



使用者指南

AWS Systems Manager 自動化 Runbook 參考



AWS Systems Manager 自動化 Runbook 參考: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

Automation Runbook 参考	1
檢視 Runbook 內容	3
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	4
AWSConfigRemediation-EnableAPIGatewayTracing	5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWS Batch	8
AWSSupport-TroubleshootAWSBatchJob	8
AWS CloudFormation	14
AWS-DeleteCloudFormationStack	14
AWS-EnableCloudFormationSNSNotification	15
AWS-RunCfnLint	17
AWSSupport-TroubleshootCFNCustomResource	19
AWS-UpdateCloudFormationStack	20
CloudFront	22
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	22
AWSConfigRemediation-EnableCloudFrontAccessLogs	23
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	25
AWSConfigRemediation-EnableCloudFrontOriginFailover	27
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	28
CloudTrail	30
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	30
AWS-EnableCloudTrail	32
AWS-EnableCloudTrailCloudWatchLogs	33
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	35
AWS-EnableCloudTrailKmsEncryption	36
AWSConfigRemediation-EnableCloudTrailLogFileValidation	37
AWS-EnableCloudTrailLogFileValidation	39
AWS-QueryCloudTrailLogs	40
CloudWatch	42
AWS-ConfigureCloudWatchOnEC2Instance	42
AWS-EnableCWAAlarm	43
Amazon DocumentDB	46
AWS-EnableDocDbClusterBackupRetentionPeriod	46

CodeBuild	48
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK	48
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	50
AWS CodeDeploy	51
AWSSupport-TroubleshootCodeDeploy	51
AWS Config	53
AWSSupport-SetupConfig	53
Amazon Connect	56
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	56
AWSSupport-CollectAmazonConnectContactFlowLog	63
AWS Directory Service	69
AWS-CreateDSManagementInstance	69
AWSSupport-TroubleshootADConnectorConnectivity	73
AWSSupport-TroubleshootDirectoryTrust	77
AWS AppSync	80
AWS-EnableAppSyncGraphQLApiLogging	80
Amazon Athena	82
AWS-EnableAthenaWorkGroupEncryptionAtRest	82
DynamoDB	84
AWS-ChangeDDBRWCapacityMode	85
AWS-CreateDynamoDBBackup	87
AWS-DeleteDynamoDbBackup	88
AWSConfigRemediation-DeleteDynamoDbTable	89
AWS-DeleteDynamoDbTableBackups	90
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	91
AWSConfigRemediation-EnablePITRForDynamoDbTable	93
AWS-EnableDynamoDbAutoscaling	94
AWS-RestoreDynamoDBTable	97
AWS Database Migration Service	99
AWSSupport-TroubleshootDMSTableErrors	100
Amazon EBS	105
AWSSupport-AnalyzeEBSResourceUsage	105
AWS-ArchiveEBSSnapshots	111
AWS-AttachEBSVolume	114
AWSSupport-CalculateEBSPerformanceMetrics	115
AWS-CopySnapshot	121

AWS-CreateSnapshot	122
AWS-DeleteSnapshot	123
AWSConfigRemediation-DeleteUnusedEBSVolume	124
AWS-DeregisterAMIs	125
AWS-DetachEBSVolume	127
AWSConfigRemediation-EnableEbsEncryptionByDefault	128
AWS-ExtendEbsVolume	129
AWSSupport-ModifyEBSSnapshotPermission	131
AWSConfigRemediation-ModifyEBSVolumeType	133
Amazon EC2	135
AWS-ASGEnterStandby	136
AWS-ASGExitStandby	137
AWS-CreateImage	138
AWS-DeleteImage	140
AWS-PatchAsgInstance	141
AWS-PatchInstanceWithRollback	143
AWS-QuarantineEC2Instance	146
AWS-ResizeInstance	148
AWS-RestartEC2Instance	149
AWS-SetupJupyter	149
AWS-StartEC2Instance	153
AWS-StopEC2Instance	154
AWS-TerminateEC2Instance	154
AWS-UpdateLinuxAmi	155
AWS-UpdateWindowsAmi	158
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	161
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	163
AWSEC2-CloneInstanceAndUpgradeSQLServer	164
AWSEC2-CloneInstanceAndUpgradeWindows	168
AWSEC2-ConfigureSTIG	171
AWSEC2-PatchLoadBalancerInstance	206
AWSEC2-SQLServerDBRestore	207
AWSSupport-ActivateWindowsWithAmazonLicense	212
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	215
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	219
AWSSupport-CheckXenToNitroMigrationRequirements	224

AWSSupport-ConfigureEC2Metadata	227
AWSSupport-ContainEC2Instance	230
AWSSupport-CopyEC2Instance	239
AWSSupport-EnableWindowsEC2SerialConsole	244
AWSSupport-ExecuteEC2Rescue	252
AWSSupport-ListEC2Resources	255
AWSSupport-ManageRDPSettings	257
AWSSupport-ManageWindowsService	259
AWSSupport-MigrateEC2ClassicToVPC	261
AWSSupport-MigrateXenToNitroLinux	267
AWSSupport-ResetAccess	278
AWSSupport-ResetLinuxUserPassword	280
AWSPremiumSupport-ResizeNitroInstance	286
AWSSupport-RestoreEC2InstanceFromSnapshot	292
AWSSupport-SendLogBundleToS3Bucket	296
AWSSupport-StartEC2RescueWorkflow	298
AWSPremiumSupport-TroubleshootEC2DiskUsage	308
AWSSupport-TroubleshootEC2InstanceConnect	312
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs	318
AWSSupport-TroubleshootRDP	321
AWSSupport-TroubleshootSSH	326
AWSSupport-TroubleshootSUSERegistration	329
AWSSupport-TroubleshootWindowsPerformance	331
AWSSupport-TroubleshootWindowsUpdate	338
AWSSupport-UpgradeWindowsAWSDrivers	344
Amazon ECS	348
AWSSupport-CollectECSInstanceLogs	348
AWS-InstallAmazonECSAgent	350
AWS-ECSRunTask	352
AWSSupport-TroubleshootECSContainerInstance	355
AWSSupport-TroubleshootECSTaskFailedToStart	357
AWS-UpdateAmazonECSAgent	361
Amazon EFS	363
AWSSupport-CheckAndMountEFS	363
Amazon EKS	366
AWSSupport-CollectEKSInstanceLogs	366

AWS-CreateEKSClusterWithFargateProfile	368
AWS-CreateEKSClusterWithNodegroup	372
AWS-DeleteEKSCluster	375
AWS-MigrateToNewEKSSelfManagedNodeGroup	378
AWSPremiumSupport-TroubleshootEKSCluster	383
AWSSupport-TroubleshootEKSWorkerNode	387
AWS-UpdateEKSCluster	389
AWS-UpdateEKSMangedNodeGroup	390
AWS-UpdateEKSSelfManagedLinuxNodeGroups	394
AWSSupport-SetupK8sApiProxyForEKS	398
AWSSupport-TroubleshootEbsCsiDriversForEks	408
Elastic Beanstalk	416
AWSSupport-CollectElasticBeanstalkLogs	417
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	419
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	421
AWSSupport-TroubleshootElasticBeanstalk	422
Elastic Load Balancing	425
AWSConfigRemediation-DropInvalidHeadersForALB	425
AWS-EnableCLBAccessLogs	427
AWS-EnableCLBConnectionDraining	428
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	430
AWSConfigRemediation-EnableELBDeletionProtection	431
AWSConfigRemediation-EnableLoggingForALBAndCLB	432
AWSSupport-TroubleshootCLBConnectivity	434
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	437
AWS-UpdateALBDesyncMitigationMode	438
AWS-UpdateCLBDesyncMitigationMode	440
Amazon EMR	442
AWSSupport-AnalyzeEMRLogs	442
AWSSupport-DiagnoseEMRLogsWithAthena	448
Amazon OpenSearch Service	455
AWSConfigRemediation-DeleteOpenSearchDomain	456
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	457
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	458
AWSSupport-TroubleshootOpenSearchRedYellowCluster	460
AWSSupport-TroubleshootOpenSearchHighCPU	465

EventBridge	471
AWS-AddOpsItemDedupStringToEventBridgeRule	471
AWS-DisableEventBridgeRule	473
AWS Glue	474
AWSSupport-TroubleshootGlueConnection	474
Amazon FSx	484
AWSSupport-ValidateFSxWindowsADConfig	485
GuardDuty	498
AWSConfigRemediation-CreateGuardDutyDetector	498
IAM	499
AWSSupport-TroubleshootIAMAccessDeniedEvents	500
AWS-AttachIAMToInstance	506
AWS-DeleteIAMInlinePolicy	508
AWSConfigRemediation-DeleteIAMRole	509
AWSConfigRemediation-DeleteIAMUser	511
AWSConfigRemediation-DeleteUnusedIAMGroup	513
AWSConfigRemediation-DeleteUnusedIAMPolicy	514
AWSConfigRemediation-DetachIAMPolicy	516
AWSConfigRemediation-EnableAccountAccessAnalyzer	517
AWSSupport-GrantPermissionsToIAMUser	518
AWSConfigRemediation-RemoveUserPolicies	523
AWSConfigRemediation-ReplaceIAMInlinePolicy	525
AWSConfigRemediation-RevokeUnusedIAMUserCredentials	527
AWSConfigRemediation-SetIAMPasswordPolicy	528
AWSSupport-ContainIAMPrincipal	531
Amazon Kinesis Data Streams	544
AWS-EnableKinesisStreamEncryption	544
AWS KMS	546
AWSConfigRemediation-CancelKeyDeletion	546
AWSConfigRemediation-EnableKeyRotation	547
Lambda	548
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	549
AWSConfigRemediation-DeleteLambdaFunction	550
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	551
AWSConfigRemediation-MoveLambdaToVPC	553
AWSSupport-RemediateLambdaS3Event	554

AWSSupport-TroubleshootLambdaInternetAccess	557
AWSSupport-TroubleshootLambdaS3Event	560
Amazon Managed Workflows for Apache Airflow	562
AWSSupport-TroubleshootMWAAEnvironmentCreation	562
Neptune	568
AWS-EnableNeptuneDbAuditLogsToCloudWatch	568
AWS-EnableNeptuneDbBackupRetentionPeriod	569
AWS-EnableNeptuneClusterDeletionProtection	571
Amazon RDS	573
AWS-CreateEncryptedRdsSnapshot	574
AWS-CreateRdsSnapshot	576
AWSConfigRemediation-DeleteRDSCluster	578
AWSConfigRemediation-DeleteRDSClusterSnapshot	579
AWSConfigRemediation-DeleteRDSInstance	580
AWSConfigRemediation-DeleteRDSInstanceSnapshot	582
AWSConfigRemediation-DisablePublicAccessToRDSInstance	583
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	585
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	586
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	588
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS	590
AWSConfigRemediation-EnableMultiAZOnRDSInstance	591
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	593
AWSConfigRemediation-EnableRDSClusterDeletionProtection	595
AWSConfigRemediation-EnableRDSInstanceBackup	596
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	598
AWSConfigRemediation-ModifyRDSInstancePortNumber	599
AWSSupport-ModifyRDSSnapshotPermission	601
AWSPremiumSupport-PostgreSQLWorkloadReview	603
AWS-RebootRdsInstance	617
AWSSupport-ShareRDSSnapshot	618
AWS-StartRdsInstance	622
AWS-StartStopAuroraCluster	622
AWS-StopRdsInstance	624
AWSSupport-TroubleshootConnectivityToRDS	625
AWSSupport-TroubleshootRDSIAMAuthentication	627
AWSSupport-ValidateRdsNetworkConfiguration	634

Amazon Redshift	639
AWSConfigRemediation-DeleteRedshiftCluster	640
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	641
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	643
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	644
AWSConfigRemediation-EnableRedshiftClusterEncryption	646
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	647
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	648
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	650
AWSConfigRemediation-ModifyRedshiftClusterNodeType	651
Amazon S3	653
AWS-ArchiveS3BucketToIntelligentTiering	654
AWS-ConfigureS3BucketLogging	656
AWS-ConfigureS3BucketVersioning	658
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	659
AWSConfigRemediation-ConfigureS3PublicAccessBlock	661
AWS-CreateS3PolicyToExpireMultipartUploads	663
AWS-DisableS3BucketPublicReadWrite	665
AWS-EnableS3BucketEncryption	666
AWS-EnableS3BucketKeys	667
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	668
AWSConfigRemediation-RestrictBucketSSLRequestsOnly	670
AWSSupport-TroubleshootS3PublicRead	671
AWSSupport-EmptyS3Bucket	676
AWSSupport-TroubleshootS3EventNotifications	682
AWSSupport-ContainS3Resource	689
Amazon SES	697
AWSSupport-AnalyzeSESMessagesSendingStatus	697
SageMaker AI	701
AWS-DisableSageMakerNotebookRootAccess	701
Secrets Manager	703
AWSConfigRemediation-DeleteSecret	703
AWSConfigRemediation-RotateSecret	704
安全中樞	706
AWSConfigRemediation-EnableSecurityHub	706
AWS Shield	708

AWSPremiumSupport-DDoSResiliencyAssessment	708
Amazon SNS	716
AWS-EnableSNSTopicDeliveryStatusLogging	716
AWSConfigRemediation-EncryptSNSTopic	719
AWS-PublishSNSNotification	720
Amazon SQS	721
AWS-EnableSQSEncryption	722
Step Functions	724
AWS-EnableStepFunctionsStateMachineLogging	724
Systems Manager	726
AWS-BulkDeleteAssociation	727
AWS-BulkEditOpsItems	728
AWS-BulkResolveOpsItems	731
AWS-ConfigureMaintenanceWindows	733
AWS-CreateManagedLinuxInstance	734
AWS-CreateManagedWindowsInstance	737
AWSConfigRemediation-EnableCWLoggingForSessionManager	739
AWS-ExportOpsDataToS3	741
AWS-ExportPatchReportToS3	742
AWS-SetupInventory	744
AWS-SetupManagedInstance	748
AWS-SetupManagedRoleOnEC2Instance	749
AWSSupport-TroubleshootManagedInstance	750
AWSSupport-TroubleshootPatchManagerLinux	753
AWSSupport-TroubleshootSessionManager	756
第三方	761
AWS-CreateJiraIssue	761
AWS-CreateServiceNowIncident	763
AWS-RunPacker	766
Amazon VPC	767
AWS-CloseSecurityGroup	768
AWSSupport-ConfigureDNSQueryLogging	769
AWSSupport-ConfigureTrafficMirroring	772
AWSSupport-ConnectivityTroubleshooter	775
AWSSupport-TroubleshootVPN	778
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	783

AWSConfigRemediation-DeleteUnusedENI	785
AWSConfigRemediation-DeleteUnusedSecurityGroup	786
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	787
AWSConfigRemediation-DeleteVPCFlowLog	788
AWSConfigRemediation-DetachAndDeleteInternetGateway	789
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	791
AWS-DisableIncomingSSHOnPort22	793
AWS-DisablePublicAccessForSecurityGroup	794
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	796
AWSSupport-EnableVPCFlowLogs	797
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	803
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	805
AWS-ReleaseElasticIP	807
AWS-RemoveNetworkACLUnrestrictedSSHRDP	808
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	809
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	810
AWSSupport-SetupIPMonitoringFromVPC	811
AWSSupport-TerminateIPMonitoringFromVPC	824
AWS WAF	827
AWS-AddWAFRegionalRuleToRuleGroup	827
AWS-AddWAFRegionalRuleToWebAcl	829
AWSConfigRemediation-EnableWAFClassicLogging	832
AWSConfigRemediation-EnableWAFClassicRegionalLogging	833
AWSConfigRemediation-EnableWAFV2Logging	834
Amazon WorkSpaces	836
AWS-CreateWorkSpace	836
AWSSupport-RecoverWorkSpace	839
X-Ray	843
AWSConfigRemediation-UpdateXRayKMSKey	843
.....	dcccxliv

Systems Manager Automation Runbook 參考

為了協助您快速入門，AWS Systems Manager 提供預先定義的 Runbook。這些 Runbook 由 Amazon Web Services AWS 支援和 維護 AWS Config。Runbook 參考說明 Systems Manager 提供的每個預先定義的 Runbook 支援，以及 AWS Config。

Important

如果您執行可使用 AWS Identity and Access Management (IAM) 服務角色叫用其他服務的自動化工作流程，請注意您必須為該服務角色設定可叫用這些服務的許可。此要求適用於所有 AWS Automation Runbook (AWS-* Runbook)，例如 AWS-ConfigureS3BucketLogging、AWS-CreateDynamoDBBackup 和 AWS-RestartEC2Instance Runbook 等。此要求也適用於您建立的任何自訂 Automation Runbook，透過使用呼叫其他 AWS 服務的動作來叫用其他服務。例如，如果您使用 `aws:executeAwsApi`、`aws:createStack` 或 `aws:copyImage` 等動作，則您必須為服務角色設定可叫用這些服務的許可。您可以將 IAM 內嵌政策新增至角色，以啟用其他 AWS 服務的許可。如需詳細資訊，請參閱[新增自動化內嵌政策以叫用其他 AWS 服務](#)。

此參考包含的主題說明 AWS AWS 支援、和擁有的每個 Systems Manager Runbook AWS Config。Runbook 由相關組織 AWS 服務。每個頁面都會提供說明，說明您在使用 Runbook 時可指定的必要和選用參數。每個頁面也會列出 Runbook 中的步驟，以及自動化的輸出，如果有的話。

此參考不包含需要核准之 Runbook 的個別頁面，例如 AWS-CreateManagedLinuxInstanceWithApproval 或 AWS-StopEC2InstanceWithApproval Runbook。包含的任何 Runbook 名稱 WithApproval，表示 Runbook 包含 [aws:approve](#) 動作。此動作會暫時暫停自動化，直到指定的委託人核准或拒絕動作為止。達到所需的核准數量後，自動化會繼續。

如需有關執行自動化的資訊，請參閱[執行簡單的自動化](#)。如需在多個目標上執行自動化的詳細資訊，請參閱[使用目標和速率控制的執行自動化](#)。

主題

- [檢視 Runbook 內容](#)
- [API Gateway](#)
- [AWS Batch](#)

- [AWS CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [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](#)
- [Amazon OpenSearch Service](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [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](#)
- [安全中樞](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [Step Functions](#)
- [Systems Manager](#)
- [第三方](#)
- [Amazon VPC](#)
- [AWS WAF](#)
- [Amazon WorkSpaces](#)
- [X-Ray](#)

檢視 Runbook 內容

您可以在 Systems Manager 主控台中檢視 Runbook 的內容。

檢視 Runbook 內容

1. 在 [https : //https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/) 開啟 AWS Systems Manager 主控台。
2. 在導覽窗格中，選擇 Documents (文件)。

-或-

如果 AWS Systems Manager 首頁先開啟，請選擇選單圖示

(三

) 以開啟導覽窗格，然後在導覽窗格中選擇文件。

3. 在類別區段中，選擇自動化文件。
4. 選擇 Runbook，接著選擇 View details (檢視詳細資訊)。
5. 選擇 Content (內容) 索引標籤。

API Gateway

AWS Systems Manager 自動化為 Amazon API Gateway 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-DeleteAPIGatewayStage](#)
- [AWSConfigRemediation-EnableAPIGatewayTracing](#)
- [AWSConfigRemediation-UpdateAPIGatewayMethodCaching](#)

AWSConfigRemediation-DeleteAPIGatewayStage

Description

AWSConfigRemediation-DeleteAPIGatewayStage Runbook 會刪除 Amazon API Gateway (API Gateway) 階段。AWS Config 必須在您的執行此自動化 AWS 區域 的中啟用。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- StageArn

類型：字串

描述：(必要) 您要刪除之 API Gateway 階段的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 刪除 StageArn 參數中指定的 API Gateway 階段。

AWSConfigRemediation-EnableAPIGatewayTracing

Description

AWSConfigRemediation-EnableAPIGatewayTracing Runbook 可在 Amazon API Gateway (API Gateway) 階段啟用追蹤。AWS Config 必須在您執行此自動化的 AWS 區域 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- StageArn

類型：字串

描述：（必要）您要啟用追蹤之 API Gateway 階段的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeScript` - 在 StageArn 參數中指定的 API Gateway 階段上啟用追蹤。

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Description

AWSConfigRemediation-UpdateAPIGatewayMethodCaching Runbook 會更新 Amazon API Gateway 階段資源的快取方法設定。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- CachingAuthorizedMethods

類型：StringList

描述：（必要）授權啟用快取的方法。清單必須是 DELETE、GET、HEADOPTIONS、PATCH、POST 和 PUT 的一些組合。針對選取的方法啟用快取，針對非選取的方法停用快取。如果選取 ANY，則會針對所有方法啟用快取，如果 NONE 選取，則會針對所有方法停用快取。

- StageArn

類型：字串

描述：(必要) API 的 REST API Gateway 階段 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 接受階段資源 ID 做為輸入，使用 API 動作更新 UpdateStage API Gateway 階段的快取方法設定，並驗證更新。

AWS Batch

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Batch。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-TroubleshootAWSBatchJob](#)

AWSSupport-TroubleshootAWSBatchJob

Description

AWSSupport-TroubleshootAWSBatchJob Runbook 可協助您疑難排解導致 AWS Batch 任務無法從 RUNNABLE STARTING 狀態進行的問題。

如何運作？

此 Runbook 會執行下列檢查：

- 如果運算環境處於 INVALID或 DISABLED 狀態。

- 如果運算環境的Max vCPU參數足夠大，足以容納任務佇列中的任務磁碟區。
- 如果任務需要的 vCPUs或記憶體資源比運算環境執行個體類型能提供的資源更多。
- 如果任務應該在 GPU 型執行個體上執行，但運算環境未設定為使用 GPU 型執行個體。
- 如果運算環境的 Auto Scaling 群組無法啟動執行個體。
- 如果啟動的執行個體可以加入基礎 Amazon Elastic Container Service (Amazon ECS) 叢集；否則，它會執行 [AWSSupport-TroubleshootECSContainerInstance](#) 執行手冊。
- 如果任何許可問題封鎖執行任務所需的特定動作。

Important

- 此 Runbook 必須在與您的任務停滯在 RUNNABLE 狀態的相同 AWS 區域中啟動。
- 此 Runbook 可以針對在 Amazon ECS AWS Fargate 或 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上排程 AWS Batch 的任務啟動。如果針對 Amazon Elastic Kubernetes Service (Amazon EKS) 上的 AWS Batch 任務啟動自動化，則啟動會停止。
- 如果執行個體可以執行任務，但無法註冊 Amazon ECS 叢集，此 Runbook 會啟動AWSSupport-TroubleshootECSContainerInstance自動化 Runbook，嘗試判斷原因。如需詳細資訊，請參閱 [AWSSupport-TroubleshootECSContainerInstance](#) 執行手冊。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- JobId

類型：字串

描述：(必要) 處於 RUNNABLE 狀態 AWS Batch 的任務 ID。

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

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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`

指示

1. 在主控台中導覽至 [AWSSupport-TroubleshootAWSBatchJob](#) AWS Systems Manager 。
2. 選取執行自動化
3. 針對輸入參數，輸入下列內容：

- `AutomationAssumeRole` (選用)：

(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `JobId` (必要)：

停滯在 `RUNNABLE` 狀態 AWS Batch 的任務 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.

b9e32

4. 選取執行。

5. 請注意，自動化會啟動。

6. 文件會執行下列步驟：

- PreflightPermissionChecks：

針對起始使用者/角色執行飛行前 IAM 許可檢查。如果有任何缺少的許可，此步驟會提供全域輸出區段中缺少的 API 動作。

- ProceedOnlyIfUserHasPermission：

分支是根據您是否具有 Runbook 所有必要動作的許可。

- AWSBatchJobEvaluation：

針對 AWS Batch 任務執行檢查，確認其存在且處於 RUNNABLE 狀態。

- ProceedOnlyIfBatchJobExistsAndIsInRunnableState：

根據任務是否存在且處於 RUNNABLE 狀態的分支。

- BatchComputeEnvironmentEvaluation：

針對 AWS Batch 運算環境執行檢查。

- ProceedOnlyIfComputeEnvironmentChecksAreOK：

根據運算環境檢查是否成功進行分支。

- UnderlyingInfraEvaluation：

針對基礎 Auto Scaling 群組或 Spot Fleet 請求執行檢查。

- ProceedOnlyIfInstancesNotJoiningEcsCluster：

分支取決於是否有執行個體未加入 Amazon ECS 叢集。

- EcsAutomationRunner：

為未加入叢集的執行個體執行 Amazon ECS 自動化。

- ExecutionResults :

根據先前的步驟產生輸出。

7. 完成後，會提供評估報告 HTML 檔案的 URI :

成功執行 Runbook 的報告的 S3 主控台連結和 Amazon S3 URI

▼ Outputs

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-3606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnoNEEWmt8eY" 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/updating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY".
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-XXXXXXXXXXXXXXXXXXXX-3606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-3606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnoNEEWmt8eY" 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/updating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY".
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.
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS CloudFormation

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS CloudFormation。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWS-DeleteCloudFormationStack

Description

刪除 AWS CloudFormation 堆疊。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- StackNameOrId

類型：字串

描述：(必要) 要刪除的 CloudFormation 堆疊之名稱或唯一 ID

AWS-EnableCloudFormationSNSNotification

Description

AWS-EnableCloudFormationSNSNotification Runbook 會為您指定的 () 堆疊啟用 Amazon Simple Notification Service AWS CloudFormation (Amazon SNS AWS CloudFormation) 通知。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- StackArn

類型：字串

描述：(必要) 您要為其啟用 Amazon SNS 通知的 AWS CloudFormation 堆疊 ARN 或名稱。

- NotificationArn

類型：字串

描述：(必要) 您要與 AWS CloudFormation 堆疊建立關聯的 Amazon SNS 主題 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- cloudformation:DescribeStacks
- cloudformation:UpdateStack
- kms:解密
- kms:產生資料金鑰
- sns:Publish
- sqs:GetQueueAttributes

文件步驟

- CheckCfnSnsLimits (aws:executeScript) - 驗證尚未與您指定的 AWS CloudFormation 堆疊建立關聯的 Amazon SNS 主題數量上限。
- EnableCfnSnsNotification (aws:executeAwsApi) - 啟用 AWS CloudFormation 堆疊的 Amazon SNS 通知。
- VerificationCfnSnsNotification (aws:executeScript) - 驗證堆疊是否已啟用 Amazon SNS 通知 AWS CloudFormation 。

輸出

CheckCfnSnsLimits.NotificationArnList - 接收 AWS CloudFormation 堆疊 Amazon SNS 通知的 ARNs 清單。

VerificationCfnSnsNotification.VerifySnsTopicsResponse - API 操作的回應，確認 AWS CloudFormation 堆疊已啟用 Amazon SNS 通知。

AWS-RunCfnLint

Description

此 Runbook 使用 [AWS CloudFormation Linter](#) `cfn-python-lint` () 來驗證 YAML 和 JSON 範本是否符合 AWS CloudFormation 資源規格。AWS-RunCfnLint Runbook 會執行其他檢查，例如確保已輸入資源屬性的有效值。如果驗證不成功，則 `RunCfnLintAgainstTemplate` 步驟會失敗，且會在錯誤訊息中提供 Linter 工具的輸出。此 Runbook 使用 `using cfn-lint v0.24.4`。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ConfigureRuleFlag

類型：字串

描述：（選用）規則要傳遞至 `--configure-rule` 參數的組態選項。

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

- FormatFlag

類型：字串

描述：(選用) 要傳遞給 `--format` 參數以指定輸出格式的值。

有效值：預設 | 安靜 | 可剖析 | json

預設：Default

- IgnoreChecksFlag

類型：字串

描述：(選用) 要傳遞至 `--ignore-checks` 參數的規則 ID。不會檢查這些規則。

範例：E1001,E1003,W7001

- IncludeChecksFlag

類型：字串

描述：(選用) 要傳遞至 `--include-checks` 參數的規則 ID。將會檢查這些規則。

範例：E1001,E1003,W7001

- InfoFlag

類型：字串

描述：(選用) `--info` 參數的選項。包含啟用範本處理的其他記錄資訊的選項。

預設：false

- TemplateFileName

類型：字串

描述：S3 儲存貯體中範本檔案的名稱或鍵。

- TemplateS3BucketName

類型：字串

描述：包含套件程式範本的 S3 儲存貯體名稱。

- RegionsFlag

類型：字串

描述：(選用) 要傳遞到的值，讓 `--regions` 參數根據指定的 測試範本 AWS 區域。

範例：us-east-1、us-west-1

文件步驟

RunCfnLintAgainstTemplate – 根據指定的 AWS CloudFormation 範本執行 `cfn-python-lint` 工具。

輸出

RunCfnLintAgainstTemplate.output – `cfn-python-lint` 工具中的 stdout。

AWSSupport-TroubleshootCFNCustomResource

Description

AWSSupport-TroubleshootCFNCustomResource Runbook 可協助診斷 AWS CloudFormation 堆疊在建立、更新或刪除自訂資源時失敗的原因。Runbook 會檢查用於自訂資源的服務權杖，以及傳回的錯誤訊息。檢閱自訂資源的詳細資訊後，執行手冊輸出會提供自訂資源堆疊行為和疑難排解步驟的說明。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- StackName

類型：字串

描述：(必要) 自訂資源失敗的 AWS CloudFormation 堆疊名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- validateCloudFormationStack - 驗證 AWS CloudFormation 堆疊是否存在於相同的 AWS 帳戶和中 AWS 區域。
- checkCustomResource - 分析 AWS CloudFormation 堆疊、檢查失敗的自訂資源，並輸出有關如何對失敗的自訂資源進行故障診斷的資訊。

AWS-UpdateCloudFormationStack

Description

使用存放在 Amazon S3 儲存貯體中的 AWS CloudFormation 範本來更新 AWS CloudFormation 堆疊。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LambdaAssumeRole

類型：字串

描述：（必要）Lambda 所擔任角色的 ARN

- StackNameOrId

類型：字串

描述：（必要）要更新的 AWS CloudFormation 堆疊名稱或唯一 ID

- TemplateUrl

類型：字串

描述：（必要）包含已更新 CloudFormation 範本的 S3 儲存貯體位置（例如 `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`）

CloudFront

AWS Systems Manager 自動化為 Amazon CloudFront 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

Description

AWSConfigRemediation-EnableCloudFrontDefaultRootObject Runbook 會為您指定的 Amazon CloudFront (CloudFront) 分佈設定預設根物件。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- CloudFrontDistributionId

類型：字串

描述：(必要) 您要為其設定預設根物件的 CloudFront 分佈 ID。

- DefaultRootObject

類型：字串

描述：(必要) 當檢視器請求指向您的根 URL 時，您希望 CloudFront 傳回的物件。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 為您在 CloudFrontDistributionId 參數中指定的 CloudFront 分佈設定預設根物件。

AWSConfigRemediation-EnableCloudFrontAccessLogs

Description

AWSConfigRemediation-EnableCloudFrontAccessLogs Runbook 會為您指定的 Amazon CloudFront (CloudFront) 分佈啟用存取記錄。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- BucketName

類型：字串

描述：（必要）您要存放存取日誌的 Amazon Simple Storage Service (Amazon S3) 儲存貯體名稱。AWS 區域 不支援 af-south-1、ap-east-1、eu-south-1 和 me-south-1 中的儲存貯體。

- CloudFrontId

類型：字串

描述：（必要）您要啟用存取登入的 CloudFront 分佈 ID。

- IncludeCookies

類型：布林值

有效值：true | false

描述：（必要）如果您想要將 Cookie 包含在存取日誌中，請將此參數設為 true。

- 字首

類型：字串

描述：（選用）您希望 CloudFront 在您的分佈存取日誌前綴filenames的選用字串，例如 myprefix/。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

Note

`s3:GetBucketLocation` API 只能用於相同帳戶中的 S3 儲存貯體。您無法將其用於跨帳戶 S3 儲存貯體。

文件步驟

- `aws:executeScript` - 為您在 `CloudFrontDistributionId` 參數中指定的 CloudFront 分佈啟用存取記錄。

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Description

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity Runbook 會為您指定的 Amazon CloudFront (CloudFront) 分佈啟用原始存取身分。此自動化會為 Amazon Simple Storage Service (Amazon S3) 原始伺服器類型的所有原始伺服器指派相同的 CloudFront 原始伺服器存取身分，而沒有您指定的 CloudFront 分佈的原始伺服器存取身分。此自動化不會授予 CloudFront 原始存取身分的讀取許可，以存取 Amazon S3 儲存貯體中的物件。您必須更新 Amazon S3 儲存貯體許可，以允許存取。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- CloudFrontDistributionId

類型：字串

描述：（必要）您要啟用原始伺服器容錯移轉的 CloudFront 分佈 ID。

- OriginAccessIdentityId

類型：字串

描述：（必要）要與原始伺服器建立關聯的 CloudFront 原始存取身分 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

- `cloudfront:UpdateDistribution`

文件步驟

- `aws:executeScript` - 為您在 `CloudFrontDistributionId` 參數中指定的 CloudFront 分佈啟用原始存取身分，並驗證原始存取身分是否已指派。

AWSConfigRemediation-EnableCloudFrontOriginFailover

Description

AWSConfigRemediation-EnableCloudFrontOriginFailover Runbook 會為您指定的 Amazon CloudFront (CloudFront) 分佈啟用原始伺服器容錯移轉。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `CloudFrontDistributionId`

類型：字串

描述：（必要）您要啟用原始伺服器容錯移轉的 CloudFront 分佈 ID。

- OriginGroupId

類型：字串

描述：（必要）原始伺服器群組的 ID。

- PrimaryOriginId

類型：字串

描述：（必要）原始伺服器群組中主要原始伺服器的 ID。

- SecondaryOriginId

類型：字串

描述：（必要）原始伺服器群組中次要原始伺服器的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 為您在 CloudFrontDistributionId 參數中指定的 CloudFront 分佈啟用原始伺服器容錯移轉，並驗證是否已啟用容錯移轉。

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Description

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS Runbook 會為您指定的 Amazon CloudFront (CloudFront) 分佈啟用檢視器通訊協定政策。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- CloudFrontDistributionId

類型：字串

描述：（必要）您要啟用檢視器通訊協定政策的 CloudFront 分佈 ID。

- ViewerProtocol 政策

類型：字串

有效值：https-only , redirect-to-https

描述：（必要）檢視器可用來存取原始伺服器中檔案的通訊協定。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

- `cloudfront:UpdateDistribution`
- `cloudfront:GetDistribution`

文件步驟

- `aws:executeScript` - 為您在 `CloudFrontDistributionId` 參數中指定的 CloudFront 分佈啟用檢視器通訊協定政策，並驗證政策是否已指派。

CloudTrail

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS CloudTrail。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

Description

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail Runbook 會建立 AWS CloudTrail (CloudTrail) 追蹤，將日誌檔案從多個 AWS 區域 交付到您選擇的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- BucketName

類型：字串

描述：(必要) 您要上傳日誌的 Amazon S3 儲存貯體名稱。

- keyPrefix

類型：字串

描述：(選用) Amazon S3 金鑰字首，位於您為日誌檔案交付指定的儲存貯體名稱之後。

- TrailName

類型：字串

描述：(必要) 要建立的 CloudTrail 追蹤名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

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

文件步驟

- `aws:executeAwsApi` - 接受線索名稱和 Amazon S3 儲存貯體名稱做為輸入，並建立 CloudTrail 線索。
- `aws:executeAwsApi` - 在建立的追蹤上啟用記錄，並開始將日誌交付到您指定的 Amazon S3 儲存貯體。
- `aws:assertAwsResourceProperty` - 驗證 CloudTrail 追蹤是否已建立。

AWS-EnableCloudTrail

Description

建立 AWS CloudTrail 追蹤並設定記錄至 S3 儲存貯體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName

類型：字串

描述：(必要) 指定發佈日誌檔的 S3 儲存貯體名稱。

 Note

S3 儲存貯體必須存在，且儲存貯體政策必須授予 CloudTrail 寫入它的許可。如需詳細資訊，請參閱[適用於 CloudTrail 的 Amazon S3 儲存貯體政策](#)。

- TrailName

類型：字串

描述：(必要) 新的追蹤名稱。

AWS-EnableCloudTrailCloudWatchLogs

Description

此 Runbook 會更新一或多個 AWS CloudTrail 追蹤的組態，以將事件傳送至 Amazon CloudWatch Logs 日誌群組。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- CloudWatchLogsLogGroupArn

類型：字串

描述：(必要) 交付 CloudTrail 日誌的 CloudWatch Logs 日誌群組 ARN。

- CloudWatchLogsRoleArn

類型：字串

描述：(必要) CloudWatch Logs Logs IAM 角色的 ARN 假設寫入指定的日誌群組。

- TrailNames

類型：StringList

描述：(必要) 以逗號分隔的 CloudTrail 追蹤名稱清單，其事件要傳送到 CloudWatch Logs。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- cloudtrail:UpdateTrail
- iam:PassRole

文件步驟

- aws:executeScript - 更新指定的 CloudTrail 追蹤，將事件交付至指定的 CloudWatch Logs 日誌群組。

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Description

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS Runbook 會使用您指定的 AWS CloudTrail () 客戶受管金鑰來加密 AWS Key Management Service (CloudTrail AWS KMS) 追蹤。此 Runbook 應僅用作基準，以確保您的 CloudTrail 追蹤根據最低建議的安全最佳實務進行加密。我們建議使用不同的 KMS 金鑰加密多個線索。CloudTrail 摘要檔案不會加密。如果您先前已將追蹤true的 EnableLogFileValidation 參數設定為 `true`，請參閱AWS CloudTrail 《使用者指南》中的 [CloudTrail 預防性安全最佳實務](#)主題的「使用伺服器端加密搭配 AWS KMS 受管金鑰」一節，以取得詳細資訊。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KMSKeyId

類型：字串

描述：（必要）您要用來加密TrailName參數中指定之追蹤的客戶受管金鑰的 ARN、金鑰 ID 或金鑰別名。

- TrailName

類型：字串

描述：（必要）您要更新以進行加密的線索 ARN 或名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeAwsApi` - 對您在 `TrailName` 參數中指定的線索啟用加密。
- `aws:executeAwsApi` - 收集您在 `KMSKeyId` 參數中指定的客戶受管金鑰的 ARN。
- `aws:assertAwsResourceProperty` - 確認 CloudTrail 追蹤已啟用加密。

AWS-EnableCloudTrailKmsEncryption

Description

此 Runbook 會更新一或多個 AWS CloudTrail 線索的組態，以使用 AWS Key Management Service (AWS KMS) 加密。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- KMSKeyId

類型：字串

描述：(必要) 您要用來加密參數中指定之追蹤的客戶受管金鑰的金鑰 ID TrailName。此值可以是「alias/」字首的別名名稱、別名的完整指定 ARN，或金鑰的完整指定 ARN。

- TrailNames

類型：StringList

描述：(必要) 您希望更新以逗號分隔的追蹤清單，以加密。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 啟用您在 TrailName 參數中指定的線索 AWS KMS 加密。

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Description

AWSConfigRemediation-EnableCloudTrailLogFileValidation Runbook 會為您的 AWS CloudTrail 追蹤啟用日誌檔案驗證。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- TrailName

類型：字串

描述：（必要）您要啟用日誌驗證之追蹤的名稱或 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeAwsApi` - 為您在 AWS CloudTrail `TrailName` 參數中指定的追蹤啟用日誌驗證。
- `aws:assertAwsResourceProperty` - 確認您的追蹤已啟用日誌驗證。

AWS-EnableCloudTrailLogFileValidation

Description

AWS-EnableCloudTrailLogFileValidation Runbook 會為您指定的 AWS CloudTrail 線索啟用日誌檔案驗證。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `TrailNames`

類型：StringList

描述：（必要）您想要啟用日誌驗證的 CloudTrail 追蹤名稱的逗號分隔清單。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

文件步驟

- aws:executeScript - 為您在 TrailNames 參數中指定的 AWS CloudTrail 線索啟用日誌驗證。

AWS-QueryCloudTrailLogs

Description

AWS-QueryCloudTrailLogs Runbook 會從您選擇的 Amazon Simple Storage Service (Amazon S3) 儲存貯體建立 Amazon Athena 資料表，其中包含 AWS CloudTrail (CloudTrail) 日誌。Amazon S3 建立資料表後，自動化會執行您指定的 SQL 查詢，然後刪除資料表。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- Query

類型：字串

描述：（必要）您要執行的 SQL 查詢。

- SourceBucketPath

類型：字串

描述：（必要）Amazon S3 儲存貯體的名稱，其中包含您要查詢的 CloudTrail 日誌檔案。

- TableName

類型：字串

描述：（選用）自動化建立的 Athena 資料表名稱。

預設：Cloudtrail_logs

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

文件步驟

- aws:executeAwsApi - 建立 Athena 資料表。
- aws:executeAwsApi - 執行您在 Query 參數中指定的查詢字串。
- aws:executeScript - 輪詢並等待查詢完成。
- aws:executeAwsApi - 取得查詢的結果。
- aws:executeAwsApi - 刪除自動化建立的資料表。

CloudWatch

AWS Systems Manager 自動化為 Amazon CloudWatch 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-ConfigureCloudWatchOnEC2Instance](#)
- [AWS-EnableCWAAlarm](#)

AWS-ConfigureCloudWatchOnEC2Instance

Description

啟用或停用受管執行個體上的 Amazon CloudWatch 詳細監控。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 您要在其中啟用 CloudWatch 監控的 Amazon EC2 執行個體 ID。

- 屬性

類型：字串

描述：(選用) 不支援此參數。在此列出回溯相容性的此參數。

- status

有效值：已啟用 | 已停用

描述：(選用) 指定是否啟用或停用 CloudWatch。

預設：Enabled

文件步驟

configureCloudWatch - 在具有指定狀態的 Amazon EC2 執行個體上設定 CloudWatch。

輸出

此自動化沒有輸出。

AWS-EnableCWAlarm

Description

AWS-EnableCWAlarm Runbook 會為 中尚無 AWS 資源 AWS 帳戶 的資源建立 Amazon CloudWatch (CloudWatch) 警示。系統會為下列 AWS 資源建立 CloudWatch 警示：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體
- Amazon Elastic Block Store (Amazon EBS) 磁碟區
- Amazon Simple Storage Service (Amazon S3) 儲存貯體
- Amazon Relational Database Service (Amazon RDS) 叢集

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ComparisonOperator

類型：字串

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

描述：（必要）比較指定的統計資料和閾值時要使用的算術操作。

- MetricName

類型：字串

描述：（必要）與警示相關聯的指標名稱。

- 期間

類型：整數

有效值：10 | 30 | 60 | 60 的倍數

描述：（必要）套用統計資料的期間，以秒為單位。

- ResourceARNs

類型：StringList

描述：（必要）以逗號分隔的資源 ARNs 清單，以建立的 CloudWatch 警示

- 統計數字

類型：字串

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

描述：（必要）與警示相關聯的指標統計資料。

- Threshold

類型：整數

描述：（必要）要與指定統計資料比較的值。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- cloudwatch:PutMetricAlarm

文件步驟

- aws:executeScript - 根據您在參數中指定之資源的 Runbook ResourceARNs 參數中指定的值，建立 CloudWatch 警示。

輸出

EnableCWAAlarm.FailedResources: 未建立 CloudWatch 警示的資源 ARNs 映射清單，以及失敗的原因。

EnableCWAAlarm.SuccessfulResources: 已成功建立 CloudWatch 警示的資源 ARNs 清單。

Amazon DocumentDB

AWS Systems Manager 自動化為 Amazon DocumentDB 提供預先定義的 Runbook（與 MongoDB 相容）。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

AWS-EnableDocDbClusterBackupRetentionPeriod

Description

AWS-EnableDocDbClusterBackupRetentionPeriod Runbook 會為您指定的 Amazon DocumentDB 叢集啟用備份保留期間。此功能會設定自動備份保留的總天數。若要修改叢集，叢集必須處於可用狀態，引擎類型為 docdb。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DBClusterResourceId

類型：字串

描述：(必要) 您要為其啟用備份保留期的 Amazon DocumentDB 叢集的資源 ID。

- BackupRetentionPeriod

類型：整數

描述：(必要) 保留自動備份的天數。必須是 7-35 天的值。

- PreferredBackupWindow

類型：字串

描述：(選用) 國際標準時間協同 (UTC) 的每日時間範圍，格式為 hh24:mm-hh24:mm，例如 07:14-07:44。值必須至少為 30 分鐘，且不能與偏好的維護時段衝突。

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

文件步驟

- GetDocDbClusterIdentifier (aws:executeAwsApi) - 使用提供的資源 ID 傳回 Amazon DocumentDB 叢集識別符。
- VerifyDocDbEngine (aws:assertAwsResourceProperty) - 驗證 Amazon DocumentDB 引擎類型 docdb 是為了防止意外變更其他 Amazon RDS 引擎類型。

- `VerifyDocDbStatus (aws:waitAwsResourceProperty)` - 驗證 Amazon DocumentDB 叢集狀態為 `available`。
- `ModifyDocDbRetentionPeriod (aws:executeAwsApi)` - 使用指定 Amazon DocumentDB 叢集提供的值來設定保留期間。
- `VerifyDocDbBackupsEnabled (aws:executeScript)` - 驗證 Amazon DocumentDB 叢集的保留期間，如果指定，則表示已成功設定偏好的備份時段。

輸出

`ModifyDocDbRetentionPeriod.ModifyDbClusterResponse` - `ModifyDBCluster` API 操作的回應。

`VerifyDocDbBackupsEnabled.VerifyDbClusterBackupsEnabledResponse` - 步驟的輸出，`VerifyDocDbBackupsEnabled` 確認成功修改 Amazon DocumentDB 叢集。

CodeBuild

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS CodeBuild。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Description

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` Runbook 會使用您指定的 AWS Key Management Service () 客戶受管金鑰來加密 AWS CodeBuild (CodeBuild AWS KMS) 專案的建置成品。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用 。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KMSKeyId

類型：字串

描述：(必要) 您要用來加密ProjectId參數中指定 CodeBuild 專案的客戶受管金鑰的 AWS KMS Amazon Resource Name (ARN)。

- ProjectId

類型：字串

描述：(必要) 您要加密其建置成品的 CodeBuild 專案 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeAwsApi - 從專案 ID 收集 CodeBuild 專案名稱。

- `aws:executeAwsApi` - 啟用您在 `ProjectId` 參數中指定的 CodeBuild 專案加密。
- `aws:assertAwsResourceProperty` - 驗證 CodeBuild 專案上是否已啟用加密。

輸出

`UpdateLambdaConfig.UpdateFunctionConfigurationResponse` - `UpdateFunctionConfiguration` API 呼叫的回應。

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Description

`AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` Runbook 會從您指定的 AWS CodeBuild (CodeBuild) 專案中刪除 `AWS_ACCESS_KEY_ID`和 `AWS_SECRET_ACCESS_KEY`環境變數。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用 。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `ResourceId`

類型：字串

描述：(必要) 您想要刪除其存取金鑰環境變數的 CodeBuild 專案 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 刪除 ResourceId 參數中指定之 CodeBuild 專案的存取金鑰環境變數。

AWS CodeDeploy

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS CodeDeploy。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-TroubleshootCodeDeploy](#)

AWSSupport-TroubleshootCodeDeploy

Description

AWSSupport-TroubleshootCodeDeploy Runbook 可協助診斷 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上 AWS CodeDeploy 部署失敗的原因。Runbook 會輸出步驟，協助您進一步解決問題或故障診斷。也提供 CodeDeploy 的最佳實務，協助您避免未來的類似問題。

此 Runbook 可協助您解決下列問題：

- CodeDeploy 代理程式未安裝或未於 Amazon EC2 執行個體上執行

- Amazon EC2 執行個體未連接 AWS Identity and Access Management (IAM) 執行個體設定檔
- 連接至 Amazon EC2 執行個體的 IAM 執行個體設定檔沒有必要的 Amazon Simple Storage Service (Amazon S3) 許可
- Amazon S3 中儲存的修訂遺失，或所使用的 Amazon S3 儲存貯體位於與 Amazon EC2 執行個體 AWS 區域 不同的 中
- 應用程式規格 (AppSpec) 檔案問題
- 「檔案已存在於位置」錯誤
- 失敗的 CodeDeploy 受管生命週期事件關聯
- 失敗的客戶受管生命週期事件關聯
- 部署期間的縮減事件

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DeploymentId

類型：字串

描述：（必要）失敗的部署 ID。

- InstanceId

類型：字串

描述：（必要）部署失敗的 Amazon EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeAwsApi - 驗證為 DeploymentId 和 InstanceId 參數提供的值。
- aws:executeScript - 從 Amazon EC2 執行個體收集資訊，例如執行個體的狀態和 IAM 執行個體設定檔詳細資訊。
- aws:executeScript - 檢閱指定的部署，並傳回有關部署失敗原因的分析。

AWS Config

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Config。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-SetupConfig](#)

AWSSupport-SetupConfig

Description

AWSSupport-SetupConfig Runbook 會建立 AWS Identity and Access Management (IAM) 服務連結角色、由 提供支援的組態記錄器 AWS Config，以及具有 Amazon Simple Storage Service

(Amazon S3) 儲存貯體的交付管道，其中 會 AWS Config 傳送組態快照和組態歷史記錄檔案。如果您 為 AggregatorAccountId 和 AggregatorAccountRegion 參數指定值，則 Runbook 也會建立資料彙總的授權，以從多個 和多個 收集 AWS Config 組態 AWS 帳戶 和合規資料 AWS 區域。若要進一步了解如何從多個帳戶和區域彙總資料，請參閱《AWS Config 開發人員指南》中的 [多帳戶多區域資料彙總](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- AggregatorAccountId

類型：字串

描述：（選用）將新增彙總器的 ID，以彙總來自多個帳戶和 AWS 帳戶 的 AWS Config 組態和合規資料 AWS 區域。彙總器也會使用此帳戶來授權來源帳戶。

- AggregatorAccountRegion

類型：字串

描述：（選用）將新增彙總器的區域，以彙總來自多個帳戶和區域的 AWS Config 組態和合規資料。

- IncludeGlobalResourcesRegion

類型：字串

預設：us-east-1

描述：（必要）若要避免在每個區域中記錄全域資源資料，請指定一個區域來記錄全域資源資料。

- 分區

類型：字串

預設：aws

描述：（必要）您要從中收集 AWS Config 組態和合規資料的分割區。

- S3BucketName

類型：字串

預設：aws-config-delivery-channel

描述：（選用）您要套用至為交付管道建立的 Amazon S3 儲存貯體的名稱。帳戶 ID 會附加到名稱的結尾。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:executeScript` - AWS Config 如果服務連結的 IAM 角色不存在，請為 建立該角色。
- `aws:executeScript` - 如果組態記錄器不存在，則建立組態記錄器。
- `aws:executeScript` - 建立 Amazon S3 儲存貯體，以便在交付管道尚未存在時使用。
- `aws:executeScript` - 使用 Runbook 建立的資源建立交付管道。
- `aws:executeAwsApi` - 啟動組態記錄器。
- `aws:executeScript` - 如果您為 `AggregatorAccountId`和 `AggregatorAccountRegion` 參數指定值，則會設定多帳戶和多區域資料彙總的授權。

Amazon Connect

AWS Systems Manager 自動化為 Amazon Connect 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

Description

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows` 可協助您將電話號碼與 Amazon Connect 執行個體中的聯絡流程建立關聯。透過在輸入逗號分隔值 (CSV) 檔案中提供電話號碼和聯絡流程的映射，Runbook 會在 14.5 分鐘內將盡可能多的電話號碼與聯絡流程建立關聯。Runbook 會產生所有電話號碼和聯絡流程對的 CSV 檔案，無法在時間限制內建立關聯，以便您在下次執行時輸入。

如何運作？

Runbook `AWSsupport-AssociatePhoneNumbersToConnectContactFlows` 可協助您使用存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的映射資料的 CSV 檔案，將電話號碼與 Amazon Connect 執行個體中的聯絡流程建立關聯。Amazon S3 輸入 CSV 檔案應符合下列格式，其 `PhoneNumber` 值為 [E.164 格式](#)。

