambda 函数的 Amazon 资源名称 (ARN)。

- SecretId

类型：字符串

描述：(必需) 要轮换的密钥的 Amazon 资源名称 (ARN)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

文档步骤

- `aws:executeAwsApi` - 轮换您在 `SecretId` 参数中指定的密钥。
- `aws:executeScript` - 验证是否已对密钥启用轮换。

Security Hub CSPM

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Security Hub CSPM 有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-EnableSecurityHub](#)

AWSConfigRemediation-EnableSecurityHub

描述

AWSConfigRemediation-EnableSecurityHub 运行手册为你运行自动化的 AWS 区域 位置启用 AWS Security Hub CSPM (Security Hub CSPM)。AWS 账户 有关 Security Hub CSPM 的信息，请参阅[什么是？AWS Security Hub CSPM](#) 在《AWS Security Hub 用户指南》中。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- EnableDefaultStandards

类型：布尔值

默认：True

描述：(必填) 如果设置为true，则启用 Security Hub CSPM 指定的默认安全标准。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- securityhub:DescribeHub
- securityhub:EnableSecurityHub
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文档步骤

- aws:executeAwsApi-在当前账户和区域中启用 Security Hub CSPM。
- aws:executeAwsApi-验证 Security Hub CSPM 是否已启用。

AWS Shield

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS Shield有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

AWSPremiumSupport-DDoSResiliencyAssessment

描述

AWS Systems Manager 自动化运行手册可帮助您根据 AWS Shield Advanced 保护措施检查 DDoS 漏洞和资源配置。AWSPremiumSupport-DDoSResiliencyAssessment AWS 账户它为易受分布式拒绝服务 (DDoS) 攻击的资源提供配置设置报告。它用于收集、分析和评估以下资源：Amazon Route 53、Amazon 负载均衡器、Amazon CloudFront 分配 AWS Global Accelerator 以及根据推荐的 AWS Shield Advanced 保护最佳实践进行配置设置的 AWS 弹性 IP。最终配置报告将以 HTML 文件形式在您选择的 Amazon S3 存储桶中提供。

如何工作？

此运行手册包含一系列检查，用于为公开访问启用的各种类型资源，以及它们是否按照 [AWS DDoS 最佳实践白皮书](#) 中的建议进行保护措施配置。运行手册将执行以下操作：

- 检查订阅 AWS Shield Advanced 是否已启用。
- 如果已启用，它会查找是否有任何受 Shield Advanced 保护资源。
- 它会在 AWS 账户 中查找所有全球和区域资源，并检查这些资源是否受到 Shield 保护。
- 它需要用于评估的资源类型参数、Amazon S3 存储桶名称和 Amazon S3 存储桶 AWS 账户 ID (S3BucketOwner)。
- 它以 HTML 报告的形式返回调查发现，该报告存储在提供的 Amazon S3 存储桶中。

输入参数 AssessmentType 决定是否对所有资源进行检查。默认情况下，运行手册会检查是否有所有类型的资源。如果只选择了 GlobalResources 或 RegionalResources 参数，运行手册将仅对选定资源类型执行检查。

Important

- 访问AWSPremiumSupport-*运行手册需要订阅 Business + Support、Enterprise Support 或统一运营订阅。有关更多信息，请参阅[比较 AWS 支持 计划](#)。
- 此运行手册需要 ACTIVE[AWS Shield Advanced 订阅](#)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AssessmentType

类型：字符串

描述：(可选) 确定要针对 DDoS 弹性评测进行评估的资源类型。默认情况下，运行手册将评估全局和区域资源。对于区域资源，运行手册描述了所有应用程序 (ALB) 和网络 (NLB) 负载均衡器，以及您的 AWS 账户/区域的所有 Auto Scaling 组。

有效值：['Global Resources', 'Regional Resources', 'Global and Regional Resources']

默认：全球和区域资源

- S3BucketName

类型：AWS::S3::Bucket::Name

描述：(必需) 要将报告上传到的 Amazon S3 存储桶名称。

允许的模式：`^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3BucketOwnerAccount

类型：字符串

描述：(可选) 拥有 Amazon S3 存储桶的。AWS 账户 如果 Amazon S3 存储桶属于不同的存储桶，请指定此参数 AWS 账户，否则您可以将此参数留空。

允许的模式：`^$|^[0-9]{12,13}$`

- S3BucketOwnerRoleArn

类型：AWS::IAM::Role::Arn

描述：(可选) 具有描述 Amazon S3 存储桶和 AWS 账户 阻止公有访问配置的权限的 IAM 角色的 ARN (如果存储桶位于其他存储桶中)。AWS 账户如果未指定此参数，运行手册将使用 AutomationAssumeRole 或启动此运行手册的 IAM 用户 (如果 AutomationAssumeRole 未指定)。请参阅运行手册描述中的“所需权限”部分。

允许的模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3BucketPrefix

类型：字符串

描述：(可选) Amazon S3 内用于存储结果的路径的前缀。

允许的模式：`^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$|^$`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- autoscaling:DescribeAutoScalingGroups
- cloudfront:ListDistributions
- ec2:DescribeAddresses
- ec2:DescribeNetworkAcls
- ec2:DescribeInstances
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- globalaccelerator:ListAccelerators
- iam:GetRole

- iam:ListAttachedRolePolicies
- route53:ListHostedZones
- route53:GetHealthCheck
- shield:ListProtections
- shield:GetSubscriptionState
- shield:DescribeSubscription
- shield:DescribeEmergencyContactSettings
- shield:DescribeDRTAccess
- waf:GetWebACL
- waf:GetRateBasedRule
- wafv2:GetWebACL
- wafv2:GetWebACLForResource
- waf-regional:GetWebACLForResource
- waf-regional:GetWebACL
- s3:ListBucket
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketEncryption
- s3:GetAccountPublicAccessBlock
- s3:PutObject

自动化承担角色的 IAM policy 示例

JSON

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

```

        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>",
    "Effect": "Allow"
},
{
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>/*",
    "Effect": "Allow"
},
{
    "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:ListDistributions",
        "ec2:DescribeInstances",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkAcls",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "globalaccelerator:ListAccelerators",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "route53:ListHostedZones",
        "route53:GetHealthCheck",
        "shield:ListProtections",
        "shield:GetSubscriptionState",
        "shield:DescribeSubscription",
        "shield:DescribeEmergencyContactSettings",

```

```

        "shield:DescribeDRTAccess",
        "waf:GetWebACL",
        "waf:GetRateBasedRule",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "waf-regional:GetWebACLForResource",
        "waf-regional:GetWebACL"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": "iam:PassRole",
    "Resource":
"arn:aws:iam::111122223333:role/automation-assume-role-name",
    "Effect": "Allow"
}
]
}

```

说明

1. 导航到 AWS Systems Manager 控制台 [AWSPremiumSupport-DDoSResiliencyAssessment](#) 中的。
2. 选择 Execute automation (执行自动化)
3. 要输入参数，请输入内容：

- AutomationAssumeRole (可选)：

AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 允许 Systems Manager Automation 代表您执行操作。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AssessmentType (可选)：

确定要针对 DDoS 弹性评测进行评估的资源类型。默认情况下，运行手册会评价全球和区域资源。

- S3BucketName (必填)：

要将评估报告保存为 HTML 格式的 Amazon S3 存储桶的名称。

- S3BucketOwner (可选)：

用于所有权验证的 Amazon S3 存储桶的 AWS 账户 ID。如果报告需要发布到跨账户 Amazon S3 存储桶，则需要提供 AWS 账户 ID；如果 Amazon S3 存储桶与自动启动 AWS 账户相同，则为可选。

- S3BucketPrefix (可选) :

Amazon S3 内用于存储结果的路径的前缀。

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

ssm-admin
arn:aws:iam:::role/ssm-admin

S3BucketName
(Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.

Select an existing S3 Bucket

S3BucketPrefix
(Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix>

String

ResourceType
(Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources.

Global and Regional Resources

S3BucketOwner
(Required) The Account ID of the Amazon S3 bucket for ownership verification.

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- CheckShieldAdvancedState:

验证是否已订阅 AWS Shield Advanced 以及运行手册是否有权访问 Amazon S3 存储桶。AWS 账户

- S3BucketSecurityChecks:

检查“S3BucketName”中指定的 Amazon S3 存储桶是否允许匿名或公开读取或写入访问权限，该存储桶是否启用了静态加密，以及“S3BucketOwner”中提供的 AWS 账户 ID 是否是 Amazon S3 存储桶的所有者。

- BranchOnShieldAdvancedStatus:

分支机构根据 AWS Shield Advanced 订阅状态 and/or Amazon S3 存储桶所有权状态记录步骤。

- ShieldAdvancedConfigurationReview:

审查 Shield Advanced 配置以确保存在最低限度的必要详情。例如：AWS Shield 响应小组 (SRT) 团队的 IAM 访问权限、联系人列表详细信息和 SRT 主动参与状态。

- ListShieldAdvancedProtections:

列出受 Shield 保护的资源，并为每个服务创建一组受保护的资源。

- BranchOnResourceTypeAndCount:

根据资源类型参数的值和受 Shield 保护的全球资源的数量对文档步骤进行分支。

- ReviewGlobalResources:

查看 Shield Advanced 受保护的全球资源，例如 Route 53 托管区域、CloudFront 分布和全球加速器。

- BranchOnResourceType:

根据资源类型选择对文档记录进行分支（如果是全球、区域或两者）。

- ReviewRegionalResources:

查看受 Shield Advanced 保护的区域资源，例如应用程序负载均衡器、网络负载均衡器、经典负载均衡器、Amazon Elastic Compute Cloud (Amazon EC2) 实例（弹性 IP）。

- SendReportToS3:

将 DDoS 评估报告详情上传至 Amazon S3 存储桶。

7. 完成后，将在 Amazon S3 存储桶中提供评估报告 HTML 文件的 URI：

运行手册成功执行后该报告的 S3 控制台链接和 Amazon S3 URI

▼ Outputs

SendReportToS3.AssessmentReportS3ConsoleUrl

https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

SendReportToS3.AssessmentReportS3Uri

S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

Execution status

Overall status	All executed steps	# Succeeded
✔ Success	9	9
# Failed	# Cancelled	# TimedOut
0	0	0

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)

- [支持自动化 workflow 登录页面](#)

AWS 服务文档

- [AWS Shield Advanced](#)

Amazon SNS

AWS Systems Manager Automation 为 Amazon 简单通知服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)
- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

AWS-EnableSNSTopicDeliveryStatusLogging

描述

该AWS-EnableSNSTopicDeliveryStatusLogging运行手册为亚马逊 Data Firehose、Lambda 或HTTP亚马逊简单队列服务 (Amazon S Platform application QS) 终端节点配置传输状态日志。这样，Amazon SNS 就可以将失败的警报以及成功警报通知的示例百分比记录到亚马逊。CloudWatch如果已经为该主题配置了交付状态日志，则运行手册将使用您为输入参数指定的新值替换现有配置。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- EndpointType

类型：字符串

有效值：

- HTTP
- Firehose
- Lambda
- 应用程序
- SQS

描述：(必填) 您要记录其传输状态通知消息的 Amazon SNS 主题终端节点的类型。

- TopicArn

类型：字符串

描述：(必填) 您要为其配置传送状态日志的 Amazon SNS 主题的 ARN。

- SuccessFeedbackRoleArn

类型：字符串

描述：(必填) Amazon SNS 用于向其发送成功通知消息的日志的 IAM 角色的 ARN。CloudWatch

- SuccessFeedbackSampleRate

类型：字符串

有效值：0-100

描述：(必填) 指定 Amazon SNS 主题的成功采样消息的百分比。

- FailureFeedbackRoleArn

类型：字符串

描述：(必填) Amazon SNS 用于向其发送失败通知消息日志的 IAM 角色的 ARN。CloudWatch

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:PassRole
- sns:GetTopicAttributes
- sns:SetTopicAttributes

文档步骤

- aws:executeAwsApi-将SuccessFeedbackRoleArn参数的值应用于 Amazon SNS 主题。
- aws:executeAwsApi-将SuccessFeedbackSampleRate参数的值应用于 Amazon SNS 主题。
- aws:executeAwsApi-将FailureFeedbackRoleArn参数的值应用于 Amazon SNS 主题。
- aws:executeScript-确认已在 Amazon SNS 主题上启用配送状态记录。

输出

VerifyDeliveryStatusLoggingEnabled.GetTopicAttributesResponse -来自 GetTopicAttributes API 操作的响应。

VerifyDeliveryStatusLoggingEnabled.VerifyDeliveryStatusLoggingEnabled -表示成功验证传送状态记录的消息。

AWSConfigRemediation-EncryptSNSTopic

描述

该操作AWSConfigRemediation-EncryptSNSTopic手册允许对您使用 () 客户托管密钥指定的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题进行 AWS Key Management Service 加密。AWS KMS此运行手册应仅用作基准，以确保根据建议的最低安全性最佳实践对 Amazon SNS 主题进行加密。我们建议使用不同的客户托管密钥对多个主题进行加密。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- KmsKeyArn

类型：字符串

描述：(必需) 要用于加密 Amazon SNS 主题的 AWS KMS 客户托管密钥的 Amazon 资源名称 (ARN) 。

- TopicArn

类型：字符串

描述：(必需) 要加密的 Amazon SNS 主题的 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

文档步骤

- `aws:executeAwsApi` - 加密您在 `TopicArn` 参数中指定的 Amazon SNS 主题。
- `aws:assertAwsResourceProperty` - 确认已对 Amazon SNS 主题启用加密。

AWS-PublishSNSNotification

描述

向 Amazon SNS 发布一个通知。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- Message

类型：字符串

描述：(必需) 包含在 SNS 通知中的消息。

- TopicArn

类型：字符串

描述：(必需) 向其发布通知的 SNS 主题的 ARN。

Amazon SQS

AWS Systems Manager Automation 为亚马逊简单队列服务 (Amazon SQS) Simple SQS 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableSQSEncryption](#)

AWS-EnableSQSEncryption

描述

该AWS-EnableSQSEncryption运行手册支持对亚马逊简单队列服务 (Amazon SQS) 队列进行静态加密。可以使用亚马逊 SQS 托管密钥 (SSE-SQS) 或 () 托管密钥 (SSE-KMS) 对亚马逊 SQS 队列进行AWS Key Management Service 进行AWS KMS加密。您分配给队列的密钥必须具有密钥策略，其中包括所有有权使用该队列的委托人的权限。启用加密后，匿名ReceiveMessage请求SendMessage和对加密队列的请求将被拒绝。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- QueueUrl