輸入 CSV 檔案的範例

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

自動化 Runbook 也會在 `DestinationFileBucket` 和 `DestinationFilePath` 中指定的目的地位置建立下列檔案。

- **`automation:EXECUTION_ID/ResourceIdList.csv`** : 包含 `AssociatePhoneNumberContactFlow` API 所需的 `PhoneNumberId` 和 `ContactFlowId` 對的暫存檔案。
- **`automation:EXECUTION_ID/ErrorResourceList.csv`** : 包含電話號碼和聯絡流程對的檔案，因為錯誤而無法處理，例如 `ResourceNotFoundException` 的格式 `PhoneNumber,ContactFlowName,ErrorMessage`。
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`** : 包含未處理的電話號碼和聯絡流程對的檔案。Runbook 會嘗試在 14.5 分鐘 (AWS Lambda 函數逾時的 15 分鐘 - 緩衝的 30 秒) 內處理盡可能多的電話號碼和聯絡流程。如果因為時間限制而無法處理某些電話號碼/聯絡流程，則 Runbook 會將它們包含在 CSV 檔案中，以做為下次執行 Runbook 的輸入。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

```
{
  "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": [
        "arn:aws:iam::AWS_ACCOUNT_ID:role/AutomationAssumeRole",
        "arn:aws:iam::AWS_ACCOUNT_ID:role/AutomationAssumeRole/*",
        "arn:aws:iam::AWS_ACCOUNT_ID:policy/AutomationAssumeRolePolicy",
        "arn:aws:iam::AWS_ACCOUNT_ID:policy/AutomationAssumeRolePolicy/*",
        "arn:aws:lambda::AWS_ACCOUNT_ID:function:*",
        "arn:aws:lambda::AWS_ACCOUNT_ID:layer:*",
        "arn:aws:logs::AWS_ACCOUNT_ID:log-group:*",
        "arn:aws:logs::AWS_ACCOUNT_ID:retention-policy:*",
        "arn:aws:connect::AWS_ACCOUNT_ID:contact-flow:*",
        "arn:aws:s3:::AWS_ACCOUNT_ID",
        "arn:aws:s3:::AWS_ACCOUNT_ID/*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```

    ],
    "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"
  }
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-AssociatePhoneNumbersToConnectContactFlows](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN) , 可讓 Systems Manager Automation 代表您執行動作。如果未指定角色, Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `ConnectInstanceId` (必要)

Amazon Connect 執行個體的 ID。

- `SourceFileBucket` (必要)

存放 CSV 檔案的 Amazon S3 儲存貯體, 其中包含電話號碼和聯絡流程對。

- `SourceFilePath` (必要)

CSV 檔案的 Amazon S3 物件金鑰, 其中包含電話號碼和聯絡流程對。例如: `path/to/input.csv`。

- `DestinationFileBucket` (必要)

自動化將放置中繼檔案和結果報告的 Amazon S3 儲存貯體。

- `DestinationFilePath` (選用)

中 `DestinationFileBucket` 繼檔案和結果報告的 Amazon S3 物件路徑。例如, 如果您指定 `path/to/files/`, 檔案會存放在 `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`。

- `S3BucketOwnerAccount` (選用)

擁有您要上傳聯絡流程日誌之 Amazon S3 儲存貯體的 AWS 帳號。如果您未指定此參數, 則 Runbook 會使用自動化執行所在使用者或角色 AWS 的帳戶 ID。

- `S3BucketOwnerRoleArn` (選用)

IAM 角色的 ARN, 具有取得 Amazon S3 儲存貯體和帳戶區塊公開存取設定、儲存貯體加密組態、儲存貯體 ACLs、儲存貯體政策狀態, 以及將物件上傳至儲存貯體的許可。如果未指定此參數, 則 Runbook 會使用啟動此 Runbook 的 `AutomationAssumeRole` (如果指定) 或 使用者 (如果 `AutomationAssumeRole` 未指定)。請參閱 Runbook 描述中的必要許可區段。

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. test-role	ConnectInstanceId (Required) The ID of your Amazon Connect instance. 01234567-89ab-cdef-0123-456789abcdef
SourceFileBucket (Required) The Amazon S3 bucket name that stores the CSV file which contains the pairs of phone numbers and Contact Flows.	SourceFilePath (Required) The Amazon S3 object key of the CSV file that contains the pairs of phone numbers and Contact Flows. Example: 'path/to/input.csv'. String
DestinationFileBucket (Required) The Amazon S3 bucket that the automation will copy the file to be processed, the report, and any non-processed phone number and Contact Flow pair.	DestinationFilePath (Optional) The Amazon S3 object path in 'DestinationFileBucket' to copy the file to be processed, the report, and any non-processed phone number and Contact Flow pair. For example, if you specify 'path/to/files/', the files will be stored under 's3://<DestinationFileBucket>/path/to/files/<automation:EXECUTION_ID>'. 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. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- CheckConnectInstanceExistence

檢查 中提供的 Amazon Connect 執行個體是否存在ConnectInstanceId。

- CheckS3BucketPublicStatus

檢查 中指定的 Amazon S3 儲存貯體是否SourceFileBucketDestinationFileBucket允許匿名或公有讀取或寫入存取許可。

- CheckSourceFileExistenceAndSize

檢查 中指定的來源 CSV 檔案SourceFilePath是否存在，以及檔案大小是否超過 25 MiB 的限制。

- GenerateResourceIdMap

下載 中指定的來源 CSV 檔案SourceFilePath，並ContactFlowId為每個資源識別 PhoneNumberId和。完成後，它會將包含 PhoneNumber、PhoneNumberId、ContactFlowName和的 CSV 檔案上傳至 ContactFlowId 中指定的目的地 Amazon S3 儲存貯體DestinationFileBucket。如果PhoneNumberId無法識別特定號碼的，則 CSV 檔案中的 將是空的。

- AssociatePhoneNumbersToContactFlows

使用 AWS CloudFormation 堆疊在帳戶中建立 AWS Lambda 函數。AWS Lambda 函數會將每個數字與 SourceFileBucket和 中指定的來源 CSV 檔案中列出的聯絡流程建立關聯，SourceFilePath堆疊會 AWS CloudFormation 叫用 函數。AWS Lambda 函數會盡可能將電話號碼映射到聯絡流程，然後再逾時 (15 分鐘)。因錯誤而無法處理的電話號碼和聯絡流程清單會上傳至 [automation:EXECUTION_ID]/ErrorResourceList.csv。

因為在單一執行中可處理的電話號碼數量超過上限而無法處理的電話號碼會上傳到 [automation:EXECUTION_ID]/NonProcessedResourceList.csv。如果此步驟失敗，則會前往DescribeCloudFormationErrorFromStackEvents步驟，以顯示堆疊 AWS CloudFormation 事件失敗的原因。

- WaitForPhoneNumberContactFlowAssociationCompletion

等待建立對應電話號碼至聯絡流程的 AWS Lambda 函數，且 AWS CloudFormation 堆疊完成其調用。

- GenerateReport

產生報告，其中包含對應至聯絡流程的電話號碼數量、因錯誤而無法處理的電話號碼數量，以及因單一執行中可處理的電話號碼數量上限而無法處理的電話號碼數量。如果適用 [automation:EXECUTION_ID]/NonProcessedResourceList.csv，報告也會顯示 [automation:EXECUTION_ID]/ErrorResourceList.csv 或 的位置 (Amazon S3 URI 和 Amazon S3 主控台 URL)。

- **DeleteCloudFormationStack**

刪除 AWS CloudFormation 堆疊，包括用於映射的 Lambda 函數。

- **DescribeCloudFormationErrorFromStackEvent**

描述AssociatePhoneNumbersToContactFlows步驟 AWS CloudFormation 堆疊的錯誤。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- GenerateReport.OutputPayload

電話號碼和聯絡流程關聯的輸出。此報告包含下列資訊：

- 輸入 CSV 檔案中列出的電話號碼和聯絡流程對數量
- 與輸入 CSV 檔案中指定的聯絡流程相關聯的電話號碼數量
- 由於錯誤而無法與聯絡流程建立關聯的電話號碼數量
- 由於時間限制，與聯絡流程無關的電話號碼數量
- CSV 檔案的位置 (Amazon S3 URI 和 Amazon S3 主控台 URL)，其中包含因錯誤而無法關聯的電話號碼和聯絡流程對
- CSV 檔案的位置 (Amazon S3 URI 和 Amazon S3 主控台 URL)，其中包含因時間限制而未關聯的電話號碼和聯絡流程對
- DescribeCloudFormationErrorFromStackEvents.Events

如果AssociatePhoneNumbersToContactFlows步驟失敗，顯示 AWS CloudFormation 堆疊事件的輸出。

使用少量電話號碼和聯絡流程輸出執行

```
▼ 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
=====
}
```

使用大量電話號碼和聯絡流程輸出執行，以及由於錯誤或時間限制而未關聯的電話號碼

```
▼ 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.
=====
}
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSSupport-CollectAmazonConnectContactFlowLog

Description

`AWSsupport-CollectAmazonConnectContactFlowLog` 自動化 Runbook 用於收集特定聯絡 ID 的 Amazon Connect 聯絡流程日誌。透過提供 Amazon Connect 執行個體 ID 和聯絡人 ID，Runbook 會從 Amazon CloudWatch 日誌群組搜尋聯絡人的聯絡流程日誌，並將其上傳至請求參數中指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。Runbook 會產生輸出，提供 Amazon S3 主控台 URL 和 AWS CLI 命令供您下載日誌。

如何運作？

`AWSsupport-CollectAmazonConnectContactFlowLog` 自動化 Runbook 有助於收集存放在已設定 CloudWatch 日誌群組中特定聯絡人 ID 的 Amazon Connect 聯絡流程日誌，並將其上傳至指定的 Amazon S3 儲存貯體。為了協助保護從 Amazon Connect 聯絡流程收集之日誌的安全性，自動化會評估 Amazon S3 儲存貯體組態，以判斷儲存貯體是否授予公有 `read` 或 `write` 存取許可，且由 `S3BucketOwnerAccountId` 參數中指定的 AWS 帳戶所擁有。如果您的 Amazon S3 儲存貯體使用伺服器端加密搭配 AWS Key Management Service 金鑰 (SSE-KMS)，請確定執行此自動化的使用者或 AWS Identity and Access Management (IAM) 角色具有 AWS KMS 金鑰的 `kms:GenerateDataKey` 許可。如需 Amazon Connect 執行個體產生的日誌的詳細資訊，請參閱 [存放在 Amazon CloudWatch 日誌群組中的流程日誌](#)。

 Important

CloudWatch Logs Insights 查詢會根據查詢的資料量產生費用。免費方案客戶僅需針對超出 Service Quotas 的使用量支付費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

```
{
  "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"
    }
  ]
}
```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-CollectAmazonConnectContactFlowLog](#) 中導覽至。

2. 選擇 Execute automation (執行自動化)。

3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ConnectInstanceId (必要)：

Amazon Connect 執行個體的 ID。

- ContactId (必要)：

您要收集聯絡人流程日誌的聯絡人 ID。

- S3BucketName (必要)：

帳戶中您要上傳聯絡流程日誌的 Amazon S3 儲存貯體名稱。請確定儲存貯體政策不會將不必要的讀取/寫入許可授予不需要存取所收集日誌的各方。

- S3ObjectPrefix (選用)：

Amazon S3 儲存貯體中的 Amazon S3 物件路徑，用於上傳的聯絡流程日誌。例如，如果您指定 CollectedLogs，日誌將上傳為 s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz。如果您未指定此參數，則會使用 Systems Manager Automation 執行 ID，例如：s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz。注意：如果您指定的值 S3ObjectPrefix 並使用相同的 【ContactId】 執行此自動化，則聯絡人流程日誌將被覆寫。

- S3BucketOwnerAccount (選用)：

擁有您要上傳聯絡流程日誌之 Amazon S3 儲存貯體的 AWS 帳號。如果您未指定此參數，則 Runbook 會使用自動化執行所在使用者或角色 AWS 的帳戶 ID。

- S3BucketOwnerRoleArn (選用)：

IAM 角色的 ARN，具有取得 Amazon S3 儲存貯體和帳戶區塊公開存取設定、儲存貯體加密組態、儲存貯體 ACLs、儲存貯體政策狀態，以及將物件上傳至儲存貯體的許可。如果未指定此參數，則 Runbook 會使用啟動此 Runbook 的 AutomationAssumeRole（如果指定）或使用者（如果 AutomationAssumeRole 未指定）。請參閱 Runbook 說明中的必要許可區段。

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}.gr'. 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}.gr'. 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. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- CheckConnectInstanceExistence

檢查 中提供的 Amazon Connect 執行個體是否為 ConnectInstanceId ACTIVE。

- CheckS3BucketPublicStatus

檢查 中指定的 Amazon S3 儲存貯體是否 S3BucketName 允許匿名或公有讀取或寫入存取許可。

- GenerateLogSearchTimeRange

根據 和 DescribeContact API LastUpdateTimestamp 傳

回 StartTimeEndTimeStartQuery 的步驟產生 InitiationTimestamp 和。

StartTime 將是 之前的一小時 InitiationTimestamp，EndTime 並將是 之後的一小時 LastUpdateTimestamp。

- StartQuery

啟動 CloudWatch Logs 日誌群組 ContactId 中提供的 查詢日誌，該群組與 中提供的 Amazon Connect 執行個體相關聯 ConnectInstanceId。查詢執行時間 60 分鐘後逾時。如果您的查詢逾時，請減少要搜尋的時間範圍。您可以在 CloudWatch 主控台中檢視目前進行中的查詢，以及您最近的查詢歷史記錄。如需詳細資訊，請參閱 [檢視執行中的查詢或查詢歷史記錄](#)。

- WaitForQueryCompletion

等待 CloudWatch Logs 查詢日誌ContactId，讓提供的 完成。請注意，查詢會在執行時間 60 分鐘後逾時。如果您的查詢逾時，請減少要搜尋的時間範圍。您可以在 Amazon Connect 主控台中檢視目前進行中的查詢，以及您最近的查詢歷史記錄。如需詳細資訊，請參閱[檢視執行中的查詢或查詢歷史記錄](#)。

- UploadContactFlowLog

取得查詢結果，並將聯絡流程日誌上傳至 中指定的 Amazon S3 儲存貯體S3BucketName。

- GenerateReport

傳回已上傳聯絡流程日誌的 Amazon S3 主控台 URL，以及可用來下載日誌檔案的 CLI AWS 命令範例。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- GenerateReport.OutputPayload

輸出，告訴您 Runbook 已成功擷取指定聯絡人的聯絡流程日誌。此報告也包含 Amazon S3 主控台 URL 和範例 AWS CLI 命令，讓您可以下載日誌檔案。

▼ 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
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS Directory Service

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Directory Service。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWS-CreateDSManagementInstance

Description

AWS-CreateDSManagementInstance Runbook 會建立 Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體，供您用來管理 AWS Directory Service 目錄。管理執行個體無法用於管理 AD Connector 目錄。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- AmiId

類型：字串

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

描述：(必要) 您要用來啟動管理執行個體的 Amazon Machine Image(AMI) ID。

- DirectoryId

類型：字串

描述：(必要) 您要管理的 AWS Directory Service 目錄 ID。執行個體會加入您指定的目錄。

- IamInstanceProfileName

類型：字串

描述：(必要) 您指定的名稱會套用至自動化建立並連接至管理執行個體的 IAM 執行個體描述檔。

- InstanceType

類型：字串

預設：t3.medium

允許的值：

- 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：(必要) 您要啟動的執行個體類型。

- KeyPairName

類型：字串

描述：(選用) 建立執行個體時要使用的金鑰對。如果您未指定值，則不會與執行個體建立任何金鑰對關聯。

- RemoteAccessCidr

類型：字串

描述：(必要) 您要允許 RDP 流量 (連接埠 3389) 的 CIDR 區塊。您指定的 CIDR 區塊會套用至傳入規則，而此規則會新增至自動化建立的安全群組。

- SecurityGroupName

類型：字串

描述：(必要) 您指定的名稱會套用至自動化所建立並與管理執行個體相關聯的安全群組。

- 標籤

類型：MapList

描述：(選用) 您要套用至自動化所建立資源的鍵值對。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceState`
- `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`

文件步驟

- `aws:executeAwsApi` - 收集您在 `DirectoryId` 參數中指定的目錄詳細資訊。
- `aws:executeAwsApi` - 取得啟動目錄之虛擬私有雲端 (VPC) 的 CIDR 區塊。
- `aws:executeAwsApi` - 使用您在 `SecurityGroupName` 參數中指定的值建立安全群組。
- `aws:executeAwsApi` - 為新建立的安全群組建立傳入規則，允許來自您在 `RemoteAccessCidr` 參數中指定 CIDR 的 RDP 流量。
- `aws:executeAwsApi` - 使用您在 `IamInstanceProfileName` 參數中指定的值建立 IAM 角色和執行個體描述檔。
- `aws:executeAwsApi` - 根據您在 `Runbook` 參數中指定的值啟動 Amazon EC2 執行個體。
- `aws:executeAwsApi` - 建立 AWS Systems Manager 文件，將新啟動的執行個體加入您的目錄。
- `aws:runCommand` - 將新執行個體加入您的目錄。
- `aws:runCommand` - 在新執行個體上安裝遠端伺服器管理工具。

AWSSupport-TroubleshootADConnectorConnectivity

Description

AWSSupport-TroubleshootADConnectorConnectivity Runbook 會驗證 AD Connector 的下列先決條件：

- 檢查與 AD Connector 相關聯的安全群組和網路存取控制清單 (ACL) 規則是否允許所需的流量。
- 檢查 AWS Security Token Service AWS Systems Manager、和 Amazon CloudWatch 介面 VPC 端點是否存在與 AD Connector 相同的虛擬私有雲端 (VPC) 中。

當先決條件檢查成功完成時，執行手冊會在與 AD Connector 相同的子網路中啟動兩個 Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro 執行個體。然後，使用 netcat 和 nslookup 公用程式執行網路連線測試。

[執行此自動化（主控台）](#)

Important

使用此 Runbook 可能會針對自動化期間建立 AWS 帳戶 的 Amazon EC2 執行個體、Amazon Elastic Block Store 磁碟區和 Amazon Machine Image(AMI)，向 收取額外費用。如需詳細資訊，請參閱 [Amazon Elastic Compute Cloud 定價](#) 和 [Amazon Elastic Block Store 定價](#)。

如果 aws:deletestack 步驟失敗，請前往 AWS CloudFormation 主控台 手動刪除堆疊。此 Runbook 建立的堆疊名稱開頭為 AWSSupport-TroubleshootADConnectorConnectivity。如需有關刪除 AWS CloudFormation 堆疊的資訊，請參閱 AWS CloudFormation 《使用者指南》中的 [刪除堆疊](#)。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DirectoryId

類型：字串

描述：(必要) 您要疑難排解連線的 AD Connector 目錄 ID。

- Ec2InstanceProfile

類型：字串

字元上限：128

描述：(必要) 您要指派給啟動執行連線測試之執行個體的執行個體設定檔名稱。您指定的執行個體描述檔必須連接AmazonSSManagedInstanceCore政策或同等許可。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:assertAwsResourceProperty` - 確認 `DirectoryId` 參數中指定的目錄是 AD Connector。
- `aws:executeAwsApi` - 收集 AD Connector 的相關資訊。
- `aws:executeAwsApi` - 收集與 AD Connector 相關聯的安全群組資訊。
- `aws:executeAwsApi` - 收集與 AD Connector 子網路相關聯的網路 ACL 規則的相關資訊。
- `aws:executeScript` - 評估 AD Connector 安全群組規則，以確認允許必要的傳出流量。
- `aws:executeScript` - 評估 AD Connector 網路 ACL 規則，以確認允許必要的傳出和傳入網路流量。
- `aws:executeScript` - 檢查 AWS Systems Manager AWS Security Token Service 和 Amazon CloudWatch 介面端點是否存在於與 AD Connector 相同的 VPC 中。
- `aws:executeScript` - 編譯先前步驟中執行之檢查的輸出。
- `aws:branch` - 會根據先前步驟的輸出來配置自動化。如果安全群組和網路 ACLs 缺少必要的傳出和傳入規則，自動化會停止在此。
- `aws:createStack` - 建立 AWS CloudFormation 堆疊以啟動 Amazon EC2 執行個體，以執行連線測試。
- `aws:executeAwsApi` - 收集新啟動的 Amazon EC2 執行個體 IDs。
- `aws:waitForAwsResourceProperty` - 等待第一個新啟動的 Amazon EC2 執行個體報告由 管理 AWS Systems Manager。
- `aws:waitForAwsResourceProperty` - 等待第二個新啟動的 Amazon EC2 執行個體報告由 管理 AWS Systems Manager。
- `aws:runCommand` - 從第一個 Amazon EC2 執行個體對現場部署 DNS 伺服器 IP 地址執行網路連線測試。
- `aws:runCommand` - 從第二個 Amazon EC2 執行個體對內部部署 DNS 伺服器 IP 地址執行網路連線測試。
- `aws:changeInstanceState` - 停止用於連線測試的 Amazon EC2 執行個體。
- `aws:deleteStack` - 刪除 AWS CloudFormation 堆疊。
- `aws:executeScript` - 輸出在自動化無法刪除 AWS CloudFormation 堆疊時如何手動刪除堆疊的指示。

AWSSupport-TroubleshootDirectoryTrust

Description

AWSSupport-TroubleshootDirectoryTrust Runbook 會診斷 AWS Managed Microsoft AD 和 Microsoft Active Directory 之間的信任建立問題。自動化會確認目錄類型支援信任，然後會檢查關聯的安全群組規則、網路存取控制清單 (網路 ACL)，以及路由表來檢查是否有潛在的連線能力問題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DirectoryId

類型：字串

允許模式：`^d-【a-z0-9】{10}$`

描述：（必要）AWS Managed Microsoft AD 要故障診斷的 ID。

- RemoteDomainCidrs

類型：StringList

允許模式：`^((【0-9】|【1-9】 【0-9】|1【0-9】{2}|2【0-4】 【0-9】|25【0-5】)\.){3}(【0-9】|【1-9】 【0-9】|1【0-9】{2}|2【0-4】 【0-9】|25【0-5】)(v(3【0-2】|【1-2】 【0-9】|【1-9】))$`

描述：(必要) 您正在嘗試與其建立信任關係的遠端網域 CIDR。您可以使用逗號分隔值新增多個 CIDR。例如：172.31.48.0/20, 192.168.1.10/32。

- RemoteDomainName

類型：字串

描述：(必要) 您正在與其建立信任關係的遠端網域完整網域名稱。

- RequiredTrafficACL

類型：字串

描述：(必要) 的預設連接埠需求 AWS Managed Microsoft AD。在大多數情況下，您不應修改預設值。

預設：`{"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

類型：字串

描述：(必要) 的預設連接埠需求 AWS Managed Microsoft AD。在大多數情況下，您不應修改預設值。

預設：`{"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

類型：字串

描述：(選用) 要針對其進行故障診斷的信任關係 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:assertAwsResourceProperty` - 確認目錄類型為 AWS Managed Microsoft AD。
- `aws:executeAwsApi` - 取得 的相關資訊 AWS Managed Microsoft AD。
- `aws:branch` - 如果為 `TrustId` 輸入參數提供值，則分支自動化。
- `aws:executeAwsApi` - 取得信任關係的相關資訊。
- `aws:executeAwsApi` - 取得 的條件式轉送器 DNS IP `RemoteDomainName` 地址。
- `aws:executeAwsApi` - 取得已新增至 的 IP 路由相關資訊 AWS Managed Microsoft AD。
- `aws:executeAwsApi` - 取得 AWS Managed Microsoft AD 子網路 CIDRs。
- `aws:executeAwsApi` - 取得與 相關聯之安全群組的相關資訊 AWS Managed Microsoft AD。
- `aws:executeAwsApi` - 取得與 相關聯之網路 ACLs 的相關資訊 AWS Managed Microsoft AD。
- `aws:executeScript` - 確認 `RemoteDomainCidrs` 是有效的值。確認 AWS Managed Microsoft AD 具有 的條件式轉送器，而且 AWS Managed Microsoft AD 如果 `RemoteDomainCidrs` 是非 RFC `RemoteDomainCidrs` 1918 IP 地址，則必要的 IP 路由已新增至 。
- `aws:executeScript` - 評估安全群組規則。
- `aws:executeScript` - 評估網路 ACLs。

輸出

`evalDirectorySecurityGroup.output` - 評估與 相關聯的安全群組規則是否 AWS Managed Microsoft AD 允許建立信任的必要流量。

`evalAclEntries.output` - 評估與 相關聯的網路 ACLs 是否 AWS Managed Microsoft AD 允許建立信任的必要流量。

evaluateRemoteDomainCidr.output – 評估 RemoteDomainCidrs 是否為有效值的結果。確認 AWS Managed Microsoft AD 具有的條件式轉送器，而且 AWS Managed Microsoft AD 如果 RemoteDomainCidrs 是非 RFC RemoteDomainCidrs 1918 IP 地址，則必要的 IP 路由已新增至。

AWS AppSync

AWS Systems Manager 自動化為提供預先定義的 Runbook AWS AppSync。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableAppSyncGraphQLApiLogging](#)

AWS-EnableAppSyncGraphQLApiLogging

Description

AWS-EnableAppSyncGraphQLApiLogging Runbook 會為您指定的 AWS AppSync GraphQL API 啟用欄位層級記錄和請求層級記錄。即使已啟用記錄功能，Runbook 仍會將變更套用至指定的 GraphQL API。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `ApiId`

類型：字串

描述：(必要) 您要為其啟用記錄的 API ID。

- `FieldLogLevel`

類型：字串

有效值：錯誤 | ALL

描述：(必要) 欄位記錄層級。

- `CloudWatchLogsRoleArn`

類型：字串

描述：(必要) AWS AppSync 擔任發佈至 Amazon CloudWatch Logs 之服務角色的 ARN。

- `ExcludeVerboseContent`

類型：布林值

預設：False

描述：(選用) 將設定為 True 以排除標頭、內容和評估的映射範本等資訊，無論記錄層級為何。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws : executeAwsApi - 收集與主要身分驗證類型相關的身分驗證類型和組態資訊。
- aws : branch - 根據身分驗證類型的分支。
- aws : executeAwsApi - 根據 Runbook 輸入參數指定的值更新 AWS AppSync GraphQL API 的記錄組態。

輸出

- EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse : 來自UpdateGraphQLApi呼叫的回應。
- EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse : 來自UpdateGraphQLApi呼叫的回應。
- EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse : 來自UpdateGraphQLApi呼叫的回應。
- EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse : 來自UpdateGraphQLApi呼叫的回應。

Amazon Athena

AWS Systems Manager 自動化為 Amazon Athena 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

AWS-EnableAthenaWorkGroupEncryptionAtRest

Description

AWS-EnableAthenaWorkGroupEncryptionAtRest Runbook 會為您指定的 Amazon Athena 工作群組啟用靜態加密。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- WorkGroup

類型：字串

描述：(必要) 您要為其啟用靜態加密的工作群組。

- EncryptionOption

類型：字串

有效值：SSE_S3 | SSE_KMS | CSE_KMS

描述：(必要) 指定使用的加密選項。您可以選擇使用 Amazon S3 受管金鑰 (SSE_S3) 進行伺服器端加密、使用 AWS KMS 受管金鑰進行伺服器端加密 (SSE_KMS)，或使用 AWS KMS 受管金鑰進行用戶端加密 (CSE_KMS)。

- KmsKeyId

類型：字串

描述：(選用) 如果您使用的是 AWS KMS 加密選項，請指定金鑰 ARN、金鑰 ID 或您要使用的金鑰的金鑰別名。

- EnableMinimumEncryptionConfiguration

類型：布林值

預設：True

描述：（選用）針對寫入 Amazon S3 的查詢和計算結果，強制執行工作群組的最低加密層級。啟用時，工作群組使用者只能在提交查詢時，將加密設定為管理員或更高層級設定的最低層級。此設定不適用於啟用 Spark 的工作群組。

- EnforceWorkGroupConfiguration

類型：布林值

預設：True

描述：（選用）如果設定為 True，工作群組的設定會覆寫用戶端設定。如果設定為 False，則會使用用戶端設定。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:branch - 根據 EncryptionOption 參數中指定的加密選項進行分支。
- aws:executeAwsApi - 此步驟會使用指定的加密設定更新 Athena 工作群組。
- aws:executeAwsApi - 使用指定的加密設定更新 Athena 工作群組。
- aws:assertAwsResourceProperty - 驗證工作群組的加密已啟用。

DynamoDB

AWS Systems Manager 自動化為 Amazon DynamoDB 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

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

AWS-ChangeDDBRWCapacityMode

Description

AWS-ChangeDDBRWCapacityMode Runbook 會將一或多個 Amazon DynamoDB (DynamoDB) 資料表的讀取/寫入容量模式變更為隨需模式或佈建模式。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- CapacityMode

類型：字串

有效值：PROVISIONED | PAY_PER_REQUEST

描述：(必要) 所需的讀取/寫入容量模式。從隨需 (pay-per-request) 切換到佈建容量時，必須設定初始佈建容量值。初始佈建容量值是根據過去 30 分鐘內資料表和全域次要索引的耗用讀取和寫入容量來估計。

- ReadCapacityUnits

類型：整數

預設：0

描述：(選用) 在 DynamoDB 傳回調節例外狀況之前，每秒耗用的強烈一致讀取數量上限。

- TableNames

類型：字串

描述：(必要) DynamoDB 資料表名稱的逗號分隔清單，以變更的讀取/寫入容量模式。

- WriteCapacityUnits

類型：整數

預設：0

描述：(選用) DynamoDB 傳回限流例外狀況之前每秒耗用的寫入數上限。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- dynamodb:DescribeTable
- dynamodb:UpdateTable

文件步驟

- `aws:executeScript` - 變更 `TableNames` 參數中指定之 DynamoDB 資料表的讀取/寫入容量模式。

輸出

`ChangeDDBRWCapacityMode.SuccessesTables` - 已成功變更容量模式的 DynamoDB 資料表名稱清單

`ChangeDDBRWCapacityMode.FailedTables` - DynamoDB 資料表名稱的映射清單，其中變更容量模式失敗，以及失敗的原因。

AWS-CreateDynamoDBBackup

Description

建立 Amazon DynamoDB 資料表的備份。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BackupName

類型：字串

描述：(必要) 要建立的備份之名稱。

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- TableName

類型：字串

描述：(必要) DynamoDB 資料表的名稱。

AWS-DeleteDynamoDbBackup

Description

刪除 Amazon DynamoDB 資料表的備份。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BackupArn

類型：字串

描述：(必要) 要刪除的 DynamoDB 資料表之 ARN。

AWSConfigRemediation-DeleteDynamoDbTable

Description

AWSConfigRemediation-DeleteDynamoDbTable Runbook 會刪除您指定的 Amazon DynamoDB (DynamoDB) 資料表。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- TableName

類型：字串

描述：（必要）您要刪除的 DynamoDB 資料表名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- dynamodb>DeleteTable
- dynamodb:DescribeTable

文件步驟

- aws:executeScript - 刪除 TableName 參數中指定的 DynamoDB 資料表。
- aws:executeScript - 確認已刪除 DynamoDB 資料表。

AWS-DeleteDynamoDbTableBackups

Description

根據保留天數或計數刪除 DynamoDB 資料表備份。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- RetentionCount

類型：字串

預設：10

描述：(選用) 要為資料表保留的備份數量。如果備份的數量超過指定，則會刪除超過指定數量的最舊備份。只能使用 RetentionCount 或 RetentionDays 其中之一，不能同時使用兩者。

- RetentionDays

類型：字串

描述：(選用) 要為資料表保留備份的天數。比指定天數更舊的備份都會刪除。只能使用 RetentionCount 或 RetentionDays 其中之一，不能同時使用兩者。

- TableName

類型：字串

描述：(必要) DynamoDB 資料表的名稱。

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Description

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable Runbook 會使用您為 KMSKeyId 參數指定的 AWS Key Management Service () 客戶受管金鑰來加密 Amazon DynamoDB (DynamoDB AWS KMS) 資料表。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KMSKeyId

類型：字串

描述：（必要）您要用來加密TableName參數中指定之 DynamoDB 資料表的客戶受管金鑰 ARN。

- TableName

類型：字串

描述：（必要）您要加密的 DynamoDB 資料表名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

- dynamodb:UpdateTable

文件步驟

- `aws:executeAwsApi` - 加密您在 `TableName` 參數中指定的 DynamoDB 資料表。
- `aws:waitForAwsResourceProperty` - 驗證 DynamoDB 資料表的 `Enabled` 屬性 `SSESpecification` 設定為 `true`。
- `aws:assertAwsResourceProperty` - 確認 DynamoDB 資料表已使用 `KMSKeyId` 參數中指定的客戶受管金鑰加密。

AWSConfigRemediation-EnablePITRForDynamoDbTable

Description

AWSConfigRemediation-EnablePITRForDynamoDbTable Runbook 會在您指定的 Amazon DynamoDB 資料表上啟用 point-in-time 復原 (PITR)。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- TableName

類型：字串

描述：（必要）啟用point-in-time復原的 DynamoDB 資料表名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- dynamodb:DescribeContinuousBackups
- dynamodb:UpdateContinuousBackups

文件步驟

- aws:executeAwsApi - 在您於 TableName 參數中指定的 DynamoDB 資料表上啟用point-in-time 復原。
- aws:assertAwsResourceProperty - 確認 DynamoDB 資料表上已啟用point-in-time復原。

AWS-EnableDynamoDbAutoscaling

Description

AWS-EnableDynamoDbAutoscaling Runbook 會為您指定的佈建容量 Amazon DynamoDB 資料表啟用 Application Auto Scaling。Application Auto Scaling 可動態調整佈建的輸送量容量，以回應流量模式。如需詳細資訊，請參閱《Amazon [DynamoDB 開發人員指南](#)》中的使用 [DynamoDB 自動擴展自動管理輸送量容量](#)。 DynamoDB

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- TableName

類型：字串

描述：(必要) 您要啟用 Application Auto Scaling 的 DynamoDB 資料表名稱。

- MinReadCapacity

類型：整數

描述：(必要) DynamoDB 資料表的佈建輸送量讀取容量單位數目下限。

- MaxReadCapacity

類型：整數

描述：(必要) DynamoDB 資料表的佈建輸送量讀取容量單位數量上限。

- TargetReadCapacityUtilization

類型：整數

描述：(必要) 所需的目標讀取容量使用率。目標使用率是某個時間點的已耗用佈建輸送量百分比。您可以將自動擴展目標使用率值設定為 20% 到 90%。

- ReadScaleOutCooldown

類型：整數

描述：(必要) 等待先前的讀取容量向外擴展活動生效的秒數。

- ReadScaleInCooldown

類型：整數

描述：(必要) 讀取容量縮減活動完成後，另一個縮減活動開始之前的秒數。

- MinWriteCapacity

類型：整數

描述：(必要) DynamoDB 資料表的佈建輸送量寫入單位數目下限。

- MaxWriteCapacity

類型：整數

描述：(必要) DynamoDB 資料表的佈建輸送量寫入單位數量上限。

- TargetWriteCapacityUtilization

類型：整數

描述：(必要) 所需的目標寫入容量使用率。目標使用率是某個時間點的已耗用佈建輸送量百分比。您可以將自動擴展目標使用率值設定為 20% 到 90%。

- WriteScaleOutCooldown

類型：整數

描述：(必要) 等待先前的寫入容量向外擴展活動生效的秒數。

- WriteScaleInCooldown

類型：整數

描述：(必要) 寫入容量縮減活動完成後，另一個縮減活動開始之前的秒數。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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 資料表上設定 Application Auto Scaling。
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep) - 休眠以避免 API 調節。
- PutScalingPolicyWrite (aws:executeAwsApi) - 設定 DynamoDB 資料表的目標寫入容量使用率。
- PutScalingPolicyWriteDelay (aws:sleep) - 休眠以避免 API 調節。
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi) - 設定 DynamoDB 資料表的最小和最大讀取容量單位。
- RegisterAppAutoscalingTargetReadDelay (aws:sleep) - 休眠以避免 API 調節。
- PutScalingPolicyRead (aws:executeAwsApi) - 設定 DynamoDB 資料表的目標讀取容量使用率。
- VerifyDynamoDbAutoscalingEnabled (aws:executeScript) - 驗證應用程式 Auto Scaling 已根據您指定的值為 DynamoDB 資料表啟用。

輸出

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

AWS-RestoreDynamoDBTable

Description

AWS-RestoreDynamoDBTable Runbook 會還原您使用 point-in-time 復原 (PITR) 指定的 Amazon DynamoDB 資料表。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- EnablePointInTimeRecoverAsNeeded

類型：布林值

預設：true

描述：（選用）判斷自動化是否視需要開啟point-in-time復原以還原資料表。

- GlobalSecondaryIndexOverride

類型：字串

描述：（選用）取代新資料表現有次要索引的新全域次要索引。

- LocalSecondaryIndexOverride

類型：字串

描述：（選用）取代新資料表現有次要索引的新本機次要索引。

- RestoreDateTime

類型：字串

描述：（必要）您想要在過去 35 天內將資料表還原至的point-in-time復原。使用以下格式指定日期和時間：DD/MM/YYYY HH:MM:SS

- SourceTableArn

類型：字串

描述：（必要）您要還原之資料表的 ARN。

- SseSpecificationOverride

類型：字串

描述：（選用）用於新資料表的伺服器端加密設定。

- TargetTableName

類型：字串

描述：（必要）要還原的資料表名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeScript - 使用point-in-time復原還原您在 TargetTableName 參數中指定的 DynamoDB 資料表。

AWS Database Migration Service

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Database Migration Service。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-TroubleshootDMSTableErrors](#)

AWSSupport-TroubleshootDMSTableErrors

Description

自動化 AWS Systems Manager AWSSupport-TroubleshootDMSTableErrors Runbook 可協助您自動化資料庫遷移任務或無伺服器複寫來源Table errors中找到的疑難排解程序 AWS Database Migration Service。當資料庫遷移任務或在 AWS DMS 服務中建立的無伺服器複寫無法從來源端點（來源資料庫）遷移至目標端點（目標資料庫）時，會發生這些錯誤。此 Runbook 會分析 CloudWatch 日誌的簽章錯誤訊息，特別是專注於傳統資料庫遷移任務的任務日誌，以及無伺服器複寫的無伺服器日誌。它也針對 AWS DMS 遷移Table error期間遇到的常見錯誤訊息，提供目標性建議和修復步驟。

如何運作？

Runbook 會執行下列步驟：

- 擷取所提供 AWS DMS ARN 的相關資訊，可以是資料庫遷移任務或無伺服器複寫。
- 透過檢查 DescribeReplicationTasks API（適用於資料庫遷移任務）和 DescribeReplications API（適用於無伺服器複寫）回應中的FreshStartDate值，驗證所提供的 AWS DMS 資源是否已啟動至少一次。如果資源尚未啟動，自動化會引發錯誤。
- 如果資源已啟動，自動化會使用 TableStatistics資訊檢查TableError狀態中的資料表。如果找不到錯誤，自動化會在顯示訊息，確認在指定的資料庫遷移任務或無伺服器複寫中找不到資料表錯誤後結束工作流程。
- 如果找到TableError狀態為的資料表，自動化會檢查指定 AWS DMS 資源是否已啟用 CloudWatch 記錄。如果未啟用記錄，自動化會在顯示表示未啟用記錄的訊息後結束工作流程。

注意：CloudWatch 記錄預期會啟用，因為自動化依賴這些日誌來分析和識別處於 TableError 狀態的資料表問題。

- 如果啟用記錄，自動化會分析 CloudWatch 日誌，並為每個處於 TableError 狀態的資料表產生報告。報告包含常見錯誤訊息的建議，並提供相關的錯誤日誌，以協助識別和解決防止資料表從 AWS DMS 來源端點成功遷移至 AWS DMS 目標端點的問題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DMSArn

類型：字串

描述：（必要）資料庫遷移任務或無伺服器複寫的 ARN

允許模式：`^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

類型：字串

描述：（選用）此參數定義指定資料庫遷移任務或無伺服器複寫的 CloudWatch 日誌分析時間範圍的開始。提供時，只會收集和分析此特定時間之後產生的日誌。請注意，如果 `startDate` 和 之間的時間範圍 `endDate` 太長，工作流程可能會逾時。值應以 ISO 6081 日期時間格式提供。

允許模式：`^$|^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3})Z$`

- EndTimeRange

類型：字串

描述：(選用) 此參數會設定指定資料庫遷移任務或無伺服器複寫之 CloudWatch 日誌分析的時間範圍結束。提供時，只會收集和分析在此特定時間之前產生的日誌。請注意，如果 startDate 和 之間的時間範圍 endDate 太長，工作流程可能會逾時。值應以 ISO 6081 日期時間格式提供。

允許模式：`^\d{4}-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3}Z$`

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

自動化擔任角色的 IAM 政策範例

```
{
  "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": "*"
    }
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-TroubleshootDMSTableErrors](#) 中導覽至 。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN) ，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- DMSArn

資料庫遷移任務的 ARN 或具有資料表錯誤的無伺服器複寫。

- StartTimeRange

(選用) ISO 6081 日期時間格式，定義用於分析指定資料庫遷移任務或無伺服器複寫之 CloudWatch 日誌的時間範圍開始。

- EndTimeRange

(選用) ISO 6081 日期時間格式，定義用於分析指定資料庫遷移任務或無伺服器複寫之 CloudWatch 日誌的時間範圍結束。

4. 從頁面底部選取執行按鈕。

5. 自動化啟動。

6. 文件會執行下列步驟：

- validateDMSInputTypeAndGatherDetails

驗證指定的 AWS DMS ARN 輸入，並收集後續步驟中所需的資料庫遷移任務或無伺服器複寫的基本詳細資訊。

- branchOnTableErrors

根據在上述步驟中找到的資料表錯誤數目，將工作流程分支。如果計數大於 0，則繼續 - `branchOnCWLoggingStatus` 步驟。否則，請繼續 - `outputNoTableErrors` 步驟。

- `outputNoTableErrors`

輸出訊息，指出指定的資料庫遷移任務或無伺服器複寫中找不到資料表錯誤。

- `branchOnCWLoggingStatus`

根據在上述步驟中找到的 CloudWatch 記錄狀態來配置工作流程。如果啟用，則繼續 - `gatherTableDetails` 步驟。否則，請繼續 - `outputNoCWLoggingEnabled` 步驟。

- `outputNoCWLoggingEnabled`

輸出訊息，指出指定的資料庫遷移任務或無伺服器複寫中未啟用 CloudWatch 記錄。

- `gatherTableDetails`

收集失敗資料表的 `FullLoadEndTime` 時間戳記，並計算時間範圍值以分析 CloudWatch 日誌。

- `analyzeCloudWatchLogs`

根據簽章錯誤訊息分析 CloudWatch 日誌群組中找到的日誌，並將報告傳回給使用者。

7. 執行完成後，請檢閱輸出區段以取得執行的詳細結果。

- 找不到資料表錯誤的輸出

如果在提供的資料庫遷移任務或無伺服器複寫中找不到資料表錯誤，自動化會顯示輸出，說明相同內容。

- 未啟用 CloudWatch 登入的輸出

如果在提供的資料庫遷移任務或無伺服器複寫中未啟用 CloudWatch 記錄，自動化會顯示說明相同的輸出，並提供啟用記錄的步驟。

- 記錄分析報告

輸出報告，從提供的資料庫遷移任務或無伺服器複寫中識別 `Table error` 處於狀態的資料表、區分錯誤類型、列出遇到的錯誤訊息，以及為每個已識別的資料表提供目標修復步驟和建議。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)

- [執行自動化](#)
- [設定 自動化](#)
- [支援自動化工作流程登陸頁面](#)

Amazon EBS

AWS Systems Manager 自動化為 Amazon Elastic Block Store 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-AnalyzeEBSResourceUsage](#)
- [AWS-ArchiveEBSSnapshots](#)
- [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

Description

AWSSupport-AnalyzeEBSResourceUsage 自動化 Runbook 用於分析 Amazon Elastic Block Store (Amazon EBS) 上的資源用量。它會分析磁碟區用量，並識別指定 AWS 區域中廢棄的磁碟區、影像和快照。

如何運作？

Runbook 會執行下列四個任務：

1. 驗證 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否存在，或建立新的 Amazon S3 儲存貯體。
2. 收集所有處於可用狀態的 Amazon EBS 磁碟區。
3. 收集已刪除來源磁碟區的所有 Amazon EBS 快照。
4. 收集任何非終止的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體未使用的所有 Amazon Machine Image (AMIs)。

Runbook 會產生 CSV 報告，並將其存放在使用者提供的 Amazon S3 儲存貯體中。提供的儲存貯體應按照結尾所述的 AWS 安全最佳實務進行保護。如果使用者提供的 Amazon S3 儲存貯體不存在於帳戶中，則 Runbook 會建立新的 Amazon S3 儲存貯體，名稱格式為 <User-provided-name>-awssupport-YYYY-MM-DD，使用自訂 AWS Key Management Service (AWS KMS) 金鑰加密，啟用物件版本控制、封鎖公開存取，並要求 請求使用 SSL/TLS。

如果您想要指定自己的 Amazon S3 儲存貯體，請確定已依照下列最佳實務進行設定：

- 封鎖對儲存貯體的公開存取 (IsPublic設定為 False)。
- 開啟 Amazon S3 存取記錄。
- [僅允許對儲存貯體提出 SSL 請求](#)。
- 開啟物件版本控制。
- 使用 AWS Key Management Service (AWS KMS) 金鑰來加密您的儲存貯體。

Important

使用此 Runbook 可能會對您的帳戶產生額外費用，以建立 Amazon S3 儲存貯體和物件。如需可能產生之費用的詳細資訊，請參閱 [Amazon S3 定價](#)。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName

類型：AWS::S3::Bucket::Name

描述：(必要) 您帳戶中要上傳報告的 Amazon S3 儲存貯體。確保儲存貯體政策不會將不必要的讀取/寫入許可授予不需要存取所收集日誌的各方。如果指定的儲存貯體不存在於帳戶中，則自動化會在以名稱格式 啟動自動化的區域中建立新的儲存貯體<User-provided-name>-awssupport-YYYY-MM-DD，並以自訂 AWS KMS 金鑰加密。

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

- CustomerManagedKmsKeyArn

類型：字串

描述：(選用) 自訂 AWS KMS 金鑰 Amazon Resource Name (ARN)，用於加密在帳戶中不存在指定的儲存貯體時將建立的新 Amazon S3 儲存貯體。如果嘗試建立儲存貯體但未指定自訂 AWS KMS 金鑰 ARN，自動化會失敗。

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

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

具有執行此 Runbook 所需的最低 IAM 許可的政策範例：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "Read_Only_Permissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ssm:DescribeAutomationExecutions"
    ]
  }]
}
```

```

    ],
    "Resource": ""
  }, {
    "Sid": "KMS_Generate_Permissions",
    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }, {
    "Sid": "S3_Read_Only_Permissions",
    "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": "S3_Create_Permissions",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutObject",
      "s3:PutBucketLogging",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketTagging",
      "s3:PutBucketVersioning",
      "s3:PutEncryptionConfiguration"
    ],
    "Resource": "*"
  }
]
}

```

指示

請依照下列步驟設定自動化：

1. 導覽至 AWS Systems Manager 主控台中的 [AWSSupport-AnalyzeEBSResourceUsage](#)。

2. 對於輸入參數，輸入以下內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName (必要)：

帳戶中要上傳報告的 Amazon S3 儲存貯體。

- CustomerManagedKmsKeyArn (選用)：

自訂 AWS KMS 金鑰 Amazon Resource Name (ARN)，用於加密如果指定儲存貯體不存在於帳戶中時將建立的新 Amazon S3 儲存貯體。

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

S3 Bucket

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.

arn:aws:iam::[redacted]:role/[redacted]

×

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

3. 選取執行。

4. 自動化啟動。

5. 自動化 Runbook 會執行下列步驟：

- checkConcurrency：

確保區域中只有一個此 Runbook 的啟動。如果 Runbook 找到另一個正在進行的執行，則會傳回錯誤並結束。

- verifyOrCreateS3bucket：

驗證 Amazon S3 儲存貯體是否存在。如果沒有，它會在以名稱格式 啟動自動化的區域中建立新的 Amazon S3 儲存貯體 `<User-provided-name>-awssupport-YYYY-MM-DD`，並使用自訂 AWS KMS 金鑰加密。

- gatherAmiDetails：

搜尋任何 Amazon EC2 執行個體未使用的 AMIs 會產生名稱格式為 `<region>-images.csv`，並將其上傳至 Amazon S3 儲存貯體。

- `gatherVolumeDetails`：

驗證處於可用狀態的 Amazon EBS 磁碟區、使用名稱格式產生報告 `<region>-volume.csv`，並在 Amazon S3 儲存貯體中上傳報告。

- `gatherSnapshotDetails`：

尋找已刪除的 Amazon EBS 磁碟區的 Amazon EBS 快照，以名稱格式產生報告 `<region>-snapshot.csv`，並將其上傳至 Amazon S3 儲存貯體。

6. 完成後，請檢閱輸出區段以取得執行的詳細結果。

▼ Outputs	
<code>gatherVolumeDetails.gatherVolumeDetailsOutput</code> No volume found in available state in region eu-central-1	<code>verifyOrCreateS3bucket.createdNewBucket</code> true
<code>gatherAmiDetails.gatherAmiDetailsOutput</code> 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.	
<code>gatherSnapshotDetails.gatherSnapshotDetailsOutput</code> 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.	

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS-ArchiveEBSSnapshots

Description

AWS-ArchiveEBSSnapshots Runbook 透過指定已套用至快照的標籤，協助您封存 Amazon Elastic Block Store (Amazon EBS) 磁碟區的快照。或者，如果您的快照未加上標籤，您可以提供磁碟區的 ID。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 描述

類型：字串

描述：(選用) Amazon EBS 快照的描述。

- DryRun

類型：字串

有效值：是 | 否

描述：(必要) 檢查您是否具有動作所需的許可，而無需實際提出請求，並提供錯誤回應。

- RetentionCount

類型：字串

描述：(選用) 您要封存的快照數量。如果您指定 的值，請勿指定此參數的值RetentionDays。

- RetentionDays

類型：字串

描述：(選用) 您要封存的快照過去天數。如果您指定 的值，請勿指定此參數的值RetentionCount。

- SnapshotWithTag

類型：字串

有效值：是 | 否

描述：(必要) 指定是否標記您要封存的快照。

- TagKey

類型：字串

描述：(選用) 指派給您要封存之快照的標籤索引鍵。

- TagValue

類型：字串

描述：(選用) 指派給您要封存之快照的標籤值。

- VolumeId

類型：字串

描述：(選用) 您要封存其快照的磁碟區 ID。如果您的快照未加上標籤，請使用此參數。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

文件步驟

aws:executeScript - 使用您使用 TagKey 和 TagValue 參數或 VolumeId 參數指定的標籤封存快照。

AWS-AttachEBSVolume

Description

將 Amazon Elastic Block Store (Amazon EBS) 磁碟區連接至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 裝置

類型：字串

描述：(必要) 裝置名稱 (例如 /dev/sdh 或 xvdh)。

- InstanceId

類型：字串

描述：(必要) 您想要連接磁碟區的執行個體之 ID。

- VolumeId

類型：字串

描述：（必要）Amazon EBS 磁碟區的 ID。磁碟區和執行個體必須位於相同的可用區域內。

AWSSupport-CalculateEBSPerformanceMetrics

Description

AWSSupport-CalculateEBSPerformanceMetrics Runbook 透過計算效能指標並將其發佈至 CloudWatch 儀表板，協助診斷 Amazon EBS 效能問題。儀表板會顯示目標 Amazon EBS 磁碟區或連接至目標 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的所有磁碟區的預估平均 IOPS 和輸送量。對於 Amazon EC2 執行個體，它也會顯示執行個體的平均 IOPS 和輸送量。Runbook 會將連結輸出至新建立的 CloudWatch 儀表板，其中會顯示相關的計算 CloudWatch 指標。CloudWatch 儀表板會在您的帳戶中建立，名稱為：AWSSupport-`<ResourceId>`-EBS-Performance-`<automation:EXECUTION_ID>`。

如何運作？

Runbook 會執行下列步驟：

- 確保指定的時間戳記有效。
- 驗證資源 ID (Amazon EBS 磁碟區或 Amazon EC2 執行個體) 是否有效。
- 當您提供 Amazon EC2 做為 ResourceID 時，它會建立具有該 Amazon EC2 執行個體實際總 IOPS/Throughput 的 CloudWatch 儀表板，以及連接至 Amazon EC2 執行個體之所有 Amazon EBS 磁碟區的預估平均 IOPS/Throughput 圖表。
- 當您提供 Amazon EBS 磁碟區做為 ResourceID 時，它會建立具有該磁碟區的預估平均 IOPS/輸送量圖表的 CloudWatch 儀表板。
- 產生 CloudWatch 儀表板後，如果預估平均 IOPS 或預估平均輸送量分別超過最大 IOPS 或最大輸送量，則連接到 Amazon EC2 執行個體的磁碟區或磁碟區可能會產生微量爆量。

Note

對於爆量磁碟區 (gp2、sc2 和 st1)，應考慮最大 IOPS/輸送量，直到您有爆量平衡為止。完全使用爆量平衡後，即變成零，請考慮基準 IOPS/輸送量指標。

⚠ Important

建立 CloudWatch 儀表板可能會導致您的 帳戶產生額外費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價指南](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

範例政策

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
```

```

        "Resource": "arn:aws:cloudwatch::Account-id:dashboard/*-EBS-
Performance-*"
    },
    {
        "Sid": "VisualEditor1",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeVolumes",
            "ec2:DescribeInstanceTypes"
        ],
        "Resource": "*"
    }
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-CalculateEBSPerformanceMetrics](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ResourceID (必要)：

Amazon EC2 執行個體或 Amazon EBS 磁碟區的 ID。

- 開始時間 (必要)：

在 CloudWatch 中檢視資料的開始時間。時間的格式必須為 yyyy-mm-ddThh:mm:ss，UTC 則為。

- 結束時間 (必要)：

在 CloudWatch 中檢視資料的結束時間。時間的格式必須為 yyyy-mm-ddThh:mm:ss，UTC 則為。

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. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- CheckResourceIdAndTimeStamps：

檢查結束時間是否大於開始時間至少一分鐘，以及所提供的資源是否存在。

- CreateCloudWatchDashboard：

計算 Amazon EBS 效能，並根據您的資源 ID 顯示圖形。如果您為參數資源 ID 提供 Amazon EBS 磁碟區 ID，此 Runbook 會建立 CloudWatch 儀表板，其中包含 Amazon EBS 磁碟區預估的平均 IOPS 和預估的平均輸送量。如果您為參數資源 ID 提供 Amazon EC2 執行個體 ID，此 Runbook 會建立 CloudWatch 儀表板，其中包含 Amazon EC2 執行個體的平均總 IOPS 和平均總輸送量，以及連接至 Amazon EC2 執行個體的所有 Amazon EBS 磁碟區預估平均 IOPS 和預估平均輸送量。

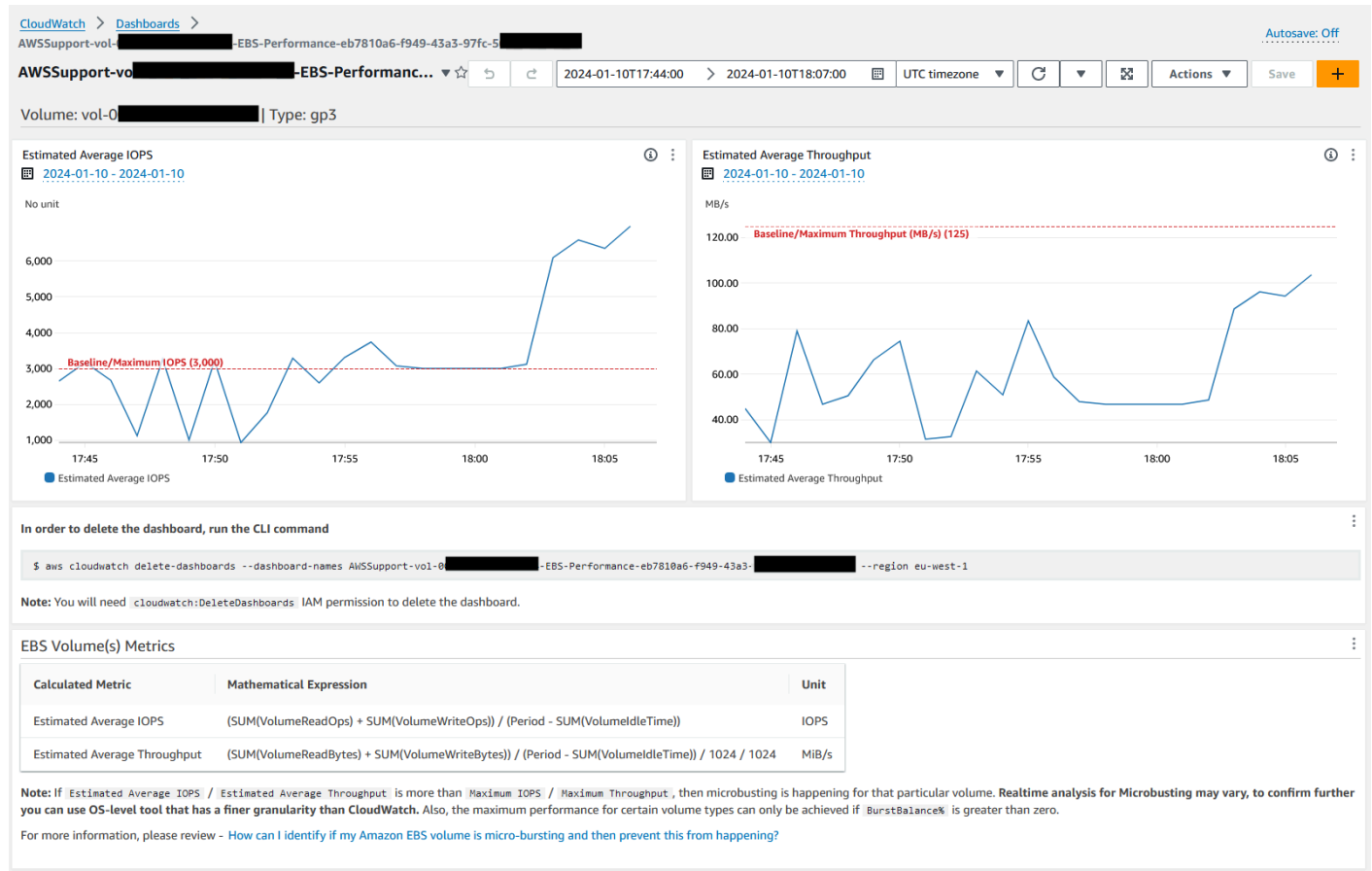
7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

▼ 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.

將資源 ID 作為 Amazon EC2 執行個體的 CloudWatch Dashboard 範例



資源 ID 為 Amazon EBS 磁碟區 ID 的 CloudWatch Dashboard 範例



參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [如何識別我的 Amazon EBS 磁碟區是否具有微爆量，然後防止這種情況發生？](#)
- [如何使用 CloudWatch 檢視 EC2 執行個體的 Amazon EBS 效能彙總指標？](#)

AWS-CopySnapshot

Description

複製 Amazon Elastic Block Store (Amazon EBS) 磁碟區的point-in-time快照。您可以在相同 AWS 區域 或區域中將快照複製到另一個區域。加密的 Amazon EBS 快照副本會保持加密。未加密快照的副本仍保持未加密狀態。若要複製從另一個帳戶共用的加密快照，您必須擁有用於加密快照之 KMS 金鑰的許可。複製另一個快照建立的快照，具有一個不應用於任何用途的任意磁碟區 ID。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 描述

類型：字串

描述：（選用）Amazon EBS 快照的描述。

- SnapshotId

類型：字串

描述：（必要）要複製的 Amazon EBS 快照 ID。

- SourceRegion

類型：字串

描述：(選用) 來源快照目前存在的區域。

文件步驟

copySnapshot - 複製 Amazon EBS 磁碟區的快照。

輸出

copySnapshot.SnapshotId - 新快照的 ID。

AWS-CreateSnapshot

Description

建立 Amazon EBS 磁碟區的快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 描述

類型：字串

描述：(選用) 快照的描述

- Volumeld

類型：字串

描述：(必要) 磁碟區的 ID。

AWS-DeleteSnapshot

Description

刪除 Amazon EBS 磁碟區的快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- SnapshotId

類型：字串

描述：(必要) EBS 快照的 ID。

AWSConfigRemediation-DeleteUnusedEBSVolume

Description

AWSConfigRemediation-DeleteUnusedEBSVolume Runbook 會刪除未使用的 Amazon Elastic Block Store (Amazon EBS) 磁碟區。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- CreateSnapshot

類型：布林值

描述：(選用) 如果設定為 true，自動化會在刪除之前建立 Amazon EBS 磁碟區的快照。

- Volumeld

類型：字串

描述：(必要) 您要刪除的 Amazon EBS 磁碟區的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeScript` - 驗證您在 `VolumeId` 參數中指定的 Amazon EBS 磁碟區不在使用中，並根據您為 `CreateSnapshot` 參數選擇的值建立快照。
- `aws:branch` - 根據您為 `CreateSnapshot` 參數選擇的值進行分支。
- `aws:waitForAwsResourceProperty` - 等待快照完成。
- `aws:executeAwsApi` - 如果快照建立失敗，刪除快照。
- `aws:executeAwsApi` - 刪除您在 `VolumeId` 參數中指定的 Amazon EBS 磁碟區。
- `aws:executeScript` - 驗證已刪除 Amazon EBS 磁碟區。

AWS-DeregisterAMIs

Description

AWS-DeregisterAMIs Runbook 透過指定已套用至 的標籤，協助您取消註冊 Amazon Machine Images(AMIs)AMIs。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- DryRun

類型：字串

有效值：是 | 否

描述：（必要）檢查您是否擁有動作所需的許可，而無需實際提出請求，並提供錯誤回應。

- RetainNumber

類型：字串

描述：（選用）您要保留AMIs的數量。如果您指定的值，請勿為此參數指定值Age。

- 年齡

類型：字串

描述：（選用）您要保留AMIs的過去天數。如果您指定的值，請勿為此參數指定值RetainNumber。

- TagKey

類型：字串

描述：（必要）指派給您要取消註冊AMIs之標籤的索引鍵。

- TagValue

類型：字串

描述：（必要）指派給AMIs您要取消註冊之標籤值。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DeregisterImage
- ec2:DescribeImages

文件步驟

- aws:executeAwsApi - 驗證您為 Runbook 輸入參數指定的值。
- aws:executeAwsApi - AMIs 使用您使用 TagKey 和 TagValue 參數指定的標籤取消註冊。

AWS-DetachEBSVolume

Description

從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體分離 Amazon EBS 磁碟區。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- LambdaAssumeRole

類型：字串

描述：(選用) Lambda 所擔任角色的 ARN

- Volumeld

類型：字串

描述：(必要) EBS 磁碟區的 ID。磁碟區和執行個體必須位於相同的可用區域內

AWSConfigRemediation-EnableEbsEncryptionByDefault

Description

AWSConfigRemediation-EnableEbsEncryptionByDefault Runbook 會在您執行自動化 AWS 區域的 AWS 帳戶和中的所有新 Amazon Elastic Block Store (Amazon EBS) 磁碟區上啟用加密。執行自動化之前建立的磁碟區不會加密。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeAwsApi - 啟用目前帳戶和區域中的預設 Amazon EBS 加密設定。
- aws:assertAwsResourceProperty - 驗證是否已啟用預設 Amazon EBS 加密設定。

AWS-ExtendEbsVolume

Description

AWS-ExtendEbsVolume Runbook 會增加 Amazon EBS 磁碟區的大小，並擴展檔案系統。此自動化支援 xfs 和 ext4 檔案系統。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- DriveLetter

類型：字串

描述：(選用) 您要延伸其檔案系統的磁碟機字母。Windows 執行個體需要此參數。

- InstanceId

類型：字串

描述：(選用) 您要延伸之 Amazon EBS 磁碟區的 Amazon EC2 執行個體 ID。

- KeepSnapshot

類型：布林值

預設：true

描述：(選用) 決定是否在增加 Amazon EBS 磁碟區大小之前，先建立快照。

- MountPoint

類型：字串

描述：(選用) 您要擴充其檔案系統之磁碟機的掛載點。Linux 執行個體需要此參數。

- SizeGib

類型：字串

描述：(必要) 您要修改 Amazon EBS 磁碟區的大小，以 GiB 為單位。

- VolumeId

類型：字串

描述：(必要) 您要擴展的 EBS 磁碟區的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeScript` - 將磁碟區的大小增加到您在 `VolumeId` 參數中指定的值，並擴展檔案系統。

AWSsupport-ModifyEBSSnapshotPermission

Description

AWSsupport-ModifyEBSSnapshotPermission Runbook 可協助您修改多個 Amazon Elastic Block Store (Amazon EBS) 快照的許可。使用此 Runbook，您可以建立快照 `Public` 或 `Private` 並與其他 共用 AWS 帳戶。使用此 Runbook 無法與其他帳戶共用使用預設 KMS 金鑰加密的快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- AccountIds

類型：StringList

預設：none

描述：（選用）您要與其共用快照的帳戶 IDs。如果您No輸入 參數的值，則需要此Private參數。

- AccountPermissionOperation

類型：字串

有效值：新增 | 移除

預設：none

描述：（選用）要執行的操作類型。

- 私有

類型：字串

有效值：是 | 否

描述：（必要）如果您想要與特定帳戶共用快照，請輸入 No 作為值。

- SnapshotIds

類型：StringList

描述：（必要）您要修改其許可的 Amazon EBS 快照 IDs。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `ec2:DescribeSnapshots`
- `ec2:ModifySnapshotAttribute`

文件步驟

1. `aws:executeScript` - 驗證 `SnapshotIds` 參數中提供的快照 IDs。驗證 IDs 之後，指令碼會檢查加密快照，並在找到任何快照時輸出清單。
2. `aws:branch` - 根據您為 `Private` 參數輸入的值來配置自動化。
3. `aws:executeScript` - 修改指定快照的許可，以與指定的帳戶共用快照。
4. `aws:executeScript` - 修改快照的許可，將快照從 `變更為 Public Private`。

輸出

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Result`

`MakePrivate.Result`

`MakePrivate.Commands`

AWSConfigRemediation-ModifyEBSVolumeType

Description

AWSConfigRemediation-ModifyEBSVolumeType Runbook 會修改 Amazon Elastic Block Store (Amazon EBS) 磁碟區的磁碟區類型。修改磁碟區類型後，磁碟區會進入 `optimizing` 狀態。如需監控磁碟區修改進度的資訊，請參閱《Amazon EC2 使用者指南》中的[監控磁碟區修改進度](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- EbsVolumeId

類型：字串

描述：(必要) 您要修改的 Amazon EBS 磁碟區的 ID。

- EbsVolumeType

類型：字串

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

描述：您要變更 Amazon EBS 磁碟區的磁碟區類型。如需有關 Amazon EBS 磁碟區類型的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的 [Amazon EBS 磁碟區類型](#)。Amazon EC2

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:waitForAwsResourceProperty - 驗證磁碟區的狀態為 available 或 in-use。
- aws:executeAwsApi - 修改您在 EbsVolumeId 參數中指定的 Amazon EBS 磁碟區。
- aws:waitForAwsResourceProperty - 確認磁碟區的類型已變更為您在 EbsVolumeType 參數中指定的值。

Amazon EC2

AWS Systems Manager 自動化為 Amazon Elastic Compute Cloud 提供預先定義的 Runbook。Amazon Elastic Block Store 的 Runbook 位於 Runbook 參考的 [Amazon EBS](#) 區段。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [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-ConfigureSTIG](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSSupport-ActivateWindowsWithAmazonLicense](#)
- [AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2](#)

- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSSupport-CheckXenToNitroMigrationRequirements](#)
- [AWSSupport-ConfigureEC2Metadata](#)
- [AWSSupport-ContainEC2Instance](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)
- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

AWS-ASGEnterStandby

Description

變更 Auto Scaling 群組中 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的待命狀態。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：（必要）您要在 Auto Scaling 群組中變更待命狀態的 Amazon EC2 執行個體 ID。

- LambdaRoleArn

類型：字串

描述：（選用）角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

AWS-ASGExitStandby

Description

變更 Auto Scaling 群組中 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的待命狀態。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：（必要）您要變更 Auto Scaling 群組中待命狀態的 EC2 執行個體 ID。

- LambdaRoleArn

類型：字串

描述：（選用）角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

AWS-CreateImage

Description

從 Amazon Elastic Compute Cloud Amazon Machine Image(Amazon EC2AMI) 執行個體建立新的 ()。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) EC2 執行個體的 ID。