类型：字符串

描述：(必填) 您要启用加密的 Amazon SQS 队列的 URL。

- KmsKeyId

类型：字符串

描述：(可选) 用于加密的密 AWS KMS 钥。此值可以是全局唯一标识符、别名或密钥的 ARN，也可以是以“alias/”为前缀的别名。您也可以通过指定别名 aws/sqs 来使用 AWS 托管密钥。

- KmsDataKeyReusePeriodSeconds

类型：字符串

有效值：60-86400

默认：300

描述：(可选) Amazon SQS 队列在再次调用之前可以重复使用数据密钥对消息进行加密或解密的时间长度 (以秒为单位)。AWS KMS

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

文档步骤

- `SelectKeyType (aws:branch)` : 基于指定密钥的分支。
- `PutAttributeSseKms (aws:executeAwsApi)`-更新 Amazon SQS 队列以使用为加密指定的 AWS KMS 密钥。
- `PutAttributeSseSqs (aws:executeAwsApi)`-更新 Amazon SQS 队列以使用默认密钥进行加密。
- `VerifySqsEncryptionKms (aws:assertAwsResourceProperty)`-验证是否已在 Amazon SQS 队列上启用加密。
- `VerifySqsEncryptionDefault (aws:assertAwsResourceProperty)`-验证是否已在 Amazon SQS 队列上启用加密。

Step Functions

AWS Systems Manager 自动化为 AWS Step Functions (Step Functions) 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-EnableStepFunctionsStateMachineLogging](#)

AWS-EnableStepFunctionsStateMachineLogging

描述

AWS-EnableStepFunctionsStateMachineLogging运行手册启用或更新您指定的 AWS Step Functions 状态机上的日志记录。最低日志级别必须设置为ALLERROR、或FATAL。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 级别

类型：字符串

有效值：全部 | 错误 | 致命

描述：(必填) 您要启用加密的 Amazon SQS 队列的 URL。

- LogGroupArn

类型：字符串

描述：(必填) 您要向其发送状态机 CloudWatch 日志的 Amazon 日志组的 ARN。

- StateMachineArn

类型：字符串

描述：(必填) 要启用登录功能的状态机的 ARN。

- IncludeExecutionData

类型：布尔值

默认值：False

描述：(可选) 确定日志中是否包含执行数据。

- TracingConfiguration

类型：布尔值

默认值：False

描述：(可选) 确定是否启用 AWS X-Ray 跟踪。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine
- states:UpdateStateMachine

文档步骤

- EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)-使用指定的日志配置更新指定的状态机。
- VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)-验证是否已为指定状态机启用日志记录。

输出

- EnableStepFunctionsStateMachineLogging.Response-来自 UpdateStateMachine API 调用的响应。

Systems Manager

AWS Systems Manager 自动化为 Systems Manager 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-BulkDeleteAssociation](#)
- [AWS-BulkEditOpsItems](#)

- [AWS-BulkResolveOpsItems](#)
- [AWS-ConfigureMaintenanceWindows](#)
- [AWS-CreateManagedLinuxInstance](#)
- [AWS-CreateManagedWindowsInstance](#)
- [AWSConfigRemediation-EnableCWLoggingForSessionManager](#)
- [AWS-ExportOpsDataToS3](#)
- [AWS-ExportPatchReportToS3](#)
- [AWS-SetupInventory](#)
- [AWS-SetupManagedInstance](#)
- [AWS-SetupManagedRoleOnEC2Instance](#)
- [AWSSupport-TroubleshootManagedInstance](#)
- [AWSSupport-TroubleshootPatchManagerLinux](#)
- [AWSSupport-TroubleshootSessionManager](#)

AWS-BulkDeleteAssociation

描述

AWS-BulkDeleteAssociation 运行手册可帮助您一次最多删除 50 个 Systems Manager State Manager 关联。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AssociationIds

类型：StringList

描述：(必需) 要删除的关联的 ID 列表 (以逗号分隔)。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DeleteAssociation

文档步骤

- aws:executeScript - 删除您在 AssociationIds 参数中指定的关联。

AWS-BulkEditOpsItems

描述

AWS-BulkEditOpsItems 运行手册可帮助您编辑的状态、严重性、类别或优先级。AWS Systems Manager OpsItems 此自动化一次最多可以编辑 50 个 OpsItems。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 类别

类型：字符串

有效值：

- 可用性
- 成本
- 无更改
- 性能
- 恢复
- 安全性

默认：无变化

描述：(可选) 您要为编辑的内容指定的新类别 OpsItems。

- OpsItemIds

类型：StringList

描述：(必填) 要编辑的以逗号分隔的 OpsItems ID 列表 (例如，oi-xxxxxxxxxxxxxx、oi-xxxxxxxxxxxxxx)。

- 优先级

类型：字符串

有效值：

- 无更改

- 1
- 2
- 3
- 4
- 5

默认：无变化

描述：(可选) 编辑的内容 OpsItems 相对于系统 OpsItems 中其他内容的重要性。

- 严重性

类型：字符串

有效值：

- 无更改
- 1
- 2
- 3
- 4

默认：无变化

描述：(可选) 已编辑内容的严重性 OpsItems。

- WaitTimeBetweenEditsInSecs

类型：字符串

有效值：0.0-2.0

默认：0.8

描述：(可选) 自动化在调用 UpdateOpsItems 操作之间等待的时间。

- Status

类型：字符串

有效值：

- InProgress
- 无更改
- 打开
- 已解决

默认：无变化

描述：(可选) 已编辑内容的新状态 OpsItems。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文档步骤

- aws:executeScript-根据 OpsItems 您为Category、Priority和OpsItemIds参数指定的值编辑您在Status参数中指定的值。Severity

AWS-BulkResolveOpsItems

描述

AWS-BulkResolveOpsItems运行手册解析的结果与您指定的过滤器 AWS Systems Manager OpsItems 相匹配。您也可以 OpsItems 使用OpsInsightsId参数指定 OpsItemId 要添加到已解析的中。如果您为 S3BucketName 参数指定了一个值，则结果摘要会发送到 Amazon Simple Storage Service (Amazon S3) Service 存储桶。要在结果摘要发送到 Amazon S3 存储桶后收到通知，请为 SnsTopicArn 参数指定一个值。这种自动化一次最多可以解决 1,000 OpsItems 个问题。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 筛选条件

类型：字符串

描述：(必填) 用于返回 OpsItems 要解析的过滤器的键值对。例如，[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]。要详细了解可用于筛选 OpsItems 响应的选项，请参阅 AWS Systems Manager API 参考[OpsItemFilters](#)中的。

- OpsInsightId

类型：字符串

描述：(可选) 您要添加到已解析的相关资源标识符 OpsItems。

- S3BucketName

类型：字符串

描述：(可选) 要将结果摘要发送到的 Amazon S3 存储桶的名称。

- SnsMessage

类型：字符串

描述：(可选) 您希望 Amazon Simple Notification Service (Amazon SNS) 在自动化完成时发送的通知。

- SnsTopicArn

类型：字符串

描述：(可选) 您希望在结果摘要发送到 Amazon S3 时通知的 Amazon SNS 主题的 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文档步骤

- aws:executeScript- OpsItems 根据您指定的过滤器收集和解析问题。如果您为 OpsInsightId 参数指定了一个值，该值将作为相关资源进行添加。
- aws:executeScript - 如果您为 S3BucketName 参数指定了一个值，则结果摘要随后会发送到 Amazon S3 存储桶。
- aws:executeScript - 如果您为 SnsTopicArn 参数指定了一个值，则在结果摘要发送到 Amazon S3 之后，系统会向 Amazon SNS 主题发送通知，包括 SnsMessage 参数值 (如果已指定) 。

AWS-ConfigureMaintenanceWindows

描述

AWS-ConfigureMaintenanceWindows 运行手册可帮助您启用或禁用多个 Systems Manager 维护时段。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- MaintenanceWindows

类型：StringList

描述：(必需) 要启用或禁用的维护时段 ID 的逗号分隔列表。

- MaintenanceWindowsStatus

类型：字符串

有效值："True" | "False"

默认："False"

描述：(必需) 确定是启用还是禁用维护时段。指定“True”可启用维护时段，指定“False”可禁用维护时段。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetMaintenanceWindow
- ssm:UpdateMaintenanceWindow

文档步骤

- `aws:executeScript` - 收集您在 `MaintenanceWindows` 参数中指定的维护时段的状态，并启用或禁用维护时段。

AWS-CreateManagedLinuxInstance

描述

创建为 Systems Manager 配置的 Linux EC2 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- `Amild`

类型：字符串

描述：(必需) 用于启动实例的 AMI ID。

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- `GroupName`

类型：字符串

默认：SSMSecurityGroupForLinuxInstances

描述：(必需) 要创建的安全组名称。

- HttpTokens

类型：字符串

有效值：可选 | 必需

默认：可选

描述：(可选) IMDSv2 使用令牌支持的会话。将 HTTP 令牌的使用设置为 optional 或 required 以确定 imdsv2 是可选的还是必需的。

- InstanceType

类型：字符串

默认：t2.medium

描述：(必需) 要启动的实例类型。默认为 t2.medium。

- KeyPairName

类型：字符串

描述：(必需) 创建实例时使用的密钥对。

- RemoteAccessCidr

类型：字符串

默认值：0.0.0.0/0

描述：(必需) 创建向 CIDR 指定的 IP 开放 SSH 端口 (端口范围 22) 的安全组 (默认值为 0.0.0.0/0)。如果安全组已存在，则不会对其进行修改，也不会更改规则。

- RoleName

类型：字符串

默认：SSMManagedInstanceProfileRole

描述：(必需) 要创建的角色名称。

- StackName

类型：字符串

默认：CreateManagedInstanceStack{{自动化:execution_ID}}

描述：(可选) 指定此运行手册使用的堆栈名称

- SubnetId

类型：字符串

默认：Default

描述：(必需) 新实例将部署到此子网；如果未指定，则部署到默认子网。

- VpcId

类型：字符串

默认：Default

描述：(必需) 新实例将部署到此 Amazon Virtual Private Cloud (Amazon VPC)；如果未指定，则部署到默认 Amazon VPC。

AWS-CreateManagedWindowsInstance

描述

创建为 Systems Manager 配置的 Windows Server EC2 实例。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Windows

参数

参数

- Amild

类型：字符串

默认：{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}

描述：(必需) 用于启动实例的 AMI ID。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- GroupName

类型：字符串

默认：SSMSecurityGroupForLinuxInstances

描述：(必需) 要创建的安全组名称。

- HttpTokens

类型：字符串

有效值：可选 | 必需

默认：可选

描述：(可选) IMDSv2 使用令牌支持的会话。将 HTTP 令牌的使用设置为 optional 或 required 以确定 imdsv2 是可选的还是必需的。

- InstanceType

类型：字符串

默认：t2.medium

描述：(必需) 要启动的实例类型。默认为 t2.medium。

- KeyPairName

类型：字符串

描述：(必需) 创建实例时使用的密钥对。

- RemoteAccessCidr

类型：字符串

默认值：0.0.0.0/0

描述：(必需) 创建向 CIDR 指定的 IP 开放 RDP 端口 (端口范围 3389) 的安全组 (默认值为 0.0.0.0/0)。如果安全组已存在，则不会对其进行修改，也不会更改规则。

- RoleName

类型：字符串

默认：SSMManagedInstanceProfileRole

描述：(必需) 要创建的角色名称。

- StackName

类型：字符串

默认：CreateManagedInstanceStack{{自动化:execution_ID}}

描述：(可选) 指定此运行手册使用的堆栈名称

- SubnetId

类型：字符串

默认：Default

描述：(必需) 新实例将部署到此子网；如果未指定，则部署到默认子网。

- VpcId

类型：字符串

默认：Default

描述：（必需）新实例将部署到此 Amazon Virtual Private Cloud (Amazon VPC)；如果未指定，则部署到默认 Amazon VPC。

AWSConfigRemediation-EnableCWLoggingForSessionManager

描述

AWSConfigRemediation-EnableCWLoggingForSessionManager 运行手册允许 AWS Systems Manager 会话管理器（会话管理器）会话将输出日志存储到 Amazon CloudWatch (CloudWatch) 日志组。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- DestinationLogGroup

类型：字符串

描述：（必填）CloudWatch 日志组的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm:CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

文档步骤

- aws:executeScript-接受 CloudWatch 日志组以更新存储 Session Manager 会话输出日志首选项的文档，如果该首选项不存在，则创建一个。

AWS-ExportOpsDataToS3

描述

本运行手册在 AWS Systems Manager Explorer 中检索 OpsData 摘要列表，并将其导出到指定亚马逊简单存储服务 (Amazon S3) 存储桶中的对象。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- columnFields

类型：StringList

描述：(必需) 要写入到输出文件的列字段。

- filters

类型：字符串

描述：(可选) get OpsSummary 请求的过滤器。

- resultAttribute

类型：字符串

描述：(可选) 获取OpsSummary请求的结果属性。

- s3 BucketName

类型：字符串

描述：(必需) 要将输出文件下载到的 S3 存储桶。

- sns SuccessMessage

类型：字符串

描述：(可选) 在运行手册完成时发送的消息。

- sns TopicArn

类型：字符串

描述：(必需) 下载完成时要通知的 Amazon Simple Notification Service (Amazon SNS) 主题 ARN。

- syncName

类型：字符串

描述：(可选) 资源数据同步的名称。

文档步骤

get OpsSummaryStep — 检索多达 5,000 个操作摘要，立即将其导出为 CSV 文件。

输出

OpsData 对象 — 如果运行手册成功运行，您将在目标 S3 存储桶中找到导出的 OpsData 对象。

AWS-ExportPatchReportToS3

描述

此运行手册在 AWS Systems Manager 补丁管理器中检索补丁摘要数据和补丁详情的列表，并将其导出到指定 Amazon Simple Storage Service (Amazon S3) 存储桶中的 .csv 文件。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- assumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，则 Systems Manager Automation 使用运行此文档的用户的权限。

- s3 BucketName

类型：字符串

描述：(必需) 要下载输出文件的 S3 存储桶。

- sns TopicArn

类型：字符串

描述：(可选) 下载完成时要通知的 Amazon Simple Notification Service (Amazon SNS) 主题 Amazon 资源名称 (ARN) 。