- NoReboot

類型：布林值

描述：(選用) 在建立映像之前不要重新開機執行個體。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateImage",
    "ec2:DescribeImages"
  ],
  "Resource": [
    "*"
  ]
}
```

AWS-DeleteImage

Description

刪除 Amazon Machine Image(AMI) 和所有相關聯的快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ImageId

類型：字串

描述：(必要) AMI 的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

AWS-PatchAsgInstance

Description

在 Auto Scaling 群組中修補 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 要修補的執行個體之 ID。請勿指定設定為在維護時段執行的執行個體 ID。

- LambdaRoleArn

類型：字串

描述：(選用) 角色的 ARN，允許自動化建立的 Lambda 代表您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- WaitForInstance

類型：字串

預設：PT2M

描述：(選用) 自動化應休眠的持續時間，以允許執行個體恢復服務。

- WaitForReboot

類型：字串

預設：PT5M

描述：(選用) 自動化應休眠的持續時間，以允許修補的執行個體重新啟動。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

Description

使 EC2 執行個體符合適用的修補程式基準。在失敗時復原根磁碟區。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 套用修補程式基準的 EC2 InstanceId。

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- ReportS3Bucket

類型：字串

描述：（選用）程序期間產生的合規報告的 Amazon S3 儲存貯體目的地。

文件步驟

步驟號碼	步驟名稱	自動化動作
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand
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	deleteCloudFormationTemplate	aws:deleteStack

輸出

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

AWS-QuarantineEC2Instance

Description

使用 AWS-QuarantineEC2Instance Runbook，您可以將安全群組指派給不允許任何傳入或傳出流量的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

Important

執行此 Runbook 之前，應仔細檢閱 RDP 設定的變更。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 管理 RDP 設定的受管執行個體之 ID。

- IsolationSecurityGroup

類型：字串

描述：(必要) 您要指派給執行個體的安全群組名稱，以防止傳入或傳出流量。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- aws:executeAwsApi - 收集執行個體的詳細資訊。
- aws:executeScript - 驗證執行個體不是 Auto Scaling 群組的一部分。
- aws:executeAwsApi - 建立連接到執行個體之根磁碟區的快照。
- aws:waitForAwsResourceProperty - 等待快照狀態為 completed。
- aws:executeAwsApi - 將 IsolationSecurityGroup 參數中指定的安全群組指派給您的執行個體。

輸出

GetEC2InstanceResources.RevokedSecurityGroupsIds

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Description

變更 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的執行個體類型。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InstanceId

類型：字串

描述：(必要) 執行個體的 ID。

- InstanceType

類型：字串

描述：(必要) 執行個體類型。

AWS-RestartEC2Instance

Description

重新啟動一或多個 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceIds

類型：StringList

描述：（必要）要重新啟動的 Amazon EC2 執行個體 IDs。

AWS-SetupJupyter

Description

AWS-SetupJupyter Runbook 可協助您在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上設定 Jupyter Notebook。您可以指定現有的執行個體，或提供自動化的 Amazon Machine

Image(AMI) ID 來啟動和設定新的執行個體。開始之前，您必須在參數存放區中建立SecureString參數，以用作 Jupyter Notebook 的密碼。參數存放區是 中的工具 AWS Systems Manager。如需有關建立參數的資訊，請參閱AWS Systems Manager 《使用者指南》中的[建立參數](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- Amild

類型：字串

描述：（選用）AMI您要用來啟動新執行個體和設定 Jupyter Notebook 的 ID。

- InstanceId

類型：字串

描述：（必要）您要設定 Jupyter Notebook 的執行個體 ID。

- InstanceType

類型：字串

預設：t3.medium

描述：（選用）如果您要啟動新的執行個體來設定 Jupyter Notebook，請指定要使用的執行個體類型。

- JupyterPasswordSSMKey

類型：字串

描述：（必要）您要用作 Jupyter Notebook 密碼的參數存放區中的SecureString參數名稱。

- KeyPairName

類型：字串

描述：（選用）您要與新啟動的執行個體建立關聯的金鑰對。

- RemoteAccessCidr

類型：字串

預設：0.0.0.0/0

描述：（選用）您要允許 SSH 流量的 CIDR 範圍。

- RoleName

類型：字串

預設：SSMManagedInstanceProfileRole

描述：（選用）新啟動執行個體的執行個體設定檔名稱。

- StackName

類型：字串

預設：CreateManagedInstanceStack{{automation:EXECUTION_ID}}

描述：（選用）您希望自動化使用的 AWS CloudFormation 堆疊名稱。

- SubnetId

類型：字串

預設：Default

描述：（選用）您要啟動要使用的新執行個體的子網路。

- VpcId

類型：字串

預設：Default

描述：（選用）您想要在其中啟動新執行個體的虛擬私有雲端 (VPC) ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:executeScript` - 使用您為 Runbook 輸入參數指定的值，在您指定的執行個體或新啟動的執行個體上設定 Jupyter Notebook。

AWS-StartEC2Instance

Description

啟動一或多個 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `InstanceId`

類型：StringList

描述：(必要) 要啟動的 EC2 執行個體。

AWS-StopEC2Instance

Description

停止一或多個 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceIds

類型：StringList

描述：(必要) 要停止的 EC2 執行個體。

AWS-TerminateEC2Instance

Description

終止一或多個 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：StringList

描述：(必要) 要終止的一個或多個 EC2 執行個體之 ID。

AWS-UpdateLinuxAmi

Description

使用 Linux 發行套件和 Amazon 軟體更新 Amazon Machine Image(AMI)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ExcludePackages

類型：字串

預設：none

描述：(選用) 在各種條件下，要保留不更新的套件之名稱。根據預設 ("none")，無排除套件。

- IamInstanceProfileName

類型：字串

預設：ManagedInstanceProfile

描述：(必要) 可讓 Systems Manager 管理執行個體的執行個體描述檔。

- IncludePackages

類型：字串

預設：all

描述：(選用) 僅更新這些具名的套件。根據預設 ("all")，會套用所有可用的更新。

- InstanceType

類型：字串

預設：t2.micro

描述：(選用) 做為工作空間主機啟動的執行個體類型。執行個體類型因區域而異。

- MetadataOptions

類型：StringMap

預設：{"HttpEndpoint" : "enabled" , "HttpTokens" : "optional"}

描述：(選用) 執行個體的中繼資料選項。如需詳細資訊，請參閱 [InstanceMetadataOptionsRequest](#)。

- PostUpdateScript

類型：字串

預設：none

描述：(選用) 套用套件更新後要執行的指令碼之 URL。預設 ("none") 為不執行指令碼。

- PreUpdateScript

類型：字串

預設：none

描述：(選用) 套用更新前要執行的指令碼之 URL。預設 ("none") 為不執行指令碼。

- SecurityGroupIds

類型：字串

描述：(必要) 您希望套用至 的安全群組 IDs 的逗號分隔清單AMI。

- SourceAmild

類型：字串

描述：(必要) 來源 Amazon Machine Image ID。

- SubnetId

類型：字串

描述：(選用) 您要啟動執行個體的子網路 ID。如果您已刪除預設 VPC，則需要此參數。

- TargetAmiName

類型：字串

預設：UpdateLinuxAmi_from_{{SourceAmiId}}_on_{{global:DATE_TIME}}

描述：(選用) 要建立的新 AMI 之名稱。預設為系統產生的字串，包括來源 AMI ID，以及建立時間和日期。

AWS-UpdateWindowsAmi

Description

更新 Microsoft Windows Amazon Machine Image(AMI)。根據預設，此 Runbook 會安裝所有 Windows 更新、Amazon 軟體和 Amazon 驅動程式。接著會執行 Sysprep 以建立新的 AMI。支援 Windows Server 2008 R2 或更新版本。

Important

如果您的執行個體 AWS Systems Manager 使用 VPC 端點連線至 [Amazon S3](#)，除非在 us-east-1 區域中使用，否則此 Runbook 將會失敗。執行個體必須啟用 TLS 1.2，才能使用此 Runbook。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 類別

類型：字串

描述：(選用) 指定一個或多個更新類別。您可以使用逗號分隔值篩選類別。選項：Application, Connectors, CriticalUpdates, DefinitionUpdates, DeveloperKits, Drivers, FeaturePacks, 有效格式包括單一項目，例如：CriticalUpdates。或者您可以指定逗號分隔清單：CriticalUpdates,SecurityUpdates。備註：逗號旁不得有任何空格。

- ExcludeKbs

類型：字串

描述：(選用) 指定一個或多個要排除的 Microsoft 知識庫 (KB) 文章 ID。您可以使用逗號分隔值排除多個 ID。有效格式：KB9876543 或 9876543。

- IamInstanceProfileName

類型：字串

預設：ManagedInstanceProfile

描述：(必要) 可讓 Systems Manager 管理執行個體的角色名稱。

- IncludeKbs

類型：字串

描述：(選用) 指定一個或多個要包含的 Microsoft 知識庫 (KB) 文章 ID。您可以使用逗號分隔值安裝多個 ID。有效格式：KB9876543 或 9876543。

- InstanceType

類型：字串

預設：t2.medium

描述：(選用) 做為工作空間主機啟動的執行個體類型。執行個體類型因區域而異。預設為 t2.medium。

- MetadataOptions

類型：StringMap

預設：{"HttpEndpoint" : "enabled" , "HttpTokens" : "optional"}

描述：(選用) 執行個體的中繼資料選項。如需詳細資訊，請參閱 [InstanceMetadataOptionsRequest](#)。

- PostUpdateScript

類型：字串

描述：(選用) 做為字串提供的指令碼。它會在安裝 OS 更新後執行。

- PreUpdateScript

類型：字串

描述：(選用) 做為字串提供的指令碼。它會在安裝 OS 更新前執行。

- PublishedDateAfter

類型：字串

描述：(選用) 指定更新應在其後發佈的日期。例如，假設指定 01/01/2017，則 Windows Update 搜尋會傳回在 01/01/2017 當天或之後發佈的任何更新。

- PublishedDateBefore

類型：字串

描述：(選用) 指定更新應在其之前發佈的日期。例如，假設指定 01/01/2017，則 Windows Update 搜尋會傳回在 01/01/2017 當天或之前發佈的任何更新。

- PublishedDaysOld

類型：字串

描述：(選用) 指定更新從發佈日期起的天數。例如，假設指定 10，則 Windows Update 搜尋會傳回在發佈前 10 天或更多天之前的任何更新。

- SecurityGroupIds

類型：字串

描述：(必要) 您希望套用至的安全群組 IDs 的逗號分隔清單AMI。

- SeverityLevels

類型：字串

描述：(選用) 指定一個或多個與更新關聯的 MSRC 嚴重性等級。您可以使用逗號分隔值篩選嚴重性等級。根據預設，會選取所有安全層級的修補程式。如果提供值，則更新清單會以這些值篩選。選項：Critical，Important，Low，Moderate 或 Unspecified。有效格式包括單一項目，例如：Critical。或者，您可以指定逗號分隔清單：Critical，Important，Low。

- SourceAmild

類型：字串

描述：(必要) 來源 AMI ID。

- SubnetId

類型：字串

描述：(選用) 您要啟動執行個體的子網路 ID。如果您已刪除預設 VPC，則需要此參數。

- TargetAmiName

類型：字串

預設：UpdateWindowsAmi_from_{{SourceAmild}}_on_{{global:DATE_TIME}}

描述：(選用) 要建立的新 AMI 之名稱。預設為系統產生的字串，包括來源 AMI ID，以及建立時間和日期。

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Description

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck Runbook 會為您指定的 Amazon EC2 Auto Scaling (Auto Scaling) 群組啟用運作狀態檢查。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- AutoScalingGroupARN

類型：字串

描述：(必要) 您要啟用運作狀態檢查之自動擴展群組的 Amazon Resource Name (ARN)。

- HealthCheckGracePeriod

類型：整數

預設：300

描述：(選用) Auto Scaling 在檢查已開始服務的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的運作狀態之前等待的時間，以秒為單位。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeScript` - 針對您在 `AutoScalingGroupARN` 參數中指定的 Auto Scaling 群組啟用運作狀態檢查。

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Description

AWSConfigRemediation-EnforceEC2InstanceIMDSv2 Runbook 需要您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，才能使用執行個體中繼資料服務第 2 版 (IMDSv2)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `InstanceId`

類型：字串

描述：（必要）您想要使用 IMDSv2 的 Amazon EC2 執行個體 ID。IMDSv2

- `AutomationAssumeRole`

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `HttpPutResponseHopLimit`

類型：整數

描述：(選用) 從 IMDS 服務返回請求者的 Hop 回應限制。EC2 執行個體託管容器設定為 EC2 或更高。設為 0 不變更 (預設)。

允許模式：`^([1-5]?\d|6[0-4])$`

預設：0

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

- `aws:executeScript` - 在您 `required` 於 `InstanceId` 參數中指定的 Amazon EC2 執行個體上將 `HttpTokens` 選項設定為。
- `aws:assertAwsResourceProperty` - 驗證 Amazon EC2 執行個體上需要 IMDSv2。Amazon EC2

AWSEC2-CloneInstanceAndUpgradeSQLServer

Description

AMI 從 Windows Server 執行 SQL Server 2008 或更新版本的 EC2 執行個體建立，然後將 AMI 升級到較新版本的 SQL Server。僅支援英文版本的 SQL Server。

支援下列升級路徑：

- SQL Server 2008 升級至 SQL Server 2017、2016 或 2014
- SQL Server 2008 R2 升級至 SQL Server 2017、2016 或 2014
- SQL Server 2012 升級至 SQL Server 2019、2017、2016、2014
- SQL Server 2014 升級至 SQL Server 2019、2017 或 2016

- SQL Server 2016 升級至 SQL Server 2019 或 2017

如果您使用的是舊版 Windows Server 與 SQL Server 2019 不相容，則自動化文件必須將您的 Windows Server 版本升級至 2016。

升級為多步驟程序，可能需要 2 小時才能完成。自動化會從執行個體建立 AMI，然後從指定 AMI 中的新 啟動暫時執行個體SubnetID。與原始執行個體相關聯的安全群組會套用至暫時執行個體。然後，自動化會在臨時執行個體TargetSQLVersion上執行 就地升級。升級之後，自動化AMI會從暫時執行個體建立新的，然後終止暫時執行個體。

您可以在 VPC AMI中啟動新的 來測試應用程式功能。結束測試後，在執行另一次升級前，請先安排應用程式停機時間，再完全切換至已升級的執行個體。

Note

如果您想要修改從新 啟動之 EC2 AMI 執行個體的電腦名稱，請參閱[重新命名託管 SQL Server 獨立執行個體的電腦](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

先決條件

- TLS 1.2 版。
- 僅支援英文版本的 SQL Server。
- EC2 執行個體必須使用 Windows Server 2008 R2 (或更新版本) 和 SQL Server 2008 (或更新版本) 的 Windows Server 版本。

- 確認 SSM Agent 安裝於您的執行個體上。如需詳細資訊，請參閱[在 Windows Server 的 EC2 執行個體上安裝和設定 SSM Agent](#)。
- 將執行個體設定為使用 AWS Identity and Access Management (IAM) 執行個體設定檔角色。如需詳細資訊，請參閱[建立 Systems Manager 的 IAM 執行個體設定檔](#)。
- 驗證執行個體在執行個體開機磁碟中有 20 GB 的可用磁碟空間。
- 針對使用自有授權 (BYOL) 的 SQL Server 版本執行個體，適用下列額外的事前準備：
 - 提供包含目標 SQL Server 安裝媒體的 EBS 快照 ID。若要執行此作業：
 1. 確認 EC2 執行個體執行的是 Windows Server 2008 R2 或更新版本。
 2. 在執行個體執行的相同可用區域中建立 6 GB 的 EBS 磁碟區。將磁碟區連結到執行個體。例如，將其掛載為 D 磁碟機。
 3. 在 ISO 按一下滑鼠右鍵，並將其掛載至執行個體，例如做為 E 磁碟機。
 4. 從磁碟機 E:\ 將 ISO 的內容複製到磁碟機 D:\
 5. 建立步驟 2 中所建立 6 GB 磁碟區的 EBS 快照。

限制

- 升級僅能在使用 Windows 身分驗證的 SQL Server 上執行。
- 確認執行個體上沒有待定的安全性修補程式更新。開啟 Control Panel (控制面板)，接著選擇 Check for updates (檢查更新)。
- 不支援在 HA 和鏡像模式中的 SQL Server 部署。

參數

- `IamInstanceProfile`

類型：字串

描述：(必要) IAM 執行個體描述檔。

- `InstanceId`

類型：字串

描述：(必要) 執行 Windows Server 2008 R2 (或更新版本) 或 SQL Server 2008 (或更新版本) 的執行個體。

- `KeepPreUpgradeImageBackup`

類型：字串

描述：(選用) 如果設定為 `true`，自動化不會刪除升級前從執行個體建立的 AMI。如果設定為 `true`，則必須刪除 AMI。AMI 預設為刪除。

- SubnetId

類型：字串

描述：(必要) 為升級程序提供子網路。確認子網路具有對 AWS 服務、Amazon S3 和 Microsoft 的傳出連線 (以下載修補程式)。

- SQLServerSnapshotId

類型：字串

描述：(條件式) 目標 SQL Server 安裝媒體的快照 ID。此參數對使用 BYOL SQL Server 版本的執行個體是必要項目。此參數對於 SQL Server 授權包含的執行個體 (使用 AWS 提供的 Amazon Machine Image for Windows Server 搭配 Microsoft SQL Server 啟動的執行個體) 而言是選用的。

- RebootInstanceBeforeTakingImage

類型：字串

描述：(選用) 如果設定為 `true`，自動化會在建立預先升級 AMI 之前重新啟動執行個體。根據預設，自動化不會在升級前重新啟動。

- TargetSQLVersion

類型：字串

描述：(選用) 選取目標 SQL Server 版本。

可能的目標：

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014

預設目標：SQL Server 2016

輸出

AMIId：從升級至較新版本的 SQL Server 執行個體建立的 AMI ID。

AWSEC2-CloneInstanceAndUpgradeWindows

Description

從 Windows Server 2008 R2、2012 R2、2016 或 2019 執行個體建立 Amazon Machine Image(AMI)，然後將 升級AMI到 Windows Server 2016、2019 或 2022。支援的升級路徑如下。

- Windows Server 2008 R2 至 Windows Server 2016。
- Windows Server 2012 R2 到 Windows Server 2016。
- Windows Server 2012 R2 到 Windows Server 2019。
- Windows Server 2012 R2 至 Windows Server 2022。
- Windows Server 2016 至 Windows Server 2019。
- Windows Server 2016 年至 Windows Server 2022 年。
- Windows Server 2019 年至 Windows Server 2022 年。

升級操作為多步驟程序，可能需要 2 小時才能完成。我們建議在至少配備 2 個 vCPU 或 4GB RAM 的執行個體上執行作業系統升級。自動化會從執行個體建立 AMI，然後從SubnetId您指定的 中新建立的 AMI 啟動暫時執行個體。與原始執行個體相關聯的安全群組會套用至暫時執行個體。然後，自動化會在臨時執行個體TargetWindowsVersion上執行 就地升級。若要將 Windows Server 2008 R2 執行個體升級至 Windows Server 2016、2019 或 2022，就地升級會執行兩次，因為不支援直接將 Windows Server 2008 R2 升級到 Windows Server 2016、2019 或 2022。自動化也會更新或安裝 AWS 臨時執行個體所需的驅動程式。升級之後，自動化會從暫時執行個體建立新的 AMI，然後終止暫時執行個體。

您可以從 Amazon Virtual Private Cloud (Amazon VPC) 中升級的 AMI 啟動測試執行個體，以測試應用程式功能。結束測試後，在執行另一次升級前，請先安排應用程式停機時間，再完全切換至已升級的 AMI。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows Server 2008 R2、2012 R2、2016 或 2019 Standard 和 Datacenter 版本

先決條件

- TLS 1.2 版。
- 確認 SSM Agent 安裝於您的執行個體上。如需詳細資訊，請參閱[在 Windows Server 的 EC2 執行個體上安裝和設定 SSM Agent](#)。
- Windows PowerShell 3.0 或更新版本必須安裝在您的執行個體上。
- 對於加入 Microsoft Active Directory 網域的執行個體，建議您指定沒有連線到您的網域控制站的 SubnetId，以協助避免主機名稱衝突。
- 執行個體子網路必須具有網際網路的傳出連線，這可讓您存取 AWS 服務 Amazon S3，以及從 Microsoft 下載修補程式的存取權。如果子網路是公有子網路且執行個體具有公有 IP 地址，或子網路是私有子網路且具有將網際網路流量傳送至公有 NAT 裝置的路由，則符合此需求。
- 此自動化僅適用於 Windows Server 2008 R2、2012 R2、2016 和 2019 執行個體。
- 使用為 Systems Manager 提供必要許可的 AWS Identity and Access Management (IAM) 執行個體設定檔來設定 Windows Server 執行個體。如需詳細資訊，請參閱[建立 Systems Manager 的 IAM 執行個體設定檔](#)。
- 確認執行個體在開機磁碟中有 20 GB 的可用磁碟空間。
- 如果執行個體未使用 AWS 提供的 Windows 授權，請指定包含 2012 R2 安裝媒體的 Amazon EBS Windows Server 快照 ID。若要執行此作業：
 - 驗證 EC2 執行個體正在執行 Windows Server 2012 或更新版本。
 - 在執行個體執行的相同可用區域中建立 6 GB 的 EBS 磁碟區。將磁碟區連結到執行個體。例如，將其掛載為 D 磁碟機。
 - 在 ISO 按一下滑鼠右鍵，並將其掛載至執行個體，例如做為 E 磁碟機。
 - 從磁碟機 E:\ 將 ISO 的內容複製到磁碟機 D:\
 - 從上述步驟 2 建立的 6 GB 磁碟區建立 EBS 快照。

限制

此自動化不支援升級 Windows 網域控制站、叢集或 Windows 桌面作業系統。此自動化也不支援安裝了下列角色的 Windows Server EC2 執行個體。

- 遠端桌面工作階段主機 (RDSH)
- 遠端桌面連線代理人 (RDCB)
- 遠端桌面虛擬化主機 (RDVH)
- 遠端桌面 Web 存取 (RDWA)

參數

- AlternativeKeyPairName

類型：字串

描述：(選用) 升級程序期間要使用的替代金鑰對名稱。這在指派給原始執行個體的金鑰對無法使用的情況下非常有用。如果原始執行個體未指派金鑰對，您必須為此參數指定值。

- BYOLWindowsMediaSnapshotId

類型：字串

描述：(選用) 要複製的 Amazon EBS 快照 ID，其中包含 Windows Server 2012R2 安裝媒體。只有在您升級 BYOL 執行個體時需要。

- IamInstanceProfile

類型：字串

描述：(必要) 可讓 Systems Manager 管理執行個體的 IAM 執行個體設定檔名稱。

- InstanceId

類型：字串

描述：(必要) Windows Server 執行 2008 R2、2012 R2、2016 或 2019 的 EC2 執行個體。

- KeepPreUpgradeImageBackUp

類型：字串

描述：(選用) 如果設定 True，自動化不會刪除升級前從 EC2 執行個體建立的 AMI。如果設為 True，則您必須刪除 AMI。AMI 預設為刪除。

- SubnetId

類型：字串

描述：(必要) 這是升級程序的子網路，也是來源 EC2 執行個體所在的子網路。確認子網路具有對 AWS 服務、Amazon S3 和 Microsoft 的傳出連線 (以下載修補程式)。

- TargetWindowsVersion

類型：字串

描述：(必要) 選取目標 Windows 版本。

預設：2022

- RebootInstanceBeforeTakingImage

類型：字串

描述：(選用) 如果設為 True，則自動化在建立預先升級的 AMI 之前會重新開機執行個體。根據預設，自動化在升級之前不會重新開機。

AWSEC2-ConfigureSTIG

安全技術實作指南 (STIGs) 是 Defense Information Systems Agency (DISA) 為保護資訊系統和軟體而建立的組態強化標準。若要讓您的系統符合 STIG 標準，您必須安裝、設定和測試各種安全設定。

Amazon EC2 提供 Systems Manager 命令文件 AWSEC2-ConfigureSTIG，可用來將 STIG 設定套用至執行個體。本文件可協助您快速建置符合 STIG 標準的映像。STIG Systems Manager 文件會掃描組態錯誤並執行修復指令碼。它還會在 Windows AMIs 上安裝來自國防部 (DoD) 的 InstallRoot，以安裝和更新 DoD 憑證，並移除不必要的憑證以維持 STIG 合規。使用 STIG Systems Manager 文件無需額外費用。

Note

AWSEC2-ConfigureSTIG 是命令文件。若要在 AWS Systems Manager 主控台 AWSEC2-ConfigureSTIG 中搜尋，請選取類別 命令文件。

此頁面列出 Amazon EC2 支援 STIGs 強化元件套用至 EC2 執行個體的所有 STIG。

您可以選擇要套用的 STIG 合規類別。

合規層級

- 高 (類別 I)

最嚴重的風險 包含任何可能導致機密性、可用性或完整性遺失的漏洞。

- 中 (類別 II)

包括可能導致失去機密性、可用性或完整性，但可以降低風險的任何漏洞。

- 低 (類別 III)

包含任何會降低防範機密性、可用性或完整性遺失之措施的漏洞。

主題

- [STIG 強化元件下載](#)
- [Windows STIG 設定](#)
- [Windows STIG 版本歷史記錄](#)
- [Linux STIG 設定](#)
- [Linux STIG 版本歷史記錄](#)

STIG 強化元件下載

Amazon 會將 STIG 強化元件分組為每個版本的作業系統相關套件。套件是封存檔案，適用於其下載和執行的目標作業系統。Linux 元件套件會儲存為 TAR 檔案 (.tgz 副檔名)。Windows 元件套件會儲存為 ZIP 檔案 (.zip 副檔名)。

Amazon 會將元件套件存放在每個的映像建置器 S3 STIG儲存貯體中 AWS 區域。使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。

Important

除了少數例外，Systems Manager 文件下載的 STIG 強化元件不會安裝第三方套件。如果執行個體上已安裝第三方套件，且 Amazon EC2 支援該套件的相關 STIGs，則會套用這些 STIGs。

元件儲存路徑和套件檔案名稱的模式和範例如下：

元件儲存路徑

s3://aws-windows-downloads-*<region>*/STIG/*<bundle file name>*

元件路徑變數

region

AWS 區域（每個區域都有自己的元件儲存貯體。）

bundle file name

格式為 *<os bundle name>_<YYYY>_Q<quarter>[_<release>].<file extension>*。請注意，名稱在節點之間有底線，而不是句點。

os bundle name

作業系統套件的標準名稱字首為 LinuxAWSConfigureSTIG或 AWSConfigureSTIG。為了維持回溯相容性，Windows 的下載不包含平台字首。

YYYY

發行的四位數年份。

quarter

識別年份的季度：1、2、3 或 4。

release

從 1 開始的增量數字，每個新版本以 1 遞增。發行版本不會包含在每季的第一個發行版本中，只會在後續版本中新增。

file extension

壓縮檔案格式 tgz(Linux) 或 zip(Windows)。

套件檔案名稱範例

- LinuxAWSConfigureSTIG_2023_Q1_2.tgz
- AWSConfigureSTIG_2022_Q4.zip

Windows STIG 設定

Amazon EC2 Windows STIG AMIs 和強化元件專為獨立伺服器而設計，並套用本機群組政策。STIG 相容元件從 Windows AMIs 的國防部 (DoD) 安裝 InstallRoot，以下載、安裝和更新 DoD 憑證。它們也會移除不必要的憑證，以維持 STIG 合規。目前，Amazon EC2 支援下列 Windows Server 版本的 STIG 基準：2012 R2、2016、2019 和 2022。

本節列出 Amazon EC2 為您的 Windows 基礎設施支援的目前 STIG 設定，後面接著版本歷史記錄日誌。

您可以套用低、中或高 STIG 設定。

Windows STIG 低 (類別 III)

下列清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需 Windows STIG 的完整清單，請參閱 [STIGs Document Library](#) (STIG 文件庫)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

- Windows Server 2022 STIG 第 2 版第 2 版

V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 和 V-254481

- Windows Server 2019 STIG 第 3 版第 2 版

V-205691、V-205819、V-205858、V-205859、V-205860、V-205870、V-205871 以及 V-205923

- Windows Server 2016 STIG 第 2 版第 9 版

V-224916、V-224917、V-224918、V-224919、V-224931、V-224942 以及 V-225060

- Windows Server 2012 R2 MS STIG 第 3 版第 5 版

V-225537、V-225536、V-225526、V-225525、V-225514、V-225511、V-225490、V-225489、V-225488 以及 V-225250

- Microsoft .NET Framework 4.0 STIG 第 2 版第 2 版

沒有 STIG 設定適用於類別 III 漏洞的 Microsoft .NET Framework。

- Windows Firewall STIG 第 2 版第 2 版

V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 和 V-242008

- Internet Explorer 11 STIG 第 2 版第 5 版

V-223016, V-223056 和 V-223078

- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)

V-235727, V-235731, V-235751, V-235752 和 V-235765

Windows STIG Medium (類別 II)

下列清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需 Windows STIG 的完整清單，請參閱 [STIGs Document Library](#) (STIG 文件庫)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

Note

除了 Amazon EC2 針對類別 II 漏洞支援的 STIG 強化設定之外，Windows STIG Medium 類別還包括適用於 Windows STIG low (類別 III) 的所有列出的 STIG 強化設定。

- Windows Server 2022 STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 III (低) 漏洞支援的所有 STIG 強化設定，以及：

V-254247、V-254265、V-254269、V-254270、V-254271、V-254272、V-254273、
V-254274、V-254276、V-254277、V-254278、V-254285、V-254286、V-254287、
V-254288、V-254289、V-254290、V-254291、V-254292、V-254300、V-254301、
V-254302、V-254303、V-254304、V-254305、V-254306、V-254307、V-254308、
V-254309、V-254310、V-254311、V-254312、V-254313、V-254314、V-254315、
V-254316、V-254317、V-254318、V-254319、V-254320、V-254321、V-254322、
V-254323、V-254324、V-254325、V-254326、V-254327、V-254328、V-254329、
V-254330、V-254331、V-254332、V-254333、V-254334、V-254339、V-254341、
V-254342、V-254344、V-254345、V-254346、V-254347、V-254348、V-254349、
V-254350、V-254355、V-254356、V-254356、V-254358、V-254359、V-254360、
V-254361、V-254362、V-254364、V-254365、V-254366、V-254367、V-254368、
V-254369、V-254370、V-254371、V-254372、V-254373、V-254375、V-254376、
V-254377、V-254379、V-254380、V-254382、V-254383、V-254384、V-254431、
V-254432、V-254433、V-254434、V-254435、V-254436、V-254438、V-254439、
V-254442、V-254443、V-254444、V-254445、V-254449、V-254450、V-254451、
V-254452、V-254453、V-254454、V-254455、V-254456、V-254459、V-254460、
V-254461、V-254462、V-254463、V-254464、V-254468、V-254470、V-254471、
V-254472、V-254473、V-254476、V-254477、V-254478、V-254479、V-254480、
V-254482、V-254483、V-254484、V-254485、V-254486、V-254487、V-254488、
V-254489、V-254490、V-254493、V-254494、V-254495、V-254497、V-254499、

V-254501、V-254502、V-254503、V-254504、V-254505、V-254507、V-254508、
V-254509、V-254510、V-254511、和 V-254512

- Windows Server 2019 STIG 第 3 版第 2 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-205625、V-205626、V-205627、V-205629、V-205630、V-205633、V-205634、
V-205635、V-205636、V-205637、V-205638、V-205639、V-205643、V-205644、
V-205648、V-205649、V-205650、V-205651、V-205652、V-205655、V-205656、
V-205659、V-205660、V-205662、V-205671、V-205672、V-205673、V-205675、
V-205676、V-205678、V-205679、V-205680、V-205681、V-205682、V-205683、
V-205684、V-205685、V-205686、V-205687、V-205688、V-205689、V-205690、
V-205692、V-205693、V-205694、V-205697、V-205698、V-205708、V-205709、
V-205712、V-205714、V-205716、V-205717、V-205718、V-205719、V-205720、
V-205722、V-205729、V-205730、V-205733、V-205747、V-205751、V-205752、
V-205754、V-205756、V-205758、V-205759、V-205760、V-205761、V-205762、
V-205764、V-205765、V-205766、V-205767、V-205768、V-205769、V-205770、
V-205771、V-205772、V-205773、V-205774、V-205775、V-205776、V-205777、
V-205778、V-205779、V-205780、V-205781、V-205782、V-205783、V-205784、
V-205795、V-205796、V-205797、V-205798、V-205801、V-205808、V-205809、
V-205810、V-205811、V-205812、V-205813、V-205814、V-205815、V-205816、
V-205817、V-205821、V-205822、V-205823、V-205824、V-205825、V-205826、
V-205827、V-205828、V-205830、V-205832、V-205833、V-205834、V-205835、
V-205836、V-205837、V-205838、V-205839、V-205840、V-205841、V-205842、
V-205861、V-205863、V-205865、V-205866、V-205867、V-205868、V-205869、
V-205872、V-205873、V-205874、V-205911、V-205912、V-205915、V-205916、
V-205917、V-205918、V-205920、V-205921、V-205922、V-205924、V-205925、
V-236001、和 V-257503

- Windows Server 2016 STIG 第 2 版第 9 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-224850、V-224852、V-224853、V-224854、V-224855、V-224856、V-224857、
V-224858、V-224859、V-224866、V-224867、V-224868、V-224869、V-224870、
V-224871、V-224872、V-224873、V-224881、V-224882、V-224883、V-224884、
V-224885、V-224886、V-224887、V-224888、V-224889、V-224890、V-224891、
V-224892、V-224893、V-224894、V-224895、V-224896、V-224897、V-224898、

V-224899、 V-224900、 V-224901、 V-224902、 V-224903、 V-224904、 V-224905、
V-224906、 V-224907、 V-224908、 V-224909、 V-224910、 V-224911、 V-224912、
V-224913、 V-224914、 V-224915、 V-224920、 V-224922、 V-224924、 V-224925、
V-224926、 V-224927、 V-224928、 V-224929、 V-224930、 V-224935、 V-224936、
V-224937、 V-224938、 V-224939、 V-224940、 V-224941、 V-224943、 V-224944、
V-224945、 V-224946、 V-224947、 V-224948、 V-224949、 V-224951、 V-224952、
V-224953、 V-224955、 V-224956、 V-224957、 V-224959、 V-224960、 V-224962、
V-224963、 V-225010、 V-225013、 V-225014、 V-225015、 V-225016、 V-225017、
V-225018、 V-225019、 V-225021、 V-225022、 V-225023、 V-225024、 V-225028、
V-225029、 V-225030、 V-225031、 V-225032、 V-225033、 V-225034、 V-225035、
V-225038、 V-225039、 V-225040、 V-225041、 V-225042、 V-225043、 V-225047、
V-225049、 V-225050、 V-225051、 V-225052、 V-225055、 V-225056、 V-225057、
V-225058、 V-225059、 V-225061、 V-225062、 V-225063、 V-225064、 V-225065、
V-225066、 V-225067、 V-225068、 V-225069、 V-225072、 V-225073、 V-225074、
V-225076、 V-225078、 V-225080、 V-225081、 V-225082、 V-225083、 V-225084、
V-225086、 V-225087、 V-225088、 V-225089、 V-225092、 V-225093、 V-236000、 和
V-257502

- Windows Server 2012 R2 MS STIG 第 3 版第 5 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-225574、 V-225573、 V-225572、 V-225571、 V-225570、 V-225569、 V-225568、
V-225567、 V-225566、 V-225565、 V-225564、 V-225563、 V-225562、 V-225561、
V-225560、 V-225559、 V-225558、 V-225557、 V-225555、 V-225554、 V-225553、
V-225551、 V-225550、 V-225549、 V-225548、 V-225546、 V-225545、 V-225544、
V-225543、 V-225542、 V-225541、 V-225540、 V-225539、 V-225538、 V-225535、
V-225534、 V-225533、 V-225532、 V-225531、 V-225530、 V-225529、 V-225528、
V-225527、 V-225524、 V-225523、 V-225522、 V-225521、 V-225520、 V-225519、
V-225518、 V-225517、 V-225516、 V-225515、 V-225513、 V-225510、 V-225509、
V-225508、 V-225506、 V-225504、 V-225503、 V-225502、 V-225501、 V-225500、
V-225494、 V-225486、 V-225478、 V-225477、 V-225475、 V-225474、 V-225472、
V-225471、 V-225470、 V-225469、 V-225464、 V-225463、 V-225461、 V-225458、
V-225457、 V-225456、 V-225455、 V-225454、 V-225453、 V-225452、 V-225448、
V-225443、 V-225442、 V-225441、 V-225415、 V-225414、 V-225413、 V-225411、
V-225410、 V-225409、 V-225408、 V-225407、 V-225406、 V-225405、 V-225404、
V-225402、 V-225401、 V-225400、 V-225398、 V-225397、 V-225395、 V-225393、
V-225391、 V-225389、 V-225386、 V-225385、 V-225384、 V-225383、 V-225382、

V-225381、 V-225380、 V-225379、 V-225378、 V-225377、 V-225375、 V-225374、
V-225373、 V-225372、 V-225371、 V-225370、 V-225369、 V-225368、 V-225367、
V-225356、 V-225353、 V-225352、 V-225351、 V-225350、 V-225349、 V-225348、
V-225347、 V-225346、 V-225345、 V-225344、 V-225341、 V-225340、 V-225339、
V-225338、 V-225337、 V-225329、 V-225326、 V-225325、 V-225317、 V-225316、
V-225315、 V-225314、 V-225305、 V-225304、 V-225303、 V-225302、 V-225301、
V-225300、 V-225299、 V-225298、 V-225297、 V-225296、 V-225295、 V-225294、
V-225293、 V-225292、 V-225291、 V-225290、 V-225289、 V-225288、 V-225287、
V-225286、 V-225285、 V-225284、 V-225283、 V-225282、 V-225281、 V-225280、
V-225279、 V-225278、 V-225277、 V-225276、 V-225275、 V-225273、 V-225272、
V-225271、 V-225270、 V-225269、 V-225268、 V-225267、 V-225266、 V-225265、
V-225264、 V-225263、 V-225261、 V-225260、 V-225259、 和 V-225239

- Microsoft .NET Framework STIG 4.0 第 2 版第 2 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-225238

- Windows Firewall STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-241989, V-241990, V-241991, V-241993, V-241993, V-241998, V-241998, V-242003 和
V-242003

- Internet Explorer 11 STIG 第 2 版第 5 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-223015、 V-223017、 V-223018、 V-223019、 V-223020、 V-223021、 V-223022、
V-223023、 V-223024、 V-223025、 V-223026、 V-223027、 V-223028、 V-223029、
V-223030、 V-223031、 V-223032、 V-223033、 V-223034、 V-223035、 V-223036、
V-223037、 V-223038、 V-223039、 V-223040、 V-223041、 V-223042、 V-223043、
V-223044、 V-223045、 V-223046、 V-223048、 V-223049、 V-223050、 V-223051、
V-223052、 V-223053、 V-223054、 V-223055、 V-223057、 V-223058、 V-223059、
V-223060、 V-223061、 V-223062、 V-223063、 V-223064、 V-223065、 V-223066、
V-223067、 V-223068、 V-223069、 V-223070、 V-223071、 V-223072、 V-223073、
V-223074、 V-223075、 V-223076、 V-223077、 V-223079、 V-223080、 V-223081、
V-223082、 V-223083、 V-223084、 V-223085、 V-223086、 V-223087、 V-223088、
V-223089、 V-223090、 V-223091、 V-223092、 V-223093、 V-223094、 V-223095、

V-223096、V-223097、V-223098、V-223099、V-223100、V-223101、V-223102、
V-223103、V-223104、V-223105、V-223106、V-223107、V-223108、V-223109、
V-223110、V-223111、V-223112、V-223113、V-223114、V-223115、V-223116、
V-223117、V-223118、V-223119、V-223120、V-223121、V-223122、V-223123、
V-223124、V-223125、V-223126、V-223127、V-223128、V-223129、V-223130、
V-223131、V-223132、V-223133、V-223134、V-223135、V-223136、V-223137、
V-223138、V-223139、V-223140、V-223141、V-223142、V-223143、V-223144、
V-223145、V-223146、V-223147、V-223148、V-223149、V-250540、和 V-250541

- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)

V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730,
V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740,
V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749,
V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767,
V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 V-246736

- Microsoft Defender STIG 第 2 版第 4 版

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436,
V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445,
V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465
V-213466

Windows STIG High (類別 I)

下列清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需 Windows STIG 的完整清單，請參閱 [STIGs Document Library](#) (STIG 文件庫)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

Note

除了 Amazon EC2 針對類別 I 漏洞支援的 STIG 強化設定之外，Windows STIG High 類別還包括適用於 Windows STIG Medium 和 Low 類別的所有列出的 STIG 強化設定。

- Windows Server 2022 STIG 第 2 版第 2 版

V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 和 V-254500

- Windows Server 2019 STIG 第 3 版第 2 版

包括 Amazon EC2 針對類別 II 和 III (中和和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-205653、V-205654、V-205711、V-205713、V-205724、V-205725、V-205757、V-205802、V-205804 以及 V-205919

- Windows Server 2016 STIG 第 2 版第 9 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-224874、V-224932、V-224933、V-224934、V-224954、V-224958、V-224961、V-225025、V-225044 以及 V-225079

- Windows Server 2012 R2 MS STIG 第 3 版第 5 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-225556、V-225552、V-225547、V-225507、V-225505、V-225498、V-225497、V-225496、V-225493 以及 V-225274

- Microsoft .NET Framework STIG 4.0 第 2 版第 2 版

包括 Amazon EC2 針對 Microsoft .NET Framework 的類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定。類別 I 漏洞不適用其他 STIG 設定。

- Windows Firewall STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-241992, V-241997 和 V-242002

- Internet Explorer 11 STIG 第 2 版第 5 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-252910

- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-235758 和 V-235759

- Microsoft Defender STIG 第 2 版第 4 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-213426, V-213426, V-213452, V-213452, V-213452, V-213453, V-213453 和 V-213453

Windows STIG 版本歷史記錄

本節記錄每季 STIG 更新的 Windows 元件版本歷史記錄。若要查看季度的變更和發佈版本 , 請選擇標題以展開資訊。

2025 年Q1變更 - 05/04/2025 :

針對 2025 年第一季版本的所有 STIG 元件 , 更新了 STIGS for Internet Explorer 11 STIG 第 2 版。

- STIG-Build-Windows-Low 2025.1.x 版
- STIG-Build-Windows-Medium 2025.1.x 版
- STIG-Build-Windows-High 2025.1.x 版

2024 年第 Q4變更 - 12/10/2024 :

已更新 STIG 版本並針對 2024 年Q4 季版本套用 STIGS , 如下所示 :

STIG-Build-Windows-Low 2024.4.0 版

- Windows Server 2022 STIG 第 2 版第 2 版
- Windows Server 2019 STIG 第 3 版第 2 版
- Windows Server 2016 STIG 第 2 版第 9 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 第 2 版第 2 版
- Internet Explorer 11 STIG 第 2 版第 5 版
- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)

STIG-Build-Windows-Medium 2024.4.0 版

- Windows Server 2022 STIG 第 2 版第 2 版

- Windows Server 2019 STIG 第 3 版第 2 版
- Windows Server 2016 STIG 第 2 版第 9 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 第 2 版第 2 版
- Internet Explorer 11 STIG 第 2 版第 5 版
- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)
- Defender STIG 第 2 版第 4 版

STIG-Build-Windows-High 2024.4.0 版

- Windows Server 2022 STIG 第 2 版第 2 版
- Windows Server 2019 STIG 第 3 版第 2 版
- Windows Server 2016 STIG 第 2 版第 9 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 第 2 版第 2 版
- Internet Explorer 11 STIG 第 2 版第 5 版
- Microsoft Edge STIG 第 2 版第 2 版 (僅限 Windows Server 2022)
- Defender STIG 第 2 版第 4 版

2024 年Q3 季變更 - 10/04/2024 (無變更) :

2024 年第三季發行版本的 Windows 元件 STIGS 沒有變更。

2024 年Q2 季變更 - 05/10/2024 (無變更) :

2024 年第二季發行版本的 Windows 元件 STIGS 沒有變更。

2024 年Q1變更 - 02/23/2024 (無變更) :

2024 年第一季發行的 Windows 元件 STIGS 沒有變更。

2023 年Q4 季變更 - 12/07/2023 (無變更) :

2023 年第 4 季發行版本的 Windows 元件 STIGS 沒有變更。

2023 年Q3 季變更 - 10/04/2023 (無變更) :

2023 年第三季發行版本的 Windows 元件 STIGS 沒有變更。

2023 年Q2 季變更 - 05/03/2023 (無變更) :

2023 年第二季發行版本的 Windows 元件 STIGS 沒有變更。

2023 年Q1變更 - 03/27/2023 (無變更) :

2023 年第一季發行的 Windows 元件 STIGS 沒有變更。

2022 年第 Q4變更 - 02/01/2023 :

已更新 STIG 版本並針對 2022 年Q4 季版本套用 STIGS , 如下所示 :

STIG-Build-Windows-Low 2022.4.0 版

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft Edge STIG 第 1 版第 6 版 (僅限 Windows Server 2022)

STIG-Build-Windows-Medium 2022.4.0 版

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft Edge STIG 第 1 版第 6 版 (僅限 Windows Server 2022)

- Defender STIG 第 2 版第 4 版 (僅限 Windows Server 2022)

STIG-Build-Windows-High 2022.4.0 版

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft Edge STIG 第 1 版第 6 版 (僅限 Windows Server 2022)
- Defender STIG 第 2 版第 4 版 (僅限 Windows Server 2022)

2022 年Q3 季變更 - 09/30/2022 (無變更) :

2022 年第三季發行版本的 Windows 元件 STIGS 沒有變更。

2022 年Q2 季變更 - 08/02/2022 :

已更新 STIG 版本 , 並針對 2022 年Q2 季版本套用 STIGS。

STIG-Build-Windows-Low 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 4 版
- Windows Server 2016 STIG 第 2 版第 4 版
- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-Medium 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 4 版
- Windows Server 2016 STIG 第 2 版第 4 版

- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-High 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 4 版
- Windows Server 2016 STIG 第 2 版第 4 版
- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

2022 年Q1變更 - 08/02/2022 (無變更) :

2022 年第一季版本 Windows 元件 STIGS 沒有變更。

2021 年Q4 季變更 - 12/20/2021 :

已更新 STIG 版本，並針對 2021 年第 4 季版本套用 STIGS。

STIG-Build-Windows-Low 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 3 版
- Windows Server 2016 STIG 第 2 版第 3 版
- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-Medium 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 3 版
- Windows Server 2016 STIG 第 2 版第 3 版

- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-High 1.5.0 版

- Windows Server 2019 STIG 第 2 版第 3 版
- Windows Server 2016 STIG 第 2 版第 3 版
- Windows Server 2012 R2 MS STIG 第 3 版第 3 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 第 1 版第 19 版

2021 年Q3 季變更 - 09/30/2021 :

已更新 STIG 版本，並針對 2021 年第三季版本套用 STIGS。

STIG-Build-Windows-Low 1.4.0 版

- Windows Server 2019 STIG 第 2 版第 2 版
- Windows Server 2016 STIG 第 2 版第 2 版
- Windows Server 2012 R2 MS STIG 第 3 版第 2 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 第 1 版第 7 版
- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-Medium 1.4.0 版

- Windows Server 2019 STIG 第 2 版第 2 版
- Windows Server 2016 STIG 第 2 版第 2 版
- Windows Server 2012 R2 MS STIG 第 3 版第 2 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 第 1 版第 7 版

- Internet Explorer 11 STIG 第 1 版第 19 版

STIG-Build-Windows-High 1.4.0 版

- Windows Server 2019 STIG 第 2 版第 2 版
- Windows Server 2016 STIG 第 2 版第 2 版
- Windows Server 2012 R2 MS STIG 第 3 版第 2 版
- Microsoft .NET Framework 4.0 STIG 第 2 版第 1 版
- Windows Firewall STIG 第 1 版第 7 版
- Internet Explorer 11 STIG 第 1 版第 19 版

Linux STIG 設定

本節包含 Amazon EC2 支援的 Linux STIG 強化設定相關資訊，後面接著版本歷史記錄日誌。如果 Linux 發行版本沒有自己的 STIG 強化設定，Amazon EC2 會使用 RHEL 設定。支援的 STIG 強化設定適用於以 Linux 發行版本為基礎的 Amazon EC2 Linux AMIs 和元件，如下所示：

- Red Hat Enterprise Linux (RHEL) 7 STIG 設定
 - RHEL 7
 - CentOS 7
 - Amazon Linux 2 (AL2)
- RHEL 8 STIG 設定
 - RHEL 8
 - CentOS 8
 - Amazon Linux 2023 (AL 2023)
- RHEL 9 STIG 設定
 - RHEL 9
 - CentOS Stream 9

Linux STIG Low (類別 III)

下列清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需完整清單，請參閱 [STIG 文件庫](#)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

RHEL 7 STIG 第 3 版第 14 版

- RHEL 7/CentOS 7/AL2

V-204452, V-204576 和 V-204605

RHEL 8 STIG 第 2 版第 2 版

- RHEL 8/CentOS 8/AL 2023

V-230241, V-230281, V-244527, V-230269, V-230270, V-230285, V-230346, V-230381, V-230395, V-230491, V-230468, V-230469, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 V-230253

RHEL 9 STIG 第 2 版第 3 版

- RHEL 9/CentOS 串流 9

V-257782, V-257824, V-258138, V-258037, V-257880, V-257795, V-257796, V-258173, V-258069, V-258076, V-258067, V-257946 和 V-257947

Ubuntu 18.04 STIG 第 2 版第 15 版

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219180, V-219210, V-219301, V-219327, V-219332 和 V-219333

Ubuntu 20.04 STIG 第 2 版第 2 版

V-238203, V-238202, V-238234, V-238235, V-238237, V-238323, V-238373, V-238221, V-238222, V-238223, V-238224, V-238226, V-238362, V-238357 和 V-238308

Ubuntu 22.04 STIG 第 2 版第 3 版

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581 和 V-260596

Ubuntu 24.04 STIG 第 1 版第 1 版

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752 和 V-270818

Linux STIG Medium (類別 II)

下列清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需完整清單，請參閱 [STIG 文件庫](#)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

Note

除了 Amazon EC2 針對類別 II 漏洞支援的 STIG 強化設定之外，Linux STIG Medium 類別還包括適用於 Linux STIG Low (類別 III) 的所有列出的 STIG 強化設定。

RHEL 7 STIG 第 3 版第 15 版

包括 Amazon EC2 針對類別 III (低) 漏洞支援的所有 STIG 強化設定，以及：

- RHEL 7/CentOS 7/AL2

V-204405、 V-204406、 V-204407、 V-204408、 V-204409、 V-204410、 V-204411、
V-204412、 V-204413、 V-204414、 V-204415、 V-204416、 V-204417、 V-204418、
V-204422、 V-204423、 V-204426、 V-204427、 V-204431、 V-204434、 V-204435、
V-204437、 V-204449、 V-204450、 V-204451、 V-204457、 V-204466 , V-204490、
V-204491、 V-204503、 V-204507、 V-204508、 V-204510、 V-204511、 V-204512、
V-204514、 V-204515、 V-204516、 V-204517、 V-204521、 V-204524、 V-204531、
V-204536、 V-204537、 V-204538、 V-204539、 V-204540、 V-204541、 V-204542、
V-204543、 V-204544、 V-204545、 V-204546、 V-204547、 V-204548、 V-204549、
V-204550、 V-204551、 V-204552、 V-204553、 V-204554、 V-204555 , V-204556、
V-204557、 V-204558、 V-204559、 V-204560、 V-204562、 V-204563、 V-204564、
V-204565、 V-204566、 V-204567、 V-204568、 V-204572、 V-204578、 V-204579、
V-204584、 V-204585、 V-204587、 V-204588、 V-204589、 V-204590、 V-204591、
V-204592、 V-204593、 V-204595、 V-204596、 V-204597、 V-204598、 V-204599、
V-204600、 V-204601、 V-204602、 V-204609、 V-204610、 V-204611、 V-204612、
V-204613、 V-204614、 V-204615、 V-204616、 V-204617、 V-204619、 V-204622、

V-204625、V-204630、V-204631、V-204633、V-233307、V-237634、V-237635、
V-251703、V-255925、V-255927、V-255928、和 V-256970

RHEL 8 STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

- RHEL 8/CentOS 8/AL 2023

V-230238、V-230239、V-230257、V-230258、V-230259、V-230262、V-230273、
V-230275、V-230316、V-230325、V-230366、V-230478、V-230488、V-230489、
V-230505、V-230523、V-230550、V-230559、V-230560、V-230561、V-237640、
V-244547、V-256974、V-230525、V-244544、V-230248、V-230249、V-230250、
V-230245、V-230246、V-230247、V-230397、V-230399、V-230400、V-230401、
V-244543、V-230228、V-230298、V-230387、V-230482、V-230231、V-230233、
V-230324、V-230365、V-230370、V-230373、V-230378、V-230383、V-230236、
V-230314、V-230315、V-244523、V-257258、V-230266、V-230267、V-230268、
V-230280、V-230310、V-230311、V-230312、V-230502、V-230532、V-230535、
V-230536、V-230537、V-230538、V-230539、V-230540、V-230541、V-230542、
V-230543、V-230544、V-230545、V-230546、V-230547、V-230548、V-230549、
V-244550、V-244551、V-244552、V-244553、V-244554、V-250317、V-251718、
V-230237、V-230313、V-230356、V-230357、V-230358、V-230359、V-230360、
V-230361、V-230362、V-230363、V-230368、V-230369、V-230375、V-230376、
V-230377、V-244524、V-244533、V-251713、V-251717、V-251714、V-251715、
V-251716、V-230332、V-230333、V-230335、V-230337、V-230339、V-230341、
V-230343、V-230345、V-230240、V-230282、V-250315、V-250316、V-230255、
V-230277、V-230278、V-230348、V-230353、V-230386、V-230390、V-230392、
V-230394、V-230396、V-230393、V-230398、V-230402、V-230403、V-230404、
V-230405、V-230406、V-230407、V-230408、V-230409、V-230410、V-230411、
V-230412、V-230413、V-230418、V-230419、V-230421、V-230422、V-230423、
V-230424、V-230425、V-230426、V-230427、V-230428、V-230429、V-230430、
V-230431、V-230432、V-230433、V-230434、V-230435、V-230436、V-230437、
V-230438、V-230439、V-230444、V-230446、V-230447、V-230448、V-230449、
V-230455、V-230456、V-230462、V-230463、V-230464、V-230465、V-230466、
V-230467、V-230471、V-230472、V-230473、V-230474、V-230480、V-230483、
V-244542、V-230503、V-230507、V-244525、V-230244、V-230286、V-230287、
V-230288、V-230290、V-230291、V-230296、V-230330、V-230382、V-230526、

V-230527、V-230555、V-230556、V-244526、V-244528、V-237642、V-237643、和
V-251711

RHEL 9 STIG 第 2 版第 3 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

- RHEL 9/CentOS 串流 9

V-257981、V-257780、V-257825、V-257827、V-257828、V-257829、V-257830、
V-257831、V-257832、V-257833、V-257834、V-257836、V-257838、V-257839、
V-257840、V-257841、V-257842、V-257882、V-257883、V-257884、V-257885、
V-257889、V-257890、V-257891、V-257892、V-257893、V-257894、V-257895、
V-257896、V-257897、V-257898、V-257899、V-257900、V-257901、V-257902、
V-257903、V-257904、V-257905、V-257906、V-257907、V-257908、V-257909、
V-257910、V-257911、V-257912、V-257913、V-257914、V-257915、V-257918、
V-257919、V-257920、V-257921、V-257922、V-257923、V-257928、V-257929、
V-257930、V-257934、V-257935、V-257943、V-257948、V-257954、V-257978、
V-257980、V-258035、V-258041、V-258046、V-258052、V-258063、V-258068、
V-258081、V-258082、V-258083、V-258089、V-258120、V-258124、V-258126、
V-258140、V-258141、V-258151、V-258234、V-257886、V-257916、V-257917、
V-257952、V-257936、V-257939、V-257940、V-258036、V-258038、V-257887、
V-257924、V-257925、V-258145、V-258152、V-258153、V-258154、V-258156、
V-258157、V-258158、V-258159、V-258160、V-258161、V-258162、V-258163、
V-258164、V-258165、V-258166、V-258167、V-258168、V-258169、V-258170、
V-258171、V-258172、V-258176、V-258177、V-258178、V-258179、V-258180、
V-258181、V-258182、V-258183、V-258184、V-258185、V-258186、V-258187、
V-258188、V-258189、V-258190、V-258191、V-258192、V-258193、V-258194、
V-258195、V-258196、V-258197、V-258198、V-258199、V-258200、V-258201、
V-258202、V-258203、V-258204、V-258205、V-258206、V-258207、V-258208、
V-258209、V-258210、V-258211、V-258212、V-258213、V-258214、V-258215、
V-258216、V-258217、V-258218、V-258219、V-258220、V-258221、V-258222、
V-258223、V-258224、V-258225、V-258226、V-258227、V-258228、V-258229、
V-257781、V-257783、V-257786、V-257797、V-257798、V-257799、V-257800、
V-257801、V-257802、V-257803、V-257809、V-257810、V-257811、V-257812、
V-257813、V-257815、V-257816、V-257942、V-257957、V-257958、V-257959、
V-257960、V-257961、V-257962、V-257963、V-257964、V-257965、V-257966、

V-257967、 V-257968、 V-257969、 V-257970、 V-257971、 V-257972、 V-257973、
V-257974、 V-257975、 V-257976、 V-257977、 V-258077、 V-258128、 V-258129、
V-258043、 V-258049、 V-258071、 V-258072、 V-258073、 V-258074、 V-258075、
V-258104、 V-258105、 V-258107、 V-258108、 V-258109、 V-258110、 V-258111、
V-258117、 V-258119、 V-257979、 V-257982、 V-257983、 V-257985、 V-257987、
V-257988、 V-257992、 V-257993、 V-257994、 V-257995、 V-257996、 V-257997、
V-257998、 V-257999 , V-258000、 V-258001、 V-258002、 V-258003、 V-258004、
V-258005、 V-258006、 V-258007、 V-258008、 V-258009、 V-258010、 V-258011、
V-258130、 V-257814、 V-258054、 V-258055、 V-258056、 V-258057、 V-258060、
V-258070、 V-258080、 V-258088、 V-258091、 V-258092、 V-258093、 V-258095、
V-258097、 V-258098、 V-258099、 V-258100、 V-258101、 V-258102、 V-258103、
V-258112、 V-258113、 V-258114、 V-258115、 V-258116、 V-258118、 V-258233、
V-257951、 V-257953、 V-258142、 V-258144、 V-258146、 V-258147、 V-258148、
V-258150、 V-258064、 V-258065、 V-258066、 V-258232、 V-258237、 V-258239、
V-258240、 V-257788 , V-257790、 V-257791、 V-257792、 V-257793、 V-257794、
V-257817、 V-258175、 V-257804、 V-257805、 V-257806、 V-257807、 V-257808、
V-258034、 V-258039、 V-257888 , V-257926、 V-257927、 V-257933、 V-258084、
V-258085、 V-257949、 V-258040、 V-257818、 V-257849、 V-258122、 V-258123、
V-258133、 V-257944、 V-258028、 V-258079、 V-258125、 和 V-258137

Ubuntu 18.04 STIG 第 2 版第 15 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-219149、 V-219155、 V-219156、 V-219160、 V-219166、 V-219168、 V-219176、 V-219181、
V-219184、 V-219186、 V-219188、 V-219189、 V-219190、 V-219191、 V-219192、 V-219193、
V-219194、 V-219195、 V-219196、 V-219197、 V-219198、 V-219199、 V-219200、 V-219201、
V-219202、 V-219203、 V-219204、 V-219205、 V-219206、 V-219207、 V-219208、 V-219209、
V-219213、 V-219214、 V-219215、 V-219216、 V-219217、 V-219218、 V-219219、 V-219220、
V-219221、 V-219222、 V-219223、 V-219224、 V-219225、 V-219226、 V-219227、 V-219228、
V-219229、 V-219230、 V-219231、 V-219232、 V-219233、 V-219234、 V-219235、 V-219236、
V-219238、 V-219239、 V-219240、 V-219241、 V-219242、 V-219243、 V-219244、 V-219250、
V-219254、 V-219257、 V-219263、 V-219264、 V-219265、 V-219266、 V-219267、 V-219268、
V-219269、 V-219270、 V-219271、 V-219272、 V-219273、 V-219274、 V-219275、 V-219276、
V-219277、 V-219279、 V-219281、 V-219287、 V-219291、 V-219297、 V-219298、 V-219299、
V-219300、 V-219303、 V-219304、 V-219306、 V-219309、 V-219310、 V-219311、 V-219312、
V-219315、 V-219318、 V-219319、 V-219323、 V-219326、 V-219328、 V-219330、 V-219331、

V-219335、 V-219336、 V-219337、 V-219338、 V-219339、 V-219342、 V-219344、 V-233779、 V-233780、 和 V-255906

Ubuntu 20.04 STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 III (低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-238200、 V-238205、 V-238207、 V-238231、 V-238329、 V-238337、 V-238339、 V-238340、 V-238344、 V-238345、 V-238346、 V-238347、 V-238348、 V-238349、 V-238350、 V-238351、 V-238352、 V-238371、 V-238376、 V-238377、 V-238378、 V-238209、 V-238325、 V-238330、 V-238333 , V-238369、 V-238230、 V-238338、 V-238341、 V-238342、 V-238343、 V-238324、 V-238353、 V-238228、 V-238225、 V-238227、 V-238299、 V-238238、 V-238239、 V-238240、 V-238241、 V-238242、 V-238244、 V-238245、 V-238246、 V-238247、 V-238248、 V-238249、 V-238250、 V-238251、 V-238252、 V-238253、 V-238254、 V-238255、 V-238256、 V-238257、 V-238258、 V-238264、 V-238268、 V-238271、 V-238277、 V-238278、 V-238279、 V-238280、 V-238281、 V-238282、 V-238283、 V-238284、 V-238285、 V-238286、 V-238287、 V-238288、 V-238289、 V-238290、 V-238291、 V-238292、 V-238293、 V-238294、 V-238295、 V-238297、 V-238300、 V-238301、 V-238302、 V-238304、 V-238309、 V-238310、 V-238315、 V-238316、 V-238317、 V-238318、 V-238319、 V-238320、 V-251505、 V-238360、 V-238210、 V-238211、 V-238212、 V-238213、 V-238220、 V-255912、 V-238355、 V-238236、 V-238303、 V-238356、 V-238359、 V-238370、 V-238334、 和 V-238232

Ubuntu 22.04 STIG 第 2 版第 3 版

包括 Amazon EC2 針對類別 III (低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-260546、 V-260473、 V-260474、 V-260478、 V-260485、 V-260486、 V-260487、 V-260488、 V-260489、 V-260490、 V-260495、 V-260496、 V-260497、 V-260498、 V-260499、 V-260500、 V-260508、 V-260513、 V-260522、 V-260540、 V-260542、 V-260543、 V-260547、 V-260554、 V-260572、 V-260590、 V-260475、 V-260491、 V-260510、 V-260511、 V-260492、 V-260493、 V-260494、 V-260507、 V-260591、 V-260594、 V-260597、 V-260598、 V-260599、 V-260600、 V-260601、 V-260602、 V-260603、 V-260604、 V-260605、 V-260606、 V-260607、 V-260608、 V-260609、 V-260610、 V-260611、 V-260612、 V-260613、 V-260614、 V-260615、 V-260616、 V-260617、 V-260618、 V-260619、 V-260620、 V-260621、 V-260622、 V-260623、 V-260624、 V-260625、 V-260626、 V-260627、 V-260628、 V-260629、 V-260630、 V-260631、 V-260632、 V-260633、 V-260634、 V-260635、 V-260636、 V-260637、 V-260638、 V-260639、 V-260640、 V-260641、 V-260642、 V-260643、 V-260644、 V-260645、 V-260646、 V-260647、 V-260648、 V-260649、 V-260471、 V-260514、 V-260553、 V-260573、 V-260576、 V-260574、 V-260560、 V-260561、 V-260562、 V-260563、 V-260564、 V-260565、 V-260566、 V-260567、 V-260569、

V-260527、V-260528、V-260530、V-260533、V-260534、V-260575、V-260505、V-260506、V-260512、V-260582、V-260584、V-260585、V-260586、V-260477、V-260545、V-260555、V-260556、V-260557、V-260509、V-260588、V-260589、V-260537、V-260538、和 V-260535

Ubuntu 24.04 STIG 第 1 版第 1 版

包括 Amazon EC2 針對類別 III（低）漏洞支援的所有 STIG 強化設定，以及：

V-270649、V-270651、V-270652、V-270653、V-270654、V-270656、V-270657、V-270659、V-270660、V-270661、V-270662、V-270663、V-270669、V-270672、V-270673、V-270674、V-270676、V-270678、V-270679、V-270680、V-270681、V-270683、V-270684、V-270685、V-270686、V-270687、V-270688、V-270689、V-270692、V-270693、V-270696、V-270697、V-270698、V-270699、V-270700、V-270701、V-270702、V-270703、V-270704、V-270705、V-270709、V-270715、V-270716、V-270718、V-270720、V-270721、V-270722、V-270723、V-270724、V-270725、V-270726、V-270727、V-270728、V-270729、V-270730、V-270731、V-270732、V-270733、V-270737、V-270739、V-270740、V-270741、V-270742、V-270743、V-270746、V-270750、V-270753、V-270755、V-270756、V-270757、V-270758、V-270759、V-270760、V-270765、V-270766、V-270767、V-270768、V-270769、V-270770、V-270771、V-270772、V-270773、V-270775、V-270776、V-270777、V-270778、V-270779、V-270780、V-270781、V-270782、V-270783、V-270784、V-270785、V-270786、V-270787、V-270788、V-270789、V-270790、V-270791、V-270792、V-270793、V-270794、V-270795、V-270796、V-270797、V-270798、V-270799、V-270800、V-270801、V-270802、V-270803、V-270804、V-270805、V-270806、V-270807、V-270808、V-270809、V-270810、V-270811、V-270812、V-270813、V-270814、V-270815、V-270821、V-270822、V-270823、V-270824、V-270825、V-270826、V-270827、V-270828、V-270829、V-270830、V-270831、和 V-270832

Linux STIG High（類別 I）

以下清單包含 Amazon EC2 對基礎設施支援的 STIG 設定。如果支援的設定不適用於您的基礎設施，Amazon EC2 會略過該設定並繼續進行。例如，某些 STIG 強化設定可能不適用於獨立伺服器。組織特定的政策也可能會影響適用的設定，例如要求管理員檢閱文件設定。

如需完整清單，請參閱 [STIG 文件庫](#)。如需有關如何檢視完整清單的詳細資訊，請參閱 [STIG 檢視工具](#)。

Note

除了 Amazon EC2 針對類別 I 漏洞支援的 STIG 強化設定之外，Linux STIG High 類別還包括適用於 Linux STIG Medium 和 Low 類別的所有列出的 STIG 強化設定。

RHEL 7 STIG 第 3 版第 15 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

- RHEL 7/CentOS 7/AL2

V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620 和 V-204621

RHEL 8 STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

- RHEL 8/CentOS 8/AL 2023

V-230223, V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, V-230558 和 V-244540

RHEL 9 STIG 第 2 版第 3 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

- RHEL 9/CentOS 串流 9

V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-258059, V-258230, V-258238, V-257784, V-257785, V-257984, V-257986, V-258078, V-258094 和 V-258235

Ubuntu 18.04 STIG 第 2 版第 15 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507 和 V-264388

Ubuntu 20.04 STIG 第 2 版第 2 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-238218, V-238219, V-238201, V-251504, V-238326, V-238327 和 V-238380

Ubuntu 22.04 STIG 第 2 版第 3 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-260482, V-260483, V-260523, V-260524, V-260469, V-260526, V-260529, V-260570, V-260571, V-260579 和 V-260539

Ubuntu 24.04 STIG 第 1 版第 1 版

包括 Amazon EC2 針對類別 II 和 III (中和低) 漏洞支援的所有 STIG 強化設定 , 以及 :

V-270647, V-270648, V-270665, V-270666, V-270708, V-270717, V-270711, V-270712, V-270713 和 V-270714

Linux STIG 版本歷史記錄

本節記錄每季 STIG 更新的 Linux 元件版本歷史記錄。若要查看季度的變更和發佈版本 , 請選擇標題以展開資訊。

2025 年Q1變更 - 04/11/2025 :

更新了下列 STIG 版本 , 為 2025 年第一季版本套用了 STIGS , 並新增了對 Ubuntu 24.04 的支援 :

STIG-Build-Linux-Low 2025.1.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 2 版
- RHEL 9 STIG 第 2 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 2 版
- Ubuntu 22.04 STIG 第 2 版第 3 版
- Ubuntu 24.04 STIG 第 1 版第 1 版

STIG-Build-Linux-Medium 2025.1.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 2 版
- RHEL 9 STIG 第 2 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 2 版
- Ubuntu 22.04 STIG 第 2 版第 3 版

- Ubuntu 24.04 STIG 第 1 版第 1 版

STIG-Build-Linux-High 2025.1.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 2 版
- RHEL 9 STIG 第 2 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 2 版
- Ubuntu 22.04 STIG 第 2 版第 3 版
- Ubuntu 24.04 STIG 第 1 版第 1 版

2024 年第 Q4變更 - 12/10/2024 :

已更新下列 STIG 版本、為 2024 年第 4 季版本套用 STIGS，並新增 Linux 元件兩個新輸入參數的相關資訊：

STIG-Build-Linux-Low 2024.4.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 1 版
- RHEL 9 STIG 第 2 版第 2 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 1 版
- Ubuntu 22.04 STIG 第 2 版第 2 版

STIG-Build-Linux-Medium 2024.4.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 1 版
- RHEL 9 STIG 第 2 版第 2 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 1 版
- Ubuntu 22.04 STIG 第 2 版第 2 版

STIG-Build-Linux-High 2024.4.x 版

- RHEL 7 STIG 第 3 版第 15 版
- RHEL 8 STIG 第 2 版第 1 版
- RHEL 9 STIG 第 2 版第 2 版
- Ubuntu 18.04 STIG 第 2 版第 15 版
- Ubuntu 20.04 STIG 第 2 版第 1 版
- Ubuntu 22.04 STIG 第 2 版第 2 版

2024 年Q3 季變更 - 10/04/2024 (無變更) :

2024 年第三季發行版本的 Linux 元件 STIGS 沒有變更。

2024 年Q2 季變更 - 05/10/2024 :

已更新 STIG 版本，並針對 2024 年第二季版本套用 STIGS。也新增了對 RHEL 9、CentOS Stream 9 和 Ubuntu 22.04 的支援，如下所示：

STIG-Build-Linux-Low 2024.2.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 14 版
- RHEL 9 STIG 第 1 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 14 版
- Ubuntu 20.04 STIG 第 1 版第 12 版
- Ubuntu 22.04 STIG 第 1 版第 1 版

STIG-Build-Linux-Medium 2024.2.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 14 版
- RHEL 9 STIG 第 1 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 14 版
- Ubuntu 20.04 STIG 第 1 版第 12 版

- Ubuntu 22.04 STIG 第 1 版第 1 版

STIG-Build-Linux-High 2024.2.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 14 版
- RHEL 9 STIG 第 1 版第 3 版
- Ubuntu 18.04 STIG 第 2 版第 14 版
- Ubuntu 20.04 STIG 第 1 版第 12 版
- Ubuntu 22.04 STIG 第 1 版第 1 版

2024 年Q1變更 - 02/06/2024 :

已更新 STIG 版本並針對 2024 年第一季版本套用 STIGS , 如下所示 :

STIG-Build-Linux-Low 2024.1.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 13 版
- Ubuntu 18.04 STIG 第 2 版第 13 版
- Ubuntu 20.04 STIG 第 1 版第 11 版

STIG-Build-Linux-Medium 2024.1.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 13 版
- Ubuntu 18.04 STIG 第 2 版第 13 版
- Ubuntu 20.04 STIG 第 1 版第 11 版

STIG-Build-Linux-High 2024.1.x 版

- RHEL 7 STIG 第 3 版第 14 版
- RHEL 8 STIG 第 1 版第 13 版
- Ubuntu 18.04 STIG 第 2 版第 13 版
- Ubuntu 20.04 STIG 第 1 版第 11 版

2023 年Q4 季變更 - 12/07/2023 :

已更新 STIG 版本，並針對 2023 年第 4 季版本套用 STIGS，如下所示：

STIG-Build-Linux-Low 2023.4.x 版

- RHEL 7 STIG 第 3 版第 13 版
- RHEL 8 STIG 第 1 版第 12 版
- Ubuntu 18.04 STIG 第 2 版第 12 版
- Ubuntu 20.04 STIG 第 1 版第 10 版

STIG-Build-Linux-Medium 2023.4.x 版

- RHEL 7 STIG 第 3 版第 13 版
- RHEL 8 STIG 第 1 版第 12 版
- Ubuntu 18.04 STIG 第 2 版第 12 版
- Ubuntu 20.04 STIG 第 1 版第 10 版

STIG-Build-Linux-High 2023.4.x 版

- RHEL 7 STIG 第 3 版第 13 版
- RHEL 8 STIG 第 1 版第 12 版
- Ubuntu 18.04 STIG 第 2 版第 12 版
- Ubuntu 20.04 STIG 第 1 版第 10 版

2023 年Q3 季變更 - 10/04/2023 :

已更新 STIG 版本並針對 2023 年第三季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 12 版
- RHEL 8 STIG 第 1 版第 11 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 9 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 12 版
- RHEL 8 STIG 第 1 版第 11 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 9 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 12 版
- RHEL 8 STIG 第 1 版第 11 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 9 版

2023 年Q2 季變更 - 05/03/2023 :

已更新 STIG 版本並針對 2023 年第二季版本套用 STIGS , 如下所示 :

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 11 版
- RHEL 8 STIG 第 1 版第 10 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 8 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 11 版
- RHEL 8 STIG 第 1 版第 10 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 8 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 11 版

- RHEL 8 STIG 第 1 版第 10 版
- Ubuntu 18.04 STIG 第 2 版第 11 版
- Ubuntu 20.04 STIG 第 1 版第 8 版

2023 年Q1變更 - 03/27/2023 :

已更新 STIG 版本，並針對 2023 年第一季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 10 版
- RHEL 8 STIG 第 1 版第 9 版
- Ubuntu 18.04 STIG 第 2 版第 10 版
- Ubuntu 20.04 STIG 第 1 版第 7 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 10 版
- RHEL 8 STIG 第 1 版第 9 版
- Ubuntu 18.04 STIG 第 2 版第 10 版
- Ubuntu 20.04 STIG 第 1 版第 7 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 10 版
- RHEL 8 STIG 第 1 版第 9 版
- Ubuntu 18.04 STIG 第 2 版第 10 版
- Ubuntu 20.04 STIG 第 1 版第 7 版

2022 年第 Q4變更 - 02/01/2023 :

已更新 STIG 版本並針對 2022 年第 4 季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 9 版

- RHEL 8 STIG 第 1 版第 8 版
- Ubuntu 18.04 STIG 第 2 版第 9 版
- Ubuntu 20.04 STIG 第 1 版第 6 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 9 版
- RHEL 8 STIG 第 1 版第 8 版
- Ubuntu 18.04 STIG 第 2 版第 9 版
- Ubuntu 20.04 STIG 第 1 版第 6 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 9 版
- RHEL 8 STIG 第 1 版第 8 版
- Ubuntu 18.04 STIG 第 2 版第 9 版
- Ubuntu 20.04 STIG 第 1 版第 6 版

2022 年Q3 季變更 - 09/30/2022 (無變更) :

2022 年第三季發行版本的 Linux 元件 STIGS 沒有變更。

2022 年Q2 季變更 - 08/02/2022 :

推出 Ubuntu 支援、更新 STIG 版本，並針對 2022 年第二季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 7 版
- RHEL 8 STIG 第 1 版第 6 版
- Ubuntu 18.04 STIG 第 2 版第 6 版 (新)
- Ubuntu 20.04 STIG 第 1 版第 4 版 (新)

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 7 版

- RHEL 8 STIG 第 1 版第 6 版
- Ubuntu 18.04 STIG 第 2 版第 6 版 (新)
- Ubuntu 20.04 STIG 第 1 版第 4 版 (新)

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 7 版
- RHEL 8 STIG 第 1 版第 6 版
- Ubuntu 18.04 STIG 第 2 版第 6 版 (新)
- Ubuntu 20.04 STIG 第 1 版第 4 版 (新)

2022 年Q1變更 - 04/26/2022 :

重構為包含更佳的容器支援。將先前的 AL2 指令碼與 RHEL 7 結合。已更新 STIG 版本並針對 2022 年第一季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 6 版
- RHEL 8 STIG 第 1 版第 5 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 6 版
- RHEL 8 STIG 第 1 版第 5 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 6 版
- RHEL 8 STIG 第 1 版第 5 版

2021 年Q4 季變更 - 12/20/2021 :

已更新 STIG 版本，並針對 2021 年第 4 季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 5 版
- RHEL 8 STIG 第 1 版第 4 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 5 版
- RHEL 8 STIG 第 1 版第 4 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 5 版
- RHEL 8 STIG 第 1 版第 4 版

2021 年Q3 季變更 - 09/30/2021 :

已更新 STIG 版本，並針對 2021 年第三季版本套用 STIGS，如下所示：

Linux STIG Low (類別 III)

- RHEL 7 STIG 第 3 版第 4 版
- RHEL 8 STIG 第 1 版第 3 版

Linux STIG Medium (類別 II)

- RHEL 7 STIG 第 3 版第 4 版
- RHEL 8 STIG 第 1 版第 3 版

Linux STIG High (類別 I)

- RHEL 7 STIG 第 3 版第 4 版
- RHEL 8 STIG 第 1 版第 3 版

AWSEC2-PatchLoadBalancerInstance

Description

升級和修補連接到任何負載平衡器（傳統、ALB 或 NLB）的 Amazon EC2 執行個體 (Windows 或 Linux) 次要版本。預設連線耗盡時間會在修補執行個體之前套用。您可以藉由為 ConnectionDrainTime 參數輸入以分鐘 (1-59) 為單位的自訂耗盡時間來覆寫等待時間。

自動化工作流程如下：

1. 將決定執行個體連接的負載平衡器或目標群組，並驗證執行個體是否正常運作。
2. 執行個體會從負載平衡器或目標群組中移除。
3. 自動化會等待指定的連線耗盡時間期間。
4. 呼叫 [AWS-RunPatchBaseline](#) 自動化來修補執行個體。
5. 執行個體會重新連接至負載平衡器或目標群組。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

先決條件

- 確認 SSM Agent 安裝於您的執行個體上。如需詳細資訊，請參閱[在 Windows Server 的 EC2 執行個體上使用 SSM Agent](#)。

參數

- InstanceId

類型：字串

描述：（必要）要修補與負載平衡器（傳統、ALB 或 NLB）相關聯的執行個體 ID。

- ConnectionDrainTime

類型：字串

描述：(選用) 負載平衡器的連線耗盡時間，以分鐘為單位 (1-59)。

- S3BucketLog

類型：字串

描述：(選用) 用來存放命令輸出回應的 Amazon S3 儲存貯體名稱。您可以指定您擁有的儲存貯體或與您共用的儲存貯體。如果您提供此參數，您還必須提供 runCommandAssumeRole。

- runCommandAssumeRole

類型：字串

描述：(選用) 用於在執行個體上執行命令的 IAM 角色 ARN。該角色必須和服務 `ssm.amazonaws.com` 主體具有信任關係，必須連接 AmazonSSMManagedInstanceCore 政策，且必須具有為 S3BucketLog 指定的 Amazon S3 儲存貯體的寫入許可。

AWSEC2-SQLServerDBRestore

Description

AWSEC2-SQLServerDBRestore Runbook 會將存放在 Amazon S3 中的 Microsoft SQL Server 資料庫備份還原至在 Amazon Elastic Compute Cloud (EC2) Linux 執行個體上執行的 SQL Server 2017。您可以提供自己的執行 SQL Server 2017 Linux 的 EC2 執行個體。如果未提供 EC2 執行個體，自動化會啟動並設定具有 SQL Server 2017 的新 Ubuntu 16.04 EC2 執行個體。自動化支援還原完整、差異和交易日誌備份。此自動化接受多個資料庫備份檔案，並可自動還原所提供檔案中每個資料庫最新有效的備份。

若要將現場部署 SQL Server 資料庫的備份和還原自動化至執行 SQL Server 2017 Linux 的 EC2 執行個體，您可以使用 AWS 簽署的 PowerShell 指令碼 [MigrateSQLServerToEC2Linux](#)。

Important

此 Runbook 會在每次自動化執行時重設 SQL Server 伺服器管理員 (SA) 使用者密碼。自動化完成後，您必須先再次設定自己的 SA 使用者密碼，才能連線至 SQL Server 執行個體。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

先決條件

若要執行此自動化，您必須符合下列先決條件：

- 執行此自動化的 IAM 使用者或角色必須具有與 中所述許可連接的內嵌政策[所需的 IAM 許可](#)。
- 如果您提供自己的 EC2 執行個體：
 - 您提供的 EC2 執行個體必須是執行 Microsoft SQL Server 2017 的 Linux 執行個體。
 - 您提供的 EC2 執行個體必須使用已連接 AmazonSSMManagedInstanceCore 受管政策的 AWS Identity and Access Management (IAM) 執行個體設定檔進行設定。如需詳細資訊，請參閱[建立 Systems Manager 的 IAM 執行個體設定檔](#)。
 - SSM Agent 必須安裝在 EC2 執行個體上。如需詳細資訊，請參閱[在適用於 Linux 的 EC2 執行個體上安裝和設定 SSM Agent](#)。
 - EC2 執行個體必須有足夠的可用磁碟空間，才能下載和還原 SQL Server 備份。

限制

此自動化不支援還原至 Windows Server 的 EC2 執行個體上執行的 SQL Server。此自動化只能還原與 SQL Server Linux 2017 相容的資料庫備份。如需詳細資訊，請參閱[SQL Server 2017 在 Linux 上的版本和支援的功能](#)。

參數

此自動化具有下列參數：

- DatabaseNames

類型：字串

描述：(選用) 要還原之資料庫的名稱逗號分隔清單。

- DataDirectorySize

類型：字串

描述：(選用) SQL Server Data 目錄在新 EC2 執行個體上所需的磁碟區大小 (GiB)。

預設值：100

- KeyPair

類型：字串

描述：(選用) 建立新 EC2 執行個體時要使用的鍵組。

- IamInstanceProfileName

類型：字串

描述：(選用) 要連接到新 EC2 執行個體的 IAM 執行個體設定檔。IAM 執行個體設定檔必須連接 AmazonSSMManagedInstanceCore 受管政策。

- InstanceId

類型：字串

描述：(選用) 在 Linux 上執行 SQL Server 2017 的執行個體。如果未提供 InstanceId，自動化將使用提供的 InstanceType 和 SQLServerEdition 啟動新的 EC2 執行個體。

- InstanceType

類型：字串

描述：(選用) 要啟動之 EC2 執行個體的執行個體類型。

- IsS3PresignedUrl

類型：字串

描述：(選用) 如果 S3Input 是預先簽章的 S3 URL，請指出 yes。

預設值：否

有效值：是 | 否

- LogDirectorySize

類型：字串

描述：(選用) SQL Server Log 目錄在新 EC2 執行個體上所需的磁碟區大小 (GiB)。

預設值：100

- S3Input

類型：字串

描述：(必要) S3 儲存貯體名稱、S3 物件金鑰的逗號分隔清單，或包含要還原之 SQL 備份檔案的預先簽章 S3 URL 逗號分隔清單。

- SQLServerEdition

類型：字串

描述：(選用) 要在新建立的 EC2 執行個體上安裝的 SQL Server 2017 版本。

有效值：標準 | 企業 | Web | Express

- SubnetId

類型：字串

描述：(選用) 要啟動新 EC2 執行個體的子網路。子網路必須具有 AWS 服務的傳出連線。如果未提供 SubnetId 的值，自動化將使用預設子網路。

- TempDbDirectorySize

類型：字串

描述：(選用) SQL Server TempDB 目錄在新 EC2 執行個體上所需的磁碟區大小 (GiB)。

預設值：100

所需的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