- sns SuccessMessage

类型：字符串

描述：(可选) 运行手册完成时要发送的消息的文本。

- targets

类型：字符串

描述：(必需) 实例 ID 或通配符 (*)，用于指示是报告特定实例还是所有实例的补丁数据。

文档步骤

ExportReportStep — 此步骤的操作取决于targets参数的值。如果 targets 的格式为 instanceids=*，则该步骤最多可检索您账户中实例的 10,000 个补丁摘要，并将数据导出到 .csv 文件。

如果 targets 的格式为 instanceids=<instance-id>，则该步骤会检索您账户中指定实例的补丁摘要和所有补丁，并将其导出到 .csv 文件。

输出

PatchSummary/Patches 对象 — 如果运行手册成功运行，则导出的补丁报告对象将下载到您的目标 S3 存储桶。

AWS-SetupInventory

描述

为一个或多个托管实例创建 Systems Manager Inventory 关联。系统根据关联中的计划从实例收集元数据。有关更多信息，请参阅[AWS Systems Manager 清单](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- 应用程序

类型：字符串

默认值：启用

描述：(可选) 收集有关已安装的应用程序的元数据。

- AssociatedDocName

类型：字符串

默认：AWS-GatherSoftwareInventory

描述：(可选) 用于从托管实例收集清单的运行手册的名称。

- AssociationName

类型：字符串

描述：(可选) 将分配给实例的清单关联的名称。

- AssocWaitTime

类型：字符串

默认值：PT5M

描述：(可选) 到达清单关联开始时间时，清单集合应暂停的时间。时间使用 ISO 8601 格式。

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AwsComponents

类型：字符串

默认值：启用

描述：(可选) 收集诸如 amazon-ssm-agent AWS t 之类的组件的元数据。

- CustomInventory

类型：字符串

默认值：启用

描述：(可选) 收集自定义清单元数据。

- 文件

类型：字符串

描述：(可选) 收集有关实例上的文件的元数据。有关如何收集此类清单数据的更多信息，请参阅[使用文件和 Windows 注册表清单](#)。需要 SSMAgent 版本 2.2.64.0 或更高版本。Linux 示例：

```
[{"Path":"/usr/bin", "Pattern":["aws*", "*ssm*"],"Recursive":false}, {"Path":"/var/log", "Pattern":["amazon*.*"], "Recursive":true, "DirScanLimit":1000}]
```

 Windows example:

```
[{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]
```

- InstanceDetailedInformation

类型：字符串

默认值：启用

描述：(可选) 收集有关实例的其他信息，包括 CPU 型号、速度和内核数等。

- InstanceIds

类型：字符串

默认值：*

描述：(必需) 要清点的 EC2 实例。

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- NetworkConfig

类型：字符串

默认值：启用

描述：(可选) 收集有关网络配置的元数据。

- OutputS3BucketName

类型：字符串

描述：(可选) 要将清单日志数据写入到的 Amazon S3 存储桶的名称。

- OutputS3KeyPrefix

类型：字符串

描述：(可选) 要将清单日志数据写入到的 Amazon S3 键前缀 (子文件夹)。

- OutputS3Region

类型：字符串

描述：(可选) Amazon S3 AWS 区域 所在位置的名称。

- Schedule

类型：字符串

默认值：cron(0 */30 * * * ? *)

描述：(可选) 清单关联计划的 cron 表达式。默认为每 30 分钟一次。

- Services

类型：字符串

默认值：启用

描述：（可选，仅限 Windows 操作系统，需要 SSMAgent 版本 2.2.64.0 或更高版本）收集有关服务配置的数据。

- WindowsRegistry

类型：字符串

描述：（可选）收集有关 Microsoft Windows 注册表项的元数据。有关如何收集此类清单数据的更多信息，请参阅[使用文件和 Windows 注册表清单](#)。需要 SSM Agent 版本 2.2.64.0 或更高版本。示例：[{"路径": "HKEY_CURRENT_CONFIG\\System", "Recursive": true}, {"路径": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Amazon\\", "": ["aMiname"]}]] MachineImage ValueNames

- WindowsRoles

类型：字符串

默认值：启用

描述：（可选）收集有关实例上的 Windows 角色的信息。仅适用于 Windows 操作系统。需要 SSMAgent 版本 2.2.64.0 或更高版本。

- WindowsUpdates

类型：字符串

默认值：启用

描述：（可选）收集有关实例上的所有 Windows 更新的数据。

AWS-SetupManagedInstance

描述

为实例配置一个 AWS Identity and Access Management (IAM) 角色以获得 Systems Manager 访问权限。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要配置的 EC2 实例的 ID

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- RoleName

类型：字符串

默认：SSMRoleForManagedInstance

描述：(可选) EC2 实例的 IAM 角色的名称。如果此角色不存在，则创建此角色。指定此值时，请验证该角色是否包含AmazonSSMManagedInstanceCore托管策略。

AWS-SetupManagedRoleOnEC2Instance

描述

使用 `SSMRoleForManagedInstance` 托管 IAM 角色配置实例以获得 Systems Manager 访问权限。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 要配置的 EC2 实例的 ID

- LambdaAssumeRole

类型：字符串

描述：(可选) 允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- RoleName

类型：字符串

默认：SSMRoleForManagedInstance

描述：(可选) EC2 实例的 IAM 角色的名称。如果此角色不存在，则创建此角色。指定此值时，请验证该角色是否包含AmazonSSMManagedInstanceCore托管策略。

AWSsupport-TroubleshootManagedInstance

描述

AWSsupport-TroubleshootManagedInstance运行手册可帮助您确定亚马逊弹性计算云 (Amazon EC2) 实例为何未报告为由 AWS Systems Manager托管。此运行手册将审查该实例的 VPC 配置，包括安全组规则、VPC 端点、网络访问控制列表 (ACL) 规则和路由表。它还会确认包含所需权限的 AWS Identity and Access Management (IAM) 实例配置文件已附加到该实例。

Important

本自动化操作手册不评估 IPv6 规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux , macOS, Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必填) 未报告为由 Systems Manager 管理的亚马逊 EC2 实例的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:StartAutomationExecution
- iam:ListRoles
- iam:GetInstanceProfile
- iam:ListAttachedRolePolicies
- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcEndpoints

文档步骤

- `aws:executeScript` - 收集实例的 `PingStatus`。
- `aws:branch` - 根据实例是否已报告为由 Systems Manager 管理的状态进行分支。
- `aws:executeAwsApi` - 收集有关该实例的详细信息，包括 VPC 配置。
- `aws:executeScript` - 如果适用，收集与已部署结合 Systems Manager 使用的 VPC 端点相关的其他详细信息，并确认附加到 VPC 端点的安全组允许 TCP 端口 443 上有来自该实例的入站流量。
- `aws:executeScript` - 检查路由表是否允许流向 VPC 端点或公共 Systems Manager 端点的流量。
- `aws:executeScript` - 检查网络 ACL 规则是否允许流向 VPC 端点或公共 Systems Manager 端点的流量。
- `aws:executeScript` - 检查与实例关联的安全组是否允许流向 VPC 端点或公有 Systems Manager 端点的出站流量。
- `aws:executeScript` - 检查附加到实例的实例配置文件是否包含提供所需权限的托管策略。
- `aws:branch` - 根据实例的操作系统进行分支。
- `aws:executeScript` - 提供对 `ssmagent-toolkit-linux` Shell 脚本的引用。
- `aws:executeScript` - 提供 `ssmagent-toolkit-windows` PowerShell 脚本参考。
- `aws:executeScript` - 生成自动化的最终输出。
- `aws:executeScript` - 如果实例 `PingStatus` 的为 `Online`，则返回该实例已由 Systems Manager 管理。

AWSsupport-TroubleshootPatchManagerLinux

描述

该AWSsupport-TroubleshootPatchManagerLinux运行手册使用中的工具 Patch Manager 对可能导致 Linux-based 托管节点补丁失败的常见问题进行故障排除。AWS Systems Manager本运行手册的主要目标是确定补丁命令失败的根本原因并提出补救方案。

如何工作？

AWSsupport-TroubleshootPatchManagerLinux运行手册会考虑您提供的情侣实例 ID/Command ID 以进行故障排除。如果未提供命令 ID，则它会在所提供的实例上选择最近 30 天内最新失败的补丁命令。检查命令状态、先决条件满足情况和操作系统分发后，运行手册会下载并运行日志分析器软件包。输出包括问题的根本原因以及修复问题所需的操作。

文档类型

自动化

所有者

Amazon

平台

- Amazon Linux 2 和 AL2023
- 红帽企业 Linux 8.X 和 9.X
- Centos 8.X 和 9.X
- SUSE 15.X

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:SendCommand
- ssm:DescribeDocument
- ssm:GetCommandInvocation
- ssm:ListCommands
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:GetDocument
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

说明

按照这些步骤对自动化进行配置：

1. 在 AWS Systems Manager 控制台 [AWSsupport-TroubleshootPatchManagerLinux](#) 中导航到。
2. 选择 Execute automation (执行自动化) 。
3. 对于输入参数，请输入以下内容：

- InstanceId (必填)：

使用交互式实例选择器选择补丁命令失败的基于 Linux 的 SSM 托管节点 (亚马逊弹性计算云 (Amazon EC2) 或混合激活服务器) 的 ID，或者手动输入 SSM 托管实例的 ID。

- AutomationAssumeRole (可选)：

输入允许 Automation 代表您执行操作的 IAM 角色的 ARN。如果未指定角色，Automation 将使用启动此运行手册的用户的权限。

- RunCommandId (可选)：

输入AWS-RunPatchBaseline文档的失败运行命令 ID。如果您未提供命令 ID，则运行手册将在选定实例上查找最近 30 天内最新的失败补丁命令。

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.

☒ Show interactive instance picker

i-0[REDACTED]

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Choose an option ▼

RunCommandId
(Optional) Failed Run Command ID of AWS-RunPatchBaseline. If not provided, we look for the latest unsuccessful execution of AWS-RunPatchBaseline for the instance and evaluate it. To confirm the command ID, look under Command History tab in the Run Command Console under AWS Systems Manager.

42[REDACTED]e

4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- CheckConcurrency:

确保只有一次针对同一个实例执行此运行手册。如果 runbook 发现针对同一实例的另一个执行正在进行中，则会返回错误并结束。

- ValidateCommand身份证:

验证是否已为 AWS-RunPatchBaseline SSM 文档执行了作为输入参数的命令 ID。如果未提供命令 ID，则运行手册将考虑选定实例在过去 30 天AWS-RunPatchBaseline内最近一次执行失败的情况。

- BranchOnCommandStatus:

确认所提供命令的状态为失败。否则，运行手册将结束执行并生成一份报告，说明所提供的命令已成功执行。

- VerifyPrerequisites:

确认上述先决条件已满足。

- GetPlatformDetails:

检索操作系统 (OS) 的发行版和版本。

- GetDownload网址 :

检索 L PatchManager og Analyzer 软件包的下载 URL。

- EvaluatePatchManagerLogs:

在实例上下载并执行 PatchManager Log Analyzer python 软件包以评估日志文件。

- GenerateReport:

生成运行手册执行的最终报告，其中包括已发现的问题和建议的解决方案。

7. 完成后，请查看“输出”部分，了解执行的详细结果：

```

▼ Outputs

GenerateReport.output
Starting 'python3 main.py i-0[REDACTED] 3e016680-82f4-45f4-845c-aa4685b4fab Ubuntu 22.04'

=====
TROUBLESHOOTING RESULTS
=====

[PROBLEM] :
The error found in the log file at /var/lib/amazon/ssm/i-0[REDACTED]/document/orchestration/3e016680-82f4-45f4-845c-aa4685b4fab/awsrunShellScript/PatchLinux/stdout is :
Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz.failed to run commands: exit status 156

[SOLUTION] :
Here are some suggestions to troubleshoot the issue:
Possible reasons for the above error are :
1. Network connectivity issue while accessing the s3 service endpoint from the instance to download the payload.
2. Instance doesn't have the required permissions to access the specified Amazon Simple Storage Service (Amazon S3) bucket.
3. No space left on the Instance.

To resolve this, ensure network connectivity to S3 endpoint from the instance. For more details, see information about required access to S3 buckets for Patch Manager in https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.
For testing purpose, try to manually access the above payload URL using curl or wget from within Instance. Command to run:
curl https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz --output payload.tar.gz

```

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)

- [设置自动化](#)
- [支持自动化工作流登录页面](#)

AWSupport-TroubleshootSessionManager

描述

AWSupport-TroubleshootSessionManager 运行手册可帮助您排除导致您无法使用会话管理器连接到托管 Amazon Elastic Compute Cloud (Amazon EC2) 实例的常见问题。会话管理器是一个工具 AWS Systems Manager。此运行手册检查以下各项：

- 检查实例是否正在运行并报告为由 Systems Manager 管理。
- 如果实例未报告为由 Systems Manager 管理，则运行 AWSupport-TroubleshootManagedInstance 运行手册。
- 检查安装在该实例上的 SSM Agent 的版本。
- 检查包含建议的会话管理器 AWS Identity and Access Management (IAM) 策略的实例配置文件是否已附加到 Amazon EC2 实例。
- 从实例收集 SSM 代理日志。
- 分析您的会话管理器首选项。
- AWSupport-AnalyzeAWSEndpointReachabilityFromEC2 运行手册以分析实例与会话管理器、AWS Key Management Service (AWS KMS)、亚马逊简单存储服务 (Amazon S3) 和 CloudWatch 亚马逊 CloudWatch 日志 (日志) 的终端节点的连接。

注意事项

- 不支持混合托管节点。
- 此运行手册仅检查建议的托管 IAM policy 是否已附加到实例配置文件。它不会分析 IAM 或实例配置文件中包含的 AWS KMS 权限。

Important

AWSupport-AnalyzeAWSEndpointReachabilityFromEC2 运行手册使用 [VPC Reachability Analyzer](#) 分析来源和服务端点之间的网络连接。每次在来源和目标之间运行分析时，您需要支付费用。有关详细信息，请参阅 [Amazon VPC 定价](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

类型：字符串

描述：(必需) 您无法使用会话管理器连接到的 Amazon EC2 实例的 ID。

- SessionPreferenceDocument

类型：字符串

默认：SSM-SessionManagerRunShell

描述：(可选) 会话首选项文档的名称。如果您在启动会话时未指定自定义会话首选项文档，则使用默认值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateNetworkInsightsPath

- `ec2:DeleteNetworkInsightsAnalysis`
- `ec2:DeleteNetworkInsightsPath`
- `ec2:StartNetworkInsightsAnalysis`
- `tiros>CreateQuery`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeManagedPrefixLists`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribePrefixLists`
- `ec2:DescribeRegions`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTransitGatewayAttachments`
- `ec2:DescribeTransitGatewayConnects`
- `ec2:DescribeTransitGatewayPeeringAttachments`
- `ec2:DescribeTransitGatewayRouteTables`
- `ec2:DescribeTransitGateways`
- `ec2:DescribeTransitGatewayVpcAttachments`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`

- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `ec2:GetManagedPrefixListEntries`
- `ec2:GetTransitGatewayRouteTablePropagations`
- `ec2:SearchTransitGatewayRoutes`
- `elasticloadbalancing:DescribeListeners`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeRules`
- `elasticloadbalancing:DescribeTags`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:DescribeTargetHealth`
- `iam:GetInstanceProfile`
- `iam:ListAttachedRolePolicies`
- `iam:ListRoles`
- `iam:PassRole`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `tiros:GetQueryAnswer`
- `tiros:GetQueryExplanation`

文档步骤

1. `aws:waitForAwsResourceProperty` : 最多等 6 分钟，目标实例就能通过状态检查。
2. `aws:executeScript` : 解析会话首选项文档。
3. `aws:executeAwsApi` : 获取附加到您的实例的实例配置文件的 ARN。
4. `aws:executeAwsApi` : 检查您的实例是否报告为由 Systems Manager 管理。
5. `aws:branch` : 根据您的实例是否报告为由 Systems Manager 管理进行分支。
6. `aws:executeScript` : 检查您的实例上安装的 SSM Agent 是否支持会话管理器。
7. `aws:branch` : 根据用于收集 `ssm-cli` 日志的实例的平台进行分支。
8. `aws:runCommand` : 从 Linux 或 macOS 实例收集 `ssm-cli` 的输出日志。
9. `aws:runCommand` : 从 Windows 实例收集 `ssm-cli` 的输出日志。
10. `aws:executeScript` : 解析 `ssm-cli` 日志。
11. `aws:executeScript` : 检查建议的 IAM policy 是否已附加到实例配置文件。
12. `aws:branch` : 确定是否根据 `ssm-cli` 日志评估 `ssmmessages` 端点连接。
13. `aws:executeAutomation` : 评估实例是否可以连接到 `ssmmessages` 端点。
14. `aws:branch` : 根据 `ssm-cli` 日志和会话首选项，确定是否评估 Amazon S3 端点连接。
15. `aws:executeAutomation` : 评估实例是否可以连接到 Amazon S3 端点。
16. `aws:branch` : 决定是否根据 `ssm-cli` 日志和会话首选项评估 AWS KMS 端点连接。
17. `aws:executeAutomation` : 评估实例是否可以连接到 AWS KMS 终端节点。
18. `aws:branch` : 根据 CloudWatch 日志和您的会话首选项确定是否评估 `ssm-cli` 日志端点连接。
19. `aws:executeAutomation` : 评估实例是否可以连接到 `CloudWatch logs` 端点。
20. `aws:executeAutomation` : 运行 `AWSSupport-TroubleshootManagedInstance` 运行手册。
21. `aws:executeScript` : 编译先前步骤的输出并输出一个报告。

输出

- `generateReport.EvalReport` - 运行手册以纯文本形式执行的检查结果。

Third-party

AWS Systems Manager 自动化为第三方产品和服务提供预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

AWS-CreateJiraIssue

描述

在 Jira 中创建问题。

Note

为了更好地控制和验证，我们建议[克隆](#)AWS-CreateJiraIssue运行手册以创建自己的私有版本。在克隆的运行手册中，为JiraURL参数添加[验证逻辑](#)，以确保它在执行之前与您批准的Jira实例相匹配。然后使用克隆的运行手册代替运行手册，AWS-managed并限制IAM的执行权限。AWS-CreateJiraIssue这种方法为您提供了更大的灵活性，并确保参数符合您组织的安全性和合规性要求。

[运行此自动化（控制台）](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AssigneeName

类型：字符串

描述：(必需) 应向其分配问题的人员的用户名。

- DueDate

类型：字符串

描述：(必需) yyyy-mm-dd 格式的问题的到期日期。

- IssueDescription

类型：字符串

描述：(必需) 问题的详细说明。

- IssueSummary

类型：字符串

描述：(必需) 问题的小结。

- IssueTypeName

类型：字符串

描述：(必填) 您要创建的问题类型的名称 (例如，任务 Sub-task、错误等)。

- JiraURL

类型：字符串

描述：(必需) Jira 实例的 URL。

- JiraUsername

类型：字符串

描述：(必需) 创建问题将使用的用户的名称。

- PriorityName

类型：字符串

描述：(可选) 问题的优先级的名称。

- ProjectKey

类型：字符串

描述：(必需)应在其中创建问题的项目的密钥。

- SSMPParameterName

类型：字符串

描述：(必需)包含 Jira 用户的 API 密钥或密码的加密 SSM 参数的名称。

文档步骤

`aws:createStack`-创建 CloudFormation 堆栈以创建 Lambda IAM 角色和函数。

`aws:invokeLambdaFunction` - 调用 Lambda 函数以创建 Jira 问题

`aws:deleteStack`-删除创建的 CloudFormation 堆栈。

输出

IssuedId: 新创建的 Jira 事务的 ID

AWS-CreateServiceNowIncident

描述

在事件表中创建 ServiceNow 事件。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 类别

类型：字符串

描述：(可选) 事件的类别。

有效值：无 | Inquiry/Help | 软件 | 硬件 | 网络 | 数据库

默认值：None

- 说明

类型：字符串

描述：(必需) 有关事件的详细说明。

- 影响

类型：字符串

描述：(可选) 事件对业务的影响。

有效值：High | Medium | Low

默认值：Low

- ServiceNowInstanceUsername

类型：字符串

描述：(必需) 创建事件时使用的用户的名称。

- ServiceNowInstancePassword

类型：字符串

描述：(必填) 包含 ServiceNow 用户密码的加密 SSM 参数的名称。

- ServiceNowInstanceURL

类型：字符串

描述：(必填) ServiceNow 实例的 URL

- ShortDescription

类型：字符串

描述：(必需) 事件的简要描述。

- 子类别

类型：字符串

描述：(可选) 事件的子类别。

有效值：None | Antivirus | Email | Internal Application | Operating System | CPU | Disk | Keyboard | Hardware | Memory | Monitor | Mouse | DHCP | DNS | IP Address | VPN | Wireless | DB2 | MS SQL Server | Oracle

默认值：None

文档步骤

Push_incident — 将事件信息推送到 ServiceNow。

输出

Push_incident.incidentID — 创建的事件 ID。

AWS-RunPacker

描述

本运行手册使用 HashiCorp [Packer](#) 工具来验证、修复或构建用于创建机器映像的打包程序模板。本运行手册使用 Packer v1.11.2。

Note

如果您指定了 `vpc_id` 值，则还必须指定公有子网的 `subnet_id` 值。除非您修改子网的 IPv4 公有寻址属性，否则还必须将 `associate_public_ip_address` 设置为 `true`。

⚠ Important

Packer 配置器在临时 EC2 实例上以根级权限执行。创作 Packer 模板时，请遵循最低权限做法。避免向置备者授予访问敏感实例元数据或本地凭证文件的权限。如果您已向[默认主机管理配置](#)使用的 IAM 角色添加了其他策略，请注意，在实例上以 root 身份运行的任何进程都可以访问这些扩展的权限。查看您的 Packer 模板，确保它们仅包含受信任的命令。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- Force

类型：布尔值

描述：在以前生成中的构件禁止生成运行时，强制生成器运行的 Packer 选项。

- Mode

类型：字符串

描述：在根据模板进行验证时使用 Packer 的模式或命令。选项包括 Build、Validate 和 Fix。

- **TemplateName**

类型：字符串

描述：S3 存储桶中的模板文件的名称或键。

- **TemplateS3BucketName**

类型：字符串

描述：包含 Packer 模板的 S3 存储桶的名称。

文档步骤

RunPackerProcessTemplate — 使用 Packer 工具对模板运行所选模式。

输出

RunPackerProcessTemplate.output — Packer 工具中的标准输出。

RunPackerProcessTemplate.fixed_template_key — 存储在 S3 存储桶中的模板名称，仅在“修复”模式下运行时使用。

RunPackerProcessTemplate.s3_bucket — 包含仅在“修复”模式下运行时使用的固定模板的 S3 存储桶的名称。

Amazon VPC

AWS Systems Manager Automation 为亚马逊 Virtual Private Cloud 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CloseSecurityGroup](#)
- [AWSSupport-ConfigureDNSQueryLogging](#)
- [AWSSupport-ConfigureTrafficMirroring](#)
- [AWSSupport-ConnectivityTroubleshooter](#)
- [AWSSupport-TroubleshootVPN](#)
- [AWSConfigRemediation-DeleteEgressOnlyInternetGateway](#)

- [AWSConfigRemediation-DeleteUnusedENI](#)
- [AWSConfigRemediation-DeleteUnusedSecurityGroup](#)
- [AWSConfigRemediation-DeleteUnusedVPCNetworkACL](#)
- [AWSConfigRemediation-DeleteVPCFlowLog](#)
- [AWSConfigRemediation-DetachAndDeleteInternetGateway](#)
- [AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway](#)
- [AWS-DisableIncomingSSHOnPort22](#)
- [AWS-DisablePublicAccessForSecurityGroup](#)
- [AWSConfigRemediation-DisableSubnetAutoAssignPublicIP](#)
- [AWSSupport-EnableVPCFlowLogs](#)
- [AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch](#)
- [AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket](#)
- [AWS-ReleaseElasticIP](#)
- [AWS-RemoveNetworkACLUnrestrictedSSHRDP](#)
- [AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules](#)
- [AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules](#)
- [AWSSupport-SetupIPMonitoringFromVPC](#)
- [AWSSupport-TerminateIPMonitoringFromVPC](#)

AWS-CloseSecurityGroup

描述

此运行手册将从您指定的安全组中删除所有入口和出口规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- SecurityGroupId

类型：字符串

描述：(必填) 要关闭的安全组的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文档步骤

- aws:executeScript-从您在参数中指定的安全组中移除所有入口和出口规则。SecurityGroupId

AWSsupport-ConfigureDNSQueryLogging

描述

AWSsupport-ConfigureDNSQueryLogging 运行手册为源自虚拟私有云 (VPC) 的或为 Amazon Route 53 托管区的 DNS 查询配置日志记录。您可以选择将查询日志发布到亚马逊日 CloudWatch 志、亚马逊简单存储服务 (Amazon S3) Service 或亚马逊 Data Firehose。有关查询日志记录和解析器查询日志的更多信息，请参阅[公共 DNS 查询日志记录](#)和[解析器查询日志记录](#)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LogDestinationArn

类型：字符串

描述：(可选) 您要向其发送查询日志的 CloudWatch 日志组、Amazon S3 存储桶或 Firehose 流的 ARN。请注意，Route 53 公共 DNS 查询日志记录仅支持 CloudWatch 日志组。如果您未为此参数指定值，则自动化会创建一个格式为的 CloudWatch 日志组 `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }`，以及用于发布查询日志的 IAM 资源策略。自动化创建的 CloudWatch 日志组的保留期为 14 天。

- QueryLogType

类型：字符串

描述：(可选) 要记录的查询的类型。

有效值：公开 | Resolver/Private

默认：公共

- ResourceId

类型：字符串

描述：(必需) 要记录其查询的资源的 ID。如果您为 QueryLogType 参数指定 Public，则资源必须是 Route 53 私有托管区的 ID。如果您为 QueryLogType 参数指定 Resolver/Private，则资源必须是 VPC 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeVpcs
- firehose:ListTagsForDeliveryStream
- firehose:PutRecord
- firehose:PutRecordBatch
- firehose:TagDeliveryStream
- iam:AttachRolePolicy
- iam:CreatePolicy
- iam:CreateRole
- iam:CreateServiceLinkedRole
- iam>DeletePolicy
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:PassRole
- iam:PutRolePolicy
- iam:TagRole
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs>DeleteLogDelivery

- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:DescribeResourcePolicies
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:PutRetentionPolicy
- logs:UpdateLogDelivery
- route53:CreateQueryLoggingConfig
- route53:DeleteQueryLoggingConfig
- route53:GetHostedZone
- route53resolver:AssociateResolverQueryLogConfig
- route53resolver:CreateResolverQueryLogConfig
- route53resolver:DeleteResolverQueryLogConfig
- s3:GetBucketAcl

文档步骤

- aws:executeScript - 验证您为 ResourceId 参数指定的资源是否存在，并检查资源类型是否匹配所需的 QueryLogType 选项。
- aws:executeScript - 验证您为 LogDestinationArn 参数指定的值是否匹配所需的 QueryLogType 值。
- aws:executeScript-验证 Route 53 向日志组发布日志所需的权限，如果不存在所需的 IAM 资源策略，则创建所需的 IAM 资源策略。 CloudWatch
- aws:executeScript - 对所选目标启用 DNS 查询日志记录。

AWSsupport-ConfigureTrafficMirroring

描述

AWSsupport-ConfigureTrafficMirroring 运行手册将配置流量镜像，以帮助您解决负载均衡器与 Amazon Elastic Compute Cloud (Amazon EC2) 实例之间的连接问题。流量镜像会复制来自附加到

您的实例的网络接口的入站和出站流量。要配置流量镜像，此运行手册将创建所需的目的地、筛选条件和会话。默认情况下，运行手册会为除 Amazon DNS 之外的所有协议的所有入站和出站流量配置镜像。如果您希望镜像来自特定来源和目的地的流量，则可以在自动化完成后修改入站和出站规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- SourceENI

类型：字符串

描述：(必需) 要为其配置流量镜像的弹性网络接口。

- Target

类型：字符串

描述：(必需) 镜像流量的目的地。必须指定网络接口、网络负载均衡器或网关负载均衡器端点的 ID。如果您指定了网络负载均衡器，则端口 4789 上必须有 UDP 侦听器。

- SessionNumber

类型：字符串

有效值：1-32766

描述：(必需)要使用的镜像会话的数量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateTrafficMirrorTarget
- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilter
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

文档步骤

- aws:executeScript - 运行脚本以创建一个目标。
- aws:executeAwsApi - 创建一个筛选规则。
- aws:executeAwsApi - 为所有入站流量创建一个镜像筛选规则。
- aws:executeAwsApi - 为所有出站流量创建一个镜像筛选规则。
- aws:executeAwsApi - 创建流量镜像会话。
- aws:executeAwsApi - 在筛选器或会话创建失败时删除筛选器。
- aws:executeAwsApi - 在筛选器或会话创建失败时删除目标。