```
{
  "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::ACCOUNTID:role/ROLENAME"
}
]
}

```

文件步驟

若要使用此自動化，請遵循適用於執行個體類型的步驟：

對於新的 EC2 執行個體：

1. `aws:executeAwsApi` - 在 Ubuntu 16.04 上擷取 SQL Server 2017 的 AMI ID。
2. `aws:runInstances` - 為 Linux 啟動新的 EC2 執行個體。
3. `aws:waitForAwsResourceProperty` - 等待新建立的 EC2 執行個體準備就緒。
4. `aws:executeAwsApi` - 如果執行個體尚未就緒，請重新啟動執行個體。
5. `aws:assertAwsResourceProperty` - 確認已安裝 SSM Agent。
6. `aws:runCommand` - 在 PowerShell 中執行 SQL Server 還原指令碼。

對於現有的 EC2 執行個體：

1. `aws:waitForAwsResourceProperty` - 確認 EC2 執行個體已就緒。
2. `aws:executeAwsApi` - 如果執行個體尚未就緒，請重新啟動執行個體。

3. `aws:assertAwsResourceProperty` - 確認已安裝 SSM Agent。
4. `aws:runCommand` - 在 PowerShell 中執行 SQL Server 還原指令碼。

輸出

`getInstance.InstanceId`

`restoreToNewInstance.Output`

`restoreToExistingInstance.Output`

AWSSupport-ActivateWindowsWithAmazonLicense

Description

AWSSupport-ActivateWindowsWithAmazonLicense Runbook Windows Server 會使用 Amazon 提供的授權來啟用的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。自動化會驗證並設定必要的金鑰管理服務作業系統設定，並嘗試啟用。這包括 Amazon 金鑰管理伺服器的作業系統路由，以及金鑰管理服務作業系統設定。將 `AllowOffline` 參數設定為 `true` 可讓自動化成功鎖定不受管理的執行個體 AWS Systems Manager，但需要停止和啟動執行個體。

Note

此 Runbook 不能用於自攜授權 (BYOL) 模型 Windows Server 執行個體。如需使用自有授權的詳細資訊，請參閱 [在 AWS 的 Microsoft 授權](#)。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AllowOffline

類型：字串

有效值：true | false

預設：false

描述：(選用) true 如果您允許離線 Windows 啟用修復，以防線上故障診斷失敗，或提供的執行個體不是受管執行個體，請將其設定為。

Important

離線方法需要所提供的 EC2 執行個體先停止再啟動。存放在執行個體存放磁碟區的資料會遺失。如果您不是使用彈性 IP，則公有 IP 位址會變更。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ForceActivation

類型：字串

有效值：true | false

預設：false

描述：(選用) true 如果您想要繼續，即使 Windows 已啟用，也請將其設定為。

- InstanceId

類型：字串

描述：(必要) 您的受管 Windows Server EC2 執行個體的 ID。

- SubnetId

類型：字串

預設：CreateNewVPC

描述：(選用) 僅限離線 - 用於執行離線疑難排解的 EC2Rescue 執行個體之子網路 ID。使用 SelectedInstanceSubnet 來使用與執行個體相同的子網路，或使用 CreateNewVPC 來建立新的 VPC。重要：子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

我們建議接收命令的 EC2 執行個體具有連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。您必須擁有至少 ssm:StartAutomationExecution 和 ssm:SendCommand 才能執行自動化並將命令傳送至執行個體，以及 ssm:GetAutomationExecution，才能讀取自動化輸出。如需離線修復，請參閱 所需的許可AWSsupport-StartEC2RescueWorkflow。

文件步驟

1. aws:assertAwsResourceProperty - 檢查提供的執行個體平台是 Windows。
2. aws:assertAwsResourceProperty - 確認提供的執行個體是受管執行個體：
 - a. (線上啟用修正) 如果輸入執行個體是受管執行個體，則執行 aws:runCommand 以執行 PowerShell 指令碼，嘗試修正 Windows 啟用。
 - b. (離線啟用修正) 如果輸入執行個體不是受管執行個體：
 - i. aws:assertAwsResourceProperty - 確認AllowOffline旗標設定為 true。如果是這樣，離線修正會開始，否則自動化會結束。
 - ii. aws:executeAutomation - AWSsupport-StartEC2RescueWorkflow使用 Windows 啟用離線修正指令碼叫用。指令碼使用 EC2Config 或 EC2Launch，取決於作業系統版本。
 - iii. aws:executeAwsApi - 從 讀取結果AWSsupport-StartEC2RescueWorkflow。

輸出

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Description

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook 會分析從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或彈性網路介面到 AWS 服務 端點的連線能力。不支援 IPv6。Runbook 會使用您為 ServiceEndpoint 參數指定的值來分析對端點的連線。如果在您的 VPC 中找不到 AWS PrivateLink 端點，則 Runbook 會使用目前 服務公有 IP 地址 AWS 區域。此自動化使用來自 Amazon Virtual Private Cloud 的 Reachability Analyzer。如需詳細資訊，請參閱 [Reachability Analyzer 中的什麼是 Reachability Analyzer？](#)。

此自動化會檢查下列項目：

- 檢查您的虛擬私有雲端 (VPC) 是否已設定為使用 Amazon 提供的 DNS 伺服器。
- 檢查您指定之 的 VPC AWS 服務 中是否存在 AWS PrivateLink 端點。如果找到端點，自動化會驗證privateDns屬性是否已開啟。
- 檢查 AWS PrivateLink 端點是否使用預設端點政策。

考量

- 每個來源和目的地之間的分析執行都會向您收取費用。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。
- 在自動化期間，會建立網路洞見路徑和網路洞見分析。如果自動化成功完成，則 Runbook 會刪除這些資源。如果清除步驟失敗，則 Runbook 不會刪除網路洞見路徑，您將需要手動刪除它。如果您不手動刪除網路洞見路徑，它會繼續計入您的配額 AWS 帳戶。如需 Reachability Analyzer 配額的詳細資訊，請參閱 [Reachability Analyzer 中的 Reachability Analyzer 配額](#)。
- 即使 Reachability Analyzer 傳回，使用代理、本機 DNS 解析程式或主機檔案等作業系統層級組態仍可能會影響連線能力PASS。
- 檢閱 Reachability Analyzer 執行的所有檢查評估。如果任何檢查傳回的狀態為 FAIL，即使整體連線能力檢查傳回狀態為，仍可能會影響連線能力PASS。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 來源

類型：字串

描述：(必要) Amazon EC2 執行個體的 ID 或您要從中分析可連線性的網路界面。

- ServiceEndpoint

類型：字串

描述：(必要) 您要分析可連線性之服務端點的主機名稱。

- RetainVpcReachabilityAnalysis

類型：字串

預設：false

描述：(選用) 判斷是否保留網路洞見路徑和建立的相關分析。根據預設，用於分析可連線性的資源會在成功分析後刪除。如果您選擇保留分析，則 Runbook 不會刪除分析，而且您可以在 Amazon VPC 主控台中將其視覺化。自動化輸出中提供了主控台連結。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

1. `aws:executeScript` : 嘗試解析主機名稱來驗證服務端點。
2. `aws:executeScript` : 收集 VPC 和子網路的詳細資訊。
3. `aws:executeScript` : 評估 VPC 的 DNS 組態。
4. `aws:executeScript` : 評估 VPC 端點檢查。
5. `aws:executeScript` : 尋找網際網路閘道以連線至公有服務端點。
6. `aws:executeScript` : 決定用於可連線性分析的目的地。
7. `aws:executeScript` : 使用 Reachability Analyzer 分析來源到端點的可連線性，並在分析成功時清除資源。
8. `aws:executeScript` : 產生連線能力評估報告。
9. `aws:executeScript` : 在 JSON 中產生輸出。

輸出

- `generateReport.EvalReport` - 自動化以文字格式執行的檢查結果。
- `generateJsonOutput.Output` - JSON 格式結果的最小版本。

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Description

Runbook AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 會自動從 Intel 支援的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體遷移至同等 AMD 支援的執行個體類型。此 Runbook 支援在 Nitro 系統上建置的一般用途 (M)、爆量一般用途 (T)、運算最佳化 (C) 和記憶體最佳化 (R) 執行個體。此 Runbook 可用於非由 Systems Manager 管理的執行個體。

為了降低資料遺失和停機的潛在風險，Runbook 會檢查執行個體的停止行為、執行個體是否位於 Amazon EC2 Auto Scaling 群組中、執行個體的運作狀態，以及相同可用區域中是否提供同等的 AMD 驅動執行個體類型。根據預設，如果連接執行個體存放區磁碟區，或如果執行個體是 AWS CloudFormation 堆疊的一部分，此 Runbook 不會變更執行個體類型。如果您想要變更此行為，請將 `yes` 為 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 參數指定。

Important

存取 AWSPremiumSupport-* Runbook 需要企業或商業支援訂閱。如需詳細資訊，請參閱 [比較 支援 計劃](#)。

考量

- 建議您先備份執行個體，再使用此 Runbook。
- 變更執行個體類型需要 Runbook 來停止執行個體。當執行個體停止時，存放在 RAM 或執行個體存放區磁碟區中的任何資料都會遺失，並會釋出自動公有 IPv4 地址。如需詳細資訊，請參閱 [停止和啟動執行個體](#)。
- 如果您未指定 `TargetInstanceType` 參數的值，則 Runbook 會嘗試識別相同執行個體系列中的虛擬 CPUs 和記憶體等價 AMD 執行個體。如果 Runbook 無法識別同等的 AMD 執行個體類型，則會結束。
- 透過使用 `DryRun` 選項，您可以擷取同等的 AMD 執行個體類型，並驗證需求，而不需要實際變更執行個體類型。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 確認

類型：字串

描述：(必要) 輸入 yes 以確認您的目標執行個體在執行時將會停止。

- InstanceId

類型：字串

描述：(必要) 您要變更其類型的 Amazon EC2 執行個體 ID。

- TargetInstanceType

類型：字串

預設：自動

描述：(選用) 您要變更執行個體的 AMD 執行個體類型。automatic 預設值使用虛擬 CPUs 和記憶體的同等執行個體類型。例如，m5.large 會變更為 m5a.large。

- AllowInstanceStoreInstances

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果您指定 `yes`，則 Runbook 會在已連接執行個體存放磁碟區的執行個體上執行。

- `AllowCloudFormationInstances`

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果設定為 `yes`，則 Runbook 會在屬於 AWS CloudFormation 堆疊的執行個體上執行。

- `AllowCrossGeneration`

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果設定為 `yes`，則 Runbook 會嘗試尋找相同執行個體系列中最新的同等 AMD 執行個體類型。

- `DryRun`

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果設為 `yes`，則 Runbook 會傳回同等的 AMD 執行個體類型，並驗證遷移需求，而不需要變更執行個體類型。

- `SleepWait`

類型：字串

預設：PT3S

描述：(選用) 啟動新的自動化之前，執行手冊應該等待的時間。您為此參數提供的值必須符合 ISO 8601 標準。如需建立 ISO 8601 字串的詳細資訊，請參閱[格式化 Systems Manager 的日期和時間字串](#)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:GetInstanceTypesFromInstanceRequirements`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeTags`
- `ec2:ModifyInstanceAttribute`
- `ec2:StartInstances`
- `ec2:StopInstances`

文件步驟

1. `aws:assertAwsResourceProperty`：確認目標 Amazon EC2 執行個體的狀態為 `running`、`pending`、`stopped`或`stopping`。否則，自動化會結束。
2. `aws:executeAwsApi`：從目標 Amazon EC2 執行個體收集屬性。
3. `aws:branch`：根據 Amazon EC2 執行個體的狀態配置自動化。
 - a. 如果為 `stopped`或`stopping`，自動化會持續執行，`aws:waitForAwsResourceProperty`直到 Amazon EC2 執行個體完全停止為止。
 - b. 如果 `running`或`pending`，自動化會執行，`aws:waitForAwsResourceProperty`直到 Amazon EC2 執行個體通過狀態檢查為止。
4. `aws:assertAwsResourceProperty`：檢查`aws:autoscaling:groupName`標籤是否已套用，以確認 Amazon EC2 執行個體不屬於 Auto Scaling 群組。
5. `aws:executeAwsApi`：收集目前的執行個體類型屬性，以尋找同等的 AMD 執行個體類型。
6. `aws:assertAwsResourceProperty`：確認 AWS Marketplace 產品代碼未與 Amazon EC2 執行個體相關聯。有些產品並非所有執行個體類型都提供。

7. `aws:branch`：根據您是否希望自動化檢查 Amazon EC2 執行個體是否為 AWS CloudFormation 堆疊的一部分，來配置自動化
 - a. 如果 `aws:cloudformation:stack-name` 標籤套用至執行個體，自動化會執行 `aws:assertAwsResourceProperty` 以確認執行個體不是 AWS CloudFormation 堆疊的一部分。
8. `aws:branch`：根據執行個體根磁碟區類型是否為 Amazon Elastic Block Store (Amazon EBS) 來配置自動化。
9. `aws:assertAwsResourceProperty`：確認執行個體關閉行為是 `stop`，而不是 `terminate`。
10. `aws:executeScript`：確認此 Runbook 只有一個自動化目標為目前的執行個體。如果另一個自動化已在以相同執行個體為目標進行，則會傳回錯誤並結束。
11. `aws:executeAwsApi`：傳回具有相同記憶體和 vCPUs 數量的 AMD 執行個體類型清單。
12. `aws:executeScript`：檢查是否支援目前的執行個體類型，並傳回其同等的 AMD 執行個體類型。如果沒有同等項目，則自動化會結束。
13. `aws:executeScript`：確認 AMD 執行個體類型可在相同的可用區域中使用，並驗證提供的 IAM 許可。
14. `aws:branch`：根據 `DryRun` 參數值是否為 `yes` 來配置自動化。
15. `aws:branch`：檢查原始執行個體和目標執行個體類型是否相同。如果它們相同，自動化就會結束。
16. `aws:executeAwsApi`：取得目前的執行個體狀態。
17. `aws:changeInstanceState`：停止 Amazon EC2 執行個體。
18. `aws:changeInstanceState`：如果執行個體卡在停止狀態，則強制停止執行個體。
19. `aws:executeAwsApi`：將執行個體類型變更為目標 AMD 執行個體類型。
20. `aws:sleep`：在變更執行個體類型以獲得最終一致性後等待 3 秒。
21. `aws:branch`：根據先前的執行個體狀態配置自動化。如果是 `running`，執行個體會啟動。
 - a. `aws:changeInstanceState`：如果在變更執行個體類型之前執行 Amazon EC2 執行個體，則啟動該執行個體。
 - b. `aws:waitForAwsResourceProperty`：等待 Amazon EC2 執行個體通過狀態檢查。如果執行個體未通過狀態檢查，執行個體會變更回其原始執行個體類型。
 - i. `aws:changeInstanceState`：在將 Amazon EC2 執行個體變更為其原始執行個體類型之前，先停止該執行個體。
 - ii. `aws:changeInstanceState`：強制 Amazon EC2 執行個體先停止，再將其變更為原始執行個體類型，以防卡在停止狀態。

- iii. `aws:executeAwsApi` : 將 Amazon EC2 執行個體變更為其原始類型。
- iv. `aws:sleep` : 在變更執行個體類型以獲得最終一致性後等待 3 秒。
- v. `aws:changeInstanceState` : 如果在變更執行個體類型之前執行 Amazon EC2 執行個體，則啟動該執行個體。
- vi. `aws:waitForAwsResourceProperty` : 等待 Amazon EC2 執行個體通過狀態檢查。

`22aws:sleep` : 等待 再結束 Runbook。

AWSSupport-CheckXenToNitroMigrationRequirements

Description

AWSSupport-CheckXenToNitroMigrationRequirements Runbook 會驗證 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體是否符合將執行個體類型從 Xen 類型執行個體成功變更為 Nitro 型執行個體類型的先決條件。此自動化會檢查下列項目：

- 根裝置是 Amazon Elastic Block Store (Amazon EBS) 磁碟區。
- `enaSupport` 屬性已啟用。
- ENA 模組安裝在執行個體上。
- NVMe 模組安裝在執行個體上。如果是，則已安裝模組，且指令碼會驗證模組是否已載入 `initramfs` 映像中。
- 使用裝置名稱來分析 `/etc/fstab` 和尋找要掛載的區塊型裝置。
- 根據預設，決定作業系統 (OS) 是否使用可預測的網路介面名稱。

此 Runbook 支援下列作業系統：

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

預設：false

描述：（必要）在遷移至 Nitro 型執行個體類型之前，您要檢查其先決條件的 Amazon EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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:DescribeInstancesTypes`

文件步驟

- `aws:executeAwsApi` - 收集執行個體的詳細資訊。
- `aws:executeAwsApi` - 收集執行個體 Hypervisor 的相關資訊。
- `aws:branch` - 根據目標執行個體是否已執行 Nitro 型執行個體類型進行分支。
- `aws:branch` - 檢查 Nitro 型執行個體是否支援執行個體的作業系統。
- `aws:assertAwsResourceProperty` - 驗證您指定的執行個體是由 Systems Manager 管理，且狀態為 Online。
- `aws:branch` - 根據執行個體的根裝置是否為 Amazon EBS 磁碟區進行分支。
- `aws:branch` - 根據執行個體是否啟用 ENA 屬性進行分支。
- `aws:runCommand` - 檢查執行個體上的 ENA 驅動程式。
- `aws:runCommand` - 檢查執行個體上的 NVMe 驅動程式。
- `aws:runCommand` - 檢查fstab檔案是否有無法辨識的格式。
- `aws:runCommand` - 檢查執行個體上的可預測界面名稱組態。
- `aws:executeScript` - 根據先前的步驟產生輸出。

輸出

`finalOutput.output` - 自動化執行的檢查結果。

AWSSupport-ConfigureEC2Metadata

Description

此 Runbook 可協助您設定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的執行個體中繼資料服務 (IMDS) 選項。使用此 Runbook，您可以設定下列項目：

- 強制執行 IMDSv2 用於執行個體中繼資料。
- 設定 `HttpPutResponseHopLimit` 值。
- 允許或拒絕執行個體中繼資料存取。

如需執行個體中繼資料的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[設定執行個體中繼資料服務](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `EnforceIMDSv2`

類型：字串

有效值：必要 | 選用

預設：選用

描述：（選用）強制執行 IMDSv2。如果您選擇 `required`，Amazon EC2 執行個體只會使用 IMDSv2。如果您選擇 `optional`，您可以在 IMDSv1 和 IMDSv2 之間選擇中繼資料存取。

 Important

如果您強制執行 IMDSv2，使用 IMDSv1 的應用程式可能無法正常運作。在強制執行 IMDSv2 之前，請確定您使用 IMDS 的應用程式已升級至支援 IMDSv2 的版本。如需執行個體中繼資料服務第 2 版 (IMDSv2) 的相關資訊，請參閱 [《Amazon EC2 使用者指南》中的設定執行個體中繼資料服務](#)。Amazon EC2

- `HttpPutResponseHopLimit`

類型：整數

有效值：0-64

預設：0

描述：（選用）執行個體中繼資料請求所需的 HTTP PUT 回應跳轉限制值 (1-64)。此值控制 PUT 回應可以周遊的躍點數量。若要防止回應在執行個體之外移動，1 請為 參數值指定。

- `InstanceId`

類型：字串

描述：（必要）您要設定其中繼資料設定的 Amazon EC2 執行個體 ID。

- `MetadataAccess`

類型：字串

有效值：已啟用 | 已停用

預設：啟用

描述：（選用）允許或拒絕 Amazon EC2 執行個體中的執行個體中繼資料存取。如果您指定 `disabled`，則會忽略所有其他參數，並拒絕執行個體的中繼資料存取。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

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

文件步驟

1. branchOnMetadataAccess - 根據 MetadataAccess 參數的值分支自動化。
2. disableMetadataAccess - 呼叫 ModifyInstanceMetadataOptions API 動作以停用中繼資料端點存取。
3. branchOnHttpPutResponseHopLimit - 根據HttpPutResponseHopLimit參數值分支自動化。
4. maintainHopLimitAndConfigureImdsVersion - 如果 HttpPutResponseHopLimit為 0，則維持目前的跳轉限制並變更其他中繼資料選項。
5. waitBeforeAssertingIMDSv2State - 在宣告 IMDSv2 狀態之前等待 30 秒。
6. setHopLimitAndConfigureImdsVersion - 如果 HttpPutResponseHopLimit大於 0，則使用指定的輸入參數設定中繼資料選項。
7. waitBeforeAssertingHopLimit - 在宣告中繼資料選項之前等待 30 秒。
8. assertHopLimit - 宣告 HttpPutResponseHopLimit 屬性設定為您指定的值。
9. branchVerificationOnIMDSv2Option - 根據EnforceIMDSv2參數值進行分支驗證。
- 10.assertIMDSv2IsOptional - 宣告HttpTokens值設定為 optional。
- 11.assertIMDSv2IsEnforced - Asserts HttpTokens值設定為 required。
- 12.waitBeforeAssertingMetadataState - 在宣告中繼資料狀態已停用之前等待 30 秒。
- 13.assertMetadatalIsDisabled - Asserts 中繼資料為 disabled。
- 14.describeMetadataOptions - 套用您指定的變更後，取得中繼資料選項。

輸出

describeMetadataOptions.State

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

AWSSupport-ContainEC2Instance

Description

AWSSupport-ContainEC2Instance Runbook 為文章中概述的程序提供自動化解決方案。[遇到可能遭到入侵或可疑的情況時，如何隔離 Amazon EC2 執行個體？](#) 自動化分支取決於您指定的值。

如何運作？

此 Automation Runbook 透過一系列協調步驟AWSSupport-ContainEC2Instance執行 Amazon EC2 執行個體的網路遏制。在Contain模式下執行時，它會先驗證輸入參數，並檢查執行個體是否未終止。然後，它會將目前的安全群組組態備份到 Amazon S3 儲存貯體，以供稍後還原。Runbook 會建立兩個安全群組：臨時「所有存取」安全群組和最終「容器」安全群組。它會逐漸將執行個體的網路界面從其原始安全群組轉移到全存取安全群組，最後轉移到遏制安全群組。如果指定，它會建立執行個體的未加密和加密AMI備份。對於 Auto Scaling 群組中的執行個體，它會處理必要的 Auto Scaling 群組修改，並使執行個體進入待命狀態。在Release模式下執行時，它會使用 Amazon S3 的備份設定，將執行個體還原至其原始網路組態。Runbook 支援 DryRun 參數，可在不進行實際變更的情況下預覽動作，並在整個遏制和發佈工作流程中包含全面的錯誤處理和報告機制。

Important

- 此 Runbook 會執行需要提升權限的各種操作，例如修改安全群組、建立 AMI，以及與 Auto Scaling 群組互動。這些動作可能會導致權限提升或影響您帳戶中的其他工作負載。您應該檢閱授予 AutomationAssumeRole 參數所指定角色的許可，並確保這些許可適用於預期的使用案例。如需 IAM 許可的詳細資訊，請參閱下列 AWS 文件：[AWS Identity and Access Management \(IAM\) PermissionsAWS Systems Manager Automation Permissions](#)。
- 此 Runbook 會執行可能導致工作負載無法使用或中斷的變動動作。具體而言，它會修改與目標 Amazon EC2 執行個體相關聯的安全群組，這可能會影響網路連線。此外，如果執行個體是 Auto Scaling 群組的一部分，Runbook 可能會修改群組的組態，這可能會影響其擴展行為。
- 在遏制過程中，此 Runbook 會建立其他資源，例如安全群組和 AMI。雖然這些資源已加上標籤以供識別，但您應該知道它們的建立，並確保在遏制程序完成後進行適當的清除或管理。

- 如果 Action 參數設定為 Release，此 Runbook 會嘗試將 Amazon EC2 執行個體的組態還原為其原始狀態。不過，還原程序可能會失敗，使執行個體處於不一致的狀態。Runbook 提供在發生此類失敗時手動還原的說明，但您應該準備好在還原過程中處理潛在問題。

建議您徹底檢閱 Runbook、了解其潛在影響，並在非生產環境中進行測試，然後再在您的生產環境中執行。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- autoscaling : CreateOrUpdateTags
- autoscaling : DeleteTags
- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeAutoScalingInstances
- autoscaling : DescribeTags
- 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:DescribeImages
- ec2:DescribeInstances
- ec2 : DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTags
- ec2:ModifyNetworkInterfaceAttribute
- ec2:RevokeSecurityGroupEgress
- kms:創建權限
- kms:描述金鑰
- 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

範例政策：

```
{
  "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": "*"
}
]
}
```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-ContainEC2Instance](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：

- 描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。
- 類型：AWS::IAM::Role::Arn
- 動作 (必要)：
 - 描述：(必要) 選取 Contain 以隔離 Amazon EC2 執行個體 Restore，或嘗試從先前的備份還原 Amazon EC2 執行個體組態原始組態。
 - 類型：字串
 - 允許模式：Contain|Restore
- DryRun (選用)：
 - 描述：(選用) 設為 true，自動化不會執行任何命令，而是會報告嘗試執行的動作，詳細說明每個步驟。預設值：true。
 - 類型：布林值
 - 允許的值：true|false
- CreateAMIBackup (選用)：
 - 描述：(選用) 設定為 true，Amazon EC2 執行個體 AMI 的會在執行遏制動作之前建立。
 - 類型：布林值
 - 允許的值：true|false
- KmsKey (選用)：
 - 描述：(選用) 將用於建立目標 Amazon EC2 執行個體加密 AMI 的 AWS KMS 金鑰 ID。預設值設為 alias/aws/ebs。
 - 類型：字串
 - 允許模式：^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{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 (條件式)：
 - 描述：(條件式) Amazon Amazon S3 儲存貯體，以在 Action 為時上傳組態，Contain 或在 Action 為時還原組態 Release。注意：如果帳戶中不存在提供的儲存貯體，自動化將代表您建立 Amazon S3 儲存貯體。

- TagIdentifier (選用) :
 - 描述 : (選用) 格式的標籤, Key=BatchId, Value=78925將在遏制工作流程期間新增至此 Runbook 建立或修改 AWS 的資源。此標籤可用於識別和管理在遏制過程中相關聯的資源。在還原工作流程期間, 此參數指定的標籤將從 資源中移除。注意: 標籤鍵和值區分大小寫。
 - 類型: 字串
 - 允許模式: `^$|^([Kk][Ee][Yy]=[\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{0,128})$`
- BackupS3BucketAccess (條件式) :
 - 描述 : (條件式) 在執行遏制動作後, 允許存取備份 Amazon S3 儲存貯體的 IAM 使用者或角色 ARN。當 Action為 時, 此參數為必要Contain。在 AutomationAssumeRole或 不存在的情況下, 正在執行自動化的使用者會自動新增至清單中。
 - 類型: 字串
 - 允許模式: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- IngressTrafficRules (選用) :
 - 描述 : (選用) 以逗號分隔的安全群組輸入規則對應, 其中包含[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]要套用至 Amazon EC2 執行個體的 Cidr、IpProtocol、FromPort 和 ToPort 格式。如果未提供任何規則, 則沒有任何輸入規則的安全群組將連接到 Amazon EC2 執行個體, 有效地隔離它與任何傳入流量。
 - 類型: MapList
 - 允許模式: `^\\{\\}\\$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"\\}\\}`
- EgressTrafficRules (選用) :
 - 描述 : (選用) 以逗號分隔的安全群組輸出規則對應, 其中包含[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]要套用至 Amazon EC2 執行個體的 Cidr、IpProtocol、FromPort 和 ToPort 格式。如果未提供任何規則, 則沒有任何輸出規則的安全群組將連接到 Amazon EC2 執行個體, 有效地防止所有傳出流量。
 - 類型: MapList

- 允許模式：`^\\{\\}$|^\\{"Cidr\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"IpProtocol\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"FromPort\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"ToPort\\":\\"[\\x00-\\x7F+]{0,255}\\"}\\}`
 - BackupS3KeyName (選用) :
 - 描述：(選用) 如果 Action 設定為 Restore，這會指定自動化用來嘗試還原目標 Amazon EC2 執行個體組態的 Amazon S3 金鑰。Amazon EC2 Amazon S3 金鑰通常遵循此格式：`{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json`。金鑰可從先前的遏制自動化執行的輸出取得。
 - 類型：字串
 - 允許模式：`^[a-zA-Z0-9\\.\\-\\_\\\\!*'()]/]{0,1024}$`
4. 選取執行。
 5. 自動化會啟動。
 6. 文件會執行下列步驟：
 - ValidateRequiredInputs

驗證是否已提供所有必要的輸入。
 - AssertInstancesNotTerminated

檢查目標 Amazon EC2 執行個體是否未終止 (已刪除)。
 - GetAutoScalingInstanceInfo

如果目標 Amazon EC2 執行個體是 Auto Scaling 群組的一部分，則取得 Amazon EC2 執行個體生命週期和群組名稱。
 - CheckBackupS3BucketName

檢查目標 Amazon S3 儲存貯體是否可能授予 read 或 write 公開存取其物件。如果儲存貯體不存在，則會建立新的 Amazon S3 儲存 BackupS3BucketName 貯體。
 - BranchOnActionAndMode

根據輸入參數 Action 和 分支自動化 DryRun。
 - BranchOnAutoScalingGroupMembership

根據目標 Amazon EC2 執行個體是否屬於 Auto Scaling 群組及其生命週期狀態，來配置自動化。
 - DescribeAutoScalingGroups

取得和存放相關聯的 Amazon EC2 Auto Scaling 群組組態。

- `ModifyAutoScalingGroup`

修改遏制動作的相關 Amazon EC2 Auto Scaling 群組組態，將 Amazon EC2 執行個體設定為 Standby 狀態並調整 Auto Scaling 群組 `MinSize` 容量。

- `BackupInstanceSecurityGroups`

取得和存放目標 Amazon EC2 執行個體安全群組的組態。

- `CreateAllAccessSecurityGroup`

建立臨時安全群組，允許取代目標 Amazon EC2 執行個體安全群組的所有輸入流量。

- `CreateContainmentSecurityGroup`

使用指定的輸入和輸出規則建立限制性遏制安全群組，並將暫時全存取群組取代為該群組。

- `BranchOnCreateAMIBackup`

根據 `CreateAMIBackup` 輸入參數配置自動化。

- `AssertSourceInstanceRootVolumelsEbs`

檢查目標 Amazon EC2 執行個體根磁碟區是否為 Amazon EBS。

- `CreateImage`

建立目標 Amazon EC2 執行個體 AMI 的。

- `RestoreInstanceConfiguration`

從備份還原目標 Amazon EC2 執行個體組態。

- `ReportContain`

輸出遏制動作的試轉詳細資訊。

- `ReportRestore`

輸出還原動作的試轉詳細資訊。

- `ReportRestoreFailure`

提供在還原工作流程失敗案例期間還原目標 Amazon EC2 執行個體原始組態的指示。

- `ReportContainmentFailure`

提供在遏制工作流程失敗情況下還原目標 Amazon EC2 執行個體原始組態的指示。

- `FinalOutput`

輸出遏制動作的詳細資訊。

7. 執行完成後，請檢閱輸出區段以取得執行的詳細結果：

- `FinalOutput.Output`

當 `DryRun` 設定為 `False` 時，輸出此 Runbook 所執行之遏制動作的詳細資訊。

- `RestoreInstanceConfiguration.Output`

當 `DryRun` 設定為 `False` 時，輸出此 Runbook 執行的還原動作。

- `ReportContain.Output`

當 `DryRun` 設定為 `True` 時，輸出此 Runbook 所執行之遏制動作的詳細資訊。

- `ReportRestore.Output`

將 `DryRun` 設定為 `True` 時，輸出此 Runbook 所執行還原動作的詳細資訊。

- `ReportContainmentFailure.Output`

提供在遏制工作流程失敗情況下還原目標 Amazon EC2 執行個體原始組態的指示。

- `ReportRestoreFailure.Output`

提供在還原工作流程失敗案例期間還原目標 Amazon EC2 執行個體原始組態的指示。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行簡易自動化](#)
- [設定自動化](#)
- [支援自動化工作流程](#)

AWSSupport-CopyEC2Instance

Description

AWSSupport-CopyEC2Instance Runbook 為 知識中心文章中概述的程序提供自動化解決方案 [如何將 EC2 執行個體移至另一個子網路、可用區域或 VPC？](#) 自動化分支取決於您為 `Region` 和 `SubnetId` 參數指定的值。

如果您為 SubnetId 參數指定值，但不是 Region 參數的值，自動化會建立目標執行個體的 Amazon Machine Image(AMI)，並從您指定的子網路AMI中的 啟動新的執行個體。

如果您為 SubnetId 參數和 Region 參數指定值，自動化會建立目標執行個體AMI的，將 AMI 複製到 AWS 區域 您指定的，並從您指定的子網路AMI中的 啟動新的執行個體。

如果您為 Region 參數指定值，但不是 SubnetId 參數的值，自動化會建立目標執行個體AMI的，將 AMI 複製到您指定的區域，並從目的地AMI區域中虛擬私有雲端 (VPC) 的預設子網路中的 啟動新的執行個體。

如果未指定 Region或 SubnetId 參數的值，自動化會建立目標執行個體AMI的，並從 VPC 預設子網路AMI中的 啟動新的執行個體。

若要AMI將 複製到不同的區域，您必須提供 AutomationAssumeRole 參數的值。如果自動化在waitForAvailableDestinationAmi步驟期間逾時，則 AMI可能仍在複製。如果是這種情況，您可以等待複製完成，並手動啟動執行個體。

執行此自動化之前，請注意下列事項：

- AMI是以 Amazon Elastic Block Store (Amazon EBS) 快照為基礎。對於沒有先前快照的大型檔案系統，AMI建立可能需要幾個小時。若要縮短AMI建立時間，請在建立 之前建立 Amazon EBS 快照 AMI。
- 建立 AMI不會為執行個體上的執行個體存放磁碟區建立快照。如需將執行個體存放磁碟區備份至 Amazon EBS 的資訊，請參閱[如何將 Amazon EC2 執行個體上的執行個體存放磁碟區備份至 Amazon EBS ?](#)
- 新的 Amazon EC2 執行個體具有不同的私有 IPv4 或公有 IPv6 IP 地址。您必須使用指派給新執行個體的新 IP 地址，更新舊 IP 地址（例如，在 DNS 項目中）的所有參考。如果您在來源執行個體上使用彈性 IP 地址，請務必將其連接至新的執行個體。
- 當複製啟動並嘗試聯絡網域時，可能會發生網域安全識別符 (SID) 衝突問題。擷取 AMI 之前，請使用 Sysprep 或從網域移除網域加入的執行個體，以防止衝突問題。如需詳細資訊，請參閱[如何使用 Sysprep 來建立和安裝自訂可重複使用AMIs ?](#)

執行此自動化（主控台）

Important

我們不建議使用此 Runbook 複製 Microsoft Active Directory 網域控制站執行個體。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 您要複製的執行個體 ID。

- KeyPair

類型：字串

描述：(選用) 您要與新複製的執行個體建立關聯的金鑰對。如果您要將執行個體複製到不同的區域，請確定金鑰對存在於指定的區域中。

- 區域

類型：字串

描述：(選用) 您要複製執行個體的區域。如果您為此參數指定值，但未指定 SubnetId 和 SecurityGroupIds 參數的值，自動化會嘗試在預設 VPC 中以預設安全群組啟動執行個體。如果在目的地區域中啟用 EC2-Classic，啟動將會失敗。

- SubnetId

類型：字串

描述：(選用) 您要複製執行個體的子網路 ID。如果在目的地區域中啟用 EC2-Classic，您必須為此參數提供值。

- InstanceType

類型：字串

描述：(選用) 複製的執行個體類型應啟動為。如果您未指定此參數的值，則會使用來源執行個體類型。如果執行個體複製到的區域中不支援來源執行個體類型，則自動化會失敗。

- SecurityGroupIds

類型：字串

描述：(選用) 您希望與複製的執行個體建立關聯的逗號分隔的安全群組 IDs 清單。如果您未指定此參數的值，且執行個體未複製到其他區域，則會使用與來源執行個體相關聯的安全群組。如果您要將執行個體複製到不同的區域，則會使用目的地區域中預設 VPC 的預設安全群組。

- KeepImageSourceRegion

類型：布林值

有效值：true | false

預設：true

描述：(選用) 如果您true為此參數指定，自動化不會刪除來源執行個體AMI的。如果您false為此參數指定，自動化會取消註冊AMI並刪除相關聯的快照。

- KeepImageDestinationRegion

類型：布林值

有效值：true | false

預設：true

描述：(選用) 如果您true為此參數指定，自動化不會刪除AMI複製到您指定區域的。如果您false為此參數指定，自動化會取消註冊AMI並刪除相關聯的快照。

- NoRebootInstanceBeforeTakingImage

類型：布林值

有效值：true | false

預設：false

描述：(選用) 如果您true為此參數指定，則不會在建立之前重新啟動來源執行個體AMI。使用此選項時，無法保證所建立映像的檔案系統完整性。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:CreateImage
- ec2:DeleteSnapshot
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeImages
- ec2:RunInstances

如果您要將執行個體複製到不同的區域，您也需要下列許可。

- ec2:CopyImage

文件步驟

- describeOriginalInstanceDetails - 從要複製的執行個體收集詳細資訊。
- assertRootVolumeIsEbs - 檢查根磁碟區裝置類型是否為 ebs，如果不是，則結束自動化。
- evalInputParameters - 評估為輸入參數提供的值。
- createLocalAmi - 建立來源執行個體AMI的。
- tagLocalAmi - 標記在上一個步驟中AMI建立的。
- branchAssertRegionIsSame - 根據執行個體是在相同區域還是複製到不同區域而建立的分支。
- branchAssertSameRegionWithKeyPair - 根據是否為相同區域內複製之執行個體的 KeyPair 參數提供值而進行分支。
- sameRegionLaunchInstanceWithKeyPair - 使用您指定的金鑰對，從相同子網路或您指定的子網路中的來源執行個體AMI的 啟動 Amazon EC2 執行個體。

- `sameRegionLaunchInstanceWithoutKeyPair` - 從相同子網路或您指定的子網路中的來源執行個體 AMI 的 啟動 Amazon EC2 執行個體，而不需要金鑰對。
- `copyAmiToRegion` - AMI 將 複製到目的地區域。
- `waitForAvailableDestinationAmi` - 等待複製 AMI 的狀態變成 `available`。
- `destinationRegionLaunchInstance` - 使用複製的 啟動 Amazon EC2 執行個體 AMI。
- `branchAssertDestinationAmiToDelete` - 根據您為 `KeepImageDestinationRegion` 參數提供的值來分支。
- `deregisterDestinationAmiAndDeleteSnapshots` - 取消註冊複製的 AMI 並刪除相關聯的快照。
- `branchAssertSourceAmiToDelete` - 根據您為 `KeepImageSourceRegion` 參數提供的值來分支。
- `deregisterSourceAmiAndDeleteSnapshots` - 從來源執行個體取消註冊 AMI 建立的，並刪除相關聯的快照。
- `sleep` - 將自動化休眠 2 秒。這是終端機步驟。

輸出

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunchInstance.DestinationInstanceId`

AWSSupport-EnableWindowsEC2SerialConsole

Description

Runbook `AWSSupport-EnableWindowsEC2SerialConsole` 可協助您在 Amazon EC2 Windows 執行個體上啟用 Amazon EC2 序列主控台、特殊管理主控台 (SAC) 和開機選單。透過 Amazon Elastic Compute Cloud (Amazon EC2) 序列主控台功能，您可以存取 Amazon EC2 執行個體的序列連接埠，以針對開機、網路組態和其他問題進行疑難排解。Runbook 會自動在執行中狀態且由 管理的執行個體上啟用 功能 AWS Systems Manager，以及處於停止狀態或未由 管理的執行個體上啟用 功能所需的步驟 AWS Systems Manager。

如何運作？

`AWSSupport-EnableWindowsEC2SerialConsole` 自動化 Runbook 有助於在執行 Microsoft Windows Server 的 Amazon EC2 執行個體上啟用 SAC 和開機選單。對於處於執行狀態且由 管理的執行個體 AWS Systems Manager，Runbook 會執行 AWS Systems Manager Run Command PowerShell 指令碼，以啟用 SAC 和開機功能表。對於處於已停止狀態或未受 管理的執行個體 AWS

Systems Manager，Runbook 會使用 [AWSSupport-StartEC2RescueWorkflow](#) 來建立暫時 Amazon EC2 執行個體，以離線執行所需的變更。

如需詳細資訊，請參閱[適用於 Windows 執行個體的 Amazon EC2 序列主控台](#)。

Important

- 如果您在執行個體上啟用 SAC，依賴密碼擷取的 Amazon EC2 服務將無法從 Amazon EC2 主控台運作。如需詳細資訊，請參閱[使用 SAC 疑難排解您的 Windows 執行個體](#)。
- 若要設定對序列主控台的存取，您必須在帳戶層級授予序列主控台存取，然後設定 AWS Identity and Access Management (IAM) 政策來授予存取給使用者。您還必須在每個執行個體上設定以密碼為基礎的使用者，以便使用者可以使用序列主控台進行疑難排解。如需詳細資訊，請參閱[設定對 Amazon EC2 序列主控台的存取](#)。
- 若要查看您的帳戶是否已啟用序列主控台，請參閱[檢視序列主控台的帳戶存取狀態](#)。
- 序列主控台存取僅支援在 [Nitro 系統上建置的虛擬化執行個體](#)。

如需詳細資訊，請參閱 Amazon EC2 序列主控台[先決條件](#)。

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

```
{
  "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:${Partition}:ec2:${Region}:${AccountId}:instance/
${InstanceId}",
            "arn:${Partition}:ec2:${Region}:${AccountId}:volume/
${VolumeId}",
            "arn:${Partition}:iam::${AccountId}:instance-profile/
${InstanceProfileName}",
            "arn:${Partition}:ssm:${Region}::parameter/aws/service/*",
            "arn:${Partition}:ssm:${Region}::automation-definition/
AWSSupport-StartEC2RescueWorkflow:*",
            "arn:${Partition}:ssm:${Region}::document/AWS-
ConfigureAWSPackage",
            "arn:${Partition}:ssm:${Region}::document/AWS-
RunPowerShellScript"
        ]
    }

```

```

    },
    {
      "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": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ec2.amazonaws.com"
            ]
        }
    }
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 在 AWS Systems Manager 主控台 `AWSSupport-EnableWindowsEC2SerialConsole` 中導覽至。
2. 選擇 `Execute automation` (執行自動化)。
3. 針對輸入參數，輸入下列項目：
 - `InstanceId`：(必要)

您要啟用 Amazon EC2 序列主控台 (SAC) 和開機選單的 Amazon EC2 執行個體 ID。

- AutomationAssumeRole : (選用)

IAM 角色的 Amazon Resource Name (ARN) , 可讓 Systems Manager Automation 代表您執行動作。如果未指定角色 , Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- HelperInstanceType : (條件式)

Runbook 佈建的 Amazon EC2 執行個體類型 , 以設定離線執行個體的 Amazon EC2 序列主控台。

- HelperInstanceProfileName : (條件式)

協助程式執行個體的現有 IAM 執行個體設定檔名稱。如果您在處於停止狀態或未受管理的執行個體上啟用 SAC 和開機功能表 AWS Systems Manager , 這是必要的。如果未指定 IAM 執行個體描述檔 , 自動化會代表您建立一個。

- SubnetId : (條件式)

協助程式執行個體的字網路 ID。根據預設 , 它會使用所提供執行個體所在的相同子網路。

Important

如果您提供自訂子網路 , 它必須位於與 InstanceId 相同的可用區域 , 而且必須允許存取 Systems Manager 端點。只有在目標執行個體處於已停止狀態或未由管理時 , 才需要這樣做 AWS Systems Manager。

- CreateInstanceBackupBeforeScriptExecution : (選用)

指定 True 以建立 Amazon EC2 執行個體的 Amazon Machine Images (AMI) 備份 , 然後再啟用 SAC 和開機功能表。自動化完成之後 , AMI 會持續存在。您有責任保護存取或刪除 AMI。

- BackupAmazonMachineImagePrefix : (條件式)

Amazon Machine Image (AMI) 的字首 , 如果

CreateInstanceBackupBeforeScriptExecution 參數設定為 , 則會建立此字首 True。

Input parameters	
InstanceId (Required) The ID of Amazon EC2 instance that you want to enable EC2 serial console, Special Admin Console (SAC), and boot menu. Show interactive instance picker i-01234567890abcde0	
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. EC2SerialConsole-MinimumRole-AutomationAssumeRole-7inoDR7gFLT	HelperInstanceType (Conditional) The type of Amazon EC2 instance that the runbook provisions to configure EC2 serial console for an offline instance. t3.medium
SubnetId (Conditional) The subnet ID for a helper instance. By default, the same subnet where the provided instance resides is used. Important: If you provide a custom subnet, it must be in the same Availability Zone as InstanceId, and it must allow access to the Systems Manager endpoints. This is only required if the target instance is in "stopped" state or is not managed by AWS Systems Manager. SelectedInstanceSubnet	HelperInstanceProfileName (Conditional) The name of an existing IAM instance profile for the helper instance. If you are enabling SAC and boot menu on an instance that is in "stopped" state or not managed by AWS Systems Manager, this is required. If an IAM instance profile is not specified, the automation creates one on your behalf. String
CreateInstanceBackupBeforeScriptExecution (Optional) Specify "True" to create an Amazon Machine Images (AMI) backup of the EC2 instance before enabling SAC and boot menu. The AMI will persist after the automation completes. It is your responsibility to secure access to the AMI, or to delete it. True	BackupAmazonMachineImagePrefix (Conditional) A prefix for the Amazon Machine Image (AMI) that is created if the "CreateInstanceBackupBeforeScriptExecution" parameter is set to "True". AWSsupport

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- `CheckIfEc2SerialConsoleAccessEnabled`：

檢查帳戶層級是否已啟用 Amazon EC2 序列主控台存取。注意：預設不提供對序列主控台的存取。如需詳細資訊，請參閱[設定對 Amazon EC2 序列主控台的存取](#)。

- `CheckIfEc2InstanceIsWindows`：

如果目標執行個體平台是 Windows，則宣告。

- `GetInstanceType`：

擷取目標執行個體的執行個體類型。

- `CheckIfInstanceTypeIsNitro`：

檢查執行個體類型 Hypervisor 是否為 Nitro 型。序列主控台存取僅支援在 Nitro 系統上建置的虛擬化執行個體。

- `CheckIfInstanceIsInAutoScalingGroup`：

透過呼叫 `DescribeAutoScalingInstances` API 來檢查 Amazon EC2 執行個體是否屬於 Amazon EC2 Auto Scaling 群組。如果執行個體是 Amazon EC2 Auto Scaling 群組的一部分，它會確保 .NET 執行個體的 Porting Assistant 處於待命生命週期狀態。

- `WaitForEc2InstanceStateStablized`：

等待執行個體處於執行中或停止狀態。

- `GetEc2InstanceState`：

取得執行個體的目前狀態。

- `BranchOnEc2InstanceState`：

根據上一個步驟中擷取的執行個體狀態進行分支。如果執行個體狀態正在執行，則會前往 `CheckIfEc2InstanceIsManagedBySSM` 步驟，如果沒有，則會前往 `CheckIfHelperInstanceProfileIsProvided` 步驟。

- `CheckIfEc2InstanceIsManagedBySSM`：

檢查執行個體是否由 管理 AWS Systems Manager。如果受管，則 Runbook 會使用 PowerShell

- BranchOnPreEC2RescueBackup :

根據CreateInstanceBackupBeforeScriptExecution輸入參數的分支。

- CreateAmazonMachineImageBackup :

建立執行個體的 AMI 備份。

- EnableSACAndBootMenu :

執行 PowerShell Run Command 指令碼來啟用 SAC 和開機功能表。

- RebootInstance :

重新啟動 Amazon EC2 執行個體以套用組態。如果執行個體在線上並由 管理，這是最後一個步驟 AWS Systems Manager。

- CheckIfHelperInstanceProfilesProvided :

使用臨時 Amazon EC2 執行個體，在啟用 SAC 和離線開機選單之前，檢查HelperInstanceProfileName指定的是否存在。

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu :

當執行個體處於停止狀態或未由 管理時，執行 AWSSupport-StartEC2RescueWorkflow 以啟用 SAC 和開機功能表 AWS Systems Manager。

- GetExecutionDetails :

擷取備份和離線指令碼輸出的影像 ID。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- EnableSACAndBootMenu.Output:

EnableSACAndBootMenu 步驟中命令執行的輸出。

- GetExecutionDetails.OfflineScriptOutput:

在 RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu 步驟中執行的離線指令碼輸出。

- GetExecutionDetails.BackupBeforeScriptExecution:

如果CreateInstanceBackupBeforeScriptExecution輸入參數為 True，則拍攝的 AMI 備份的影像 ID。

由 執行和管理之執行個體的執行輸出 AWS Systems Manager

Outputs	
GetExecutionDetails.BackupBeforeScriptExecution No output available yet because the step is not successfully executed EnableSACAndBootMenu.Output The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully.	GetExecutionDetails.OfflineScriptOutput No output available yet because the step is not successfully executed

在 停止或未受 管理的執行個體上執行的輸出 AWS Systems Manager

Outputs	
EnableSACAndBootMenu.Output No output available yet because the step is not successfully executed GetExecutionDetails.OfflineScriptOutput Device xvdf mapped to D Offline Windows installation found in directory D:\Windows Windows Server 2016 Datacenter (10.0.14393.6522) BCD Store found in directory D:\Boot\BCD Detecting installed drivers EC2Rescue environment variables set EC2Rescue script variables set The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. Volume successfully set offline	GetExecutionDetails.BackupBeforeScriptExecution ami-09c33701932955dde

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSsupport-ExecuteEC2Rescue

Description

此 Runbook 使用 EC2Rescue工具來故障診斷，並盡可能修復 Linux 或 指定 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的常見連線問題Windows Server。不支援具有加密根磁碟區的執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- EC2RescueInstanceType

類型：字串

有效值：t2.small | t2.medium | t2.large

預設：t2.small

描述：(必要) 執行個體的 EC2 EC2Rescue 執行個體類型。建議大小：t2.small

- LogDestination

類型：字串

描述：(選用) 帳戶中您要上傳故障診斷日誌的 Amazon S3 儲存貯體名稱。請確認儲存貯體政策不會授予不必要的讀取/寫入許可給不需要存取所收集日誌的單位。

- SubnetId

類型：字串

預設：CreateNewVPC

描述：(選用) EC2Rescue執行個體的子網路 ID。根據預設，AWS Systems Manager Automation 會建立新的 VPC。或者，使用 SelectedInstanceSubnet來使用與執行個體相同的子網路，或指定自訂子網路 ID。

Important

子網路必須與 位於相同的可用區域UnreachableInstanceId，而且必須允許存取 SSM 端點。

- `UnreachableInstanceId`

類型：字串

描述：(必要) 無法連線之 EC2 執行個體的 ID。

 Important

Systems Manager Automation 會停止此執行個體，並在嘗試任何操作之前建立 AMI。存放在執行個體存放磁碟區的資料會遺失。如果您不使用彈性 IP 地址，公有 IP 地址將會變更。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

您必須至少具有 `ssm:StartAutomationExecution` 且 `ssm:GetAutomationExecution` 才能讀取自動化輸出。如需所需許可的詳細資訊，請參閱 [AWSSupport-StartEC2RescueWorkflow](#)。

文件步驟

1. `aws:assertAwsResourceProperty` - 如果提供的執行個體是 `Windows Server`：
 - a. (EC2Rescue for Windows Server) 如果提供的執行個體是 Windows Server 執行個體：
 - i. `aws:executeAutomation` - `AWSSupport-StartEC2RescueWorkflow` 使用 Windows Server 離線指令碼的 EC2Rescue 調用。
 - ii. `aws:executeAwsApi` - 從巢狀自動化擷取備份 AMI ID。
 - iii. `aws:executeAwsApi` - 從巢狀自動化擷取 EC2Rescue 摘要。
 - b. (EC2Rescue for Linux) 如果提供的執行個體是 Linux 執行個體：
 - i. `aws:executeAutomation` - `AWSSupport-StartEC2RescueWorkflow` 使用適用於 Linux 的 EC2Rescue 離線指令碼調用
 - ii. `aws:executeAwsApi` - 從巢狀自動化擷取備份 AMI ID。
 - iii. `aws:executeAwsApi` - 從巢狀自動化擷取 EC2Rescue 摘要。

輸出

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

```
getEC2RescueForLinuxResult.Output
```

```
getLinuxBackupAmi.ImageId
```

AWSSupport-ListEC2Resources

Description

AWSSupport-ListEC2Resources Runbook 會從 AWS 區域 您指定的 傳回 Amazon EC2 執行個體和相關資源的相關資訊，例如 Amazon Elastic Block Store (Amazon EBS) 磁碟區、彈性 IP 地址和 Amazon EC2 Auto Scaling 群組。根據預設，資訊會從所有區域收集，並顯示在自動化的輸出中。或者，您可以指定 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以便將資訊上傳到 ，做為逗號分隔值 (.csv) 檔案。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName

類型：字串

描述：（選用）所收集資訊上傳到的 S3 儲存貯體名稱。

- DisplayResourceDeletionDocumentation

類型：字串

預設：true

描述：（選用）如果設定為 true，自動化會在輸出中建立與刪除資源相關的文件連結。

- RegionsToQuery

類型：字串

預設：全部

描述：（選用）您要從中收集 Amazon EC2 相關資訊的區域。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- autoscaling:DescribeAutoScalingGroups
- ec2:DescribeAddresses
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeVolumes
- ec2:DescribeSnapshots
- elasticloadbalancing:DescribeLoadBalancers

此外，若要成功將收集的資訊上傳至您指定的 S3 儲存貯體，AutomationAssumeRole 需要下列動作：

- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:PutObject

文件步驟

- `aws:executeAwsApi` - 收集為帳戶啟用的區域。
- `aws:executeScript` - 確認為帳戶啟用的區域支援 `RegionsToQuery` 參數中指定的區域。
- `aws:branch` - 如果未為帳戶啟用區域，自動化會結束。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有 EC2 執行個體。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有 Amazon Machine Image (AMI)。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有 EBS 磁碟區。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有彈性 IP 地址。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有彈性網路介面。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有 Auto Scaling 群組。
- `aws:executeScript` - 列出您指定之帳戶和區域的所有負載平衡器。
- `aws:executeScript` - 如果您為 `Bucket` 參數提供值，則將收集的資訊上傳至指定的 S3 儲存貯體。

AWSSupport-ManageRDPSettings

Description

AWSSupport-ManageRDPSettings Runbook 允許使用者管理常見的遠端桌面通訊協定 (RDP) 設定，例如 RDP 連接埠和網路層身分驗證 (NLA)。根據預設，執行手冊會讀取和輸出設定的值。

Important

執行此 Runbook 之前，應仔細檢閱 RDP 設定的變更。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 管理 RDP 設定的受管執行個體之 ID。

- NLASettingAction

類型：字串

有效值：檢查 | 啟用 | 停用

預設：Check

描述：(必要) 在 NLA 設定上執行的動作：Check，Enable，Disable。

- RDPPort

類型：字串

預設：3389

描述：(選用) 指定新的 RDP 連接埠。僅在動作設為 Modify 時使用。連接埠號碼必須為介於 1025 到 65535 的數字。備註：連接埠變更之後，RDP 服務會重新啟動。

- RDPPortAction

類型：字串

有效值：檢查 | 修改

預設：Check

描述：(必要) 要套用至 RDP 連接埠的動作。

- RemoteConnections

類型：字串

有效值：檢查 | 啟用 | 停用

預設：Check

描述：（必要）在 fDenyTSConnections 設定上執行的動作。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

接收命令的 EC2 執行個體必須具備已連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。使用者必須至少具備 ssm:SendCommand 以傳送命令給執行個體，也要有 ssm:GetCommandInvocation 才能夠讀取命令輸出。

文件步驟

aws:runCommand - 執行 PowerShell 指令碼以變更或檢查目標執行個體上的 RDP 設定。

輸出

manageRDPSettings.Output

AWSSupport-ManageWindowsService

Description

AWSSupport-ManageWindowsService Runbook 可讓您停止、啟動、重新啟動、暫停或停用目標執行個體上的任何 Windows 服務。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 管理服務的受管執行個體 ID。

- ServiceAction

類型：字串

有效值：檢查 | 重新啟動 | Force-Restart | 開始 | 停止 | Force-Stop | 暫停

預設：Check

描述：(必要) 要套用至 Windows 服務的動作。請注意，Force-Restart 和 Force-Stop 可用來重新啟動和停止具有相依服務的 服務。

- StartupType

類型：字串

有效值：檢查 | 自動 | 需求 | 停用 | DelayedAutoStart

預設：Check

描述：(必要) 要套用至 Windows 服務的啟動類型。

- WindowsServiceName

類型：字串

描述：(必要) 有效的 Windows 服務名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具備連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。使用者必須至少有 ssm : StartAutomationExecution 和 ssm : SendCommand 來執行自動化並將命令傳送至執行個體，加上 ssm : GetAutomationExecution，才能讀取自動化輸出。

文件步驟

aws:runCommand - 執行 PowerShell 指令碼，將所需的組態套用至目標執行個體上的 Windows 服務。

輸出

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

Description

AWSSupport-MigrateEC2ClassicToVPC Runbook 會將 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體從 EC2-Classic 遷移至虛擬私有雲端 (VPC)。此 Runbook 支援使用 Amazon Elastic Block Store (Amazon EBS) 根磁碟區遷移硬體虛擬機器 (HVM) 虛擬化類型的 Amazon EC2 執行個體。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- ApproverIAM

類型：StringList

描述：(選用) 可以核准或拒絕動作的 IAM 使用者的 Amazon Resource Name (ARNs)。只有在您指定 參數CutOver的值時，才會套用此MigrationType參數。

- DestinationSecurityGroupId

類型：StringList

描述：(選用) 您要與 VPC 中啟動的 Amazon EC2 執行個體建立關聯的安全群組 ID。如果您未指定此參數的值，自動化會在 VPC 中建立安全群組，並從 EC2-Classic 中的安全群組複製規則。如果規則無法複製到新的安全群組，則 VPC 的預設安全群組會與 Amazon EC2 執行個體相關聯。

- DestinationSubnetId

類型：字串

描述：(選用) 您要遷移 Amazon EC2 執行個體的子網路 ID。如果您未指定此參數的值，自動化會從 VPC 隨機選擇子網路。

- InstanceId

類型：字串

描述：(必要) 您要遷移的 Amazon EC2 執行個體 ID。

- MigrationType

類型：字串

有效值：CutOver | Test

描述：(必要) 您要執行的遷移類型。

CutOver 此選項需要核准，才能停止在 Amazon EC2 EC2-Classic 執行個體。核准此動作後，Amazon EC2 執行個體會停止，自動化會建立 Amazon Machine Image(AMI)。當AMI狀態為時available，新的 Amazon EC2 執行個體會在DestinationSubnetId您在 VPC AMI中指定的 中從此啟動。如果您在 EC2-Classic 中執行的 Amazon EC2 執行個體已連接彈性 IP 地址，執行個體將移至 VPC 中新建立的 Amazon EC2 執行個體。如果 VPC 中啟動的 Amazon EC2 執行個體

因任何原因無法建立，則會終止，並請求核准才能在 EC2-Classic 中啟動 Amazon EC2 執行個體。
EC2-Classic

Test 選項會建立AMI在 EC2-Classic 中執行的 Amazon EC2 執行個體的，而不重新啟動。EC2-Classic 由於 Amazon EC2 執行個體不會重新啟動，我們無法保證所建立映像的檔案系統完整性。當 AMI 狀態為 `available`，新的 Amazon EC2 執行個體會在 `DestinationSubnetId` 您在 VPC 中指定的 AMI 中從此啟動。如果您在 Amazon EC2 EC2-Classic 執行個體已連接彈性 IP 地址，自動化會驗證 `DestinationSubnetId` 您指定的是公有的。如果 VPC 中啟動的 Amazon EC2 執行個體因任何原因無法建立，則會終止並結束自動化。

- `SNSNotificationARNforApproval`

類型：字串

描述：（選用）您要傳送核准請求的 Amazon Simple Notification Service (Amazon SNS) 主題的 ARN。只有在您指定參數 `CutOver` 的值時，才會套用此 `MigrationType` 參數。

- `TargetInstanceType`

類型：字串

預設：t2.2xlarge

描述：（選用）您想要在 VPC 中啟動的 Amazon EC2 執行個體類型。僅支援以 Xen 為基礎的執行個體類型，例如 T2, M4 或 C4。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `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`

文件步驟

- `aws:executeAwsApi` - 收集您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體詳細資訊。
- `aws:assertAwsResourceProperty` - 確認您在 `TargetInstanceType` 參數中指定的執行個體類型是以 Xen 為基礎。
- `aws:assertAwsResourceProperty` - 確認您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體屬於 HVM 虛擬化類型。
- `aws:assertAwsResourceProperty` - 確認您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體具有 Amazon EBS 根磁碟區。
- `aws:executeScript` - 根據您為 `DestinationSecurityGroupId` 參數指定的值，視需要建立安全群組。

- `aws:branch` - 根據您在 `DestinationSubnetId` 參數中指定的值進行分支。
- `aws:executeAwsApi` - 在您執行此自動化的 AWS 區域 中識別預設 VPC。
- `aws:executeAwsApi` - 隨機選擇位於預設 VPC 中的子網路 ID。
- `aws:createImage` - 建立 AMI而不重新啟動 Amazon EC2 執行個體。
- `aws:branch` - 根據您為 `MigrationType` 參數指定的值進行分支。
- `aws:branch` - 根據您為 `DestinationSubnetId` 參數指定的值進行分支。
- `aws:runInstances` - 從AMI建立的 啟動新的執行個體，而不重新啟動 Amazon EC2 EC2-Classic 執行個體。
- `aws:changeInstanceState` - 如果上一個步驟因任何原因失敗，則終止新啟動的 Amazon EC2 執行個體。
- `aws:runInstances` - 如果`DestinationSubnetId`提供，則從AMI建立的 啟動新的執行個體，而不在 EC2-Classic 中重新啟動 Amazon EC2 執行個體。 EC2-Classic
- `aws:changeInstanceState` - 如果上一個步驟因任何原因失敗，則終止新啟動的 Amazon EC2 執行個體。
- `aws:assertAwsResourceProperty` - 確認在 Amazon EC2 EC2-Classic 執行個體的停止行為。
- `aws:approve` - 等待核准以停止 Amazon EC2 執行個體。
- `aws:changeInstanceState` - 停止在 Amazon EC2 EC2-Classic 執行個體。
- `aws:changeInstanceState` - 如有需要，強制 會停止在 Amazon EC2 EC2-Classic 執行個體。
- `aws:createImage` - 在 Amazon EC2 AMI 執行個體停止後建立。
- `aws:branch` - 根據 `DestinationSubnetId` 參數指定的值進行分支。
- `aws:runInstances` - 從在 EC2-Classic 中AMI建立的已停止 Amazon EC2 執行個體啟動新執行個體。 Amazon EC2 EC2-Classic
- `aws:approve` - 等待核准以終止新啟動的執行個體，並在上一個步驟因任何原因失敗時，在 EC2-Classic 中啟動 Amazon EC2 執行個體。 EC2-Classic
- `aws:changeInstanceState` - 終止新啟動的 Amazon EC2 執行個體。
- `aws:runInstances` - 從 參數的 EC2-Classic 中AMI建立的已停止 Amazon EC2 執行個體啟動新執行個體`DestinationSubnetId`。 Amazon EC2 EC2-Classic
- `aws:approve` - 等待核准以終止新啟動的執行個體，並在上一個步驟因任何原因失敗時，在 EC2-Classic 中啟動 Amazon EC2 執行個體。 EC2-Classic
- `aws:changeInstanceState` - 終止新啟動的 Amazon EC2 執行個體。
- `aws:changeInstanceState` - 啟動在 Amazon EC2 EC2-Classic 執行個體。

- `aws:branch` - 根據 Amazon EC2 執行個體是否有公有 IP 地址進行分支。
- `aws:executeAwsApi` - 驗證公有 IP 地址是否為彈性 IP 地址。
- `aws:branch` - 根據您在 `MigrationType` 參數中指定的值進行分支。
- `aws:executeAwsApi` - 將彈性 IP 地址移至您的 VPC。
- `aws:executeAwsApi` - 收集已移至 VPC 的彈性 IP 地址的配置 ID。
- `aws:branch` - 根據 VPC 中執行的 Amazon EC2 執行個體啟動的子網路進行分支。
- `aws:executeAwsApi` - 將彈性 IP 地址連接到 VPC 中新啟動的執行個體。
- `aws:executeScript` - 確認您 VPC 中新啟動的 Amazon EC2 執行個體為公有子網路。

輸出

`getInstanceProperties.virtualizationType` - ECAmazon EC2 EC2-Classic 執行個體的虛擬化類型。

`getInstanceProperties.rootDeviceType` - ECAmazon EC2 EC2-Classic 執行個體的根裝置類型。

`createAMIWithoutReboot.ImageId` - 在不重新啟動在 Amazon EC2 EC2-Classic 執行個體的情況下AMI建立的 ID。

`getDefaultVPC.VpcId` - 若未提供 `DestinationSubnetId` 參數的值，則會啟動新 Amazon EC2 執行個體的預設 VPC ID。

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc` - 預設 VPC 中的子網路 ID，如果未提供 `DestinationSubnetId` 參數的值，則會啟動新的 Amazon EC2 執行個體。

`launchTestInstanceDefaultVPC.InstanceIds` - 在Test遷移類型期間，在您預設 VPC 中新啟動的 Amazon EC2 執行個體 ID。

`launchTestInstanceProvidedSubnet.InstanceIds` - `DestinationSubnetId`您在Test遷移類型期間指定的 中新啟動的 Amazon EC2 執行個體 ID。

`createAMIAfterStoppingInstance.ImageId` - 停止在 Amazon EC2 EC2-Classic 執行個體後AMI建立的 ID。

`launchCutOverInstanceProvidedSubnet.InstanceIds` - `DestinationSubnetId`您在CutOver遷移類型期間指定的 中新啟動的 Amazon EC2 執行個體 ID。