输出

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.TargetIDOutput

AWSsupport-ConnectivityTroubleshooter

描述

AWSsupport-ConnectivityTroubleshooter 运行手册可诊断以下各项之间的连接问题：

- AWS 亚马逊虚拟私有云 (亚马逊 VPC) 中的资源
- AWS 同一个 Amazon VPC 中使用 VPC AWS 区域 对等互连连接的资源
- AWS Amazon VPC 中的资源和使用互联网网关的互联网资源
- AWS Amazon VPC 中的资源和使用网络地址转换 (NAT) 网关的互联网资源

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DestinationIP

类型：字符串

描述：(必需) 要连接到的资源的 IPv4 地址。

- DestinationPort

类型：字符串

默认：True

描述：(必需) 要在目的地资源上连接的端口号。

- DestinationVpc

类型：字符串

默认：全部

描述：(可选) 要测试与之连接性的 Amazon VPC 的 ID。

- SourceIP

类型：字符串

描述：(必填) 您想要测试连接的 Amazon VPC 中 AWS 资源的私有 IPv4 地址。

- SourcePortRange

类型：字符串

描述：(可选) 您的 Amazon VPC 中您想要测试连接的 AWS 资源所使用的端口范围。

- SourceVpc

类型：字符串

默认：全部

描述：(可选) 要测试连接性的 Amazon VPC 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

文档步骤

- `aws:executeScript` - 收集有关您在 `SourceIP` 参数中指定的 AWS 资源的详细信息。
- `aws:executeScript` - 使用上一步收集的路由，确定来自 AWS 资源的网络流量的目的地。
- `aws:branch` - 根据网络流量的目的地进行分支。
- `aws:executeAwsApi` - 收集有关目的地资源的详细信息。
- `aws:executeScript` - 确认为目的地 Amazon VPC 返回的 ID 匹配在 `DestinationVpc` 参数中指定的值 (如果有)。
- `aws:executeAwsApi` - 收集源资源和目的地资源的安全组规则。
- `aws:executeScript` - 确认安全组规则是否允许来源资源和目的地资源之间所需的流量。
- `aws:executeAwsApi` - 收集与来源资源和目的地资源的子网关联的网络访问控制列表 (NACL)。
- `aws:executeScript` - 确认 NACL 是否允许来源资源和目的地资源之间所需的流量。
- `aws:executeScript` - 在路由目的地是互联网网关时确认来源是否拥有与资源关联的公有 IP 地址。
- `aws:executeAwsApi` - 收集来源资源的安全组规则。
- `aws:executeScript` - 确认安全组规则是否允许从来源资源到目的地资源的所需流量。
- `aws:executeAwsApi` - 为来源资源收集与子网关联的 NACL。
- `aws:executeScript` - 确认 NACL 是否允许来自来源资源的所需流量。
- `aws:executeAwsApi` - 收集 NAT 网关的详细信息。
- `aws:executeAwsApi` - 为 NAT 网关收集与 NAT 网关的子网关联的 NACL。
- `aws:executeScript` - 确认 NACL 是否允许来自 NAT 网关的子网的所需流量。
- `aws:executeScript` - 收集与 NAT 网关的子网关联的路由。
- `aws:executeScript` - 确认 NAT 网关是否具有到互联网网关的路由。
- `aws:executeAwsApi` - 收集有关 VPC 对等连接的详细信息。
- `aws:executeScript` - 确认两个 VPC 位于同一区域，并且为目的地 VPC 返回的 ID 匹配 `DestinationVpc` 参数中指定的值 (若有)。

- `aws:executeAwsApi` - 返回目的地资源的子网。
- `aws:executeScript` - 收集与对等连接 VPC 的子网关联的路由。
- `aws:executeScript` - 确认对等连接 VPC 是否有到对等连接的路由。
- `aws:executeScript` - 确认当自动化不支持目的地时是否允许来自源资源的流量。

AWSSupport-TroubleshootVPN

描述

AWSSupport-TroubleshootVPN运行手册可帮助您跟踪和解决 AWS Site-to-Site VPN 连接中的错误。自动化包括多项自动检查，旨在跟踪IKEv1与 AWS Site-to-Site VPN 连接隧道相关的IKEv2错误。自动化将尝试匹配特定的错误及其相应的解决方案，从而形成常见问题列表。

注意：此自动化并不能纠正错误。它在上述时间范围内运行，并扫描日志组中是否存在 [VPN CloudWatch 日志组](#) 中的错误。

如何工作？

运行手册运行参数验证，以确认输入参数中包含的 Amazon CloudWatch 日志组是否存在、日志组中是否存在与 VPN 隧道日志记录相对应的日志流、VPN 连接 ID 是否存在以及隧道 IP 地址是否存在。它会在配置为 VPN 日志记录的 CloudWatch 日志组上进行 Logs Insights API 调用。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LogGroupName

类型：字符串

描述：(必填) 为 AWS Site-to-Site VPN 连接 CloudWatch 日志配置的 Amazon 日志组名称

允许的模式：`^[\\.\-_\/#A-Za-z0-9]{1,512}`

- VpnConnectionId

类型：字符串

描述：(必填) 要进行故障排除的 AWS Site-to-Site VPN 连接 ID。

允许的模式：`^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

类型：字符串

描述：(必需) 与您的 AWS Site-to-Site VPN 关联的隧道编号 1 的 IPv4 地址。

允许的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}$`

- TunnelBIPAddress

类型：字符串

描述：(可选) 与 AWS Site-to-Site VPN 关联的隧道编号 2 的 IPv4 地址。

允许的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

类型：字符串

描述：(必需) 选择您正在使用的 IKE 版本。允许的值：IKEv1、IKEv2

有效值：`['IKEv1', 'IKEv2']`

- StartTimeinEpoch

类型：字符串

描述：(可选) 日志分析的开始时间。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 进行日志分析

允许的模式：`^\d{10}|^$`

- EndTimeinEpoch

类型：字符串

描述：(可选) 日志分析的结束时间。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 进行日志分析。如果两者兼 StartTimeinEpoch/EndTimeinEpoch 而有之 LookBackPeriod ，则优 LookBackPeriod 先

允许的模式：`^\d{10}|^$`

- LookBackPeriod

类型：字符串

描述：(可选) 以小时为单位的两位数时间，用于回顾日志分析。有效范围：01 - 99。如果您还给出 StartTimeinEpoch和，则此值优先 EndTime

允许的模式：`^(\d?[1-9]| [1-9]0)|^$`

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- logs:DescribeLogGroups
- logs:GetQueryResults
- logs:DescribeLogStreams
- logs:StartQuery
- ec2:DescribeVpnConnections

说明

注意：当 CloudWatch 日志输出格式为 JSON 时，此自动化适用于为 VPN 隧道日志记录配置的日志组。

按照这些步骤对自动化进行配置：

1. 在 AWS Systems Manager 控制台[AWSsupport-TroubleshootVPN](#)中导航到。

2. 要输入参数，请输入以下内容：

- AutomationAssumeRole (可选)：

允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LogGroupName (必填)：

要验证的 Amazon CloudWatch 日志组名称。这必须是为 VPN 配置的 CloudWatch 日志组，以便向其发送日志。

- VpnConnectionId (必填)：

因为 VPN 错误而跟踪其日志组的 AWS Site-to-Site VPN 连接 ID。

- 隧道 IP 地址 (必需)：

隧道 A 与您的 AWS Site-to-Site VPN 连接关联的 IP 地址。

- TunnelBIPAddress (可选)：

与您的 AWS Site-to-Site VPN 连接关联的隧道 B IP 地址。

- ike版本 (必需)：

选择您正在使用的 IKEVersion。允许的值：IKEv1、IKEv2。

- StartTimeinEpoch (可选)：

查询错误的时间范围的起点。该范围包括在内，因此查询中包含了指定的开始时间。指定为纪元时间，即自 1970 年 1 月 1 日 00:00:00 UTC 以来的秒数。

- EndTimeinEpoch (可选)：

查询错误的时间范围的结束时间。该范围包括在内，因此查询中包含了指定的结束时间。指定为纪元时间，即自 1970 年 1 月 1 日 00:00:00 UTC 以来的秒数。

- LookBackPeriod (必填)：

回顾错误查询所需的时间（以小时为单位）。

注意：配置 StartTimeEpoch EndTimeEpoch、或 LookBackPeriod 以固定日志分析的时间范围。给出一个以小时为单位的两位数数字，以检查从自动化开始时间起过去是否有错误。或者，如果错误发生在特定的时间范围内，请使用 StartTimeEpoch 和 EndTimeEpoch，而不是 LookBackPeriod。

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. Choose an option	LogGroupName (Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs. vpnlog
VpnConnectionId (Required) The AWS Site-to-Site VPN connection id to be validated. vpn-123abc456zxc	TunnelAPIAddress (Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated. 1.1.1.1
TunnelBIPAddress (Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated. String	IKEVersion (Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both IKEv1
StartTimeEpoch (Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String	EndTimeEpoch (Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String
LookBackPeriod (Required) Time in hours to look back for log analysis 05	

3. 选择执行。

4. 自动化启动。

5. 自动化运行手册执行以下步骤：

- parameterValidation：

对自动化中包含的输入参数运行一系列验证。

- 分支OnValidationOfLogGroup:

检查参数中提到的日志组是否有效。如果无效，它会停止进一步启动自动化步骤。

- 分支OnValidationOfLogStream:

检查包含的日志组中是否存在 CloudWatch 日志流。如果无效，它会停止进一步启动自动化步骤。

- 分支OnValidationOfVpnConnectionId:

检查参数中包含的 VPN 连接 ID 是否有效。如果无效，它会停止进一步启动自动化步骤。

- 分支OnValidationOfVpnIp:

检查参数中提到的隧道 IP 地址是否有效。如果无效，它会停止进一步执行自动化步骤。

- traceError：

在包含的 CloudWatch 日志组中调用 logs insight API，并搜索与相关的错误 IKEv1/IKEv2 以及相关的建议解决方案。

6. 完成后，查看“输出”部分以了解执行的详细结果。

▼ Outputs

parameterValidation.LogGroupName

LogGroupValid

parameterValidation.VpnConnection

validVpnConnection

traceErrorTunnelIkeV2

("IKEv2ErrorCount":0)

traceErrorTunnel2IkeV2

("IKEv2ErrorCount":0)

traceErrorTunnel1IkeV1

["Error related to : AWS tunnel received DELETE for Phase 2 SA":"
Please treat below as Potential resolution of this error :

AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AWS receives Delete_SA for Phase 2 from CGW it deletes the Phase 2 of SPI mentioned in Delete_SA request.
Possible reason of CGW sending Delete_SA message can be due to any configurational changes made in CGW side

Next Steps:

* Check IPsec Logs on the CGW Device to verify if you are able to see information pertaining to this issue.

References:
[1] Tunnel stability issues during a rekey: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-fix-ikev2-tunnel-instability-rekey/
[2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/
","Error related to : AWS tunnel received DELETE for IKE_SA from CGW":"
Please treat below as Potential resolution of this error :
AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AWS receives Delete_SA from CGW, it honours the message and brings down the VPN tunnel.
There can be various reasons for CGW sending Delete_SA message like :

* A reset to clear active SAs has been performed on the CGW side
* IKE SA has been timed out
* Configurational changes have been made on CGW

Next Steps:

* Review your VPN device idle timeout settings using information from your device vendor. When there is no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates. For more information on tunnel inactivity and instability refer to this documentation [1]
* Check logs on your CGW device to verify if you are able to see information pertaining to this issue.

References:
[1] Tunnel inactivity or instability: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/
","Error related to : No proposal chosen":"
Please treat below as Potential resolution of this error :

AWS CloudWatch monitoring has detected that IKE Phase 2 parameters (such as encryption algorithm, hashing algorithm and DH group) configured on Customer Gateway (CGW) device and AWS VPN endpoint do not match or the CGW is using parameters that are not supported by the AWS VPN.

Next Steps:

* Verify that the Phase 2 parameters (Integrity algorithm, Encryption algorithm and DH group) being proposed by CGW are matching with those configured on AWS side. If you are using default settings on AWS side then verify that parameters being proposed are supported by AWS VPN. To Find list of parameters supported by

* If you want to modify the parameters on the AWS VPN side you can follow below steps:
Step 1: Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
Step 2: In the navigation pane, choose Site-to-Site VPN Connections.
Step 3: Select the Site-to-Site VPN connection, and choose Actions, Modify VPN Tunnel Options.
Step 4: For VPN Tunnel Outside IP Address, choose the tunnel endpoint IP of the VPN tunnel that you are modifying options for.
Step 5: Choose or enter new values for the tunnel options .
Step 6: Choose Save.

参考

Systems Manager Automation

- [运行此自动化（控制台）](#)
- [运行自动化](#)
- [设置自动化](#)
- [支持自动化 workflows 登录页面](#)

AWS 服务文档

- [Site-to-Site VPN 日志的内容](#)

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

描述

AWSConfigRemediation-DeleteEgressOnlyInternetGateway 运行手册删除指定的仅出口互联网网关。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- EgressOnlyInternetGatewayId

类型：字符串

描述：(必需) 要删除的仅出口互联网网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

文档步骤

- `aws:executeScript` - 删除 `EgressOnlyInternetGatewayId` 参数中指定的仅出口互联网网关。
- `aws:executeScript` - 验证仅出口互联网网关是否已被删除。

AWSConfigRemediation-DeleteUnusedENI

描述

AWSConfigRemediation-DeleteUnusedENI 运行手册将删除连接状态为 `detached` 的弹性网络接口 (ENI)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- `NetworkInterfaceId`

类型：字符串

描述：(必需) 要删除的 ENI ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

文档步骤

- `aws:executeAwsApi` - 删除您在 `NetworkInterfaceId` 参数中指定的 ENI。
- `aws:executeScript` - 验证 ENI 是否已被删除。

AWSConfigRemediation-DeleteUnusedSecurityGroup

描述

AWSConfigRemediation-DeleteUnusedSecurityGroup 运行手册将删除您在 `GroupId` 参数中指定的安全组。如果您尝试删除与 Amazon Elastic Compute Cloud (Amazon EC2) 实例关联的安全组或由另一个安全组引用的安全组，则自动化将失败。此自动化不会删除默认的安全组。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- **GroupId**

类型：字符串

描述：(必需) 要删除的安全组 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2>DeleteSecurityGroup

文档步骤

- aws:executeAwsApi - 使用您在 GroupId 参数中提供的值返回安全组名称。
- aws:branch - 确认群组名称不是“default”。
- aws:executeAwsApi - 删除 GroupId 参数中指定的安全组。
- aws:executeScript - 确认安全组已删除。

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

描述

AWSConfigRemediation-DeleteUnusedVPCNetworkACL 运行手册删除将删除不与子网关联的网络访问控制列表 (ACL)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- NetworkAcId

类型：字符串

描述：(必需) 要删除的网络 ACL 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAcl
- ec2:DescribeNetworkAcls

文档步骤

- aws:executeAwsApi - 删除 NetworkAcId 参数中指定的网络 ACL。
- aws:executeScript - 确认 NetworkAcId 参数中指定的网络 ACL 已删除。

AWSConfigRemediation-DeleteVPCFlowLog

描述

AWSConfigRemediation-DeleteVPCFlowLog 运行手册将删除您指定的虚拟私有云 (VPC) 流日志。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- FlowLogId

类型：字符串

描述：(必需) 要删除的流日志的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs

文档步骤

- aws:executeAwsApi - 删除您在 FlowLogId 参数中指定的流日志。

- `aws:executeScript` - 验证流日志是否已删除。

AWSConfigRemediation-DetachAndDeleteInternetGateway

描述

AWSConfigRemediation-DetachAndDeleteInternetGateway 运行手册将分离并删除您指定的互联网网关。如果您的虚拟私有云 (VPC) 中的任何 Amazon EC2 实例具有与之关联的弹性 IP 地址或公有 IPv4 地址，运行手册将失败。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- InternetGatewayId

类型：字符串

描述：(必需) 要删除的互联网网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

文档步骤

- `aws:waitForAwsResourceProperty` - 接受虚拟专用网关的 ID，然后等到虚拟专用网关的状态属性变为 `available` 或超时。
- `aws:executeAwsApi` - 检索指定的虚拟专用网关配置。
- `aws:branch`-基于 `VpcAttachments.state`参数值的分支。
- `aws:waitForAwsResourceProperty`-接受虚拟专用网关的 ID，并等待虚拟专用网关 `VpcAttachments.state`的属性更改为 `attached`或超时。
- `aws:executeAwsApi` - 接受虚拟专用网关 ID 和 Amazon VPC 的 ID 作为输入，并将虚拟专用网关与 Amazon VPC 分离。
- `aws:waitForAwsResourceProperty`-接受虚拟专用网关的 ID，并等待虚拟专用网关 `VpcAttachments.state`的属性更改为 `detached`或超时。
- `aws:executeAwsApi` - 接受虚拟专用网关的 ID 作为输入并将其删除。
- `aws:waitForAwsResourceProperty` - 接受虚拟专用网关的 ID 作为输入，并验证是否将其删除。
 - `aws:executeAwsApi` - 从 互联网网关 ID 收集 VPC ID。
- `aws:executeAwsApi` - 将互联网网关 ID 与 VPC 分离。
- `aws:executeAwsApi` - 删除互联网网关。

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

描述

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 运行手册将分离并删除给定的 Amazon Elastic Compute Cloud (Amazon EC2) 虚拟专用网关，该网关附加到通过 Amazon Virtual Private Cloud (Amazon VPC) 创建的虚拟私有云 (VPC) 。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- VpnGatewayId

类型：字符串

描述：(必需) 要删除的虚拟专用网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteVpnGateway
- ec2:DetachVpnGateway
- ec2:DescribeVpnGateways

文档步骤

- `aws:waitForAwsResourceProperty` - 接受虚拟专用网关的 ID，然后等到虚拟专用网关的状态属性变为 `available` 或超时。
- `aws:executeAwsApi` - 检索指定的虚拟专用网关配置。
- `aws:branch`-基于 `VpcAttachments.state`参数值的分支。
- `aws:waitForAwsResourceProperty`-接受虚拟专用网关的 ID，并等待虚拟专用网关 `VpcAttachments.state`的属性更改为`attached`或超时。
- `aws:executeAwsApi` - 接受虚拟专用网关 ID 和 Amazon VPC 的 ID 作为输入，并将虚拟专用网关与 Amazon VPC 分离。
- `aws:waitForAwsResourceProperty`-接受虚拟专用网关的 ID，并等待虚拟专用网关 `VpcAttachments.state`的属性更改为`detached`或超时。
- `aws:executeAwsApi` - 接受虚拟专用网关的 ID 作为输入并将其删除。
- `aws:waitForAwsResourceProperty` - 接受虚拟专用网关的 ID 作为输入，并验证是否将其删除。

AWS-DisableIncomingSSHOnPort22

描述

该AWS-DisableIncomingSSHOnPort22运行手册删除了允许安全组在 TCP 端口 22 上不受限制地传入 SSH 流量的规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- SecurityGroupIds

类型：字符串

描述：(必填) 要限制 SSH 流量的安全组的 ID 列表，以逗号分隔。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

文档步骤

- aws:executeAwsApi-从您在SecurityGroupIds参数中指定的安全组中移除允许通过 TCP 端口 22 传入 SSH 流量的所有规则。

输出

DisableIncomingSSTemplate.RestrictedSecurityGroupIds -已移除入站 SSH 规则的安全组的 ID 列表。

AWS-DisablePublicAccessForSecurityGroup

描述

本运行手册禁用对所有 IP 地址开放的默认 SSH 和 RDP 端口。

⚠ Important

对于满足以下两个条件的安全组，此运行手册失败并出现 `InvalidPermission.NotFound` “” 错误：1) 安全组位于非默认 VPC 中；2) 安全组的入站规则未使用以下所有四个模式指定开放端口：

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

ℹ Note

本运行手册在中国 AWS 区域 境内尚不可用。

运行此自动化 (控制台)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- GroupId

类型：字符串

描述：(必需) 端口应被禁用的安全组的 ID。

- IpAddressToBlock

类型：字符串

描述：(可选) 访问应被阻止的其他 IPv4 地址，格式为 1.2.3.4/32。

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

描述

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 运行手册将禁用您指定的子网的公有 IPv4 寻址属性。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- SubnetId

类型：字符串

描述：(必需) 要对其禁用自动分配公有 IPv4 地址属性的子网的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSubnets
- ec2:ModifySubnetAttribute

文档步骤

- aws:executeAwsApi - 禁用您在 SubnetId 参数中指定的子网的自动分配公有 IPv4 地址属性。
- aws:assertAwsResourceProperty - 验证该属性是否已被禁用。

AWSSupport-EnableVPCFlowLogs

描述

该AWSSupport-EnableVPCFlowLogs 运行手册为子网、网络接口以及您的子网、网络接口创建亚马逊虚拟私有云 (Amazon VPC) 流日志。VPCs AWS 账户如果您为子网或 VPC 创建流日志，则会监控该子网或 Amazon VPC 中的每个网络接口。流日志数据将发布到亚马逊 CloudWatch 日志组或您指定的亚马逊简单存储服务 (Amazon S3) 存储桶。有关流日志的更多信息，请参阅《Amazon VPC 用户指南》中的 [VPC 流日志](#)。

Important

当您将流日志发布到 Logs 或 Amazon S3 时，会收取已售日志的数据摄取 CloudWatch 和存档费用。有关更多信息，请参阅[流日志定价](#)

[运行此自动化 \(控制台\)](#)

 Note

选择s3作为日志目标时，请确保持续桶策略允许日志传输服务访问存储桶。有关更多信息，请参阅[流日志的 Amazon S3 存储桶权限](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- DeliverLogsPermissionArn

类型：字符串

描述：（可选）允许亚马逊弹性计算云 (Amazon EC2) 将流日志发布到您账户中的日志组的 IAM 角色的 ARN。CloudWatch 如果您为 LogDestinationType 参数指定了 s3，则不要为该参数提供值。有关更多信息，请参阅 Amazon VPC 用户指南中的[向 CloudWatch 日志发布流](#)日志。

- LogDestinationARN

类型：字符串

描述：（可选）要向其发布流日志数据的资源的 ARN。如果cloud-watch-logs为LogDestinationType参数指定，请提供要向其发布流 CloudWatch 日志数据的日志组的

ARN。或者，改用 LogGroupName。如果为 LogDestinationType 参数指定了 s3，则必须为此参数指定您要向其发布流日志数据的 Amazon S3 存储桶的 ARN。您还可以指定存储桶中的文件夹。

 Important

选择 s3 作为时，LogDestinationType 您应确保所选存储桶遵循 [Amazon S3 存储桶安全最佳实践](#)，并遵守您所在组织和地理区域的数据隐私法。

- LogDestinationType

类型：字符串

有效值：cloud-watch-logs| s3

描述：(必需) 确定流日志数据的发布位置。如果将 LogDestinationType 指定为 s3，则不要指定 DeliverLogsPermissionArn 或 LogGroupName。

- LogFormat

类型：字符串

描述：(可选) 要包含在流日志中的字段，以及它们在记录中出现的顺序。有关可用字段的列表，请参阅《Amazon VPC 用户指南》中的[流日志记录](#)。如果不为该参数指定值，则使用默认的格式创建流日志。如果指定此参数，则必须至少指定一个字段。

- LogGroupName

类型：字符串

描述：(可选) 发布流 CloudWatch 日志数据的日志日志组的名称。如果您为 LogDestinationType 参数指定了 s3，则不要为该参数提供值。

- ResourceIds

类型：StringList

描述：(必填) 要 IDs 为其创建流日志的子网、弹性网络接口或 VPC 的以逗号分隔的列表。

- TrafficType

类型：字符串

有效值：ACCEPT | REJECT | ALL

描述：(必需) 要记录的流量的类型。您可以记录资源接受或拒绝的流量，或者记录所有流量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs
- iam:AttachRolePolicy
- iam:CreateRole
- iam:CreatePolicy
- iam>DeletePolicy
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:TagRole
- iam:PassRole
- iam:PutRolePolicy
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs>DeleteLogDelivery
- logs>DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- s3:GetBucketLocation
- s3:GetBucketAcl

- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

政策示例

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMExecutionPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2FlowLogsPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFlowLogs",
        "ec2>DeleteFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:subnet/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:vpc/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway-attachment/resource-id"
      ]
    }
  ]
}
```

```

        "Sid": "IAMCreateRolePermissions",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:CreatePolicy",
            "iam>DeletePolicy",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam:GetPolicy",
            "iam:GetRole",
            "iam:TagRole",
            "iam:PassRole",
            "iam:PutRolePolicy",
            "iam:UpdateRole"
        ],
        "Resource": [
            "arn:aws:iam::111122223333:role/role-name",
            "arn:aws:iam::111122223333:role/AWSSupportCreateFlowLogsRole"
        ]
    },
    {
        "Sid": "CloudWatchLogsPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogDelivery",
            "logs:CreateLogGroup",
            "logs>DeleteLogDelivery",
            "logs>DeleteLogGroup",
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": [
            "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name",
            "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name:"
        ]
    },
    {
        "Sid": "S3Permissions",
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",

```