`launchCutOverInstanceDefaultVPC.InstanceIds` - 在CutOver遷移類型期間，在您預設 VPC 中新啟動的 Amazon EC2 執行個體 ID。

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic` - 預設 VPC 中自動化所選擇的子網路是否為公有子網路。

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic` - 您在 中指定的子網路DestinationSubnetId是否為公有子網路。

AWSsupport-MigrateXenToNitroLinux

Description

AWSsupport-MigrateXenToNitroLinux Runbook 會將 Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen 執行個體複製、準備和遷移至[Nitro執行個體類型](#)。此 Runbook 提供兩種操作類型的選項：

- `Clone&Migrate` – 此選項的工作流程包含初步檢查、測試和Clone&Migrate階段。使用 `AWSsupport-CloneXenEC2InstanceAndMigrateToNitro` Runbook 執行工作流程。
- `FullMigration` – 此選項會執行Clone&Migrate工作流程，然後執行取代根 Amazon EBS 磁碟區的額外步驟。

Important

使用此 Runbook 會在 Amazon EC2 執行個體的執行時間、建立 Amazon Elastic Block Store (Amazon EBS) 磁碟區，以及產生您的帳戶成本AMIs。如需詳細資訊，請參閱 [Amazon EC2 定價](#)和 [Amazon EBS 定價](#)。

初步檢查

自動化會在繼續遷移之前執行下列初步檢查。如果任何檢查失敗，自動化就會結束。此階段只是Clone&Migrate工作流程的一部分。

- 檢查目標執行個體是否已是Nitro執行個體類型。
- 檢查 Spot 執行個體購買選項是否用於目標執行個體。
- 檢查執行個體存放區磁碟區是否連接到目標執行個體。
- 驗證目標執行個體作業系統 (OS) 是 Linux。

- 檢查目標執行個體是否為 Amazon EC2 Auto Scaling 群組的一部分。如果它是 Auto Scaling 群組的一部分，自動化會驗證執行個體是否處於 standby 狀態。
- 驗證執行個體是由 管理 AWS Systems Manager。

測試

自動化會從目標執行個體建立 Amazon Machine Image(AMI)，並從新建立的 啟動測試執行個體AMI。此階段只是Clone&Migrate工作流程的一部分。

如果測試執行個體通過所有狀態檢查，自動化會暫停，並透過 Amazon Simple Notification Service (Amazon SNS) 通知請求指定委託人的核准。如果提供核准，自動化會終止測試執行個體、停止目標執行個體，並繼續遷移，而新建立的 AMI 會在Clone&Migrate工作流程結束時取消註冊。

Note

在提供核准之前，我們建議驗證在目標執行個體上執行的所有應用程式都已正常關閉。

複製和遷移

自動化AMI會從目標執行個體建立另一個執行個體，並啟動新執行個體以變更為Nitro執行個體類型。自動化會先完成下列先決條件，再繼續進行遷移。如果任何檢查失敗，自動化就會結束。此階段也只是Clone&Migrate工作流程的一部分。

- 開啟增強型聯網 (ENA) 屬性。
- 如果 ENA 驅動程式尚未安裝，請安裝最新版本的驅動程式，或將 ENA 驅動程式版本更新至最新版本。為了確保網路效能最大化，如果Nitro執行個體類型是第 6 代，則需要更新至最新的 ENA 驅動程式版本。
- 驗證 NVMe 模組是否已安裝。如果已安裝模組，自動化會驗證模組是否已載入。 `initramfs`
- 使用區塊型裝置名稱 (`/dev/sd*` 或 `/dev/xvd*`) 分析項目 `/etc/fstab`，並將項目取代為其各自 UUIDs。在修改組態之前，自動化會在路徑 建立檔案的備份 `/etc/fstab*`。
- 如果檔案存在，請將 `net.ifnames=0` 選項新增至 `/etc/default/grub` 檔案中的 `GRUB_CMDLINE_LINUX` 行，或新增至 中的核心，以關閉可預測界面命名 `/boot/grub/menu.lst`。
- 如果檔案存在，則移除該 `/etc/udev/rules.d/70-persistent-net.rules` 檔案。在移除檔案之前，自動化會在路徑 建立檔案的備份 `/etc/udev/rules.d/`。

驗證所有需求後，執行個體類型會變更為您指定的Nitro執行個體類型。自動化會在執行個體Nitro類型啟動後等待新建立的執行個體通過所有狀態檢查。自動化接著會等待指定委託人的核准，以建立成功啟動AMI執行個體的 Nitro。如果核准遭拒，自動化會結束，讓新建立的執行個體持續執行，目標執行個體仍會停止。

取代根 Amazon EBS 磁碟區

如果您選擇 FullMigration做為 OperationType，自動化會將目標 Amazon EC2 執行個體遷移至您指定的Nitro執行個體類型。自動化會請求指定主體的核准，以複製的 Amazon EC2 執行個體根磁碟區取代目標 Amazon EC2 執行個體的根 Amazon EBS 磁碟區。遷移成功後，複製的 Amazon EC2 執行個體會終止。如果自動化失敗，原始 Amazon EBS 根磁碟區會連接至目標 Amazon EC2 執行個體。如果連接至目標 Amazon EC2 執行個體的根 Amazon EBS 磁碟區具有套用aws:字首的標籤，則不支援 FullMigration操作。

開始之前

目標執行個體必須具有傳出網際網路存取。這是為了存取驅動程式和相依性的儲存庫，例如 kernel-devel、gcc、patch、rpm-build、wget、dracut、makelinux-headers和 unzip。視需要使用套件管理員。

需要 Amazon SNS 主題才能傳送核准和更新的通知。如需建立 Amazon SNS 主題的詳細資訊，請參閱《Amazon Simple Notification Service [開發人員指南](#)》中的[建立 Amazon SNS 主題](#)。

此 Runbook 支援下列作業系統：

- RHEL 7.x - 8.5
- Amazon Linux (2018.03)、Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS、20.04 LTS 和 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5、SUSE15SP2)

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 確認

類型：字串

描述：(必要) 讀取此自動化 Runbook 所執行動作的完整詳細資訊，然後輸入 **Yes, I understand and acknowledge** 以繼續使用 Runbook。

- ApproverIAM

類型：字串

描述：(必要) IAM 角色、使用者或使用者名稱 ARNs，這些角色、使用者或使用者名稱可以為自動化提供核准。您最多可以指定 10 個核准者。

- DeleteResourcesOnFailure

類型：布林值

描述：(選用) 判斷在自動化失敗時，是否刪除新建立 AMI 的執行個體和遷移。

有效值：True | False

預設：True

- MinimumRequiredApprovals

類型：字串

描述：(選用) 在請求核准時，繼續執行自動化所需的最低核准數量。

有效值：1-10

預設：1

- NitroInstanceType

類型：字串

描述：(必要) 您要變更Nitro執行個體的執行個體類型。支援的執行個體類型包括 M5, M6, C5, C6, R5, R6 和 T3。

預設：m5.xlarge

- OperationType

類型：字串

描述：(必要) 您要執行的操作。FullMigration 選項會執行與 相同的任務，Clone&Migrate並額外取代目標執行個體的根磁碟區。目標執行個體的根磁碟區會取代為遷移程序後新建立執行個體的根磁碟區。FullMigration 操作不支援邏輯磁碟區管理員 (LVM) 定義的根磁碟區。

有效值：Clone&Migrate | FullMigration

- SNSTopicArn

類型：字串

描述：(必要) 用於核准通知的 Amazon SNS 主題 ARN。Amazon SNS 主題用於在自動化期間傳送必要的核准通知。

- TargetInstanceId

類型：字串

描述：(必要) 要遷移的 Amazon EC2 執行個體 ID。

Clone&Migrate 工作流程

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `startOfPreliminaryChecksBranch` - 分支到初步檢查工作流程。
- `getTargetInstanceProperties` - 從目標執行個體收集詳細資訊。

- `checkIfNitroInstanceTypeIsSupportedInAZ` - 判斷目標執行個體是否支援與目標執行個體相同的可用區域中的目標 Amazon EC2 執行個體類型。
- `getXenInstanceTypeInfo` - 收集來源執行個體類型的詳細資訊。
- `checkIfInstanceHypervisorIsNitroAlready` - 檢查目標執行個體是否已以 Nitro 執行個體類型執行。
- `checkIfTargetInstanceLifecycleIsSpot` - 檢查目標執行個體的購買選項是否為 Spot。
- `checkIfOperatingSystemIsLinux` - 檢查目標執行個體作業系統是否為 Linux。
- `verifySSMConnectivityForTargetInstance` - 驗證目標執行個體是否由 Systems Manager 管理。
- `checkIfEphemeralVolumeAreSupported` - 檢查目標執行個體的目前執行個體類型是否支援執行個體存放區磁碟區。
- `verifyIfTargetInstanceHasEphemeralVolumesAttached` - 檢查目標執行個體是否已連接執行個體存放磁碟區。
- `checkIfRootVolumeIsEBS` - 檢查目標執行個體的根磁碟區類型是否為 EBS。
- `checkIfTargetInstanceIsInASG` - 檢查目標執行個體是否為 Auto Scaling 群組的一部分。
- `endOfPreliminaryChecksBranch` - 初步檢查分支的結束。
- `startOfTestBranch` - 分支到測試工作流程。
- `createTestImage` - 建立目標執行個體 AMI 的測試。
- `launchTestInstanceInSameSubnet` - AMI 使用與目標執行個體相同的組態，從測試啟動測試執行個體。
- `cleanupTestInstance` - 終止測試執行個體。
- `endOfTestBranch` - 測試分支結束。
- `checkIfTestingBranchSucceeded` - 檢查測試分支的狀態。
- `approvalToStopTargetInstance` - 等待指定主體的核准，以停止目標執行個體。
- `stopTargetEC2Instance` - 停止目標執行個體。
- `forceStopTargetEC2Instance` - 只有在上一個步驟無法停止執行個體時，強制才會停止目標執行個體。
- `startOfCloneAndMigrateBranch` - 分支到 Clone&Migrate 工作流程。
- `createBackupImage` - 建立目標執行個體 AMI 的 做為備份。
- `launchInstanceInSameSubnet` - AMI 使用與來源執行個體相同的組態，從備份啟動新的執行個體。

- `waitForClonedInstanceToPassStatusChecks` - 等待新建立的執行個體通過所有狀態檢查。
- `verifySSMConnectivityForClonedInstance` - 驗證新建立的執行個體是由 Systems Manager 管理。
- `checkAndInstallENADrivers` - 檢查 ENA 驅動程式是否已安裝在新建立的執行個體上，並視需要安裝驅動程式。
- `checkAndAddNVMeDrivers` - 檢查 NVMe 驅動程式是否已安裝在新建立的執行個體上，並視需要安裝驅動程式。
- `checkAndModifyFSTABEntries` - 檢查裝置名稱是否在 `/etc/fstab` 中使用，並視需要將其取代為 UUIDs。
- `stopClonedInstance` - 停止新建立的執行個體。
- `forceStopClonedInstance` - 只有在上一個步驟無法停止執行個體時，強制 才會停止新建立的執行個體。
- `checkENAAttributeForClonedInstance` - 檢查新建立的執行個體是否已開啟增強型聯網屬性。
- `setNitroInstanceTypeForClonedInstance` - 將新建立執行個體的執行個體類型變更為您指定的 Nitro 執行個體類型。
- `startClonedInstance` - 啟動您變更其執行個體類型的新建立執行個體。
- `approvalForCreatingImageAfterDriversInstallation` - 如果執行個體成功啟動為 Nitro 執行個體類型，自動化會等待所需主體的核准。如果提供核准，AMI 則會建立 以用作 Golden AMI。
- `createImageAfterDriversInstallation` - 建立 AMI 要用作黃金 的 AMI。
- `endOfCloneAndMigrateBranch` - Clone&Migrate 分支結束。
- `cleanupTestImage` - 取消註冊為測試 AMI 而建立的 。
- `failureHandling` - 檢查您是否選擇在失敗時終止資源。
- `onFailureTerminateClonedInstance` - 在自動化失敗時終止新建立的執行個體。
- `onFailurecleanupTestImage` - 取消註冊為測試 AMI 而建立的 。
- `onFailureApprovalToStartTargetInstance` - 如果自動化失敗， 會等待指定主體的核准，以啟動目標執行個體。
- `onFailureStartTargetInstance` - 如果自動化失敗， 會啟動目標執行個體。

Full Migration 工作流程

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

FullMigration 工作流程執行與Clone&Migrate工作流程相同的步驟，並另外執行下列步驟：

- `checkConcurrency` - 驗證此 Runbook 只有一個自動化，目標為您指定的 Amazon EC2 執行個體。如果 Runbook 找到另一個以相同執行個體為目標的進行中自動化，則自動化會結束。
- `getTargetInstanceProperties` - 從目標執行個體收集詳細資訊。
- `checkRootVolumeTags` - 判斷目標 Amazon EC2 執行個體的根磁碟區是否包含任何 AWS 預留標籤。
- `cloneTargetInstanceAndMigrateToNitro` - 使用 AWS-CloneXenInstanceToNitro Runbook 啟動子自動化。
- `branchOnTheOperationType` - 在您為 `OperationType` 參數指定的值上分支。
- `getClonedInstanceId` - 從子自動化擷取新啟動執行個體的 ID。
- `checkIfRootVolumeIsBasedOnLVM` - 判斷根分割區是否由 LVM 管理。
- `branchOnTheRootVolumeLVMStatus` - 如果從委託人收到最低必要核准，自動化會繼續進行根磁碟區替換。
- `manualInstructionsInCaseOfLVM` - 如果根磁碟區是由 LVM 管理，自動化會傳送輸出，其中包含如何手動取代根磁碟區的指示。
- `startOfReplaceRootEBSVolumeBranch` - 啟動取代根 EBS 磁碟區分支工作流程。
- `checkIfTargetInstanceIsManagedByCFN` - 判斷目標執行個體是否由 AWS CloudFormation 堆疊管理。
- `branchOnCFNStackStatus` - 根據 CloudFormation 堆疊的狀態進行分支。
- `approvalForRootVolumesReplacement(WithCFN)` - 如果目標執行個體是由 CloudFormation 啟動，自動化會在新啟動的執行個體成功啟動為 Nitro 執行個體類型後等待核准。提供核准時，目標執行個體的 Amazon EBS 磁碟區會取代為新啟動執行個體的根磁碟區。
- `approvalForRootVolumesReplacement` - 在新啟動的執行個體成功啟動為 Nitro 執行個體類型之後，等待核准。提供核准時，目標執行個體的 Amazon EBS 磁碟區會取代為新啟動執行個體的根磁碟區。
- `assertIfTargetEC2InstanceIsStillStopped` - 在取代根磁碟區之前，驗證目標執行個體是否處於 `stopped` 狀態。

- `stopTargetInstanceForRootVolumeReplacement` - 如果目標執行個體正在執行，自動化會在取代根磁碟區之前停止執行個體。
- `forceStopTargetInstanceForRootVolumeReplacement` - 如果上一個步驟失敗，強制會停止目標執行個體。
- `stopClonedInstanceForRootVolumeReplacement` - 在取代 Amazon EBS 磁碟區之前停止新建立的執行個體。
- `forceStopClonedInstanceForRootVolumeReplacement` - 如果上一個步驟失敗，強制會停止新建立的執行個體。
- `getBlockDeviceMappings` - 擷取目標和新建立執行個體的區塊型裝置映射。
- `replaceRootEbsVolumes` - 將目標執行個體的根磁碟區取代為新建立執行個體的根磁碟區。
- `EndOfReplaceRootEBSVolumeBranch` - 取代根 EBS 磁碟區分支工作流程結束。
- `checkENAAttributeForTargetInstance` - 檢查目標 Amazon EC2 執行個體的增強型聯網 (ENA) 屬性是否已開啟。
- `enableENAAttributeForTargetInstance` - 視需要開啟目標 Amazon EC2 執行個體的 ENA 屬性。
- `setNitroInstanceTypeForTargetInstance` - 將目標執行個體變更為您指定的 Nitro 執行個體類型。
- `replicateRootVolumeTags` - 從目標 Amazon EC2 執行個體複寫根 Amazon EBS 磁碟區的標籤。
- `startTargetInstance` - 在變更執行個體類型後啟動目標 Amazon EC2 執行個體。
- `onFailureStopTargetEC2Instance` - 如果目標 Amazon EC2 執行個體無法啟動為執行個體類型，則停止該 Nitro 執行個體。
- `onFailureForceStopTargetEC2Instance` - 如果上一個步驟失敗，強制會停止目標 Amazon EC2 執行個體。
- `OnFailureRevertOriginalInstanceType` - 如果目標執行個體無法啟動為執行個體類型，則將目標 Amazon EC2 執行個體還原為原始 Nitro 執行個體類型。
- `onFailureRollbackRootVolumeReplacement` - 視需要還原 `replaceRootEbsVolumes` 步驟所做的所有變更。
- `onFailureApprovalToStartTargetInstance` - 等待指定的委託人核准在復原先前的變更後啟動目標 Amazon EC2 執行個體。
- `onFailureStartTargetInstance` - 啟動目標 Amazon EC2 執行個體。
- `terminateClonedEC2Instance` - 在取代根 Amazon EBS 磁碟區後終止複製的 Amazon EC2 執行個體。

AWSSupport-ResetAccess

Description

此 Runbook 將在指定的 EC2 執行個體上使用 EC2Rescue 工具，使用 EC2 主控台 (Windows) 重新啟用密碼解密，或產生並新增新的 SSH 金鑰對 (Linux)。如果您遺失金鑰對，此自動化會建立啟用密碼的 AMI，可讓您藉由您擁有的金鑰對來啟動新的 EC2 執行個體 (Windows)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- EC2RescueInstanceType

類型：字串

有效值：t2.small | t2.medium | t2.large

預設：t2.small

描述：(必要) EC2Rescue 執行個體的 EC2 執行個體類型。建議大小：t2.small。

- InstanceId

類型：字串

描述：(必要) 您想要重設存取權的 EC2 執行個體之 ID。

 Important

Systems Manager Automation 會停止此執行個體，並在嘗試任何操作之前建立 AMI。存放在執行個體存放磁碟區的資料會遺失。如果您不是使用彈性 IP，則公有 IP 位址會變更。

- SubnetId

類型：字串

預設：CreateNewVPC

描述：(選用) EC2Rescue 執行個體的子網路 ID。根據預設，Systems Manager Automation 會建立新的 VPC。或者藉由 SelectedInstanceSubnet 使用與執行個體相同的子網路，或指定自訂的子網路 ID。

 Important

子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

您必須擁有至少 `ssm:StartAutomationExecution`、`ssm:GetParameter`（擷取 SSH 金鑰參數名稱）和 `ssm:GetAutomationExecution`，才能讀取自動化輸出。如需所需許可的詳細資訊，請參閱 [AWS Support - StartEC2RescueWorkflow](#)。

文件步驟

1. `aws:assertAwsResourceProperty` - 如果提供的執行個體是 Windows，則宣告。
 - a. (適用於 Windows 的 EC2Rescue) 如果提供的執行個體為 Windows：
 - i. `aws:executeAutomation` - AWS Support - StartEC2RescueWorkflow 使用 EC2Rescue for Windows 離線密碼重設指令碼調用
 - ii. `aws:executeAwsApi` - 從巢狀自動化擷取備份 AMI ID

- iii. `aws:executeAwsApi` - 從巢狀自動化擷取啟用密碼的 AMI ID
- iv. `aws:executeAwsApi` - 從巢狀自動化擷取 EC2Rescue 摘要
- b. (適用於 Linux 的 EC2Rescue) 如果提供的執行個體為 Linux :
 - i. `aws:executeAutomation` - `AWSSupport-StartEC2RescueWorkflow` 使用 EC2Rescue for Linux 離線 SSH 金鑰注入指令碼調用
 - ii. `aws:executeAwsApi` - 從巢狀自動化擷取備份 AMI ID
 - iii. `aws:executeAwsApi` - 擷取注入 SSH 金鑰的 SSM 參數名稱
 - iv. `aws:executeAwsApi` - 從巢狀自動化擷取 EC2Rescue 摘要

輸出

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getWindowsPasswordEnabledAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

`getLinuxSSHKeyParameter.Name`

AWSSupport-ResetLinuxUserPassword

Description

`AWSSupport-ResetLinuxUserPassword` Runbook 可協助您重設本機作業系統 (OS) 使用者的密碼。此 Runbook 特別適用於需要使用序列主控台存取其 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的使用者。Runbook 會在您的 AWS 帳戶和 AWS Identity and Access Management (IAM) 角色中建立臨時 Amazon EC2 執行個體，並具有擷取包含密碼之 AWS Secrets Manager 秘密值的許可。

Runbook 會停止您的目標 Amazon EC2 執行個體、分離根 Amazon Elastic Block Store (Amazon EBS) 磁碟區，並將其連接至臨時 Amazon EC2 執行個體。使用 Run Command，指令碼會在暫時執行個體上執行，以設定您指定的作業系統使用者密碼。然後，根 Amazon EBS 磁碟區會重新連接至您的目標執行個體。Runbook 也提供在自動化開始時建立根磁碟區的快照的選項。

開始之前

使用您要指派給作業系統使用者的密碼值，建立 Secrets Manager 秘密。值必須為純文字。如需詳細資訊，請參閱《AWS Secrets Manager 使用者指南》中的[建立 AWS Secrets Manager 秘密](#)。

考量

- 建議您先備份執行個體，再使用此 Runbook。請考慮將 CreateSnapshot 參數的值設定為 **Yes**。
- 變更本機使用者密碼需要 Runbook 才能停止執行個體。當執行個體停止時，儲存在記憶體或執行個體存放磁碟區中的任何資料都會遺失。此外，也會釋出任何自動指派的公有 IPv4 地址。如需停止執行個體時會發生什麼情況的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[停止和啟動執行個體](#)。
- 如果連接至目標 Amazon EC2 執行個體的 Amazon EBS 磁碟區使用客戶受管 AWS Key Management Service (AWS KMS) 金鑰加密，請確定 AWS KMS 金鑰不是 deleted 或 disabled 否則執行個體將無法啟動。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：（必要）Amazon EC2 Linux 執行個體的 ID，其中包含您要重設的作業系統使用者密碼。

- LinuxUserName

類型：字串

預設：ec2-user

描述：（選用）您要重設密碼的作業系統使用者帳戶。

- SecretArn

類型：字串

描述：（必要）包含新密碼之 Secrets Manager 秘密的 ARN。

- SecurityGroupId

類型：字串

描述：（選用）要連接到臨時 Amazon EC2 執行個體的安全群組 ID。如果您未提供此參數的值，則會使用預設的 Amazon Virtual Private Cloud (Amazon VPC) 安全群組。

- SubnetId

類型：字串

描述：（選用）您要在其中啟動 Amazon EC2 臨時執行個體的字網路 ID。根據預設，自動化會選擇與目標執行個體相同的子網路。如果您選擇提供不同的子網路，它必須與目標執行個體位於相同的可用區域，並可存取 Systems Manager 端點。

- CreateSnapshot

類型：字串

有效值：是 | 否

預設：是

描述：（選用）判斷是否在自動化執行之前建立目標 Amazon EC2 執行個體根磁碟區的快照。

- StopConsent

類型：字串

有效值：是 | 否

預設：否

描述：輸入 **Yes** 以確認您的目標 Amazon EC2 執行個體將在此自動化期間停止。當 Amazon EC2 執行個體停止時，儲存在記憶體或執行個體存放磁碟區中的任何資料都會遺失，並會釋出自動公有 IPv4 地址。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[停止和啟動執行個體](#)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

1. `aws:branch` – 根據您是否已同意停止目標 Amazon EC2 執行個體而分支。
2. `aws:assertAwsResourceProperty` – 確保 Amazon EC2 執行個體狀態為 `running` 或 `stopped` 狀態。否則，自動化會結束。
3. `aws:executeAwsApi` – 取得 Amazon EC2 執行個體屬性。
4. `aws:executeAwsApi` – 取得根磁碟區屬性。
5. `aws:branch` – 根據是否提供暫時 Amazon EC2 執行個體的子網路 ID 來配置自動化。
6. `aws:assertAwsResourceProperty` – 確保您在 `SubnetId` 參數中指定的子網路與目標 Amazon EC2 執行個體位於相同的可用區域。
7. `aws:assertAwsResourceProperty` – 確保目標 Amazon EC2 執行個體根磁碟區是 Amazon EBS 磁碟區。
8. `aws:assertAwsResourceProperty` – 確保 Amazon EC2 執行個體架構為 `arm64` 或 `x86_64`。
9. `aws:assertAwsResourceProperty` – 確保 Amazon EC2 執行個體關閉行為是 `stop`，而不是 `terminate`。
10. `aws:branch` – 確保 Amazon EC2 執行個體不是 Spot 執行個體。否則，自動化會結束。
11. `aws:executeScript` – 確保 Amazon EC2 執行個體不屬於自動擴展群組。如果執行個體是自動擴展群組的一部分，自動化會確認 Amazon EC2 執行個體處於 `Standby` 生命週期狀態。

- 12aws:createStack – 建立臨時 Amazon EC2 執行個體，用於為您指定的作業系統使用者重設密碼。
- 13aws:waitForAwsResourceProperty – 等待新啟動的暫時 Amazon EC2 執行個體執行。
- 14aws:executeAwsApi – 取得暫時 Amazon EC2 執行個體的 ID。
- 15aws:waitForAwsResourceProperty – 等待臨時 Amazon EC2 執行個體報告為由 Systems Manager 管理。
- 16aws:changeInstanceState – 停止目標 Amazon EC2 執行個體。
- 17aws:changeInstanceState – 強制目標 Amazon EC2 執行個體停止，以防卡在停止狀態。
- 18aws:branch – 根據是否請求目標 Amazon EC2 執行個體根磁碟區的快照，來配置自動化。
- 19aws:executeAwsApi – 建立目標 Amazon EC2 執行個體根 Amazon EBS 磁碟區的快照。
- 20aws:waitForAwsResourceProperty – 等待快照處於 completed 狀態。
- 21aws:executeAwsApi – 將 Amazon EBS 根磁碟區與目標 Amazon EC2 執行個體分離。
- 22aws:waitForAwsResourceProperty – 等待 Amazon EBS 根磁碟區與目標 Amazon EC2 執行個體分離。
- 23aws:executeAwsApi – 將根 Amazon EBS 磁碟區連接到臨時 Amazon EC2 執行個體。
- 24aws:waitForAwsResourceProperty – 等待 Amazon EBS 根磁碟區連接至臨時 Amazon EC2 執行個體。
- 25aws:runCommand – 在臨時 Amazon EC2 執行個體上使用 Run Command 執行 Shell 指令碼，以重設目標使用者密碼。
- 26aws:executeAwsApi – 將 Amazon EBS 根磁碟區從臨時 Amazon EC2 執行個體分離。
- 27aws:waitForAwsResourceProperty – 等待 Amazon EBS 根磁碟區與臨時 Amazon EC2 執行個體分離。
- 28aws:executeAwsApi – 發生錯誤後，將 Amazon EBS 根磁碟區從臨時 Amazon EC2 執行個體分離。
- 29aws:waitForAwsResourceProperty – 等待 Amazon EBS 根磁碟區在錯誤發生後與暫時 Amazon EC2 執行個體分離。
- 30aws:branch – 根據是否請求根磁碟區的快照來判斷發生錯誤時的復原路徑，來配置自動化。
- 31aws:executeAwsApi – 將根 Amazon EBS 磁碟區重新連接至目標 Amazon EC2 執行個體。
- 32aws:waitForAwsResourceProperty – 等待 Amazon EBS 根磁碟區連接至 Amazon EC2 執行個體。
- 33aws:executeAwsApi – 從目標 Amazon EC2 執行個體根磁碟區快照建立新的 Amazon EBS 磁碟區。

- 34aws:waitForAwsResourceProperty – 等到新的 Amazon EBS 磁碟區處於 available 狀態。
- 35aws:executeAwsApi – 將新的 Amazon EBS 磁碟區連接至目標執行個體做為根磁碟區。
- 36aws:waitForAwsResourceProperty – 等待 Amazon EBS 磁碟區處於 attached 狀態。
- 37aws:executeAwsApi – 說明 Runbook 無法建立或更新 AWS CloudFormation 堆疊時的 AWS CloudFormation 堆疊事件。
- 38aws:branch – 會根據先前的 Amazon EC2 執行個體狀態來配置自動化。如果狀態為 running，執行個體會啟動。如果處於 stopped 狀態，自動化會繼續。
- 39aws:changeInstanceState – 視需要啟動 Amazon EC2 執行個體。
- 40aws:waitForAwsResourceProperty – 等到 AWS CloudFormation 堆疊處於終端機狀態後再刪除。
- 41aws:executeAwsApi – 刪除包含暫時 Amazon EC2 執行個體的 AWS CloudFormation 堆疊。

AWSPremiumSupport-ResizeNitroInstance

Description

AWSPremiumSupport-ResizeNitroInstance Runbook 提供自動化解決方案，以調整建置於 Nitro 系統的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的大小。

為了降低資料遺失和停機的潛在風險，Runbook 會驗證下列項目：

- 執行個體停止行為。
- 如果執行個體是 Amazon EC2 Auto Scaling 群組的一部分，且處於 standby 模式。
- 執行個體狀態和租用。
- 您要變更的執行個體類型，可支援目前連接至執行個體的網路介面數量。
- 目前和目標執行個體類型的處理器架構和虛擬化類型都相同。
- 如果執行個體正在執行，表示它正在傳遞所有狀態檢查。
- 您要變更為 的執行個體類型可在相同的可用區域中使用。

如果 Amazon EC2 在變更執行個體類型後未通過狀態檢查，則 Runbook 會自動轉返至先前的執行個體類型。

根據預設，如果執行個體正在執行並連接執行個體存放區磁碟區，此 Runbook 不會變更執行個體類型。如果執行個體是 AWS CloudFormation 堆疊的一部分，則 Runbook 也不會變更執

行個體類型。如果您想要變更其中一個行為，請將 `yes` 為 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 參數指定。

Runbook 提供兩種不同的方法來指定您要變更為的執行個體類型：

- 對於以單一執行個體為目標的簡單自動化，請使用 `TargetInstanceTypeFromParameter` 參數指定您要變更為的執行個體類型。
- 若要大規模執行自動化以變更數個執行個體的執行個體類型，請使用 `TargetInstanceTypeFromTagValue` 參數指定執行個體類型。如需大規模執行自動化的詳細資訊，請參閱 [大規模執行自動化](#)。

如果您未指定任一參數的值，自動化會失敗。

Important

存取 `AWSPremiumSupport-*` Runbook 需要企業或商業支援訂閱。如需詳細資訊，請參閱 [比較 支援 計劃](#)。

考量

- 建議您先備份執行個體，再使用此 Runbook。
- 如需變更執行個體類型的相容性資訊，請參閱 [變更執行個體類型的相容性](#)。
- 如果自動化失敗並轉返原始執行個體類型，請參閱 [變更執行個體類型的疑難排解](#)。
- 變更執行個體類型需要 Runbook 來停止執行個體。當執行個體停止時，儲存在記憶體或執行個體存放磁碟區中的任何資料都會遺失。此外，也會釋出任何自動指派的公有 IPv4 地址。如需停止執行個體時所發生情況的詳細資訊，請參閱 [停止和啟動執行個體](#)。
- 透過使用 `SkipInstancesWithTagKey` 參數，您可以略過已套用特定 Amazon EC2 標籤金鑰的執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 確認

類型：字串

描述：(必要) 輸入 **yes** 以確認您的執行個體在目前執行時將會停止。

- AllowInstanceStoreInstances

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果您指定 yes，則允許 Runbook 在已連接執行個體存放磁碟區的執行個體上執行。

- AllowCloudFormationInstances

類型：字串

有效值：否 | 是

預設：否

描述：(選用) 如果您指定 yes，則 Runbook 會在屬於 AWS CloudFormation 堆疊的執行個體上執行。

- DryRun

類型：字串

有效值：否 | 是

預設：否

描述：（選用）如果您指定 yes，Runbook 會驗證調整大小需求，而不會變更執行個體類型。

- InstanceId

類型：字串

描述：（必要）您要變更其類型的 Amazon EC2 執行個體 ID。

- SkipInstancesWithTagKey

類型：字串

描述：（選用）如果您指定的標籤金鑰套用至執行個體，自動化會略過目標執行個體。

- SleepTime

類型：字串

預設：3

描述：（選用）此 Runbook 在完成之後應休眠的秒數。

- TagInstance

類型：字串

描述：（選用）使用下列格式，使用您選擇的索引鍵和值標記執行個

體：*Key=ChangingType#Value=True*。此選項可讓您追蹤此 Runbook 的目標執行個體。標籤鍵與值皆區分大小寫。

- TargetInstanceTypeFromParameter

類型：字串

描述：（選用）您要變更執行個體的執行個體類型。如果您想要使用 參數中提供的標籤索引鍵值，請將此TargetInstanceTypeFromTagValue參數保留空白。

- TargetInstanceTypeFromTagValue

類型：字串

描述：(選用) 套用至目標執行個體的標籤金鑰，其值包含您要變更的執行個體類型。如果您指定 `TargetInstanceTypeFromParameter` 參數的值，則會覆寫您為此參數指定的任何值。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `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`

文件步驟

1. `aws:assertAwsResourceProperty`：確保 Amazon EC2 執行個體不會使用 `SkipInstancesWithTagKey` 參數中指定的資源標籤金鑰進行標記。如果發現標籤金鑰已套用至執行個體，則步驟會失敗，且自動化會結束。
2. `aws:assertAwsResourceProperty`：確認目標 Amazon EC2 執行個體的狀態為 `running`、`pending`、`stopped` 或 `stopping`。否則，自動化會結束。
3. `aws:executeAwsApi`：從 Amazon EC2 執行個體收集屬性。
4. `aws:executeAwsApi`：收集目前 Amazon EC2 執行個體類型的詳細資訊。
5. `aws:branch`：檢查目前的執行個體類型和 `TargetInstanceTypeFromParameter` 參數中指定的執行個體類型是否相同。如果是，自動化會結束。

6. `aws:assertAwsResourceProperty` : 確保執行個體在 Nitro 系統上執行。
7. `aws:branch` : 確保 Amazon EC2 執行個體根磁碟區類型是 Amazon Elastic Block Store (Amazon EBS) 磁碟區。
8. `aws:assertAwsResourceProperty` : 確認執行個體關閉行為是 `stop` , 而不是 `terminate`。
9. `aws:branch` : 確保 Amazon EC2 執行個體不是 Spot 執行個體。
10. `aws:branch` : 確保 Amazon EC2 執行個體租用為預設, 而非專用主機或專用執行個體。
11. `aws:executeScript` : 確認此 Runbook 只有一個自動化目標為目前的執行個體 ID。如果另一個自動化已在以相同執行個體為目標進行, 自動化會傳回錯誤並結束。
12. `aws:branch` : 根據 Amazon EC2 執行個體的狀態配置自動化。
 - a. 如果為 `stopped` 或 `stopping` , 自動化會持續執行, `aws:waitForAwsResourceProperty` 直到 Amazon EC2 執行個體完全停止為止。
 - b. 如果 `running` 或 `pending` , 自動化會執行, `aws:waitForAwsResourceProperty` 直到 Amazon EC2 執行個體通過狀態檢查為止。
13. `aws:assertAwsResourceProperty` : 呼叫 `DescribeAutoScalingInstances` API 操作, 確認 Amazon EC2 執行個體不屬於 Auto Scaling 群組。如果執行個體是 Auto Scaling 群組的一部分, 會確保 Amazon EC2 執行個體處於 `standby` 模式。
14. `aws:branch` : 根據您是否希望自動化檢查 Amazon EC2 執行個體是否為 AWS CloudFormation 堆疊的一部分, 來配置自動化:
 - a. `aws:executeScript` 透過呼叫 `DescribeStackResources` API 操作, 確保 Amazon EC2 執行個體不屬於 AWS CloudFormation 堆疊。
15. `aws:executeAwsApi` : 傳回具有相同處理器架構類型、虛擬化類型的執行個體類型清單, 並支援目前連接至目標執行個體的網路介面數量。
16. `aws:executeAwsApi` : 從 `TargetInstanceTypeFromTagValue` 參數中指定的標籤索引鍵取得目標執行個體類型值。
17. `aws:executeScript` : 確認目前和目標執行個體類型相容。確保目標執行個體類型可在相同的子網路中使用。驗證啟動 Runbook 的主體是否具有變更執行個體類型的許可, 並在執行個體執行時停止和啟動執行個體。
18. `aws:branch` : 根據 `DryRun` 參數值是否設為 `yes` 來配置自動化。如果是 `yes` , 自動化會結束。
19. `aws:branch` : 檢查原始執行個體和目標執行個體類型是否相同。如果它們相同, 自動化就會結束。
20. `aws:executeAwsApi` : 取得目前的執行個體狀態。
21. `aws:changeInstanceState` : 停止 Amazon EC2 執行個體。

22aws:changeInstanceState：如果執行個體卡在 stopping 狀態，則強制停止執行個體。

23aws:executeAwsApi：將執行個體類型變更為目標執行個體類型。

24aws:sleep：在變更執行個體類型以獲得最終一致性後等待 3 秒。

25aws:branch：根據先前的執行個體狀態配置自動化。如果是 running，執行個體會啟動。

- a. aws:changeInstanceState：如果在變更執行個體類型之前執行 Amazon EC2 執行個體，則啟動該執行個體。
- b. aws:waitForAwsResourceProperty：等待 Amazon EC2 執行個體通過狀態檢查。如果執行個體未通過狀態檢查，執行個體會變更回其原始執行個體類型。
 - i. aws:changeInstanceState：在將 Amazon EC2 執行個體變更為其原始執行個體類型之前，先停止該執行個體。
 - ii. aws:changeInstanceState：強制 Amazon EC2 執行個體先停止，再將其變更為原始執行個體類型，以防卡在停止狀態。
 - iii. aws:executeAwsApi：將 Amazon EC2 執行個體變更為其原始類型。
 - iv. aws:sleep：在變更執行個體類型以獲得最終一致性後等待 3 秒。
 - v. aws:changeInstanceState：如果在變更執行個體類型之前執行 Amazon EC2 執行個體，則啟動該執行個體。
 - vi. aws:waitForAwsResourceProperty：等待 Amazon EC2 執行個體通過狀態檢查。

26aws:sleep：等待再結束 Runbook。

AWSSupport-RestoreEC2InstanceFromSnapshot

Description

AWSSupport-RestoreEC2InstanceFromSnapshot Runbook 可協助您從根磁碟區的正常運作 Amazon Elastic Block Store (Amazon EC2) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- EndDate

類型：字串

描述：(選用) 您希望自動化尋找快照的最後一個日期。

- InplaceSwap

類型：布林值

有效值：true | false

描述：(選用) 如果此參數的值設定為 true，則快照中新建立的磁碟區會取代連接至執行個體的現有根磁碟區。

- InstanceId

類型：字串

描述：(必要) 您要從快照還原的執行個體 ID。

- LookForInstanceStatusCheck

類型：布林值

有效值：true | false

預設：true

描述：(選用) 如果此參數的值設定為 true，自動化會檢查從快照啟動的測試執行個體上的執行個體狀態檢查是否失敗。

- SkipSnapshotsBy

類型：字串

描述：（選用）搜尋快照以還原執行個體時略過快照的間隔。例如，如果有 100 個可用的快照，而您為此參數指定了 2 的值，則每第三個快照都會檢閱一次。

預設：0

- SnapshotId

類型：字串

描述：（選用）您要從中還原執行個體的快照 ID。

- StartDate

類型：字串

描述：（選用）您希望自動化尋找快照的第一個日期。

- TotalSnapshotsToLook

類型：字串

描述：（選用）自動化檢閱的快照數量。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

1. `aws:executeAwsApi` - 收集目標執行個體的詳細資訊。
2. `aws:assertAwsResourceProperty` - 驗證目標執行個體是否存在。
3. `aws:assertAwsResourceProperty` - 驗證根磁碟區是 Amazon EBS 磁碟區。
4. `aws:assertAwsResourceProperty` - 驗證另一個自動化尚未執行以此執行個體為目標的自動化。
5. `aws:executeAwsApi` - 標記目標執行個體。
6. `aws:executeAwsApi` - 建立執行個體AMI的。
7. `aws:executeAwsApi` - 收集在上一個步驟中AMI建立之 的詳細資訊。
8. `aws:waitForAwsResourceProperty` - 等待AMI狀態變成 `available`然後再繼續。
9. `aws:executeScript` - 從新建立的 啟動新的執行個體AMI。
10. `aws:assertAwsResourceProperty` - 驗證執行個體狀態為 `available`。
11. `aws:executeAwsApi` - 收集新啟動執行個體的詳細資訊。
12. `aws:branch` - 根據您是否提供 `SnapshotId` 參數的值進行分支。
13. `aws:executeScript` - 傳回指定期間內的快照清單。
14. `aws:executeAwsApi` - 停止執行個體。
15. `aws:waitForAwsResourceProperty` - 等待磁碟區狀態為 `available`。
16. `aws:waitForAwsResourceProperty` - 等待執行個體狀態為 `stopped`。

- 17aws:executeAwsApi - 分離根磁碟區。
- 18aws:waitForAwsResourceProperty - 等待根磁碟區分離。
- 19aws:executeAwsApi - 連接新的根磁碟區。
- 20aws:waitForAwsResourceProperty - 等待連接新的磁碟區。
- 21aws:executeAwsApi - 啟動執行個體。
- 22aws:waitForAwsResourceProperty - 等待執行個體狀態為 available。
- 23aws:waitForAwsResourceProperty - 等待系統和執行個體狀態檢查通過執行個體。
- 24aws:executeScript - 執行指令碼以尋找可用來成功建立磁碟區的快照。
- 25aws:executeScript - 執行指令碼，使用自動化所識別快照中新建立的磁碟區，或使用您在 SnapshotId 參數中指定的快照中建立的磁碟區來復原執行個體。
- 26aws:executeScript - 刪除自動化建立的資源。

輸出

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

Description

AWSSupport-SendLogBundleToS3Bucket Runbook 會將 EC2Rescue 工具產生的日誌套件從目標執行個體上傳至指定的 S3 儲存貯體。Runbook 會根據目標執行個體的平台安裝平台特定的 EC2Rescue 版本。EC2Rescue 接著會用於收集所有可用的作業系統 (OS) 日誌。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 您想要收集其日誌的 Windows 或 Linux 受管執行個體之 ID。

- S3BucketName

類型：字串

描述：(必要) 供上傳日誌的 S3 儲存貯體。

- S3Path

類型：字串

預設：AWSsupport-SendLogBundleToS3Bucket/

描述：(選用) 收集日誌的 S3 路徑。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具備連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。使用者必須至少有 ssm : StartAutomationExecution 和 ssm : SendCommand 來執行自動化並將命令傳送至執行個體，加上 ssm : GetAutomationExecution，才能讀取自動化輸出。

文件步驟

1. `aws:runCommand` - 透過 安裝 `EC2RescueAWS-ConfigureAWSPackage`。
2. `aws:runCommand` - 執行 PowerShell 指令碼，使用 `EC2Rescue` 收集 Windows 故障診斷日誌。
3. `aws:runCommand` - 執行 bash 指令碼，使用 `EC2Rescue` 收集 Linux 故障診斷日誌。

輸出

`collectAndUploadWindowsLogBundle.Output`

`collectAndUploadLinuxLogBundle.Output`

AWSSupport-StartEC2RescueWorkflow

Description

`AWSSupport-StartEC2RescueWorkflow` Runbook 會在為修復執行個體而建立的協助程式執行個體上執行提供的 base64 編碼指令碼 (Bash 或 Powershell)。執行個體的根磁碟區會連接並掛載至協助程式執行個體，也稱為 `EC2Rescue` 執行個體。如果您的執行個體是 Windows，請提供 Powershell 指令碼。否則，請使用 Bash。Runbook 會設定一些可在指令碼中使用的環境變數。環境變數包含您提供之輸入的資訊，以及離線根磁碟區的資訊。離線磁碟區已掛載並可使用。例如，您可以將 `Desired State Configuration` 檔案儲存至離線的 Windows 根磁碟區，或者 `chroot` 至離線的 Linux 根磁碟區並執行離線修復。

[執行此自動化（主控台）](#)

Important

此自動化不支援從 Marketplace Amazon Machine Image (AMIs) 建立的 Amazon EC2 執行個體。

其他資訊

若要將指令碼以 base64 編碼，您可以使用 Powershell 或 Bash。Powershell：

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash：

```
base64 PATH_TO_FILE
```

以下為您可在離線指令碼中使用的環境變數清單 (取決於目標作業系統)

Windows :

變數	描述	範例值
\$env:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
\$env:EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
\$env:EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$env:EC2RESCUE_EC2RW_DIR	適用於 Windows 安裝路徑的 EC2Rescue	C:\Program Files\Amazon\EC2Rescue
\$env:EC2RESCUE_EC2RW_DIR	適用於 Windows 安裝路徑的 EC2Rescue	C:\Program Files\Amazon\EC2Rescue
\$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
\$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	離線 Windows 目前控制集路徑	HKLM:\AWSTempSystem\ControlSet001
\$env:EC2RESCUE_OFFLINE_DRIVE	離線 Windows 磁碟機字母	D:\
\$env:EC2RESCUE_OFFLINE_EBS_DEVICE	離線根磁碟區 EBS 裝置	xvdf
\$env:EC2RESCUE_OFFLINE_KERNEL_VER	離線 Windows 核心版本	6.1.7601.24214
\$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	離線 Windows 架構	AMD64

變數	描述	範例值
\$env:EC2RESCUE_OFFLINE_OS_CAPTION	離線 Windows 字幕	Windows Server 2008 R2 Datacenter
\$env:EC2RESCUE_OFFLINE_OS_TYPE	離線 Windows 作業系統類型	Server
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	離線 Windows 程式檔案目錄路徑	D:\Program Files
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	離線 Windows 程式檔案 x86 目錄路徑	D:\Program Files (x86)
\$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	離線 Windows 登錄檔目錄路徑	D:\Windows\System32\config
\$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT	離線 Windows 系統根目錄路徑	D:\Windows
\$env:EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
\$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
\$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
\$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
\$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	離線 Windows 安裝中繼資料	客戶 Powershell 物件

Linux :

變數	描述	範例值
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	適用於 Linux 安裝路徑的 EC2Rescue	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	離線裝置名稱	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	離線根磁碟區 EBS 裝置	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	離線根磁碟區掛載點	/mnt/mount
EC2RESCUE_PYTHON	Python 版本	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AMIPrefix

類型：字串

預設：AWSsupport-EC2Rescue

描述：(選用) 備份 AMI 名稱的字首。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- CreatePostEC2RescueBackup

類型：字串

有效值：true | false

預設：false

描述：(選用) 將其設定為 true，以在執行指令碼後建立 InstanceId 的 AMI，然後再啟動指令碼。自動化完成之後，AMI 會持續存在。您有責任保護對 AMI 的存取，或是將其刪除。

- CreatePreEC2RescueBackup

類型：字串

有效值：true | false

預設：false

描述：(選用) 將其設定為 true 以在執行指令碼之前建立 InstanceId 的 AMI。自動化完成之後，AMI 會持續存在。您有責任保護對 AMI 的存取，或是將其刪除。

- EC2RescueInstanceType

類型：字串

有效值：t2.small | t2.medium | t2.large | t3.small | t3.medium | t3.large | i3.large

預設：t3.medium

描述：(選用) EC2Rescue 執行個體的 EC2 執行個體類型。

- InstanceId

類型：字串

描述：(必要) EC2 執行個體的 ID。重要：AWS Systems Manager 自動化會停止此執行個體。存放在執行個體存放磁碟區的資料會遺失。如果您不是使用彈性 IP，則公有 IP 位址會變更。

- OfflineScript

類型：字串

描述：(必要) 對協助程式執行個體執行的 Base64 編碼指令碼。如果您的來源執行個體是 Linux 則使用 Bash，如果是 Windows 則使用 PowerShell。

- S3BucketName

類型：字串

描述：(選用) 您想要上傳疑難排解日誌之帳戶中的 S3 儲存貯體名稱。請確認儲存貯體政策不會授予不必要的讀取/寫入許可給不需要存取所收集日誌的單位。

- S3Prefix

類型：字串

預設：AWSSupport-EC2Rescue

描述：(選用) S3 日誌的字首。

- SubnetId

類型：字串

預設：SelectedInstanceSubnet

描述：(選用) EC2Rescue 執行個體的子網路 ID。根據預設，會使用與提供的執行個體所在相同的子網路。重要：如果您提供自訂子網路，則子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