```

        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:ListBucket",
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
}
]
}
```

文档步骤

- aws:branch - 根据为 LogDestinationType 参数指定的值进行分支。
- aws:executeScript - 检查目标亚马逊简单存储服务 (Amazon S3) Simple Storage Service 是否有可能授予对其对象的读取或public写入权限。
- aws:executeScript - 在没有为 LogDestinationARN 参数指定任何值但为 LogDestinationType 参数指定了 cloud-watch-logs 时创建一个日志组值。
- aws:executeScript - 根据运行手册参数中指定的值创建流日志。

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

描述

该AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch运行手册将向亚马逊简单存储服务 (Amazon S3) Simple Storage Service 发布流日志数据的现有 Amazon VPC 流日志替换为将流日志数据发布到您指定的 CloudWatch 亚马逊日志CloudWatch (日志) 日志组的流日志。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DestinationLogGroup

类型：字符串

描述：(必填) 要向其发布流 CloudWatch 日志数据的日志组的名称。

- DeliverLogsPermissionArn

类型：字符串

描述：(必填) 您要使用的 AWS Identity and Access Management (IAM) 角色的 ARN，该角色为亚马逊弹性计算云 (Amazon EC2) 提供向日志发布流日志数据的必要权限。 CloudWatch

- FlowLogId

类型：字符串

描述：(必需) 要替换的发布到 Amazon S3 的流日志的 ID。

- MaxAggregationInterval

类型：整数

有效值：60 | 600

描述：(可选) 捕获数据包流并聚合到流日志记录中的最长时间间隔 (以秒为单位)。

- TrafficType

类型：字符串

有效值：ACCEPT | REJECT | ALL

描述：(必需) 要记录和发布的流日志数据的类型。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs

文档步骤

- aws:executeAwsApi - 从您在 FlowLogId 参数中指定的值收集有关 VPC 的详细信息。
- aws:executeAwsApi - 根据您为运行手册参数指定的值创建一个流日志。
- aws:assertAwsResourceProperty - 验证新创建的流日志已发布到 CloudWatch 日志。
- aws:executeAwsApi - 删除发布到 Amazon S3 的流日志。
- aws:executeScript - 确认发布到 Amazon S3 的流日志已删除。

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

描述

该AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket运行手册将向亚马逊 CloudWatch 日志 (日志) 发布流日志数据的现有 Amazon VPC 流CloudWatch 日志替换为将流日志数据发布到您指定的亚马逊简单存储服务 (Amazon S3) 存储桶的流日志。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- DestinationS3BucketArn

类型：字符串

描述：(必需) 要将流日志数据发布到的 Amazon S3 存储桶的 ARN。

- FlowLogId

类型：字符串

描述：(必填) 发布到要替换的 CloudWatch 日志的流日志的 ID。

- MaxAggregationInterval

类型：整数

有效值：60 | 600

描述：(可选) 捕获数据包流并聚合到流日志记录中的最长时间间隔 (以秒为单位)。

- TrafficType

类型：字符串

有效值：ACCEPT | REJECT | ALL

描述：(必需) 要记录和发布的流日志数据的类型。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

文档步骤

- `aws:executeAwsApi` - 从您在 `FlowLogId` 参数中指定的值收集有关 VPC 的详细信息。
- `aws:executeAwsApi` - 根据您为运行手册参数指定的值创建一个流日志。
- `aws:assertAwsResourceProperty` - 验证新创建的流日志是否发布到 Amazon S3。
- `aws:executeAwsApi`-删除发布到日志的流 CloudWatch 日志。
- `aws:executeScript`-确认已删除发布到 CloudWatch 日志的流日志。

AWS-ReleaseElasticIP

描述

使用分配 ID 释放指定的弹性 IP 地址。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AllocationId

类型：字符串

描述：(必需) 弹性 IP 地址的分配 ID。

AWS-RemoveNetworkACLUnrestrictedSSHRDP

描述

AWS-RemoveNetworkACLUnrestrictedSSHRDP运行手册从指定的网络 ACL 中删除了所有网络访问控制列表 (ACL) 规则，这些规则允许从所有源地址到默认 SSH 和 RDP 端口的入口流量。包含与默认 SSH 和 RDP 端口重叠的端口范围的规则不会被删除。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- NetworkAcId

类型：字符串

描述：(必填) 要删除的网络 ACL 的 ID，这些规则允许从所有源地址到默认 SSH 和 RDP 端口的入口流量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAclEntry
- ec2:DescribeNetworkAcls

文档步骤

- aws:executeScript - 从您在 SecurityGroupId 参数中指定的安全组中移除所有允许流量来自任何源地址的入口规则。

输出

RemoveNACLEntriesAndVerify.VerificationMessage -成功删除网络 ACL 规则的验证消息。

RemoveNACLEntriesAndVerify.RulesDeletedAndApiResponses -已删除的网络 ACL 规则以及 DeleteNetworkAclEntry API 操作响应。

AWSConfigRemediation- RemoveUnrestrictedSourceIngressRules

描述

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 运行手册将从您指定的安全组中移除所有允许流量来自任何源地址的入口规则。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- SecurityGroupId

类型：字符串

描述：(必需) 要从中移除入口规则的安全组的 ID，该入口规则允许流量来自任何源地址。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

文档步骤

- aws:executeScript - 从您在 SecurityGroupId 参数中指定的安全组中移除所有允许流量来自任何源地址的入口规则。

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

描述

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules 运行手册将从您指定的虚拟私有云 (VPC) 的默认安全组中移除所有规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- GroupId

类型：字符串

描述：(必需) 要从其中移除所有规则的安全组的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文档步骤

- `aws:assertAwsResourceProperty` - 确认您在 `GroupId` 参数中指定的安全组命名为 `default`。
- `aws:executeScript` - 从您在 `GroupId` 参数中指定的安全组中移除所有规则。

AWSSupport-SetupIPMonitoringFromVPC

描述

AWSSupport-SetupIPMonitoringFromVPC 在指定子网中创建一个 Amazon Elastic Compute Cloud (Amazon EC2) 实例，然后通过持续运行 ping、MTR、traceroute 和 tracertcp 测试来监控选定的目标 IP (IPv4 或 IPv6)。结果存储在 Amazon CloudWatch Logs 日志中，并应用指标筛选器在 CloudWatch 控制面板中快速可视化延迟和丢包统计数据。

附加信息

CloudWatch 日志数据可用于网络故障排除和分析 pattern/trends。此外，当丢包 and/or 延迟达到阈值时，您可以使用 Amazon SNS 通知配置 CloudWatch 警报。这些数据也可以在开案时使用 AWS 支持，以帮助快速隔离问题，并在调查网络问题时缩短解决时间。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CloudWatchLogGroupNamePrefix

类型：字符串

默认：/AWSSupport-SetupIPMonitoringFromVPC

描述：(可选) 用于为测试结果创建的每个 CloudWatch 日志组的前缀。

- CloudWatchLogGroupRetentionInDays

类型：字符串

有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

默认：7

描述：(可选) 要保留网络监控结果的天数。

- InstanceType

类型：字符串

有效值：t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

默认：t3.micro

描述：(可选) EC2Rescue 实例的 EC2 实例类型。推荐尺寸：t3.micro。

- SubnetId

类型：字符串

描述：(必需) 监控实例的子网 ID。请注意，如果您指定私有子网，则必须确保可以访问 Internet 才能允许监控实例设置测试 (也就是说，安装 CloudWatch 日志代理，与 Systems Manager 交互和 CloudWatch)。

- TargetIPs

类型：字符串

描述：(必填) 要监控的 IPv4 IPv6 列表，以逗号分隔。and/or 不允许使用空格。最大大小为 255 个字符。注意，如果提供的 IP 无效，则 Automation 将失败并回滚测试设置。

- TestInstanceSecurityGroupId

类型：字符串

描述：(可选) 测试实例的安全组 ID。如果未指定，则自动化会在创建实例期间创建一个实例。确保安全组允许对监控 IP 进行出站访问。

- TestInstanceProfileName

类型：字符串

描述：(可选) 测试实例的现有 IAM 实例配置文件的名称。如果未指定，则自动化会在创建实例期间创建一个实例。该角色必须具有以下权限：

logs:CreateLogStream、logs:DescribeLogGroups、logs:DescribeLogStreams、logs:PutLogEvents。AWS 托管策略 AmazonSSMManagedInstanceCore。

- TestInterval

类型：字符串

描述：(可选) 测试间隔之间的分钟数。默认值为 1 分钟，最大值为 10 分钟。

- RetainDashboardAndLogsOnDeletion

类型：字符串

描述：(可选) 指定 False 在删除 AWS CloudFormation 堆栈时删除 Amazon CloudWatch 控制面板和日志。默认值为 True。默认情况下，控制面板和日志会被保留，当不再需要它们时，需要手动将其删除。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

Warning

建议传递 TestInstanceProfileName 参数或确保设置安全护栏，以防止滥用可变的 IAM 权限。

建议运行自动化的用户附加 AmazonSSMAutomationRoleIAM 托管策略。此外，用户还必须将以下策略附加到其用户账户、组或角色：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:GetRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:TagRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/SetupIPMonitoringFromVPC*",
        "arn:aws:iam::111122223333:instance-profile/SetupIPMonitoringFromVPC*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudwatch:PutDashboard",
        "cloudwatch>DeleteDashboards",
        "ec2:AuthorizeSecurityGroupEgress",
```

```

        "ec2:CreateSecurityGroup",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSecurityGroup",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplates",
        "ec2:RevokeSecurityGroupEgress",
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]
}
```

如果提供了TestInstanceProfileName参数，则不需要以下 IAM 权限即可执行运行手册：

- 我是：CreateRole

- 我是 : CreateInstanceProfile
- 我是 : DetachRolePolicy
- 我是 : AttachRolePolicy
- 我是 : AddRoleToInstanceProfile
- 我是 : RemoveRoleFromInstanceProfile
- 我是 : DeleteRole
- 我是 : DeleteRolePolicy
- 我是 : DeleteInstanceProfile

文档步骤

1. **aws:executeAwsApi**-描述提供的子网以获取 VPC ID 和 IPv6 CIDR 区块关联状态。
2. **aws:executeScript**-验证提供的目标 IP 在语法上是否正确的 IPv4 and/or IPv6 地址，获取所选实例类型的架构，如果有任何目标 IP 是 IPv6，则验证子网是否具有 IPv6 池关联。
3. **aws:createStack**-创建一个 AWS CloudFormation 堆栈，用于预置测试 Amazon EC2 实例、IAM 实例配置文件（如果未提供）、安全组（如果未提供）、CloudWatch 日志组和 CloudWatch 控制面板。

（清理）如果步骤失败：

aws:executeScript-描述 CloudFormation 堆栈事件以确定失败原因。

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

4. **aws:waitForAwsResourceProperty**-等待 CloudFormation 堆栈完成创建。

（清理）如果步骤失败：

aws:executeScript-描述 CloudFormation 堆栈事件以确定失败原因。

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

5. **aws:executeScript**-描述用于获取测试实例 ID、安全组 ID、IAM 角色、实例配置文件和控制面板名称的 CloudFormation 堆栈资源。

（清理）如果步骤失败：

aws:executeScript-描述 CloudFormation 堆栈事件以确定失败原因。

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

6. **aws:waitForAwsResourceProperty** - 等待测试实例变为托管实例。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

7. **aws:runCommand**-在测试实例上安装 CloudWatch 代理。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

8. **aws:runCommand**-为提供的每个 IP 定义网络测试脚本 (MTR、ping、tracpath 和 traceroute) 。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

9. **aws:runCommand**-使用每 TestInterval 分钟运行一次 cronjobs 启动网络测试并安排后续执行。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

10 **aws:runCommand**-将 CloudWatch 代理配置为将测试结果从推送/home/ec2-user/logs/到 CloudWatch 日志。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

11 **aws:runCommand**-为中的测试结果配置日志轮换/home/ec2-user/logs/。

12 **aws:executeScript**-为 CloudFormation 堆栈创建的所有 CloudWatch 日志组设置保留策略。

13 **aws:executeScript**-为 ping 延迟和 ping 数据包丢失创建 CloudWatch 日志组指标过滤器。

(清理) 如果步骤失败 :

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

14 **aws:executeScript**-更新 CloudWatch 仪表板以包含用于显示 ping 延迟和 ping 数据包丢失统计信息的控件。

(清理) 如果步骤失败 :

aws:executeAwsApi-删除 CloudWatch 仪表板 (如果存在) 。

aws:deleteStack-删除 CloudFormation 堆栈和所有相关资源。

15**aws:branch**-评估 SleepTime 参数。如果设置为 0，则自动化将在不删除堆栈的情况下结束。

16**aws:sleep**-等待指定的 SleepTime 持续时间后再删除 CloudFormation 堆栈。

17**aws:deleteStack**-删除 CloudFormation 堆栈。根据 RetainDashboardAndLogsOnDeletion 参数，CloudWatch 控制面板和日志组要么保留，要么删除。

(清理) 如果堆栈删除失败：

aws:executeScript-描述 CloudFormation 堆栈事件以确定删除失败的原因。

输出

更新 CloudWatchDashboard.StackUrl - CloudFormation 堆栈的网址。

更新 CloudWatchDashboard.DashboardUrl - CloudWatch 仪表板的网址。

更新 CloudWatchDashboard.DashboardName - CloudWatch 仪表板的名称。

更新 CloudWatchDashboard.LogGroups -创建的 CloudWatch 日志组列表。

描述 StackResources.HelperInstanceId -测试实例 ID。

描述 StackResources.StackName - CloudFormation 堆栈名称。

AWSSupport-TerminateIPMonitoringFromVPC

描述

AWSSupport-TerminateIPMonitoringFromVPC 终止先前由 AWSSupport-SetupIPMonitoringFromVPC 启动的 IP 监控测试。将删除与指定测试 ID 相关的数据。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AutomationExecutionId

类型：字符串

描述：(必需) 您之前运行 AWSSupport-SetupIPMonitoringFromVPC 运行手册时的自动化执行 ID。与该执行 ID 关联的所有资源都被删除。

- InstanceId

类型：字符串

描述：(必需) 监控实例的实例 ID。

- SubnetId

类型：字符串

描述：(必需) 监控实例的子网 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议运行自动化的用户附加 AmazonSSMAutomationRoleIAM 托管策略。此外，用户还必须将以下策略附加到其用户、组或角色：

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": [
          "iam:DetachRolePolicy",
          "iam:RemoveRoleFromInstanceProfile",
          "iam>DeleteRole",
          "iam>DeleteInstanceProfile",
          "iam>DeleteRolePolicy"
        ],
        "Resource": [
          "arn:aws:iam::111122223333:role/AWSSupport/SetupIPMonitoringFromVPC_*",
          "arn:aws:iam::111122223333:instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
        ],
        "Effect": "Allow"
      },
      {
        "Action": [
          "iam:DetachRolePolicy"
        ],
        "Resource": [
          "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
        ],
        "Effect": "Allow"
      },
      {
        "Action": [
          "cloudwatch>DeleteDashboards"
        ],
        "Resource": [
          "*"
        ],
        "Effect": "Allow"
      },
      {
        "Action": [
          "ec2:DescribeTags",
          "ec2:DescribeInstances",
          "ec2:DescribeSecurityGroups",
          "ec2>DeleteSecurityGroup",
          "ec2:TerminateInstances",

```

```
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

文档步骤

1. `aws:assertAwsResourceProperty`-检查 `AutomationExecutionId` 并 `InstanceId` 与同一个测试相关。
2. `aws:assertAwsResourceProperty`-检查 `SubnetId` 并 `InstanceId`与同一个测试相关。
3. `aws:executeAwsApi` - 检索测试安全组。
4. `aws:executeAwsApi`-删除 CloudWatch 仪表板。
5. `aws:changeInstanceState` - 终止测试实例。
6. `aws:executeAwsApi` - 从角色中删除 IAM 实例配置文件。
7. `aws:executeAwsApi` - 删除自动化创建的 IAM 实例配置文件。
8. `aws:executeAwsApi`-从自动化创建的角色中删除 CloudWatch 内联策略。
9. `aws:executeAwsApi`-将AmazonSSMManagedInstanceCore托管策略与自动化创建的角色分离。
- 10`aws:executeAwsApi` - 删除自动化创建的 IAM 角色。
- 11`aws:executeAwsApi` - 删除自动化创建的安全组（如果存在）。

输出

无

AWS WAF

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS WAF有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅 [查看运行手册内容](#)。

主题

- [AWS-AddWAFRegionalRuleToRuleGroup](#)

- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

AWS-AddWAFRegionalRuleToRuleGroup

描述

该AWS-AddWAFRegionalRuleToRuleGroup操作手册将现有的 AWS WAF 区域规则添加到 AWS WAF 区域规则组中。仅支持 AWS WAF 经典区域规则组。AWS WAF 经典区域规则组最多可以有 10 条规则。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- RuleGroupId

类型：字符串

描述：(必填) 要更新的规则组的 ID。

- RulePriority

类型：整数

描述：(必填) 新规则的优先级。规则优先级决定了评估区域组中规则的顺序。值较低的规则比值较高的规则具有更高的优先级。值必须是整数。如果您向一个区域规则组添加多条规则，则这些值不必是连续的。

- RuleId

类型：字符串

描述：(必填) 您要添加到区域规则组的规则的 ID。

- RuleAction

类型：字符串

描述：(必填) 指定 Web 请求符合规则条件时 AWS WAF 采取的操作。

有效值：允许 | 阻止 | 计数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetChangeTokenStatus
- waf-regional:ListActivatedRulesInRuleGroup
- waf-regional:UpdateRuleGroup

文档步骤

- GetWAFChangeToken (aws: executeAwsApi)-检索 AWS WAF 更改令牌以确保运行手册不会向服务提交冲突的请求。
- AddWAFRuleToWAFRegionalRuleGroup (aws: ExecuteScript)-将指定的规则添加到区域规则组。

AWS WAF

- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty)-验证更改令牌的状态为或。PENDING INSYNC
- VerifyRuleAddedToRuleGroup (aws: executeScript)-验证指定的 AWS WAF 规则是否已添加到目标区域规则组。

输出

- VerifyRuleAddedToRuleGroup.VerifyRuleAddedToRuleGroupResponse -验证新规则是否已添加到区域规则组的步骤的输出。
- VerifyRuleAddedToRuleGroup.ListActivatedRulesInRuleGroupResponse
-ListActivatedRulesInRuleGroup API 操作的输出。

AWS-AddWAFRegionalRuleToWebAcl

描述

该AWS-AddWAFRegionalRuleToWebAcl运行手册将现有的 AWS WAF 区域规则、规则组或基于速率的规则添加到 AWS WAF 经典区域 Web 访问控制列表 (ACL) 中。本运行手册不会更新由 AWS Firewall Manager管理的现有 AWS WAF 经典区域 Web ACL。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- WebACLIId

类型：字符串

描述：(必填) 要更新的网络 ACL 的 ID。

- ActivatedRulePriority

类型：整数

描述：(必填) 新规则的优先级。规则优先级决定评估 Web ACL 中规则的顺序。值较低的规则比值较高的规则具有更高的优先级。值必须是整数。如果您向区域 Web ACL 添加多条规则，则这些值不必是连续的。

- ActivatedRuleRuleId

类型：字符串

描述：(必填) 要添加到 Web ACL 的常规规则、基于速率的规则或组的 ID。

- ActivatedRuleAction

类型：字符串

有效值：允许 | 阻止 | 计数

描述：(可选) 指定 Web 请求符合规则条件时 AWS WAF 采取的操作。

- ActivatedRuleType

类型：字符串

有效值：常规 | 基于费率 | 群组

默认：常规

描述：(可选) 您要添加到 Web ACL 的规则类型。尽管此字段是可选字段，但请注意，如果您尝试在 Web ACL 中添加RATE_BASED规则而不设置类型，则请求会失败，因为请求默认为REGULAR规则。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetWebACL
- waf-regional:UpdateWebACL

文档步骤

- DetermineWebACLNotInFMSAndRulePriority (AWS: executeScript)-验证 AWS WAF Web ACL 是否在 Firewall Manager 安全策略中，并验证优先级 ID 是否与现有 ACL 冲突。
- AddRuleOrRuleGroupToWebACL (aws: ExecuteScript)-将指定的规则添加到 Web ACL。 AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws: executeScript)-验证指定的 AWS WAF 规则是否已添加到目标 Web ACL 中。

输出

- DetermineWebACLNotInFMSAndRulePriority.PrereqResponse : DetermineWebACLNotInFMSAndRulePriority 步骤的输出。
- VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse : AddRuleOrRuleGroupToWebACL 步骤的输出。
- VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse: VerifyRuleOrRuleGroupAddedToWebAcl 步骤的输出。

AWSConfigRemediation-EnableWAFClassicLogging

描述

该AWSConfigRemediation-EnableWAFClassicLogging运行手册允许您登录到亚马逊数据 Firehose (Firehose)，以 AWS WAF 获取您指定的网络访问控制列表 (Web ACL)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- DeliveryStreamName

类型：字符串

描述：(必填) 您要向其发送日志的 Firehose 传输流的名称。

- WebACLId

类型：字符串

描述：(必填) 要启用登录功能的 AWS WAF Web ACL 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf:GetLoggingConfiguration
- waf:GetWebAcl

- `waf:PutLoggingConfiguration`

文档步骤

- `aws:executeAwsApi` - 确认您在 `DeliveryStreamName` 中指定的传送流存在。
- `aws:executeAwsApi` - 收集参数中指定的 Web ACL 的 ARN。AWS WAF `WebACLId`
- `aws:executeAwsApi` - 为 Web ACL 启用日志记录。
- `aws:assertAwsResourceProperty` - 验证是否已在 AWS WAF Web ACL 上启用日志记录。

AWSConfigRemediation-EnableWAFClassicRegionalLogging

描述

该AWSConfigRemediation-EnableWAFClassicRegionalLogging运行手册允许您登录到亚马逊数据 Firehose (Firehose) , 以获取您 AWS WAF 指定的网络访问控制列表 (ACL)。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- `AutomationAssumeRole`

类型 : 字符串

描述 : (必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- `LogDestinationConfigs`

类型：字符串

描述：(必填) 您要向其发送日志的 Firehose 传输流的亚马逊资源名称 (ARN)。

- WebACLIId

类型：字符串

描述：(必填) 要启用登录功能的 AWS WAF Web ACL 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf-regional:GetLoggingConfiguration
- waf-regional:GetWebAcl
- waf-regional:PutLoggingConfiguration

文档步骤

- aws:executeAwsApi-收集参数中指定的 Web ACL 的 ARN。AWS WAF WebACLIId
- aws:executeAwsApi - 为 Web ACL 启用日志记录。
- aws:assertAwsResourceProperty-验证是否已在 AWS WAF Web ACL 上启用日志记录。

AWSConfigRemediation-EnableWAFV2Logging

描述

该AWSConfigRemediation-EnableWAFV2Logging运行手册允许使用指定的 Amazon Dat AWS WAF a Firehose (Firehose) 传输流记录 (AWS WAF V2) 网络访问控制列表 (Web ACL)。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。

- LogDestinationConfigs

类型：字符串

描述：(必填) 您要与网页 ACL 关联的 Firehose 传送流 ARN。

 Note

Firehose 传送流 ARN 必须以前缀开头。aws-waf-logs-例如，aws-waf-logs-us-east-2-analytics。有关更多信息，请参阅 [Amazon Data Firehose](#)。

- WebAclArn

类型：字符串

描述：(必需) 要为其启用日志记录的 Web ACL 的 ARN。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`

- `wafv2:GetLoggingConfiguration`

文档步骤

- `aws:executeScript`-启用 AWS WAF V2 Web ACL 的日志记录并验证日志记录是否具有指定的配置。

Amazon WorkSpaces

AWS Systems Manager 自动化为 Amazon WorkSpaces 提供了预定义的运行手册。有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

AWS-CreateWorkSpace

描述

AWS-CreateWorkSpace运行手册根据您为输入参数指定的值创建一个新的 Amazon WorkSpaces 虚拟桌面，称为 a WorkSpace。有关信息 WorkSpaces，请参阅[什么是亚马逊 WorkSpaces？](#) 在《亚马逊 WorkSpaces 管理指南》中。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- BundleId

类型：字符串

描述：(必填) 要用于的捆绑包的 ID Workspace。

- ComputeTypeName

类型：字符串

有效值：VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

描述：(可选) 您的计算类型 Workspace。

- DirectoryId

类型：字符串

描述：(必填) 要添加您的 Workspace 目录的 ID。

- RootVolumeEncryptionEnabled

类型：布尔值

有效值：true | false

默认：false

描述：(可选) 确定是否对根卷进行加密。Workspace

- RootVolumeSizeGib

类型：整数

描述：(必填) 的根卷的大小 Workspace。

- RunningMode

类型：字符串

有效值：ALWAYS_ON | AUTO_STOP

描述：(必填) 的运行模式 Workspace。

- RunningModeAutoStopTimeoutInMinutes

类型：整数

描述：(可选) 用户注销后 WorkSpaces停止的时间。以 60 分钟为间隔指定一个值。

- 标签

类型：字符串

描述：(可选) 要应用于的标签 Workspace。

- UserName

类型：字符串

描述：(必填) 要与关联的用户名 Workspace。

- UserVolumeEncryptionEnabled

类型：布尔值

有效值：true | false

默认：false

描述：(可选) 确定是否对的用户卷进行加密。 Workspace

- UserVolumeSizeGib

类型：整数

描述：(必填) 的用户音量大小 Workspace。

- VolumeEncryptionKey

类型：字符串

描述：(可选) 您要用来加密存储在上的数据的对称密 AWS Key Management Service 钥。
Workspace

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

文档步骤

- aws:executeScript- Workspace 根据您为输入参数指定的值创建。
- aws:waitForAwsResourceProperty-验证 is 的 Workspace 状态AVAILABLE。

输出

CreateWorkspace.WorkspaceId

AWSsupport-RecoverWorkspace

描述

AWSsupport-RecoverWorkspace运行手册在您指定的 Amazon WorkSpaces 虚拟桌面 (称为 a Workspace) 上执行恢复步骤。运行手册会重新启动 Workspace , 如果状态静止UNHEALTHY , 则 Workspace 根据您为输入参数指定的值恢复或重建。在使用本运行手册之前, 我们建议您查看《Amazon WorkSpaces 管理指南》中的“[疑难解答 WorkSpaces](#)”。

Important

恢复或重建 Workspace 是一种潜在的破坏性操作, 可能会导致数据丢失。这是因为是从上次可用的快照中恢复的, 而从快照中恢复的数据可能长达 12 小时。Workspace 恢复选项会根据最新的快照重新创建根卷和用户卷。rebuild 选项根据最新的快照重新创建用户卷, 并 Workspace 从与创建该分发包关联的映像中重新创建用户卷。Workspace 已安装的应用程序或在创建后更改的 Workspace 系统设置都将丢失。有关恢复和重建的更多信息

WorkSpaces，请参阅《Amazon WorkSpaces 管理指南》Workspace 中的“[还原 Workspace](#)和[重建 a](#)”。

[运行此自动化 \(控制台 \)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(可选) 允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 确认

类型：字符串

有效值：是

描述：(必填) 输入“是”表示您知道还原和重建操作将尝试 Workspace 从最新的快照中恢复，并且从这些快照恢复的数据可能最长为 12 小时。

- Reboot

类型：字符串

有效值：是 | 否

默认：是

描述：(必填) 确定 Workspace 是否重新启动。

- 重建

类型：字符串

有效值：是 | 否

默认：否

描述：(必填) 确定 Workspace 是否重建。

- Restore

类型：字符串

有效值：是 | 否

默认：否

描述：(必填) 确定 Workspace 是否恢复。

- WorkspaceId

类型：字符串

描述：(必填) Workspace 要恢复的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- workspaces:DescribeWorkspaces
- workspaces:DescribeWorkspaceSnapshots
- workspaces:RebootWorkspaces
- workspaces:RebuildWorkspaces
- workspaces:RestoreWorkspace
- workspaces:StartWorkspaces

文档步骤

- `aws:executeAwsApi`-收集 Workspace 您在WorkspaceId参数中指定的状态。
- `aws:assertAwsResourceProperty`-验证 Workspace 是AVAILABLE、ERRORIMPAIREDSTOPPED、或UNHEALTHY的状态。
- `aws:branch`-基于状态的分支 Workspace。
- `aws:executeAwsApi`-启动 Workspace。
- `aws:branch` - 根据您为 Action 参数指定的值进行分支。
- `aws:waitForAwsResourceProperty`-启动后等待 Workspace 状态。
- `aws:waitForAwsResourceProperty`-等待 Workspace 状态更改为AVAILABLE、ERRORIMPAIRED、或启动UNHEALTHY后。
- `aws:executeAwsApi`-收集启动 Workspace 后的状态。
- `aws:branch`-基于启动 Workspace 后的状态的分支。
- `aws:executeAwsApi`-收集用于恢复或重建的可用快照。 Workspace
- `aws:branch` - 根据您为 Reboot 参数指定的值进行分支。
- `aws:executeAwsApi`-重新启动。 Workspace
- `aws:executeAwsApi`-收集启动 Workspace 后的状态。
- `aws:waitForAwsResourceProperty`-等待状态变 Workspace 为。REBOOTING
- `aws:waitForAwsResourceProperty`-等待 Workspace 状态更改为AVAILABLEERROR、或重新启动UNHEALTHY后。
- `aws:executeAwsApi`-收集重启 Workspace 后的状态。
- `aws:branch`-根据重启 Workspace 后的状态进行分支。
- `aws:branch` - 根据您为 Restore 参数指定的值进行分支。
- `aws:executeAwsApi`-恢复。 Workspace如果恢复失败，运行手册将尝试重建。 Workspace
- `aws:waitForAwsResourceProperty`-等待状态变 Workspace 为。RESTORING
- `aws:waitForAwsResourceProperty`-等待 Workspace 状态更改为AVAILABLEERROR、或恢复UNHEALTHY后。
- `aws:executeAwsApi`-收集恢复 Workspace 后的状态。
- `aws:branch`-基于恢复 Workspace 后的状态的分支。
- `aws:branch` - 根据您为 Rebuild 参数指定的值进行分支。
- `aws:executeAwsApi`-重建。 Workspace
- `aws:waitForAwsResourceProperty`-等待状态变 Workspace 为。REBUILDING

- `aws:waitForAwsResourceProperty`-等待 Workspace 状态更改为AVAILABLEERROR、或重建UNHEALTHY后。
- `aws:executeAwsApi`-收集重建 Workspace 后的状态。
- `aws:assertAwsResourceProperty`-确认 Workspace is 的状态AVAILABLE。

X-Ray

AWS Systems Manager 自动化为用户提供了预定义的运行手册。AWS X-Ray有关运行手册的更多信息，请参阅[使用运行手册](#)。有关如何查看运行手册内容的信息，请参阅[查看运行手册内容](#)。

主题

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

AWSConfigRemediation-UpdateXRayKMSKey

描述

AWSConfigRemediation-UpdateXRayKMSKey运行手册支持使用 AWS Key Management Service (AWS KMS) 密钥对您的 AWS X-Ray 数据进行加密。本运行手册应仅用作基准，以确保您的 AWS X-Ray 数据按照建议的最低安全最佳实践进行加密。我们建议使用不同的 KMS 密钥对多组数据进行加密。

[运行此自动化 \(控制台\)](#)

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

描述：(必需) 允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称 (ARN) 。

- KeyId

类型：字符串

描述：(必填) 您要 AWS X-Ray 用于加密数据的 Amazon 资源名称 (ARN)、密钥 ID 或密钥别名。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:DescribeKey
- xray:GetEncryptionConfig
- xray:PutEncryptionConfig

文档步骤

- aws:executeAwsApi-使用您在KeyId参数中指定的 KMS 密钥对 X-Ray 数据启用加密。
- aws:waitForAwsResourceProperty-等待您的 X-Ray 加密配置状态变为。ACTIVE
- aws:executeAwsApi - 收集您在 KeyId 参数中指定的密钥的 ARN。
- aws:assertAwsResourceProperty-验证您的 X-Ray加密功能已启用。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。