- UniqueId

類型：字串

預設：{{ automation:EXECUTION_ID }}

描述：(選用) 自動化的唯一識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議執行自動化的使用者連接 AmazonSSMAutomationRole (AmazonSSMAutomationRole) IAM 受管政策。除了該政策，使用者必須擁有：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource": "arn:aws:lambda:*:An-AWS-Account-ID: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::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
        "arn:aws:iam::An-AWS-Account-ID: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"
}
]
}
```

文件步驟

1. `aws:executeAwsApi` - 描述提供的執行個體
2. `aws:executeAwsApi` - 描述提供的執行個體根磁碟區
3. `aws:assertAwsResourceProperty` - 檢查根磁碟區裝置類型是否為 EBS
4. `aws:assertAwsResourceProperty` - 檢查根磁碟區是否未加密
5. `aws:assertAwsResourceProperty` - 檢查提供子網路 ID
 - a. (使用目前的執行個體子網路) - 如果 `*SubnetId = SelectedInstanceSubnet*` , 則執行 `aws:createStack`以部署 EC2Rescue CloudFormation 堆疊
 - b. (建立新的 VPC) - 如果 `*SubnetId = CreateNewVPC*` , 則執行 `aws:createStack`以部署 EC2Rescue CloudFormation 堆疊
 - c. (使用自訂子網路) - 所有其他情況 :

`aws:assertAwsResourceProperty` - 檢查提供的子網路與提供的執行個體位於相同的可用區域

`aws:createStack` - 部署 EC2Rescue CloudFormation 堆疊
6. `aws:invokeLambdaFunction` - 執行其他輸入驗證
7. `aws:executeAwsApi` - 更新 EC2Rescue CloudFormation 堆疊以建立 EC2Rescue 協助程式執行個體
8. `aws:waitForAwsResourceProperty` - 等待 EC2Rescue CloudFormation 堆疊更新完成
9. `aws:executeAwsApi` - 描述 EC2Rescue CloudFormation 堆疊輸出以取得 EC2Rescue 協助程式執行個體 ID
10. `aws:waitForAwsResourceProperty` - 等待 EC2Rescue 協助程式執行個體成為受管執行個體
11. `aws:changeInstanceState` - 停止提供的執行個體
12. `aws:changeInstanceState` - 停止提供的執行個體
13. `aws:changeInstanceState` - 強制停止提供的執行個體

14aws:assertAwsResourceProperty - 檢查 CreatePreEC2RescueBackup 輸入值

- a. (建立 pre-EC2Rescue 備份) - 如果 *CreatePreEC2RescueBackup = true*
- b. aws:executeAwsApi - 建立所提供執行個體的 AMI 備份
- c. aws:createTags - 標記 AMI 備份

15aws:runCommand - 在 EC2Rescue 協助程式執行個體上安裝 EC2Rescue

16aws:executeAwsApi - 從提供的執行個體分離根磁碟區

17aws:assertAwsResourceProperty - 檢查提供的執行個體平台

- a. (執行個體為 Windows) :

aws:executeAwsApi - 將根磁碟區連接至 EC2Rescue 協助程式執行個體 , 做為 *xvdf*

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Powershell 中執行提供的離線指令碼

- b. (執行個體為 Linux) :

aws:executeAwsApi - 將根磁碟區以 */dev/sdf* 的形式連接至 EC2Rescue 協助程式執行個體

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Bash 中執行提供的離線指令碼

18aws:changeInstanceState - 停止 EC2Rescue 協助程式執行個體

19aws:changeInstanceState - 強制停止 EC2Rescue 協助程式執行個體

20aws:executeAwsApi - 從 EC2Rescue 協助程式執行個體分離根磁碟區

21aws:executeAwsApi - 將根磁碟區連接至提供的執行個體

22aws:assertAwsResourceProperty - 檢查 CreatePostEC2RescueBackup 輸入值

- a. (建立 post-EC2Rescue 備份) - 如果 *CreatePostEC2RescueBackup = true*
- b. aws:executeAwsApi - 建立所提供執行個體的 AMI 備份
- c. aws:createTags - 標記 AMI 備份

23aws:executeAwsApi - 還原所提供執行個體根磁碟區的終止時初始刪除狀態

24aws:changeInstanceState - 還原所提供執行個體的初始狀態 (執行中/已停止)

25aws:deleteStack - 刪除 EC2Rescue CloudFormation 堆疊

輸出

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

Description

AWSPremiumSupport-TroubleshootEC2DiskUsage Runbook 可協助您調查並可能修復 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體根和非根磁碟用量的問題。如果可能，Runbook 會嘗試透過擴展磁碟區及其檔案系統來修復問題。為了執行這些任務，此 Runbook 會根據受影響執行個體的作業系統協調執行數個 Runbook。

第一個 Runbook AWSPremiumSupport-DiagnoseDiskUsageOnWindows或會AWSPremiumSupport-DiagnoseDiskUsageOnLinux決定磁碟問題是否可以透過擴展磁碟區來緩解。

第二個 Runbook AWSPremiumSupport-ExtendVolumesOnWindows或 AWSPremiumSupport-ExtendVolumesOnLinux會使用第一個 Runbook 的輸出來執行修改磁碟區的 Python 程式碼。修改磁碟區後，執行手冊會延伸受影響磁碟區的分割區和檔案系統。

Important

存取 AWSPremiumSupport-* Runbook 需要企業或商業支援訂閱。如需詳細資訊，請參閱[比較 AWS 支援 計劃](#)。

本文件是與 AWS Managed Services (AMS) 合作建置的。AMS 可協助您更有效率且安全地管理 AWS 基礎設施。AMS 也提供營運彈性、增強的安全性和合規性、容量最佳化和節省成本的識別。如需詳細資訊，請參閱[AWS Managed Services](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、Windows

參數

- InstanceId

類型：字串

允許的值：`^i-【a-z0-9】{8,17}$`

描述：（必要）Amazon EC2 執行個體的 ID。

- VolumeExpansionEnabled

類型：布林值

描述：（選用）用於控制文件是否將延伸受影響的磁碟區和分割區的旗標。

預設：true

- VolumeExpansionUsageTrigger

類型：字串

描述：（選用）觸發延伸所需的分割區空間最低用量（百分比）。

允許的值：`^【0-9】{1,2}$`

預設：85

- VolumeExpansionCapSize

類型：字串

描述：（選用）Amazon Elastic Block Store (Amazon EBS) 磁碟區將增加到（以 GiB 為單位）的大小上限。

允許的值：`^【0-9】{1,4}$`

預設：2048

- VolumeExpansionGibIncrease

類型：字串

描述：(選用) 增加磁碟區的 GiB。將使用 VolumeExpansionGibIncrease 和 VolumeExpansionPercentageIncrease 之間的最大淨增。

允許的值：[^]【0-9】{1, 4}\$

預設：20

- VolumeExpansionPercentageIncrease

類型：字串

描述：(選用) 增加磁碟區的百分比。將使用 VolumeExpansionGibIncrease 和 VolumeExpansionPercentageIncrease 之間的最大淨增。

允許的值：[^]【0-9】{1, 2}\$

預設：20

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

1. `aws:assertAwsResourceProperty` - 檢查執行個體是否由 Systems Manager 管理
2. `aws:executeAwsApi` - 描述要取得平台的執行個體。
3. `aws:branch` - 根據執行個體的平台配置自動化。
 - a. 如果執行個體是 Windows :
 - i. `aws:executeAutomation` - 執行 `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` Runbook 以診斷執行個體上的磁碟用量問題。
 - ii. `aws:executeAwsApi` - 取得先前自動化的輸出。
 - iii. `aws:branch` - 根據診斷的輸出，以及是否有可以擴展的磁碟區來緩解提醒。
 - A. 沒有需要擴展的磁碟區：結束自動化。
 - B. 有些磁碟區需要擴展：
 - I. `aws:executeAwsApi` - 建立執行個體的 Amazon Machine Image(AMI)。
 - II. `aws:waitForAwsResourceProperty` - 等待AMI狀態為 `available`。
 - III. `aws:executeAutomation` - 執行 `AWSPremiumSupport-ExtendVolumesOnWindows` Runbook 以執行磁碟區修改，以及作業系統 (OS) 中所需的步驟，讓新空間可用。
 - b. (平台不是視窗) 如果輸入執行個體不是 Windows :
 - i. `aws:executeAutomation` - 執行 `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` Runbook 以診斷執行個體上的磁碟用量問題。
 - ii. `aws:executeAwsApi` - 取得先前自動化的輸出。

- iii. `aws:branch` - 根據診斷的輸出，以及是否有可以擴展的磁碟區來緩解提醒。
 - A. 沒有需要擴展的磁碟區：結束自動化。
 - B. 有些磁碟區需要擴展：
 - I. `aws:executeAwsApi` - 建立執行個體AMI的。
 - II. `aws:waitForAwsResourceProperty` - 等待AMI狀態為 `available`。
 - III. `aws:executeAutomation` - 執行 `AWSPremiumSupport-ExtendVolumesOnLinux` Runbook 以執行磁碟區修改，以及在作業系統中所需的步驟，讓新的空間可用。

輸出

`diagnoseDiskUsageAlertOnWindows.Output`

`extendVolumesOnWindows.Output`

`diagnoseDiskUsageAlertOnLinux.Output`

`extendVolumesOnLinux.Output`

`BackupAMILinux.ImageId`

`BackupAMIWindows.ImageId`

AWSsupport-TroubleshootEC2InstanceConnect

Description

AWSsupport-TroubleshootEC2InstanceConnect 自動化有助於分析和偵測錯誤，防止使用 Amazon EC2 Instance [Connect 連線到 Amazon EC2\) 執行個體](#)。其可識別因不支援的 Amazon Machine Image (AMI)、缺少作業系統層級套件安裝或組態、缺少 AWS Identity and Access Management (IAM) 許可或網路組態問題所造成的問題。

如何運作？

Runbook 會針對 IAM 角色或遇到 Amazon EC2 Instance Connect 問題的使用者，取得 Amazon EC2 執行個體 ID、使用者名稱、連線模式、來源 IP CIDR、SSH 連接埠和 Amazon Resource Name (ARN)。然後，它會檢查使用 Amazon EC2 Instance Connect 連線至 Amazon EC2 執行個體[的先決條件](#)：

- 執行個體正在執行且處於運作狀態。

- 執行個體位於 Amazon EC2 Instance Connect 支援 AWS 的區域。
- Amazon EC2 Instance Connect 支援執行個體的 AMI。
- 執行個體可以連線到執行個體中繼資料服務 (IMDSv2)。
- Amazon EC2 Instance Connect 套件已在作業系統層級正確安裝和設定。
- 網路組態 (安全群組、網路 ACL 和路由表規則) 允許透過 Amazon EC2 Instance Connect 連線至執行個體。
- 用於利用 Amazon EC2 Instance Connect 的 IAM 角色或使用者具有推送金鑰至 Amazon EC2 執行個體的存取權。

Important

- 若要檢查執行個體 AMI、IMDSv2 連線能力和 Amazon EC2 Instance Connect 套件安裝，執行個體必須受 SSM 管理。否則，它會略過這些步驟。如需詳細資訊，請參閱[為什麼我的 Amazon EC2 執行個體未顯示為受管節點](#)。
- 網路檢查只會偵測安全群組和網路 ACL 規則是否在 SourceIpCIDR 提供做為輸入參數時封鎖流量。否則，它只會顯示 SSH 相關規則。
- 此 Runbook 中不會驗證使用 [Amazon EC2 Instance Connect Endpoint](#) 的連線。
- 對於私有連線，自動化不會檢查 SSH 用戶端是否安裝在來源機器上，以及是否可以到達執行個體的私有 IP 地址。

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand

指示

請依照下列步驟設定自動化：

1. 在 AWS Systems Manager 主控台 [AWS Support - Troubleshoot EC2 Instance Connect](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- InstanceId (必要)：

您使用 Amazon EC2 Instance Connect 無法連線的目標 Amazon EC2 執行個體 ID。

- AutomationAssumeRole (選用)：

允許 Systems Manager Automation 代表您執行動作的 IAM 角色 ARN。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 使用者名稱 (必要)：

用於使用 Amazon EC2 Instance Connect 連線至 Amazon EC2 執行個體的使用者名稱。它用於評估是否授予此特定使用者的 IAM 存取權。

- EC2InstanceConnectRoleOrUser (必要)：

IAM 角色的 ARN 或利用 Amazon EC2 Instance Connect 將金鑰推送至執行個體的使用者。

- SSHPort (選用) :

在 Amazon EC2 執行個體上設定的 SSH 連接埠。預設值為 22。連接埠號碼必須介於 1-65535。

- SourceNetworkType (選用) :

Amazon EC2 執行個體的網路存取方法：

- 瀏覽器：您可以從 AWS 管理主控台連線。
- 公有：您可以透過網際網路（例如，您的本機電腦）連線到位於公有子網路中的執行個體。
- 私有：您可以透過執行個體的私有 IP 地址進行連線。
- SourceIpCIDR (選用) :

來源 CIDR，其中包含您將使用 Amazon EC2 Instance Connect 從中記錄之裝置的 IP 地址（例如本機電腦）。範例：172.31.48.6/32。如果公有或私有存取模式未提供任何值，則 Runbook 將不會評估 Amazon EC2 執行個體安全群組和網路 ACL 規則是否允許 SSH 流量。它會改為顯示 SSH 相關規則。

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. 選取執行。
5. 自動化會啟動。
6. 文件會執行下列步驟：

- AssertInitialState :

確保 Amazon EC2 執行個體狀態正在執行。否則，自動化會結束。

- GetInstanceProperties :

取得目前的 Amazon EC2 執行個體屬性 (PlatformDetails、PublicIpAddress、VpcId、SubnetId 和 MetadataHttpEndpoint)。

- GatherInstanceInformationFromSSM :

如果執行個體受 SSM 管理，則取得 Systems Manager 執行個體的 ping 狀態和作業系統詳細資訊。

- `CheckIfAWSRegionSupported` :

檢查 Amazon EC2 執行個體是否位於支援 Amazon EC2 Instance Connect AWS 的區域。

- `BranchOnIfAWSRegionSupported` :

如果 Amazon EC2 Instance Connect 支援該 AWS 區域，則繼續執行。否則，它會建立輸出並結束自動化。

- `CheckIfInstanceAMIsSupported` :

檢查 Amazon EC2 Instance Connect 是否支援與執行個體相關聯的 AMI。

- `BranchOnIfInstanceAMIsSupported` :

如果執行個體 AMI 受支援，它會執行作業系統層級檢查，例如中繼資料連線能力和 Amazon EC2 Instance Connect 套件安裝和組態。否則，它會檢查是否使用 AWS API 啟用 HTTP 中繼資料，然後進入網路檢查步驟。

- `CheckIMDSReachabilityFromOs`

在目標 Amazon EC2 Linux 執行個體上執行 Bash 指令碼，以檢查其是否能夠到達 IMDSv2。

- `CheckEICPackageInstallation` :

在目標 Amazon EC2 Linux 執行個體上執行 Bash 指令碼，以檢查 Amazon EC2 Instance Connect 套件是否已正確安裝和設定。

- `CheckSSHConfigFromOs`

在目標 Amazon EC2 Linux 執行個體上執行 Bash 指令碼，以檢查設定的 SSH 連接埠是否符合輸入參數 `'SSHPort.'`

- `CheckMetadataHTTPEndpointIsEnabled` :

檢查執行個體中繼資料服務 HTTP 端點是否已啟用。

- `CheckEICNetworkAccess` :

檢查網路組態（安全群組、網路 ACL 和路由表規則）是否允許透過 Amazon EC2 Instance Connect 連線至執行個體。

- `CheckIAMRoleOrUserPermissions` :

檢查用於利用 Amazon EC2 Instance Connect 的 IAM 角色或使用者是否具有使用所提供使用者名稱將金鑰推送至 Amazon EC2 執行個體的存取權。

- MakeFinalOutput :

合併所有先前步驟的輸出。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

目標執行個體具有所有必要先決條件的執行：

```
▼ 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
```

不支援目標執行個體 AMI 的執行：

```
▼ 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
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [如何使用 Amazon EC2 Instance Connect 疑難排解連線至 Amazon EC2 執行個體的問題？](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Description

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 自動化 Runbook 用於偵測在 Linux 伺服器上安裝 AWS Application Migration Service (AWS MGN) 和 AWS Elastic Disaster Recovery (AWS DRS) 複寫代理程式時常見的錯誤，以將來源伺服器遷移至 AWS 雲端。

它如何運作？

Runbook AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 採用 Amazon Simple Storage Service (Amazon S3) 路徑，其中 AWS MGN 或 AWS DRS 安裝日誌 `aws_replication_agent_installer.log` 會上傳為 參數。然後，它會執行下列任務：

- 驗證：檢查提供的日誌檔案是否有效，以及是否包含至少一個代理程式安裝。
- 剖析：針對已知 AWS MGN 或 AWS DRS 錯誤，徹底剖析日誌檔中最新的代理程式安裝。
- 錯誤偵測和解決：根據剖析，它會偵測並列出代理程式安裝程序期間的任何錯誤或問題。針對每個偵測到的錯誤，Runbook 會提供詳細的步驟，以協助解決或緩解問題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `s3:GetObject`
- `s3:ListBucket`

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName (必要)：

儲存複寫代理程式日誌的 Amazon S3 儲存貯體名稱。

- S3ObjectKey (必要)：

儲存複寫代理程式安裝程式日誌檔案的 Amazon S3 物件金鑰。範例：如果 Amazon S3 URI 為 `s3://bucket_name/path/to/file/aws_replication_agent_installer.log`，則您應該輸入 `path/to/file/aws_replication_agent_installer.log`。

- ServiceName (必要)：

安裝複寫代理程式的服務名稱。允許的值：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 <code>s3://bucket_name/path/to/file/aws_replication_agent_installer.log</code> then you should provide <code>path/to/file/aws_replication_agent_installer.log</code> 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. 選取執行。
5. 自動化會啟動。

6. 文件會執行下列步驟：

- **ValidateInput**

確保複寫代理程式日誌檔案有效，並使用提供的 Amazon S3 儲存貯體名稱和物件路徑存取，然後傳回最新代理程式安裝的位元組數。

- **CheckReplicationAgentLogErrors**

讀取從最新安裝位元組開始的複寫代理程式日誌檔案，並搜尋已知的 AWS MGN 或 AWS DRS 錯誤。

- **MakeFinalOutput**

建立先前檢查的輸出，包括所發現錯誤和疑難排解建議的相關資訊。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

▼ 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:
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSSupport-TroubleshootRDP

Description

AWSSupport-TroubleshootRDP Runbook 允許使用者檢查或修改目標執行個體上的常見設定，這可能會影響遠端桌面通訊協定 (RDP) 連線，例如 RDP 連接埠、網路層身分驗證 (NLA) 和 Windows 防火牆設定檔。或者，如果使用者明確允許離線修復，則可藉由停用和啟動執行個體以離線套用變更。根據預設，執行手冊會讀取和輸出設定的值。

Important

使用此 Runbook 之前，應仔細檢閱 RDP 設定、RDP 服務和 Windows 防火牆設定檔的變更。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- 動作

類型：字串

有效值：CheckAll | FixAll | Custom

預設：Custom

描述：（選用）【自訂】使用

Firewall、RDPServiceStartupType、RDPServiceAction、RDPPortAction、NLASettingAction 和 RemoteConnections 的值來管理設定。【CheckAll】讀取設定的值而不變更。【FixAll】還原 RDP 預設設定，並停用 Windows 防火牆。

- AllowOffline

類型：字串

有效值：true | false

預設：false

描述：(選用) Fix only - 若您想在線上疑難排解失敗或所提供的執行個體非受管執行個體時允許離線 RDP 修復，請將其設定為 true。備註：對於離線修復，SSM 自動化會停止執行個體，並在嘗試任何操作前建立 AMI。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 防火牆

類型：字串

有效值：檢查 | 停用

預設：Check

描述：(選用) 檢查或停用 Windows 防火牆 (所有描述檔)。

- InstanceId

類型：字串

描述：(必要) 疑難排解 RDP 設定的受管執行個體之 ID。

- NLASettingAction

類型：字串

有效值：檢查 | 停用

預設：Check

描述：(選用) 檢查或停用網路層身分驗證 (NLA)。

- RDPPortAction

類型：字串

有效值：檢查 | 修改

預設：Check

描述：(選用) 檢查目前用於 RDP 連線的連接埠，或將 RDP 連接埠修改回 3389 並重新啟動服務。

- RDPServiceAction

類型：字串

有效值：檢查 | 開始 | 重新啟動 | Force-Restart

預設：Check

描述：(選用) 檢查、啟動、重新啟動或強制重新啟動 RDP 服務 (TermService)。

- RDPServiceStartupType

類型：字串

有效值：檢查 | Auto

預設：Check

描述：(選用) 檢查或設定 RDP 服務以在 Windows 開機時自動啟動。

- RemoteConnections

類型：字串

有效值：檢查 | 啟用

預設：Check

描述：(選用) 在 fDenyTSConnections 設定上執行的動作：Check，Enable。

- S3BucketName

類型：字串

描述：(選用) 僅限離線 - 您想要上傳疑難排解日誌之帳戶中的 S3 儲存貯體名稱。請確認儲存貯體政策不會授予不必要的讀取/寫入許可給不需要存取所收集日誌的單位。

- SubnetId

類型：字串

預設：SelectedInstanceSubnet

描述：(選用) 僅限離線 - 用於執行離線疑難排解的 EC2Rescue 執行個體之子網路 ID。如果未指定子網路 ID，AWS Systems Manager Automation 將建立新的 VPC。重要：子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具備連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。對於線上修復，使用者必須至少有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution 和 ssm:SendCommand 來執行自動化並將命令傳送至執行個體，加上 ssm:GetAutomationExecution，才能讀取自動化輸出。對於離線修復，使用者必須至少有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution、ec2:DescribeInstances 以及 ssm:GetAutomationExecution，才能讀取自動化輸出。AWSSupport-TroubleshootRDP 呼叫 AWSSupport-ExecuteEC2Rescue 以執行離線修復 - 請檢閱 的許可AWSSupport-ExecuteEC2Rescue，以確保您可以成功執行自動化。

文件步驟

1. aws:assertAwsResourceProperty - 檢查執行個體是否為Windows Server執行個體
2. aws:assertAwsResourceProperty - 檢查執行個體是否為受管執行個體
3. (線上疑難排解) 若執行個體為受管執行個體，則：
 - a. aws:assertAwsResourceProperty - 檢查提供的動作值
 - b. (線上檢查) 若 Action = CheckAll，則：

aws:runPowerShellScript - 執行 PowerShell 指令碼以取得 Windows Firewall 設定檔狀態。

aws:executeAutomation - 呼叫 AWSSupport-ManageWindowsService 以取得 RDP 服務狀態。

aws:executeAutomation - 呼叫 AWSSupport-ManageRDPSettings 以取得 RDP 設定。

- c. (線上修復) 若 Action = FixAll，則：

`aws:runPowerShellScript` - 執行 PowerShell 指令碼以停用所有 Windows 防火牆設定檔。

`aws:executeAutomation` - 呼叫 `AWSSupport-ManageWindowsService` 以啟動 RDP 服務。

`aws:executeAutomation` - 呼叫 `AWSSupport-ManageRDPSettings` 以啟用遠端連線並停用 NLA。

d. (線上管理) 若 `Action = Custom`，則：

`aws:runPowerShellScript` - 執行 PowerShell 指令碼來管理 Windows 防火牆設定檔。

`aws:executeAutomation` - 呼叫 `AWSSupport-ManageWindowsService` 來管理 RDP 服務。

`aws:executeAutomation` - 呼叫 `AWSSupport-ManageRDPSettings` 來管理 RDP 設定。

4. (離線修復) 如果執行個體不是受管執行個體，則：

a. `aws:assertAwsResourceProperty` - `Assert AllowOffline = true`

b. `aws:assertAwsResourceProperty` - 宣告動作 = `FixAll`

c. `aws:assertAwsResourceProperty` - 宣告 `SubnetId` 的值

(使用所提供執行個體的子網路) 若 `SubnetId` 為 `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi` - 擷取目前執行個體的子網路。

`aws:executeAutomation` - `AWSSupport-ExecuteEC2Rescue` 使用提供的執行個體子網路執行。

d. (使用提供的自訂子網路) 若 `SubnetId` 不是 `SELECTED_INSTANCE_SUBNET`

`aws:executeAutomation` - `AWSSupport-ExecuteEC2Rescue` 使用提供的 `SubnetId` 值執行。

輸出

`manageFirewallProfiles.Output`

`manageRDPServiceSettings.Output`

`manageRDPSettings.Output`

checkFirewallProfiles.Output

checkRDPSERVICESETTINGS.Output

checkRDPSETTINGS.Output

disableFirewallProfiles.Output

restoreDefaultRDPSERVICESETTINGS.Output

restoreDefaultRDPSETTINGS.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

Description

AWSSupport-TroubleshootSSH Runbook 安裝適用於 Linux 的 Amazon EC2Rescue 工具，然後使用 EC2Rescue 工具來檢查或嘗試修正常見問題，以防止透過 SSH 遠端連線至 Linux 機器。或者，如果使用者明確允許離線修復，則可藉由停用和啟動執行個體以離線套用變更。根據預設，執行手冊會以唯讀模式運作。

[執行此自動化（主控台）](#)

如需有關使用 AWSSupport-TroubleshootSSH Runbook 的資訊，請參閱 AWS Premium Support 中的此[AWSSupport-TroubleshootSSH故障診斷主題](#)。

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

• 動作

類型：字串

有效值：CheckAll | FixAll

預設：CheckAll

描述：(必要) 指定是否檢查問題而不修正，或是檢查並自動修正任何發現的問題。

- AllowOffline

類型：字串

有效值：true | false

預設：false

描述：(選用) Fix only - 若您想在線上疑難排解失敗或所提供的執行個體非受管執行個體時允許離線 SSH 修復，請將其設定為 true。備註：對於離線修復，SSM 自動化會停止執行個體，並在嘗試任何操作前建立 AMI。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) Linux 之 EC2 執行個體的 ID。

- S3BucketName

類型：字串

描述：(選用) 僅限離線 - 您想要上傳疑難排解日誌之帳戶中的 S3 儲存貯體名稱。請確認儲存貯體政策不會授予不必要的讀取/寫入許可給不需要存取所收集日誌的單位。

- SubnetId

類型：字串

預設：SelectedInstanceSubnet

描述：(選用) 僅限離線 - 用於執行離線疑難排解的 EC2Rescue 執行個體之子網路 ID。如果未指定子網路 ID，AWS Systems Manager Automation 將建立新的 VPC。

 Important

子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具備連接 AmazonSSMManagedInstanceCore Amazon 受管政策的 IAM 角色。對於線上修復，使用者必須至少有 ssm：DescribeInstanceInformation、ssm：StartAutomationExecution 和 ssm：SendCommand，才能執行自動化並將命令傳送至執行個體，加上 ssm：GetAutomationExecution，才能讀取自動化輸出。對於離線修補，使用者必須至少有 ssm：DescribeInstanceInformation、ssm：StartAutomationExecution、ec2：DescribeInstances 加上 ssm：GetAutomationExecution，才能讀取自動化輸出。AWSSupport-TroubleshootSSH 呼叫 AWSSupport-ExecuteEC2Rescue 以執行離線修補 - 請檢閱 的許可AWSSupport-ExecuteEC2Rescue，以確保您可以成功執行自動化。

文件步驟

1. aws:assertAwsResourceProperty - 檢查執行個體是否為受管執行個體

a. (線上修復) 如果執行個體是受管執行個體，則：

- i. aws:configurePackage - 透過 安裝適用於 Linux 的 EC2RescueAWS-ConfigureAWSPackage。
- ii. aws:runCommand - 執行 bash 指令碼以執行適用於 Linux 的 EC2Rescue。

b. (離線修復) 如果執行個體不是受管執行個體，則：

- i. aws:assertAwsResourceProperty - 宣告 AllowOffline = true
- ii. aws:assertAwsResourceProperty - 宣告動作 = FixAll
- iii. aws:assertAwsResourceProperty - 宣告 SubnetId 的值

- iv. (使用提供的執行個體子網路) 如果 SubnetId 是 SelectedInstanceSubnet , aws:executeAutomation 我們會 AWSsupport-ExecuteEC2Rescue 使用提供的執行個體子網路執行。
- v. (使用提供的自訂子網路) 如果 SubnetId 不是 SelectedInstanceSubnet , 則使用 AWSsupport-ExecuteEC2Rescue aws:executeAutomation 搭配提供的 SubnetId 值執行。

輸出

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSsupport-TroubleshootSUSERegistration

Description

AWSsupport-TroubleshootSUSERegistration Runbook 可協助您找出向 SUSE Update Infrastructure 註冊 Amazon Elastic Compute Cloud (Amazon EC2) SUSE Linux Enterprise Server 執行個體失敗的原因。自動化輸出提供解決問題的步驟，或協助您疑難排解問題。如果執行個體在自動化期間通過所有檢查，執行個體會向 SUSE 更新基礎設施註冊。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 您要故障診斷的 Amazon EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:DescribeInstanceProperties
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:ListCommands

文件步驟

- aws:assertAwsResourceProperty - 檢查 Amazon EC2 執行個體是否由 管理 AWS Systems Manager。
- aws:runCommand - 檢查 Amazon EC2 執行個體平台是否為 SLES。
- aws:runCommand - 檢查套件cloud-regionsrv-client版本是否大於或等於所需的 9.0.10 版。
- aws:runCommand - 檢查基本產品的符號連結是否損壞，並修正其損壞的連結。
- aws:runCommand - 檢查主機檔案 (/etc/hosts) 是否包含 的記錄smt-ec2-suscloud.net。自動化會移除任何重複的項目。
- aws:runCommand - 檢查是否已安裝 curl命令。
- aws:runCommand - 檢查 Amazon EC2 執行個體是否可以存取執行個體中繼資料服務 (IMDS) 地址 169.254.169.254。

- `aws:runCommand` - 檢查 Amazon EC2 執行個體是否有帳單代碼或 AWS Marketplace 產品代碼。
- `aws:runCommand` - 檢查 Amazon EC2 執行個體是否可以透過 HTTPS 到達至少 1 個區域伺服器。
- `aws:runCommand` - 檢查 Amazon EC2 執行個體是否可以透過 HTTP 連線至 Subscription Management Tool (SMT) 伺服器。
- `aws:runCommand` - 檢查 Amazon EC2 執行個體是否可以透過 HTTPS 連線至 Subscription Management Tool (SMT) 伺服器。
- `aws:runCommand` - 檢查 Amazon EC2 執行個體是否可以透過 HTTPS 到達 `smt-ec2.susecloud.net` 地址。
- `aws:runCommand` - 向 SUSE Update Infrastructure 註冊 Amazon EC2 執行個體。
- `aws:executeScript` - 收集並輸出所有先前步驟的輸出。

AWSSupport-TroubleshootWindowsPerformance

Description

Runbook `AWSSupport-TroubleshootWindowsPerformance` 可協助疑難排解 Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體上持續發生的效能問題。Runbook 會從目標執行個體擷取日誌，並分析 CPU、記憶體、磁碟和網路效能指標。或者，自動化可以擷取程序傾印，以協助您判斷效能降低的潛在原因。如果您允許此 Runbook 安裝事件和系統日誌，自動化也會使用最新的 [EC2Rescue](#) 工具來擷取事件和系統日誌。

如何運作？

Runbook 會執行下列步驟：

- 檢查 Amazon EC2 執行個體的先決條件。
- 在 Amazon EC2 Windows 執行個體的根磁碟中產生效能日誌
- 將擷取的日誌存放在資料夾中 `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- 如果提供 Amazon Simple Storage Service (Amazon S3) 儲存貯體，且自動化擔任角色具有必要的許可，則擷取的日誌會上傳至 Amazon S3 儲存貯體。
- 如果您選擇安裝 Amazon EC2 Windows 執行個體，則將最新的 `EC2Rescue` 工具安裝到 Amazon EC2 Windows 執行個體，以擷取事件和系統日誌，但不會分析程序傾印和擷取的日誌 `EC2Rescue`。

Important

- 若要執行此 Runbook，Amazon EC2 Windows 執行個體必須由 管理 AWS Systems Manager。如需詳細資訊，請參閱[為什麼我的 Amazon EC2 執行個體未顯示為受管節點](#)。
- 若要執行此執行手冊，Amazon EC2 Windows 執行個體必須在 Windows 8.1 / Windows Server 2012 R2 (6.3) 或更新版本上執行，並使用 PowerShell 4.0 或更新版本。如需詳細資訊，請參閱 [Windows 作業系統版本](#)。
- 對於產生效能日誌，根裝置上至少需要 10 GB 的可用空間。如果根磁碟大於 100 GB，則可用空間必須大於磁碟大小的 10%。如果您在執行期間傾印程序，可用空間必須大於 10 GB，加上程序耗用超過 10 GB 記憶體時程序耗用的總記憶體大小。
- 在根裝置上產生的日誌不會自動刪除。
- Runbook 不會解除安裝 EC2Rescue 工具。如需詳細資訊，請參閱[EC2Rescue 使用 Windows Server](#)。
- 最佳實務是在效能影響期間執行此自動化。您也可以定期使用 AWS Systems Manager State Manager 關聯或排程 AWS Systems Manager 維護 Windows 來執行它。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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`

(選用) 連接到執行個體描述檔的 IAM 角色或在執行個體上設定的 IAM 使用者需要下列動作，才能將日誌上傳至為參數指定的 Amazon S3 儲存貯體 `LogUploadBucketName`：

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-TroubleshootWindowsPerformance](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- `AutomationAssumeRole` (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `InstanceId` (必要)：

您要執行自動化的目標 Amazon EC2 Windows 執行個體 ID。執行個體必須由 Systems Manager 管理，才能執行自動化。

- CaptureProcessDump（選用）：

要擷取的程序傾印類型。自動化可以為程序擷取一個程序傾印，這些程序可能會在自動化開始時造成效能影響。執行個體根磁碟區需要至少 10 GB 的可用空間（根磁碟區大小大於 100 GB 時大於磁碟大小的 10%，而 10 GB 加上程序耗用超過 10 GB 記憶體時程序耗用的總記憶體大小）。

- LogCaptureDuration（選用）：

此自動化會在問題存在時擷取日誌的分鐘數 15，介於 1 和 之間。預設值為 5。

- LogUploadBucketName（選用）：

帳戶中您要上傳日誌的 Amazon S3 儲存貯體。儲存貯體必須使用伺服器端加密 (SSE) 設定，且儲存貯體政策不得將不必要的讀取/寫入許可授予不需要存取所擷取日誌的各方。Amazon EC2 Windows 執行個體必須能夠存取 Amazon S3 儲存貯體。

- InstallEC2RescueTool（選用）：

將設定為 Yes 允許 Runbook 安裝最新版本 EC2Rescue 的工具，以擷取 Windows Events 和 System Log。預設值為 No。

- 確認（必要）：

閱讀此自動化執行手冊所執行動作的完整詳細資訊，如果您同意，請輸入 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

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.

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.

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`.

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).

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.

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.

4. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- **CheckConcurrency:**

確保只有一個針對執行個體的此 Runbook 執行。如果 Runbook 找到另一個以相同執行個體為目標的執行，則會傳回錯誤並結束。

- **AssertInstanceIsWindows:**

宣告 Amazon EC2 執行個體正在 Windows 作業系統上執行。否則，自動化會結束。

- **AssertInstanceIsManagedInstance:**

宣告 Amazon EC2 執行個體由 管理 AWS Systems Manager。否則自動化會結束。

- **VerifyPrerequisites:**

驗證執行個體作業系統上的 PowerShell 版本，並確保執行個體可以透過 Systems Manager 連線以執行 PowerShell 命令。此自動化支援在 Windows 8.1 / Server 2012 R2 (6.3) 或更新版本上執行的 PowerShell 4.0 和更高版本。如果版本較舊，自動化會失敗。當您選擇將日誌上傳至 Amazon S3 儲存貯體時，此自動化會檢查 AWS Tools for PowerShell 模組是否可用。如果沒有，自動化會結束。

- **BranchOnProcessDump:**

如果您設定分支以擷取影響效能的程序傾印，則分支會依據 進行。

- **CaptureProcessDump:**

檢查執行個體是否有足夠的空間來執行此自動化（當您選擇最高 CPU/記憶體時）。

- **CapturePerformanceLogs:**

再次檢查磁碟空間，並在執行個體上執行 PowerShell 指令碼，以建立 perfmon 計數器並啟動效能監視器和 Windows 效能記錄器記錄。指令碼會在符合定義的 LogCaptureDuration 後停止。

- **SummarizePerformanceLogs:**

總結上一個步驟產生的 XML 報告 CapturePerformanceLogs，以尋找耗用最多 WorkingSet64（記憶體）和 % 處理器時間 (CPU) 的負責程序，顯示為自動化上的輸出。它會產生有關 LogicalDisk、Network Interface、Memory、TCPv4、IPv4 和 UDPv4 使用量的類似資訊，並將其儲存在 analysis_output.log 輸出資料夾中。

- **BranchOnInstallEC2Rescue:**

如果您將分支設定為在 Amazon EC2 執行個體中安裝最新的 EC2Rescue 工具，則分支。

- **InstallEC2RescueTool:**

在執行個體作業系統中安裝 EC2Rescue 工具，以使用 擷取 EC2Rescue 日誌 AWS-ConfigureAWSPackage。

- **RunEC2RescueTool:**

在執行個體作業系統中執行 EC2Rescue 工具，以擷取所有所需的日誌。只會 EC2Rescue 擷取必要的日誌以節省空間。

- **BranchOnIfS3BucketProvided:**

根據 的使用者輸入分支 LogUploadBucketName，以查看是否有儲存貯體名稱可供上傳日誌。

- **GetS3BucketPublicStatus:**

確定是否提供 Amazon S3 儲存貯體，如果提供，則確認 Amazon S3 儲存貯體不是公開的，並使用 SSE 設定。

- **UploadLogResult:**

將日誌上傳至提供的 Amazon S3 儲存貯體。如果 PowerShell 版本是 5.0 或更新版本，它會將日誌壓縮為 ZIP 封存檔並上傳。它會在上傳完成後刪除 ZIP 檔案。如果 PowerShell 版本低於 5.0，則會將檔案直接上傳至資料夾。

- **CleanUpLogsOnFailure:**

清除 CapturePerformanceLogs 步驟失敗時產生的所有日誌。如果 SSM Agent 無法正常運作，或 Windows 系統沒有回應，則 CleanUpLogsOnFailure 步驟可能會失敗或逾時。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

在目標執行個體具有所有必要先決條件的情況下執行。

▼ Outputs

CaptureProcessDump.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

CapturePerformanceLogs.Output
The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX** was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX**
Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX** created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX**
Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX** 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-**XXXXXXXXXXXX** is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX** has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX**
Data Collector Set TroubleshootWindowsPerformance-**XXXXXXXXXXXX** deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance**XXXXXXXXXXXX**
The captured log files will not be deleted by this automation, please manually delete it after analysis.
|

RunEC2RescueTool.Output
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance**XXXXXXXXXXXX**_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 %
sppsvc	Processor	0.00	106.00	9.00
WmiPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenValObj	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

目標執行個體位於 Linux 平台上且執行失敗的執行。您可以選擇步驟 ID 以查看失敗詳細資訊。

▼ Outputs

CapturePerformanceLogs.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

CleanUpLogsOnFailure.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

SummarizePerformanceLogs.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

VerifyPrerequisites.Output
No output available yet because the step is not successfully executed

Execution status

Overall status
🔴 Failed

All executed steps
2

Succeeded
1

Failed
1

Cancelled
0

TimedOut
0

Executed steps (2)

Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time	End time
XXXXXXXXXXXX	1	CheckConcurrency	aws:executeScript	🟢 Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
XXXXXXXXXXXX 0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	🔴 Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

步驟 的失敗詳細資訊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'].	

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSsupport-TroubleshootWindowsUpdate

Description

AWSsupport-TroubleshootWindowsUpdate Runbook 用於識別可能失敗 Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體 Windows 更新的問題。

如何運作？

Runbook 會執行下列步驟：

- 檢查目標 Amazon EC2 執行個體是否由 管理 AWS Systems Manager。
- 檢查 Systems Manager 修補操作是否支援 AWS Systems Manager Agent (SSM Agent) 和 Windows Server 版本。
- 檢查建議用於 Windows 更新的可用磁碟空間，以及重新啟動是否待定。待重新啟動通常表示更新正在等待中，在執行其他更新之前需要重新啟動。
- 在作業系統層級設定代理設定，有助於疑難排解連線問題。
- 執行 Amazon Simple Storage Service (Amazon S3) 端點連線能力測試，並呼叫 [GetDeployablePatchSnapshotForInstance](#) API 操作，以擷取受管節點使用的修補程式基準的目前快照。
- 如果連線失敗，會提供執行AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2手冊的選項，以分析執行個體與 Amazon S3 端點的連線。

- 驗證 Windows 更新組態並測試 Windows Server Update Services (WSUS) (如適用)。

Important

- 不支援 Active Directory 網域控制站。
- 不支援 Windows Server 2008 R2 版或舊版。
- 不支援 SSM Agent 1.2.371 或舊版。
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook 使用 [VPC Reachability Analyzer](#) 來分析來源和服務端點之間的網路連線。每個來源和目的地之間的分析執行都會向您收取費用。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。
- 並非所有支援 Systems Manager 的區域都提供 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation

- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

 Note

若要執行子 Runbook `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`，請新增[本文件](#)中列出的許可。

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-TroubleshootWindowsUpdate](#) 中導覽至 。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId (必要)：

輸入 Windows 更新失敗的 Amazon EC2 執行個體 ID。

- RunVpcReachabilityAnalyzer (選用)：

如果網路問題是由延伸檢查決定，或指定的執行個體 ID 不是受管執行個體，請指定 `true` 來執行 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 自動化。如需此子自動化的詳細資訊，請參閱 [文件](#)。預設值為 `false`。

- RetainVpcReachabilityAnalysis (選用)：

只有在 `RunVpcReachabilityAnalyzer` 為 `true` 時才相關。指定 `true` 以保留建立的網路洞見路徑和相關分析 `Reachability Analyzer`。根據預設，這些資源會在成功分析後刪除。如果您選擇保留分析，子 Runbook 不會刪除分析，您可以在 Amazon VPC 主控台中將其視覺化。主控台連結將在子自動化輸出中提供。預設值 `false`。

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance.

☒ 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.

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'.

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'.

false

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- **getWindowsServerAndSSMAgentVersion:**

驗證目標執行個體是由 管理，AWS Systems Manager 並取得 SSM Agent 版本和 Windows 版本的詳細資訊。

- **assertIfInstanceIsSsmManaged:**

確保 Amazon EC2 執行個體由 AWS Systems Manager (SSM) 管理，否則自動化會結束。

- **CheckProxy:**

檢查 Windows 執行個體的所有代理類型。

- **CheckPrerequisites:**

取得 SSM Agent 版本和 Windows 版本，並判斷其是否為 Active Directory 網域控制站 (DC)。如果執行個體是 DC 或不支援 SSM Agent 或 Windows 版本，則 Runbook 會停止。

- **CheckDiskSpace:**

如果足夠執行 Windows 更新，則透過 Windows 執行個體取得並驗證可用的磁碟空間。

- **CheckPendingReboot:**

檢查 Windows 執行個體上是否有任何待處理的重新啟動。

- **CheckS3Connectivity:**

檢查執行個體是否可以到達的 Amazon S3 端點Patchbaseline。

- **branchOnRunVpcReachabilityAnalyzer:**

如果 RunVpcReachabilityAnalyzer 為 true，則它會分支自動化，以針對偵錯 Amazon S3 連線執行更深入的分析。

- **GenerateEndpoints:**

產生端點以對 Amazon S3 端點進行延伸連線檢查。

- **analyzeAwsEndpointReachabilityFromEC2:**

呼叫自動化執行手冊 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2。以檢查所選執行個體對所需端點的可及性。

- **CheckWindowsUpdateServices:**

檢查 Windows Update 服務狀態和啟動類型。

- **CheckWindowsUpdateSettings:**

檢查透過 Windows 執行個體設定的 Windows Update 政策。

- **CheckWSUSSettings:**

檢查 Windows 更新是否使用 WSUS 或 Microsoft Update Catalog 設定，並驗證連線。

- **CheckWUGlobalSettings:**

檢查透過 Windows 執行個體設定的 Windows Update 全域設定。

- **GenerateLogs:**

將 Windows Update 日誌和 CBS 日誌下載到執行個體桌面，並檢查 Windows 事件日誌是否失敗。

- **FinalReport:**

產生所有步驟的完整報告。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

```

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
"

```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)

- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 與服務相關的文件

- 如需詳細資訊，請參閱文章 [Troubleshoot Windows Update](#)。

AWSSupport-UpgradeWindowsAWSDrivers

Description

AWSSupport-UpgradeWindowsAWSDrivers Runbook 升級或修復指定 EC2 執行個體上的儲存和網路 AWS 驅動程式。Runbook 會呼叫 SSM Agent 嘗試線上安裝最新版本的 AWS 驅動程式。如果 SSM Agent 無法聯絡，則如果明確請求，Runbook 可以執行 AWS 驅動程式的離線安裝。

此 Runbook 支援下列作業系統：

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note

線上和離線升級都會在嘗試任何操作之前建立 AMI，這會在自動化完成後持續存在。您有責任保護對 AMI 的存取，或是將其刪除。線上方法會重新啟動執行個體做為升級程序的一部分，而離線方法需要提供的 EC2 執行個體先停止再啟動。

Important

如果您的執行個體 AWS Systems Manager 使用 VPC 端點連線至，除非在 us-east-1 區域中使用，否則此 Runbook 將會失敗。此 Runbook 也會在網域控制器上失敗。若要更新網域控制器上的 AWS PV 驅動程式，請參閱[升級網域控制器 \(AWS PV 升級\)](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AllowOffline

類型：字串

有效值：true | false

預設：false

描述：(選用) 如果您允許在線上安裝無法執行時使用離線驅動程式升級，則將其設為 true。備註：離線方法需要所提供的 EC2 執行個體先停止再啟動。存放在執行個體存放磁碟區的資料會遺失。如果您不是使用彈性 IP，則公有 IP 位址會變更。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ForceUpgrade

類型：字串

有效值：true | false

預設：false

描述：(選用) 僅限離線 - 如果您允許在執行個體已安裝最新驅動程式時繼續執行離線驅動程式升級，則將其設為 true。

- InstanceId

類型：字串

描述：(必要) Windows Server 之 EC2 執行個體的 ID。

- SubnetId

類型：字串

預設：SelectedInstanceSubnet

描述：(選用) 僅限離線 - 用於執行離線驅動程式升級的 EC2Rescue 執行個體之子網路 ID。如果未指定子網路 ID，Systems Manager Automation 將建立新的 VPC。

 Important

子網路必須與 InstanceId 位於相同的可用區域，且必須允許存取 SSM 端點。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

接收命令的 EC2 執行個體必須至少具備包含 ssm:StartAutomationExecution 和 ssm:SendCommand 許可的 IAM 角色，才能執行自動化和傳送命令至執行個體，以及 ssm:GetAutomationExecution，才能讀取自動化輸出。您可以將 AmazonSSMManagedInstanceCore Amazon 受管政策附加到 IAM 角色以提供這些許可。不過，建議您針對此目的使用自動化 IAM 角色 AmazonSSMAutomationRole。如需詳細資訊，請參閱[使用 IAM 設定自動化的角色](#)。

如果您要執行離線升級，請參閱 [AWSSupport-StartEC2RescueWorkflow](#) 所需的許可。

文件步驟

1. aws:assertAwsResourceProperty - 驗證輸入執行個體是 Windows。
2. aws:assertAwsResourceProperty - 驗證輸入執行個體是受管執行個體。若是如此，則線上升級會開始，否則會評估離線升級。
 - a. (線上升級) 如果輸入執行個體是受管執行個體：
 - i. aws:createImage - 建立 AMI 備份。
 - ii. aws:createTags - 標記 AMI 備份。

- iii. `aws:runCommand` - 透過 安裝 ENA 網路驅動程式AWS-ConfigureAWSPackage。
- iv. `aws:runCommand` - 透過 安裝 NVMe 驅動程式AWS-ConfigureAWSPackage。
- v. `aws:runCommand` - 透過 安裝 AWS PV 驅動程式AWS-ConfigureAWSPackage。
- b. (離線升級) 如果輸入執行個體不是受管執行個體：
 - i. `aws:assertAwsResourceProperty` - 確認 AllowOffline 旗標設定為 true。如果是這樣，離線升級會開始，否則自動化會結束。
 - ii. `aws:changeInstanceState` - 停止來源執行個體。
 - iii. `aws:changeInstanceState` - 強制停止來源執行個體。
 - iv. `aws:createImage` - 建立來源執行個體的 AMI 備份。
 - v. `aws:createTags` - 標記來源執行個體的 AMI 備份。
 - vi. `aws:executeAwsApi` - 為執行個體啟用 ENA
 - vii. `aws:assertAwsResourceProperty` - 宣告 ForceUpgrade 旗標。
 - viii. 強制離線升級) 如果 ForceUpgrade = true，則執行 `aws:executeAutomation` 以 `AWSSupport-StartEC2RescueWorkflow` 使用驅動程式強制升級指令碼叫用。這會安裝驅動程式，無論目前安裝的版本為何
 - ix. (離線升級) 如果 ForceUpgrade = false，則執行 `aws:executeAutomation` 以 `AWSSupport-StartEC2RescueWorkflow` 呼叫驅動程式升級指令碼。

輸出

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup.ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Output`

`forceUpgradeDriversOffline.Output`

Amazon ECS

AWS Systems Manager 自動化為 Amazon Elastic Container Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

AWSSupport-CollectECSInstanceLogs

Description

AWSSupport-CollectECSInstanceLogs Runbook 會從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體收集作業系統和 Amazon Elastic Container Service (Amazon ECS) 相關日誌檔案，以協助您疑難排解常見的 Amazon ECS 問題。當自動化收集相關聯的日誌檔案時，會變更檔案系統。這些變更包括建立暫時目錄和日誌目錄、將日誌檔案複製到這些目錄，以及將日誌檔案壓縮至封存。

如果您指定 LogDestination 參數的值，目標執行個體必須安裝 Linux 執行個體的 AWS Command Line Interface (AWS CLI) 或 Windows PowerShell for Windows 執行個體 AWS 的工具。自動化會評估您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的政策狀態。為了協助保護從 Amazon EC2 執行個體收集之日誌的安全性，如果政策狀態 isPublic 設定為 true，或存取控制清單 (ACL) 將 READ|WRITE 許可授予 All Users Amazon S3 預先定義的群組，則不會上傳日誌。此外，如果您帳戶中沒有提供的儲存貯體，則不會上傳日誌。如需 Amazon S3 預先定義的群組的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 預先定義群組](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ECSInstanceid

類型：字串

描述：(必要) 您要從中收集日誌的執行個體 ID。您指定的執行個體必須由 Systems Manager 管理。

- LogDestination

類型：字串

描述：(選用) AWS 帳戶 要上傳封存日誌的 Amazon S3 儲存貯體。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- ssm:DescribeInstanceInformation

建議您在 `ECSInstanceId` 參數中指定的 Amazon EC2 執行個體具有連接 Amazon 受管政策的 IAM `AmazonSSMManagedInstanceCore` 角色。若要將日誌封存上傳至您在 `LogDestination` 參數中指定的 Amazon S3 儲存貯體，您必須新增下列許可：

- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`

文件步驟

- `assertInstanceIsManaged` - 驗證您在 `ECSInstanceId` 參數中指定的執行個體是否由 Systems Manager 管理。
- `getInstancePlatform` - 取得 `ECSInstanceId` 參數中指定執行個體之作業系統 (OS) 平台的相關資訊。
- `verifyInstancePlatform` - 根據作業系統平台分支自動化。
- `runLogCollectionScriptOnLinux` - 在 Linux 執行個體上收集作業系統和 Amazon ECS 相關日誌檔案，並在 `/var/log/collectECSlogs` 目錄中建立封存檔案。
- `runLogCollectionScriptOnWindows` - 在 Windows 執行個體上收集作業系統和 Amazon ECS 相關日誌檔案，並在 `C:\ProgramData\collectECSlogs` 目錄中建立封存檔案。
- `verifyIfS3BucketProvided` - 驗證是否已為 `LogDestination` 參數指定值。
- `runUploadScript` - 根據作業系統平台配置自動化步驟。
- `runUploadScriptOnLinux` - 將日誌封存上傳至 `LogDestination` 參數中指定的 Amazon S3 儲存貯體，並從作業系統刪除封存的日誌檔案。
- `runUploadScriptOnWindows` - 將日誌封存上傳至 `LogDestination` 參數中指定的 Amazon S3 儲存貯體，並從作業系統刪除封存的日誌檔案。

AWS-InstallAmazonECSAgent

Description

`AWS-InstallAmazonECSAgent` Runbook 會在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上安裝 Amazon Elastic Container Service (Amazon ECS) 代理程式。此 Runbook 僅支援 Amazon Linux 和 Amazon Linux 2 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InstanceIds

類型：StringList

描述：（必要）您要安裝 Amazon ECS 代理程式的 Amazon EC2 執行個體 IDs。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

文件步驟

`aws:executeScript` - 在您於 `InstanceIds` 參數中指定的 Amazon EC2 執行個體上安裝 Amazon ECS 代理程式。

輸出

`InstallAmazonECSAgent.SuccessfulInstances` - 安裝 Amazon ECS 代理程式成功所在的執行個體 ID。

`InstallAmazonECSAgent.FailedInstances` - 安裝 Amazon ECS 代理程式失敗的執行個體 ID。

`InstallAmazonECSAgent.InProgressInstances` - 正在安裝 Amazon ECS 代理程式的執行個體 ID。

AWS-ECSRunTask

Description

AWS-ECSRunTask Runbook 會執行您指定的 Amazon Elastic Container Service (Amazon ECS) 任務。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- capacityProviderStrategy

類型：字串

描述：(選用) 用於任務的容量提供者策略。

- 叢集

類型：字串

描述：(選用) 執行任務的叢集的簡短名稱或 ARN。如果您未指定叢集，則會使用預設叢集。

- count

類型：字串

描述：(選用) 要放置在叢集上之指定任務的執行個體數量。您可以為每個請求指定最多 10 個任務。

- enableECSTags

類型：布林值

描述：(選用) 指定是否對任務使用 Amazon ECS 受管標籤。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[標記您的 Amazon ECS 資源](#)。

- enableExecuteCommand

類型：布林值

描述：(選用) 決定是否為此任務中的容器啟用執行命令功能。如果為 true，這會啟用任務中所有容器的執行命令功能。

- 群組

類型：字串

描述：(選用) 要與任務建立關聯的任務群組名稱。預設值是任務定義的系列名稱。例如 family:my-family-name。

- launchType

類型：字串

有效值：EC2 | FARGATE | EXTERNAL

描述：(選用) 執行獨立任務的基礎設施。

- networkConfiguration

類型：字串

描述：(選用) 任務的網路組態。使用 awsvpc 網路模式接收自己的彈性網路介面的任務定義需要此參數，其他網路模式不支援此參數。

- 覆寫

類型：字串

描述：(選用) JSON 格式的容器覆寫清單，指定指定指定任務定義中的容器名稱，以及應接收的覆寫。您可以使用命令覆寫來覆寫任務定義或 Docker 映像中指定的容器的預設命令。您也可以覆寫任務定義或容器上的 Docker 映像中指定的現有環境變數。此外，您可以使用環境覆寫來新增環境變數。

- placementConstraints

類型：字串

描述：(選用) 用於任務的置放限制物件陣列。您可以為每個任務指定最多 10 個限制，包括任務定義中的限制，以及在執行時間指定的限制。

- placementStrategy

類型：字串

描述：(選用) 用於任務的置放策略物件。您可以為每個任務指定最多 5 個策略規則。

- platformVersion

類型：字串

描述：(選用) 任務使用的平台版本。平台版本僅針對 Fargate 上託管的任務指定。如果未指定平台版本，將使用 LATEST 平台版本。

- propagateTags

類型：字串

描述：(選用) 判斷標籤是否從任務定義傳播到任務。如果沒有指定值，則不會傳播標籤。標籤只能在任務建立期間傳播至任務。

- `referenceId`

類型：字串

描述：(選用) 用於任務的參考 ID。參考 ID 的長度上限為 1024 個字元。

- `startedBy`

類型：字串

描述：(選用) 任務啟動時指定的選用標籤。這可協助您篩選 `ListTasks` API 操作的結果，以識別哪些任務屬於特定任務。最多允許 36 個字母 (大寫和小寫)、數字、連字號 (-) 和底線 (_)。

- 標籤

類型：字串

描述：(選用) 您要套用至任務的中繼資料，以協助您分類和組織任務。每個標籤都包含使用者定義的金鑰和值。

- `taskDefinition`

類型：字串

描述：(選用) 要執行之任務定義的 `family` 和 `revision(family:revision)` 或完整 ARN。如果未指定修訂版，則會使用最新的 ACTIVE 修訂版。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ecs:RunTask`

文件步驟

`aws:executeScript` - 根據您為 Runbook 輸入參數指定的值執行 Amazon ECS 任務。

AWSSupport-TroubleshootECSContainerInstance

Description

`AWSSupport-TroubleshootECSContainerInstance` Runbook 可協助您疑難排解無法向 Amazon ECS 叢集註冊的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。此自動化會檢閱

執行個體的使用者資料是否包含正確的叢集資訊、執行個體描述檔是否包含必要的許可，以及網路組態問題。

Important

若要成功執行此自動化，Amazon EC2 執行個體的狀態必須為 `running`，Amazon ECS 叢集狀態必須為 `ACTIVE`。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：（必要）執行個體無法註冊的 Amazon ECS 叢集名稱。

- InstanceId

類型：字串

描述：（必要）您要疑難排解的 Amazon EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

文件步驟

aws : executeScript : 檢閱 Amazon EC2 執行個體是否符合向 Amazon ECS 叢集註冊所需的先決條件。

AWSSupport-TroubleshootECSTaskFailedToStart

Description

AWSSupport-TroubleshootECSTaskFailedToStart Runbook 可協助您針對 Amazon ECS 叢集中的 Amazon Elastic Container Service (Amazon ECS) 任務無法啟動的原因進行故障診斷。您必須在與 AWS 區域 任務無法啟動的相同 中執行此 Runbook。Runbook 會分析下列可能阻止任務啟動的常見問題：

- 與已設定容器登錄檔的網路連線
- 缺少任務執行角色所需的 IAM 許可
- VPC 端點連線

- 安全群組規則組態
- AWS Secrets Manager 秘密參考
- 記錄組態

Note

如果分析判斷需要測試網路連線，則會在您的帳戶中建立 Lambda 函數和必要的 IAM 角色。這些資源用於模擬失敗任務的網路連線。自動化會在不再需要這些資源時將其刪除。不過，如果自動化無法刪除資源，您必須手動執行此操作。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：（必要）任務無法啟動的 Amazon ECS 叢集名稱。

- CloudwatchRetentionPeriod

類型：整數

描述：（選用）將 Lambda 函數日誌儲存在 Amazon CloudWatch Logs 中的保留期間，以天為單位。只有在分析判斷需要測試網路連線時，才需要這樣做。

有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

預設：30

- TaskId

類型：字串

描述：（必要）失敗任務的 ID。使用最近失敗的任務。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- cloudtrail:LookupEvents
- ec2:DeleteNetworkInterface
- ec2:DescribeInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- 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: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`

文件步驟

- `aws:executeScript` - 驗證啟動自動化的使用者或角色是否具有必要的 IAM 許可。如果您沒有足夠的許可來使用此 Runbook，則缺少的必要許可會包含在自動化的輸出中。
- `aws:branch` - 根據您是否具有 Runbook 所有必要動作的許可進行分支。

- `aws:executeScript` - 如果分析判斷需要測試網路連線，請在 VPC 中建立 Lambda 函數。
- `aws:branch` - 根據上一個步驟的結果進行分支。
- `aws:executeScript` - 分析啟動任務失敗的可能原因。
- `aws:executeScript` - 刪除此自動化建立的資源。
- `aws:executeScript` - 格式化自動化的輸出，將分析結果傳回至主控台。在自動化完成之前，您可以在此步驟之後檢閱分析。
- `aws:branch` - 根據 Lambda 函數和相關資源是否已建立且需要刪除進行分支。
- `aws:sleep` - 休眠 30 分鐘，以便刪除 Lambda 函數的彈性網路界面。
- `aws:executeScript` - 刪除 Lambda 函數網路界面。
- `aws:executeScript` - 格式化 Lambda 函數網路界面刪除步驟的輸出。

AWS-UpdateAmazonECSAgent

Description

AWS-UpdateAmazonECSAgent Runbook 會在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上更新 Amazon Elastic Container Service (Amazon ECS) 代理程式。此 Runbook 僅支援 Amazon Linux 和 Amazon Linux 2 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterARN

類型：StringList

描述：(必要) 容器執行個體註冊的 Amazon ECS 叢集的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeImage
- ec2:DescribeInstance
- ec2:DescribeInstanceAttribute
- ecs:DescribeContainerInstances
- ecs:DescribeClusters
- ecs:ListContainerInstances
- ecs:UpdateContainerAgent

文件步驟

aws:executeScript - 更新您在ClusterARN參數中指定的 Amazon ECS 叢集上的 Amazon ECS 代理程式。

輸出

UpdateAmazonECSAgent.UpdatedContainers - Amazon ECS 代理程式更新成功的執行個體 ID。

UpdateAmazonECSAgent.FailedContainers - 更新 Amazon ECS 代理程式失敗的執行個體 ID。

UpdateAmazonECSAgent.InProgressContainers - 正在更新 Amazon ECS 代理程式的執行個體 ID。

Amazon EFS

AWS Systems Manager 自動化為 Amazon Elastic File System 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSsupport-CheckAndMountEFS](#)

AWSsupport-CheckAndMountEFS

Description

AWSsupport-CheckAndMountEFS Runbook 會驗證掛載 Amazon Elastic File System (Amazon EFS) 檔案系統的先決條件，並在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上掛載檔案系統。此 Runbook 支援使用 DNS 名稱掛載 Amazon EFS 檔案系統，或使用掛載目標的 IP 地址。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 動作

類型：字串

有效值：Check | CheckAndMount

描述：(必要) 判斷 Runbook 是否驗證先決條件，或驗證先決條件並掛載檔案系統。

- EfsId

類型：字串

描述：(必要) 您要掛載的檔案系統 ID。

- InstanceId

類型：字串

描述：(必要) 您要掛載檔案系統的 Amazon EC2 執行個體 ID。

- MountOptions

類型：字串

描述：(選用) 您希望在掛載檔案系統時使用的 Amazon EFS 掛載協助程式支援的選項。如果您指定 `tls` 選項，請確認已在目標執行個體上升級 `stunnel`。

- MountPoint

類型：字串

描述：(選用) 您要掛載檔案系統的目錄。如果您指定 Action 參數 `Check` 的值，則不應指定此參數。

- MountTargetIP

類型：字串

描述：(選用) 掛載目標的 IP 地址。依 IP 地址掛載適用於停用 DNS 的環境中，例如停用 DNS 主機名稱的虛擬私有雲端 (VPCs)。此外，如果您的環境使用 Amazon Route 53 (Route 53) 以外的 DNS 供應商，您可以使用此選項。

- 區域

類型：字串

描述：(必要) Amazon EC2 AWS 區域 執行個體和檔案系統所在的。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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:*

文件步驟

- aws:executeScript - 收集您在 InstanceId 參數中指定的 Amazon EC2 執行個體詳細資訊。

- `aws:executeScript` - 收集您在 `EfsId` 參數中指定之檔案系統的詳細資訊。
- `aws:executeScript` - 驗證與檔案系統相關聯的安全群組，允許來自您在 `InstanceId` 參數中指定之 Amazon EC2 執行個體的連接埠 2049 流量。
- `aws:assertAwsResourceProperty` - 驗證您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體是由 Systems Manager 管理，且狀態為 Online。
- `aws:branch` - 根據您為 Action 參數指定的值進行分支。
- `aws:runCommand` - 驗證掛載您在 `EfsId` 參數中指定之檔案系統的先決條件。
- `aws:runCommand` - 驗證掛載您在 `EfsId` 參數中指定的檔案系統的先決條件，並將檔案系統掛載到您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體。

Amazon EKS

AWS Systems Manager 自動化為 Amazon Elastic Kubernetes Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-CollectEKSIInstanceLogs](#)
- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)

AWSSupport-CollectEKSIInstanceLogs

Description

AWSSupport-CollectEKSInstanceLogs Runbook 會從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體收集作業系統和 Amazon Elastic Kubernetes Service (Amazon EKS) 相關日誌檔案，以協助您疑難排解常見問題。當自動化收集相關的日誌檔案時，會變更檔案系統結構，包括建立暫時目錄、將日誌檔案複製到暫時目錄，以及將日誌檔案壓縮至封存。此活動可能會導致 EC2 執行個體CPUUtilization增加。如需 CPUUtilization 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[執行個體指標](#)。

如果您指定 LogDestination 參數的值，自動化會評估您指定之 Amazon Simple Storage Service (Amazon S3) 儲存貯體的 policy 狀態。為了協助保護從 EC2 執行個體收集之日誌的安全性，如果 policy 狀態isPublic設定為 true，或存取控制清單 (ACL) 將READ|WRITE許可授予 All Users Amazon S3 預先定義的群組，則不會上傳日誌。如需 Amazon S3 預先定義群組的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 預先定義群組](#)。

Note

此自動化需要在連接至 EC2 執行個體的根 Amazon Elastic Block Store (Amazon EBS) 磁碟區上至少 10% 的可用磁碟空間。如果根磁碟區上的可用磁碟空間不足，自動化會停止。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- `EKSInstanceId`

類型：字串

描述：（必要）您要從中收集日誌的 Amazon EKS EC2 執行個體 ID。

- `LogDestination`

類型：字串

描述：（選用）您帳戶中要上傳封存日誌的 S3 儲存貯體。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`

我們建議接收命令的 EC2 執行個體具有連接 `AmazonSSMManagedInstanceCore` Amazon 受管政策的 IAM 角色。若要將日誌封存上傳至您在 `LogDestination` 參數中指定的 S3 儲存貯體，您必須新增 `s3:PutObject` 許可。

文件步驟

- `aws:assertAwsResourceProperty` - 確認 `EKSInstanceId` 參數中指定值的作業系統為 Linux。
- `aws:runCommand` - 收集作業系統和 Amazon EKS 相關的日誌檔案，將其壓縮為 `/var/log` 目錄中的封存。
- `aws:branch` - 確認是否已為 `LogDestination` 參數指定值。
- `aws:runCommand` - 將日誌封存上傳至您在 `LogDestination` 參數中指定的 S3 儲存貯體。

AWS-CreateEKSClusterWithFargateProfile

Description

`AWS-CreateEKSClusterWithFargateProfile` Runbook 會使用 建立 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集 AWS Fargate。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：（必要）叢集的唯一名稱。

- ClusterRoleArn

類型：字串

描述：（必要）IAM 角色的 ARN，提供 Kubernetes 控制平面代表您呼叫 AWS API 操作的許可。

- FargateProfileName

類型：字串

描述：（必要）Fargate 設定檔的名稱。

- FargateProfileRoleArn

類型：字串

描述：(必要) Amazon EKS Pod 執行 IAM 角色的 ARN。

- FargateProfileSelectors

類型：字串

描述：(必要) 將 Pod 與 Fargate 設定檔比對的選取器。

- SubnetIds

類型：StringList

描述：(必要) 您要用於 Amazon EKS 叢集IDs。Amazon EKS 會在這些子網路中建立彈性網路介面，以便在節點與 Kubernetes 控制平面之間進行通訊。您必須指定至少兩個子網路 ID。

- EKSEndpointPrivateAccess

類型：布林值

預設：True

描述：(選用) 將此值設為 True，以允許叢集 Kubernetes API 伺服器端點的私有存取。如果您啟用私有存取，叢集 VPC 中的 Kubernetes API 請求將使用私有 VPC 端點。如果您停用私有存取，且叢集中有節點或 Pod，則請確保 publicAccessCidrs 包含與節點或 Fargate AWS Fargate Pod 通訊所需的 CIDR 區塊。

- EKSEndpointPublicAccess

類型：布林值

預設：False

描述：(選用) 將此值設定為 False，以停用對叢集 Kubernetes API 伺服器端點的公開存取。如果您停用公有存取，叢集的 Kubernetes API 伺服器只能從啟動它的 VPC 內接收請求。

- PublicAccessCIDRs

類型：StringList

描述：(選用) 允許存取叢集公有 Kubernetes API 伺服器端點的 CIDR 區塊。從您指定的 CIDR 區塊之外的地址與端點的通訊遭拒。如果您已停用私有端點存取，且叢集中有節點或 Fargate Pod，則請確定您指定必要的 CIDR 區塊。

- SecurityGroupIds

類型：StringList

描述：（選用）指定一或多個安全群組，以與 Amazon EKS 在您帳戶中建立的彈性網路介面建立關聯。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

文件步驟

- CreateEKSCluster (aws : executeAwsApi) - 建立 Amazon EKS 叢集。
- VerifyEKSClusterIsActive (aws : waitForAwsResourceProperty) - 驗證叢集狀態為 ACTIVE。
- CreateFargateProfile (aws : executeAwsApi) - 為叢集建立 Fargate。
- VerifyFargateProfileIsActive (aws : waitForAwsResourceProperty) - 驗證 Fargate 設定檔狀態為 ACTIVE。

輸出

CreateEKSCluster.CreateClusterResponse

描述：從 CreateCluster API 呼叫收到的回應。

CreateFargateProfile.CreateFargateProfileResponse

描述：從 CreateFargateProfile API 呼叫收到的回應。

AWS-CreateEKSClusterWithNodegroup

Description

AWS-CreateEKSClusterWithNodegroup Runbook 會使用節點群組建立容量的 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：(必要) 叢集的唯一名稱。

- ClusterRoleArn

類型：字串

描述：(必要) IAM 角色的 ARN，提供 Kubernetes 控制平面代表您呼叫 AWS API 操作的許可。

- NodegroupName

類型：字串

描述：(必要) 節點群組的唯一名稱。

- NodegroupRoleArn

類型：字串

描述：(必要) 要與您的節點群組建立關聯的 IAM 角色 ARN。Amazon EKS 工作者節點 kubelet 協助程式會代表您呼叫 AWS APIs。節點透過 IAM 執行個體描述檔和關聯的政策，取得這些 API 呼叫的許可。啟動節點並在叢集中註冊之前，您必須先為那些節點建立啟動時要使用的 IAM 角色。

- SubnetIds

類型：StringList

描述：(必要) 您要用於 Amazon EKS 叢集IDs。Amazon EKS 會在這些子網路中建立彈性網路介面，以便在節點與 Kubernetes 控制平面之間進行通訊。您必須指定至少兩個子網路 ID。

- EKSEndpointPrivateAccess

類型：布林值

預設：True

描述：(選用) 將此值設為 True，以允許叢集 Kubernetes API 伺服器端點的私有存取。如果您啟用私有存取，叢集 VPC 中的 Kubernetes API 請求將使用私有 VPC 端點。如果您停用私有存取，且叢集中有節點或 Pod，則請確保 publicAccessCidrs 包含與節點或 Fargate AWS Fargate Pod 通訊所需的 CIDR 區塊。

- EKSEndpointPublicAccess

類型：布林值

預設：False

描述：(選用) 將此值設定為 `False`，以停用對叢集 Kubernetes API 伺服器端點的公開存取。如果您停用公有存取，叢集的 Kubernetes API 伺服器只能從啟動它的 VPC 內接收請求。

- `PublicAccessCIDRs`

類型：StringList

描述：(選用) 允許存取叢集公有 Kubernetes API 伺服器端點的 CIDR 區塊。從您指定的 CIDR 區塊之外的地址與端點的通訊遭拒。如果您已停用私有端點存取，且叢集中有節點或 Fargate Pod，則請確定您指定必要的 CIDR 區塊。

- `SecurityGroupIds`

類型：StringList

描述：(選用) 指定一或多個安全群組，以與 Amazon EKS 在您帳戶中建立的彈性網路介面建立關聯。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

文件步驟

- `CreateEKSCluster (aws : executeAwsApi)` - 建立 Amazon EKS 叢集。

- VerifyEKSClusterIsActive (aws : waitForAwsResourceProperty) - 驗證叢集狀態為 ACTIVE。
- CreateNodegroup (aws : executeAwsApi) - 建立叢集的節點群組。
- VerifyNodegroupIsActive (aws : waitForAwsResourceProperty) - 驗證節點群組狀態為 ACTIVE。

輸出

- CreateEKSCluster.CreateClusterResponse : 從 CreateCluster API 呼叫收到的回應。
- CreateNodegroup.CreateNodegroupResponse : 從 CreateNodegroup API 呼叫收到的回應。

AWS-DeleteEKSCluster

Description

此 Runbook 會刪除與 Amazon EKS 叢集相關聯的資源，包括節點群組和 Fargate 設定檔。或者，您可以選擇刪除所有自我管理節點、用於建立節點的 AWS CloudFormation 堆疊，以及叢集的 VPC CloudFormation 堆疊。如需刪除叢集的詳細資訊，請參閱《Amazon EKS 使用者指南》中的[刪除叢集](#)。

Note

如果您的叢集中有與負載平衡器相關聯的作用中服務，您必須先刪除這些服務，才能刪除叢集。如果沒有，系統就無法刪除負載平衡器。執行 AWS-DeleteEKSCluster Runbook 之前，請使用下列程序來尋找和刪除服務。

尋找和刪除叢集中的服務

1. 安裝 Kubernetes 命令列公用程式 kubectl。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的[安裝 kubectl](#)。
2. 執行下列命令，列出叢集中執行的所有服務。

```
kubectl get svc --all-namespaces
```

3. 執行下列命令來刪除任何具有相關聯 EXTERNAL-IP 值的服務。這些服務由負載平衡器提供，您必須在 Kubernetes 中刪除它們，以允許正確釋放負載平衡器和相關聯的資源。

```
kubectl delete svc  
service-name
```

您現在可以執行 AWS-DeleteEKSCluster Runbook。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- EKSClusterName

類型：字串

描述：（必要）要刪除的 Amazon EKS 叢集名稱。

- VPCCloudFormationStack

類型：字串

描述：（選用）要刪除之 EKS 叢集的 VPC AWS CloudFormation 堆疊名稱。這會刪除 VPC 的 AWS CloudFormation 堆疊和堆疊建立的任何資源。

- VPCCloudFormationStackRole

類型：字串

描述：(選用) AWS CloudFormation 擔任刪除 VPC CloudFormation 堆疊之 IAM 角色的 ARN。AWS CloudFormation 會使用角色的登入資料代表您進行呼叫。

- SelfManagedNodeStacks

類型：字串

描述：(選用) 自我管理節點的 AWS CloudFormation 堆疊名稱逗號分隔清單，這會刪除自我管理節點的 AWS CloudFormation 堆疊。

- SelfManagedNodeStacksRole

類型：字串

描述：(選用) AWS CloudFormation 擔任刪除自我管理節點堆疊之 IAM 角色的 ARN。AWS CloudFormation 會使用角色的登入資料代表您進行呼叫。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- sts:AssumeRole
- eks:ListNodegroups
- eks>DeleteNodegroup
- eks:ListFargateProfiles
- eks>DeleteFargateProfile
- eks>DeleteCluster
- cfn:DescribeStacks
- cfn>DeleteStack

文件步驟

- aws:executeScript - DeleteNodeGroups：尋找和刪除 EKS 叢集中的所有節點群組。
- aws:executeScript - DeleteFargateProfiles：尋找和刪除 EKS 叢集中的所有 Fargate 設定檔。

- `aws:executeScript - DeleteSelfManagedNodes`：刪除所有自我管理節點和用於建立節點的 CloudFormation 堆疊。
- `aws:executeScript - DeleteEKSCluster`：刪除 EKS 叢集。
- `aws:executeScript - DeleteVPCCloudFormationStack`：刪除 VPC CloudFormation 堆疊。

AWS-MigrateToNewEKSSelfManagedNodeGroup

Description

AWS-MigrateToNewEKSSelfManagedNodeGroup Runbook 可協助您建立新的 Amazon Elastic Kubernetes Service (Amazon EKS) Linux 節點群組，以將現有應用程式遷移至其中。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的[遷移至新的節點群組](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- OldStackName

類型：字串

描述：（必要）現有 AWS CloudFormation 堆疊的名稱或堆疊 ID。

- NewStackName

類型：字串

描述：（選用）為新節點群組建立的新 AWS CloudFormation 堆疊名稱。如果您未指定此參數的值，則會使用格式建立堆疊名稱：NewNodeGroup-*ClusterName*-*AutomationExecutionID*。

- ClusterControlPlaneSecurityGroup

類型：字串

描述：（選用）您希望節點用來與 Amazon EKS 控制平面通訊的安全群組 ID。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的安全群組。

- NodeInstanceType

類型：字串

描述：（選用）您要用於新節點群組的執行個體類型。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的執行個體類型。

- NodeGroupName

類型：字串

描述：（選用）新節點群組的名稱。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點群組名稱。

- NodeAutoScalingGroupDesiredCapacity

類型：字串

描述：（選用）建立新堆疊時要擴展到的所需節點數量。此數字必須大於或等於 NodeAutoScalingGroupMinSize 值，且小於或等於 NodeAutoScalingGroupMaxSize。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點群組所需容量。

- NodeAutoScalingGroupMaxSize

類型：字串

描述：（選用）節點群組可向外擴展的節點數量上限。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點群組大小上限。

- NodeAutoScalingGroupMinSize

類型：字串

描述：(選用) 節點群組可以擴展到的節點數量下限。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點群組大小下限。

- NodeImageId

類型：字串

描述：(選用) 您希望節點群組使用的 Amazon Machine Image(AMI) ID。

- NodeImageIdSSMParam

類型：字串

描述：(選用) 您希望節點群組使用的 的公AMI有 Systems Manager 參數。

- NodeVolumeSize

類型：字串

描述：(選用) GiB 中節點的根磁碟區大小。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點磁碟區大小。

- NodeVolumeType

類型：字串

描述：(選用) 您要用於節點根磁碟區的 Amazon EBS 磁碟區類型。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的磁碟區類型。

- KeyName

類型：字串

描述：(選用) 您要指派給節點的金鑰對。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的金鑰對。

- 子網路

類型：StringList

描述：(選用) 您希望用於新節點群組的子網路 IDs 逗號分隔清單。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的子網路。

- DisableIMDSv1

類型：布林值

描述：(選用) 指定 `true` 以停用執行個體中繼資料服務第 1 版 (IMDSv1)。根據預設，節點支援 IMDSv1 和 IMDSv2。

- `BootstrapArguments`

類型：字串

描述：(選用) 您要傳遞至節點引導指令碼的其他引數。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `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`

文件步驟

- `DetermineParameterValuesForNewNodeGroup` (aws : `executeScript`) - 收集用於新節點群組的參數值。
- `CreateStack` (aws : `createStack`) - 為新節點群組建立 AWS CloudFormation 堆疊。
- `GetNewStackNodeInstanceRole` (aws : `executeAwsApi`) - 取得節點執行個體角色。
- `GetNewStackSecurityGroup` (aws : `executeAwsApi`) - 步驟取得節點安全群組。
- `AddIngressRulesToNewNodeSecurityGroup` (aws : `executeAwsApi`) - 將輸入規則新增至新建立的安全群組，使其可接受來自指派給您先前節點群組的流量。
- `AddIngressRulesToOldNodeSecurityGroup` (aws : `executeAwsApi`) - 將輸入規則新增至先前的安全群組，使其可以接受來自指派給新建立節點群組的流量。
- `VerifyStackComplete` (aws : `assertAwsResourceProperty`) - 驗證新堆疊狀態為 `CREATE_COMPLETE`。

輸出

`DetermineParameterValuesForNewNodeGroup.NewStackParameters` - 用來建立新堆疊的參數。

`GetNewStackNodeInstanceRole.NewNodeInstanceRole` - 新節點群組的節點執行個體角色。

`GetNewStackSecurityGroup.NewNodeSecurityGroup` - 新節點群組的安全群組 ID。

`DetermineParameterValuesForNewNodeGroup.NewStackName` - 新節點群組的 AWS CloudFormation 堆疊名稱。

`CreateStack.StackId` - 新節點群組的 AWS CloudFormation 堆疊 ID。

AWSPremiumSupport-TroubleshootEKSCluster

Description

AWSPremiumSupport-TroubleshootEKSCluster Runbook 會診斷 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集、基礎基礎設施的常見問題，並提供建議的修補步驟。

Important

存取 `AWSPremiumSupport-*` Runbook 需要企業或商業支援訂閱。如需詳細資訊，請參閱 [比較 AWS 支援計劃](#)。

如果您指定 `S3BucketName` 參數的值，自動化會評估您指定之 Amazon Simple Storage Service (Amazon S3) 儲存貯體的政策狀態。為了協助保護從 EC2 執行個體收集之日誌的安全性，如果政策狀態 `isPublic` 設定為 `true`，或存取控制清單 (ACL) 將 `READ|WRITE` 許可授予 `All Users Amazon S3` 預先定義的群組，則不會上傳日誌。如需 Amazon S3 預先定義群組的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 預先定義群組](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：（必要）您要疑難排解的 Amazon EKS 叢集名稱。

- S3BucketName

類型：字串

描述：（必要）應上傳 Runbook 產生報告之私有 Amazon S3 儲存貯體的名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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，連接至啟動自動化之使用者或角色的 AWS Identity and Access Management (IAM) 政策必須允許對下列公有 AWS Systems Manager 參數執行 ssm:GetParameter 操作，以取得工作者節點的最新建議 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`

若要將 Runbook 產生的報告上傳至 Amazon S3 儲存貯體，您指定的 Amazon S3 儲存貯體需要下列許可。

- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`
- `s3:PutObject`

文件步驟

- `aws:executeAwsApi` - 收集指定 Amazon EKS 叢集的詳細資訊。
- `aws:executeScript` - 收集 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Auto Scaling 群組、AMI 和 Amazon EC2 GPU 圖形執行個體類型的詳細資訊。
- `aws:executeScript` - 收集 Amazon EKS 叢集的虛擬私有雲端 (VPC)、子網路、網路位址轉譯 (NAT) 閘道、子網路路由、安全群組和網路存取控制清單 (ACLs) 的詳細資訊。
- `aws:executeScript` - 收集已連接 IAM 執行個體描述檔和角色政策的詳細資訊。
- `aws:executeScript` - 收集您在 `S3BucketName` 參數中指定的 Amazon S3 儲存貯體詳細資訊。
- `aws:executeScript` - 將 Amazon VPC 子網路分類為公有或私有。
- `aws:executeScript` - 檢查 Amazon VPC 子網路是否有 Amazon EKS 叢集所需的標籤。
- `aws:executeScript` - 檢查 Amazon VPC 子網路是否有 Elastic Load Balancing 子網路所需的標籤。
- `aws:executeScript` - 檢查工作者節點 Amazon EC2 執行個體是否使用最新的 Amazon EKS 最佳化 AMI
- `aws:executeScript` - 檢查連接至工作者節點的 Amazon VPC 安全群組是否需要標籤。
- `aws:executeScript` - 檢查 Amazon EKS 叢集和工作節點 Amazon VPC 安全群組規則是否有建議傳入 Amazon EKS 叢集的規則。
- `aws:executeScript` - 檢查 Amazon EKS 叢集和工作節點 Amazon VPC 安全群組規則是否有從 Amazon EKS 叢集的建議輸出規則。
- `aws:executeScript` - 檢查 Amazon VPC 子網路的網路 ACL 組態。
- `aws:executeScript` - 檢查工作者節點 Amazon EC2 執行個體是否具有所需的受管政策。

- `aws:executeScript` - 檢查 Auto Scaling 群組是否具有叢集自動擴展所需的標籤。
- `aws:executeScript` - 檢查工作者節點 Amazon EC2 執行個體是否已連線至網際網路。
- `aws:executeScript` - 根據先前步驟的輸出產生報告。如果為 `S3BucketName` 參數指定值，產生的報告會上傳到 Amazon S3 儲存貯體。

AWSsupport-TroubleshootEKSTaskNode

Description

AWSsupport-TroubleshootEKSTaskNode Runbook 會分析 Amazon Elastic Compute Cloud (Amazon EC2) 工作者節點和 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集，協助您識別和疑難排解防止工作者節點加入叢集的常見原因。Runbook 會輸出指引，以協助您解決任何已識別的問題。

Important

若要成功執行此自動化，Amazon EC2 工作者節點的狀態必須為 `running`，Amazon EKS 叢集狀態必須為 `ACTIVE`。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：(必要) Amazon EKS 叢集的名稱。

- WorkerID

類型：字串

描述：(必要) 無法加入叢集的 Amazon EC2 工作者節點 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:assertAwsResourceProperty` - 確認您在 `ClusterName` 參數中指定的 Amazon EKS 叢集存在且處於 ACTIVE 狀態。
- `aws:assertAwsResourceProperty` - 確認您在 `WorkerID` 參數中指定的 Amazon EC2 工作者節點存在且處於 running 狀態。
- `aws:executeScript` - 執行 Python 指令碼，以協助識別工作者節點無法加入叢集的可能原因。

AWS-UpdateEKSCluster

Description

AWS-UpdateEKSCluster Runbook 可協助您將 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集更新為您想要使用的 Kubernetes 版本。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：(必要) Amazon EKS 叢集的名稱。

- 版本

類型：字串

描述：(必要) 您要更新叢集的 Kubernetes 版本。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- eks:DescribeUpdate
- eks:UpdateClusterVersion

文件步驟

- aws:executeAwsApi - 更新 Amazon EKS 叢集所使用的 Kubernetes 版本。
- aws:waitForAwsResourceProperty - 等待更新狀態為 Successful。

AWS-UpdateEKSMangedNodeGroup

Description

AWS-UpdateEKSMangedNodeGroup Runbook 可協助您更新 Amazon Elastic Kubernetes Service (Amazon EKS) 受管節點群組。您可以選擇 Version 或 Configuration 更新。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：(必要) 您要更新其節點群組的叢集名稱。

- NodeGroupName

類型：字串

描述：(必要) 要更新的節點群組名稱。

- UpdateType

類型：字串

有效值：更新節點群組版本 | 更新節點群組組態

預設：更新節點群組版本

描述：(必要) 您要在節點群組上執行的更新類型。

下列參數僅適用於Version更新類型：

- **AMIReleaseVersion**

類型：字串

描述：(選用) 您要使用的 Amazon EKS AMI 最佳化版本。根據預設會使用最新版本。

- **ForceUpgrade**

類型：布林值

描述：(選用) 如果為 true，則更新不會失敗，以回應 Pod 中斷預算違規。

- **KubernetesVersion**

類型：字串

描述：(選用) 要更新節點群組的 Kubernetes 版本。

- **LaunchTemplateId**

類型：字串

描述：(選用) 啟動範本的 ID。

- **LaunchTemplateName**

類型：字串

描述：(選用) 啟動範本的名稱。

- **LaunchTemplateVersion**

類型：字串

描述：(選用) Amazon Elastic Compute Cloud (Amazon EC2) 啟動範本版本。此參數只有在節點群組是從啟動範本建立時才有效。

下列參數僅適用於 Configuration 更新類型：

- **AddOrUpdateNodeGroupLabels**

類型：StringMap

描述：(選用) 您要新增或更新的 Kubernetes 標籤。

- **AddOrUpdateKubernetesTaintsEffect**

類型：StringList

描述：（選用）您要新增或更新的 Kubernetes 污點。

- MaxUnavailableNodeGroups

類型：整數

預設：0

描述：（選用）在版本更新期間一次無法使用的節點數量上限。

- MaxUnavailablePercentageNodeGroup

類型：整數

預設：0

描述：（選用）版本更新期間無法使用的節點百分比。

- NodeGroupDesiredSize

類型：整數

預設：0

描述：（選用）受管節點群組應維護的節點數量。

- NodeGroupMaxSize

類型：整數

預設：0

描述：（選用）受管節點群組可向外擴展的節點數量上限。

- NodeGroupMinSize

類型：整數

預設：0

描述：（選用）受管節點群組可縮減的節點數量下限。

- RemoveKubernetesTaintsEffect

類型：StringList

描述：(選用) 您要移除的 Kubernetes 污點。

- RemoveNodeGroupLabels

類型：StringList

描述：(選用) 您想要移除的以逗號分隔的標籤清單。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

文件步驟

- aws:executeScript - 根據您為 Runbook 輸入參數指定的值更新 Amazon EKS 叢集節點群組。
- aws:waitForAwsResourceProperty - 等待叢集更新狀態為 Successful。

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Description

AWS-UpdateEKSSelfManagedLinuxNodeGroups Runbook 會使用 AWS CloudFormation 堆疊更新 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集中的自我管理受管節點群組。

如果您的叢集使用自動擴展，建議您先將部署縮減至兩個複本，再使用此 Runbook。

將部署擴展到兩個複本

1. 安裝 Kubernetes 命令列公用程式 kubectl。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的[安裝 kubectl](#)。
2. 執行下列命令。

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. 執行 AWS-UpdateEKSSelfManagedLinuxNodeGroups Runbook。
4. 執行下列命令，將部署擴展回所需的複本數量。

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：（必要）Amazon EKS 叢集的名稱。

- NodeGroupName

類型：字串

描述：（必要）受管節點群組的名稱。

- ClusterControlPlaneSecurityGroup

類型：字串

描述：(必要) 控制平面安全群組的 ID。

- DisableIMDSv1

類型：布林值

描述：(選用) 決定您是否要允許執行個體中繼資料服務第 1 版 (IMDSv1) 和 IMDSv2。

- KeyName

類型：字串

描述：(選用) 執行個體的金鑰名稱。

- NodeAutoScalingGroupDesiredCapacity

類型：字串

描述：(選用) 節點群組應維護的節點數量。

- NodeAutoScalingGroupMaxSize

類型：字串

描述：(選用) 節點群組可向外擴展的節點數量上限。

- NodeAutoScalingGroupMinSize

類型：字串

描述：(選用) 節點群組可以擴展到的節點數量下限。

- NodeInstanceType

類型：字串

預設：t3.large

描述：(選用) 您要用於節點群組的執行個體類型。

- NodeImageId

類型：字串

描述：(選用) 您希望節點群組使用的 Amazon Machine Image(AMI) ID。

- `NodeImageIdSSMParam`

類型：字串

預設：`/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id`

描述：（選用）您希望節點群組使用的 的公AMI有 Systems Manager 參數。

- `StackName`

類型：字串

描述：（必要）用於更新節點群組的 AWS CloudFormation 堆疊名稱。

- 子網路

類型：字串

描述：（必要）您希望叢集使用的子網路 IDs 的逗號分隔清單。

- `VpcId`

類型：字串

預設：`Default`

描述：（必要）部署叢集的虛擬私有雲端 (VPC)。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks>DeleteNodegroup`
- `eks>DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`

- `eks:UpdateNodegroupConfig`

文件步驟

- `aws:executeScript` - 根據您為 Runbook 輸入參數指定的值更新 Amazon EKS 叢集節點群組。
- `aws:waitForAwsResourceProperty` - 等待堆疊 AWS CloudFormation 更新狀態傳回。

AWSSupport-SetupK8sApiProxyForEKS

Description

AWSSupport-SetupK8sApiProxyForEKS 自動化 Runbook 提供建立 函數的方法，該 AWS Lambda 函數可做為對 Amazon Elastic Kubernetes Service 叢集端點進行控制平面 API 呼叫的代理。它可作為 Runbook 的建置區塊，需要進行控制平面 API 呼叫，以自動化任務並疑難排解 Amazon EKS 叢集的問題。

Important

此自動化建立的所有資源都會加上標籤，以便輕鬆找到。使用的標籤為：

- `AWSSupport-SetupK8sApiProxyForEKS : true`

Note

- 自動化是協助程式 Runbook，無法做為獨立 Runbook 執行。它被調用為 Runbook 的子自動化，需要控制平面 API 呼叫 Amazon EKS 叢集。
- 請確保在使用後執行 Cleanup 操作，以避免產生不必要的成本。

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ClusterName

類型：字串

描述：(必要) Amazon Elastic Kubernetes Service 叢集的名稱。

- 作業

類型：字串

描述：(必要) 要執行的操作：在帳戶中 Setup 佈建 Lambda 函數，Cleanup 將取消佈建在設定階段中建立的資源。

允許的值：Setup | Cleanup

預設：設定

- LambdaRoleArn

類型：字串

描述：(選用) 允許函數 AWS Lambda 存取所需 AWS 服務和資源的 IAM 角色 ARN。如果未指定角色，此 Systems Manager Automation 會在您的帳戶中為 Lambda 建立一個 Automation-K8sProxy-Role-`<ExecutionId>` IAM 角色，其名稱包含 受管政策：AWSLambdaBasicExecutionRole 和 AWSLambdaVPCLambdaAccessExecutionRole。

如何運作？

Runbook 會執行下列步驟：

- 驗證自動化是否作為子執行執行執行。以獨立 Runbook 叫用時，Runbook 將無法運作，因為它不會自行執行任何有意義的工作。
- 檢查指定叢集之代理 Lambda 函數的現有 AWS CloudFormation 堆疊。
 - 如果堆疊存在，則會重複使用現有的基礎設施，而不是重新建立它。
 - 參考計數器是使用標籤來維護，以確保如果相同叢集的另一個 Runbook 重複使用，則 Runbook 不會刪除基礎設施。
- 執行為調用指定的操作類型 (Setup/Cleanup) :
 - 設定：建立或描述現有的資源。

清除：如果基礎設施未被任何其他 Runbook 使用，則移除佈建的資源。

所需的 IAM 許可

參數AutomationAssumeRole需要下列 LambdaRoleArn未傳遞的許可：

- 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`

提供 `LambdaRoleArn` 時，自動化不需要建立角色，而且可以排除下列許可：

- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:TagRole`
- `iam:UntagRole`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`

以下是範例政策，示範LambdaRoleArn未傳遞 AutomationAssumeRole 時所需的許可：

```
{
  "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:<partition>:iam::<account-id>:role/Automation-K8sProxy*"
      ],
      "Effect": "Allow",
      "Sid": "AllowCreateRoleWithRequiredTag"
    },
    {
      "Condition": {
```

```

    "StringEquals": {
      "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
  },
  "Action": [
    "iam:DeleteRole",
    "iam:TagRole",
    "iam:UntagRole"
  ],
  "Resource": [
    "arn:<partition>:iam::<account-id>:role/Automation-K8sProxy*"
  ],
  "Effect": "Allow",
  "Sid": "IAMActions"
},
{
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    },
    "StringLike": {
      "iam:PolicyARN": [
        "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaBasicExecutionRole",
        "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaVPCLAccessExecutionRole"
      ]
    }
  },
  "Action": [
    "iam:AttachRolePolicy",
    "iam:DetachRolePolicy"
  ],
  "Resource": [
    "arn:<partition>:iam::<account-id>: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:<partition>:lambda::<region-id>::<account-id>::function:Automation-K8sProxy*",
    "Effect": "Allow",
    "Sid": "LambdaActions"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    },
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:UpdateStack"
    ],
    "Resource": "arn:<partition>:cloudformation::<region-id>::<account-id>::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:<partition>:logs::<region-id>:::<account-id>::log-group:/aws/lambda/
Automation-K8sProxy*",
    "arn:<partition>:logs::<region-id>:::<account-id>::log-group:/aws/lambda/
Automation-K8sProxy*:*"
  ],
  "Effect": "Allow",
  "Sid": "LogsActions"
},
{
  "Condition": {
    "StringLikeIfExists": {
      "iam:PassedToService": "lambda.amazonaws.com"
    }
  },
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "arn:<partition>:iam::<account-id>::role/Automation-K8sProxy-Role*"
  ],
  "Effect": "Allow",
  "Sid": "PassRoleToLambda"
}
]
}

```

如果傳遞 `LambdaRoleArn`，請確保其已為公有叢集連接 [AWSLambdaBasicExecutionRole](#) 政策，並為私有叢集連接 [AWSLambdaVPCLAccessExecutionRole](#)。

建立的資源

Setup 操作期間會建立下列資源：

1. AWS Lambda 函數
2. IAM 角色：如果未提供，則為 Lambda 執行角色。
3. CloudWatch Log Group (Lambda Logs)

Lambda 函數和執行角色會保留，直到執行 *Cleanup* 操作為止。Lambda 日誌群組將保留 30 天或直到手動刪除為止。

指示

Runbook 是一種協助程式公用程式，旨在從其他 Runbook 中作為子自動化執行。它有助於建立基礎設施，讓父系 Runbook 進行 Amazon EKS K8s 控制平面 API 呼叫。若要使用 Runbook，您可以從父系自動化的內容中遵循下列步驟。

1. 設定階段：從 Runbook 使用 `aws:executeAutomation` 動作操作調用自動化，該操作想要在操作做為的情況下進行 Amazon EKS K8s 控制平面 API 呼叫 `Setup`。

輸入參數範例：

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

`aws:executeAutomation` 步驟的輸出將包含代理 Lambda 函數的 ARN。

2. 使用 Lambda Proxy：使用 `boto3 Lambda.Client.invoke(...)` 與 API 呼叫路徑和承載字符的清單，在 `aws:executeScript` 動作內叫用 Lambda 函數。Lambda 函數將傳遞承載字符作為授權標頭的一部分，以對指定的路徑執行 HTTP GET 呼叫。

Lambda 調用事件的範例：

```
{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "..."
```

Note

承載字符必須產生為父系自動化指令碼的一部分。您需要確保執行父系 Runbook 的委託人具有指定 Amazon EKS 叢集的唯一讀許可。

3. 清除階段：從 Runbook 使用 `aws:executeAutomation` 動作操作調用自動化，該操作希望在操作做為的情況下進行 Amazon EKS K8s 控制平面 API 呼叫 `Cleanup`。

輸入參數範例：

```
{
  "AutomationAssumeRole": "<role-arn>",
```

```
"ClusterName": "<eks-cluster-name>",  
"Operation": "Cleanup"  
}
```

自動化步驟

1. ValidateExecution

- 確認自動化不是以獨立執行方式執行。

2. CheckForExistingStack

- 檢查 AWS CloudFormation 堆疊是否已為指定的叢集名稱佈建。
- 傳回堆疊存在狀態，以及刪除是否安全。

3. BranchOnIsStackExists

- 根據堆疊存在進行分支的決策步驟。
- 更新現有堆疊名稱或繼續操作分支的路由。

4. UpdateStackName

- 使用現有堆疊的名稱更新 StackName 變數。
- 只有在堆疊已存在時才執行。

5. BranchOnOperation

- 根據 Operation 參數 (Setup /Cleanup) 路由自動化。
- 對於 Setup：建立新堆疊或描述現有資源的路由。
- 對於 Cleanup：如果可安全刪除，則繼續執行堆疊刪除。

6. GetClusterNetworkConfig

- 描述 Amazon EKS 叢集以取得 VPC 組態。
- 擷取端點、VPC ID、子網路 IDs、安全群組 ID 和 CA 資料。

7. ProvisionResources

- 建立具有必要資源的 AWS CloudFormation 堆疊。
- 使用必要的聯網組態佈建 Lambda 函數。
- 標記所有資源以進行追蹤和管理。

8. DescribeStackResources

- 擷取已建立/現有堆疊的相關資訊。

9. BranchOnIsLambdaDeploymentRequired

- 判斷是否需要 Lambda 程式碼部署。
- 僅繼續部署新建立的堆疊。

10DeployLambdaFunctionCode

- 使用部署套件部署 Lambda 函數程式碼。
- 使用代理實作更新函數。

11AssertLambdaAvailable

- 驗證 Lambda 函數程式碼更新是否成功。
- 等待函數處於 Successful 狀態。

12PerformStackCleanup

- 刪除 AWS CloudFormation 堆疊和相關聯的資源。
- 在Cleanup操作期間或 Setup操作失敗時執行。

輸出

LambdaFunctionArn : 代理 Lambda 函數的 ARN

參考

Systems Manager Automation

- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程](#)

AWSsupport-TroubleshootEbsCsiDriversForEks

Description

AWSsupport-TroubleshootEbsCsiDriversForEks Runbook 可協助疑難排解 Amazon Elastic Kubernetes Service (Amazon EKS) 和 Amazon EBS 容器儲存介面 (CSI) 驅動程式問題中 Amazon Elastic Block Store 磁碟區掛載的問題

Important

目前 AWS Fargate 不支援在 上執行的 Amazon EBS CSI 驅動程式。

如何運作？

Runbook 會 `AWSSupport-TroubleshootEbsCsiDriversForEks` 執行下列高階步驟：

- 驗證目標 Amazon EKS 叢集是否存在且處於作用中狀態。
- 部署必要的身分驗證資源，以根據附加元件是 Amazon EKS 受管或自我管理來進行 Kubernetes API 呼叫。
- 執行 Amazon EBS CSI 控制器運作狀態檢查和診斷。
- 對節點角色和服務帳戶角色執行 IAM 許可檢查。
- 診斷指定應用程式 Pod 的持久性磁碟區建立問題。
- 檢查 node-to-pod 排程並檢查 Pod 事件。
- 收集相關的 Kubernetes 和應用程式日誌，將其上傳至指定的 Amazon S3 儲存貯體。
- 執行節點運作狀態檢查，並驗證與 Amazon EC2 端點的連線。
- 檢閱持久性磁碟區區塊型設備附件和掛載狀態。
- 清除疑難排解期間建立的身分驗證基礎設施。
- 產生結合所有診斷結果的全方位故障診斷報告。

Note

- Amazon EKS 叢集的身分驗證模式必須設定為 `API` 或 `API_AND_CONFIG_MAP`。建議使用 Amazon EKS Access 項目。Runbook 需要 Kubernetes 角色型存取控制 (RBAC) 許可才能執行必要的 API 呼叫。
- 如果您未指定 Lambda 函數 (`LambdaRoleArn` 參數) 的 IAM 角色，自動化會在您的帳戶 `Automation-K8sProxy-Role-<ExecutionId>` 中建立名為 `<ExecutionId>` 的角色。此角色包含受管政策和 `AWSLambdaBasicExecutionRole` `AWSLambdaVPCLambdaAccessExecutionRole`。
- 某些診斷步驟需要 Amazon EKS 工作者節點為 Systems Manager 受管執行個體。如果節點不是 Systems Manager 受管執行個體，則會略過需要 Systems Manager 存取的步驟，但其他檢查會繼續進行。
- 自動化包含移除身分驗證基礎設施資源的清除步驟。即使先前的步驟失敗，此清除步驟仍會執行，這有助於防止 AWS 帳戶中的孤立資源。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

指示

請依照下列步驟來設定自動化：

1. 在 `TroubleshootEbsCsiDriversForEks-SSM-Role` 帳戶中建立 SSM 自動化角色。確認信任關係包含下列政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 將以下政策連接至 IAM 角色，授予對指定資源執行指定動作所需的許可。
 - 如果您預期將執行和資源日誌上傳到相同區域的 Amazon S3 儲存貯 AWS 體，請在 中將 取代 `arn:{partition}:s3::BUCKET_NAME/*` 為您的 `OptionalRestrictPutObjects`。
 - 如果您要在 SSM Amazon S3 儲存貯體應指向正確的 Amazon S3 儲存貯體。 `S3BucketName`
 - 如果您未指定 ，則此許可為選用 `S3BucketName`
 - Amazon S3 儲存貯體必須是私有的，且位於您執行 SSM 自動化的相同 AWS 區域中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OptionalRestrictPutObjects",
      "Effect": "Allow",
```

```

        "Action": ["s3:PutObject"],
        "Resource": ["arn:{partition}:s3::BUCKET_NAME/*"]
    },
    {
        "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:*:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
        "arn:*: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 叢集 RBAC（以角色為基礎的存取控制）所需的許可。建議的方法是在 Amazon EKS 叢集中建立存取項目。

在 Amazon EKS 主控台中，導覽至您的叢集。對於 Amazon EKS 存取項目，請確認您的存取組態設定為 `API_AND_CONFIG_MAP` 或 `API`。如需為存取項目設定身分驗證模式的步驟，請參閱 [設定存取項目](#)。

選擇建立存取項目。

- 針對 IAM 主體 ARN，選取您在上一個步驟中為 SSM 自動化建立的 IAM 角色。
- 針對類型，選取 Standard。

4. 新增存取政策：

- 針對存取範圍，選取 Cluster。
- 針對政策名稱，選取 AmazonEKSAAdminViewPolicy。

選擇 Add Policy (新增政策)。

如果您未使用存取項目來管理 Kubernetes API 許可，則必須更新 `aws-auth ConfigMap`，並在 IAM 使用者或角色之間建立角色繫結。確保您的 IAM 實體具有下列唯讀 Kubernetes API 許可：

- 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. 執行自動化 [AWSSupport-TroubleshootEbsCsiDriversForEks \(主控台 \)](#)

6. 選擇 Execute automation (執行自動化)。

7. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用) :
 - 描述：(選用) 允許 SSM Automation 代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。角色需要新增到 Amazon EKS 叢集存取項目或 RBAC 許可，以允許 Kubernetes API 呼叫。
 - 類型：AWS::IAM::Role::Arn
 - 範例：TroubleshootEbsCsiDriversForEks-SSM-Role
- EksClusterName :
 - 描述：目標 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集的名稱。
 - 類型：String
- ApplicationPodName :
 - 描述：在 Amazon EBS CSI 驅動程式發生問題的 Kubernetes 應用程式 Pod 名稱。
 - 類型：String
- ApplicationNamespace :
 - 描述：應用程式 Pod 的 Kubernetes 命名空間與 Amazon EBS CSI 驅動程式發生問題。
 - 類型：String
- EbsCsiControllerDeploymentName (選用) :

- 描述：(選用) Amazon EBS CSI 控制器 Pod 的部署名稱。
- 類型：String
- 預設：ebs-csi-controller
- EbsCsiControllerNamespace (選用)：
 - 描述：(選用) Amazon EBS CSI 控制器 Pod 的 Kubernetes 命名空間。
 - 類型：String
 - 預設：kube-system
- S3BucketName (選用)：
 - 描述：(選用) 將上傳故障診斷日誌的目標 Amazon S3 儲存貯體名稱。
 - 類型：AWS::S3::Bucket::Name
- LambdaRoleArn (選用)：
 - 描述：(選用) 允許 AWS Lambda 函數存取所需 AWS 服務和資源的 IAM 角色 ARN。
 - 類型：AWS::IAM::Role::Arn

選取執行。

8. 完成後，請檢閱輸出區段以取得執行的詳細結果。

參考

Systems Manager Automation

- [執行此自動化 \(主控台\)](#)
- [執行自動化](#)
- [設定 自動化](#)
- [支援自動化工作流程](#)

如需 Amazon EBS CSI 驅動程式的詳細資訊，請參閱 [Amazon EBS CSI 驅動程式](#)。

Elastic Beanstalk

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Elastic Beanstalk。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)
- [AWSSupport-TroubleshootElasticBeanstalk](#)

AWSSupport-CollectElasticBeanstalkLogs

Description

AWSSupport-CollectElasticBeanstalkLogs Runbook 會從 Elastic Beanstalk 啟動的 Amazon Elastic Compute Cloud (Amazon EC2) Windows Server 執行個體收集 AWS Elastic Beanstalk 相關的日誌檔案，協助您疑難排解常見問題。當自動化收集相關的日誌檔案時，會變更檔案系統結構，包括建立暫時目錄、將日誌檔案複製到暫時目錄，以及將日誌檔案壓縮至封存。此活動可能會導致 Amazon EC2 執行個體 CPU Utilization 增加。如需 CPU Utilization 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的 [執行個體指標](#)。

如果您指定 S3BucketName 參數的值，自動化會評估您指定之 Amazon Simple Storage Service (Amazon S3) 儲存貯體的政策狀態。為了協助保護從 Amazon EC2 執行個體收集之日誌的安全性，如果政策狀態 isPublic 設定為 true，或存取控制清單 (ACL) 將 READ|WRITE 許可授予 All Users Amazon S3 預先定義的群組，則不會上傳日誌。如需 Amazon S3 預先定義群組的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 預先定義群組](#)。

如果您未指定 S3BucketName 參數的值，自動化會將日誌套件上傳到執行自動化 AWS 區域所在的預設 Elastic Beanstalk Amazon S3 儲存貯體。目錄會根據下列結構命名 `elasticbeanstalk-region - accountID`。## 和 `accountID` 值會根據區域和 AWS 帳戶 您在其中執行自動化而有所不同。日誌套件將儲存至 `resources/environments/logs/bundle/ environmentID / instanceID` 目錄。`environmentID` 和 `instanceID` 值會根據您的 Elastic Beanstalk 環境和您要從中收集日誌的 Amazon EC2 執行個體而有所不同。

根據預設，連接至 Elastic Beanstalk 環境的 Amazon EC2 執行個體的 AWS Identity and Access Management (IAM) 執行個體描述檔具有必要的許可，可將套件上傳至您環境的預設 Elastic Beanstalk Amazon S3 儲存貯體。如果您指定 S3BucketName 參數的值，連接至 Amazon EC2 執行個體的執行個體描述檔必須允許指定 `s3:GetBucketAcl` Amazon S3 儲存貯體和路徑的 `s3:GetBucketPolicy` `s3:GetBucketPolicyStatus`、和 `s3:PutObject` 動作。

Note

此自動化在連接至 Amazon EC2 執行個體的根 Amazon Elastic Block Store (Amazon EBS) 磁碟區上需要至少 500 MB 的可用磁碟空間。如果根磁碟區上的可用磁碟空間不足，自動化會停止。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- EnvironmentId

類型：字串

描述：（必要）您要從中收集日誌套件的 Elastic Beanstalk 環境 ID。

- InstanceId

類型：字串

（必要）您要從中收集日誌套件的 Elastic Beanstalk 環境中的 Amazon EC2 執行個體 ID。

- S3BucketName

類型：字串

(選用) 您要上傳封存日誌的 Amazon S3 儲存貯體。

- S3BucketPath

類型：字串

(選用) 您要上傳日誌套件的 Amazon S3 儲存貯體路徑。如果您未指定 參數的值，則會忽略此 S3BucketName 參數。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

文件步驟

- aws:assertAwsResourceProperty - 確認您在 InstanceId 參數中指定的 Amazon EC2 執行個體是由 管理 AWS Systems Manager。
- aws:assertAwsResourceProperty - 確認您在 InstanceId 參數中指定的 Amazon EC2 執行個體是 Windows Server 執行個體。
- aws:runCommand - 檢查執行個體是否為 Elastic Beanstalk 環境的一部分、是否有足夠磁碟空間來綁定日誌，以及日誌上傳到的 Amazon S3 儲存貯體是否為公有。
- aws:runCommand - 收集日誌檔案，並將封存上傳到 S3BucketName 參數中指定的 Amazon S3 儲存貯體，如果未指定值，則上傳到 Elastic Beanstalk 環境的預設儲存貯體。

AWSConfigRemediation- EnableElasticBeanstalkEnvironmentLogStreaming

Description

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming Runbook 會在您指定的 AWS Elastic Beanstalk (Elastic Beanstalk) 環境中啟用記錄。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- EnvironmentId

類型：字串

描述：（必要）您要啟用登入的 Elastic Beanstalk 環境 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文件步驟

- `aws:executeAwsApi` - 啟用您在 `EnvironmentId` 參數中指定的 Elastic Beanstalk 環境記錄。
- `aws:waitForAwsResourceProperty` - 等待環境的狀態變更為 `Ready`。
- `aws:executeScript` - 確認已在 Elastic Beanstalk 環境中啟用記錄。

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Description

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications Runbook 會啟用您指定之 AWS Elastic Beanstalk (Elastic Beanstalk) 環境的通知。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `EnvironmentId`

類型：字串

描述：（必要）您要為其啟用通知的 Elastic Beanstalk 環境 ID。

- TopicArn

類型：字串

描述：（必要）您要傳送通知的 Amazon Simple Notification Service (Amazon SNS) 主題的 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文件步驟

- aws:executeAwsApi - 針對您在 EnvironmentId 參數中指定的 Elastic Beanstalk 環境啟用通知。
- aws:waitForAwsResourceProperty - 等待環境的狀態變更為 Ready。
- aws:executeScript - 驗證已為 Elastic Beanstalk 環境啟用通知。

AWSSupport-TroubleshootElasticBeanstalk

Description

AWSSupport-TroubleshootElasticBeanstalk Runbook 可協助您針對 AWS Elastic Beanstalk 環境處於 Degraded 或 Severe 狀態的潛在原因進行故障診斷。此自動化會檢查與 Elastic Beanstalk 環境相關聯的下列 AWS 資源：

- 負載平衡器、AWS CloudFormation 堆疊、Amazon EC2 Auto Scaling 群組、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和虛擬私有雲端 (VPC) 的組態詳細資訊。
- 與子網路相關聯的安全群組規則、路由表和網路存取控制清單 (ACLs) 的網路組態問題。
- 驗證 Elastic Beanstalk 端點和公有網際網路存取的連線。
- 驗證負載平衡器的狀態。

- 驗證 Amazon EC2 執行個體的狀態。
- 從 Elastic Beanstalk 環境擷取日誌套件，並選擇性地將檔案上傳至其中 支援。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- ApplicationName

類型：字串

描述：（必要）Elastic Beanstalk 應用程式的名稱。

- EnvironmentName

類型：字串

描述：（必要）Elastic Beanstalk 環境的名稱。

- AWSS3UploaderLink

類型：字串

描述：（選用）由 提供給您的 URL 支援，可將日誌套件從 Elastic Beanstalk 環境上傳至其中。此選項僅適用於已購買 支援 計劃並已開啟支援案例的客戶。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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*

文件步驟

- aws:executeScript - 驗證啟動自動化的 AWS Identity and Access Management (IAM) 委託人具有執行 Runbook 中定義之所有動作的必要許可。
- aws:branch - 根據上一個步驟的結果配置工作流程。
- aws:executeScript - 收集 Elastic Beanstalk 環境的相關資訊，包括負載平衡器、AWS CloudFormation 堆疊、Auto Scaling 群組、Amazon EC2 執行個體和 VPC 組態。

- `aws:executeScript` - 檢查與 VPC 中子網路相關聯的路由表和 ACLs 是否有網路連線問題。
- `aws:executeScript` - 檢查與 Amazon EC2 執行個體相關聯的安全群組規則是否有網路連線問題。
- `aws:executeScript` - 驗證 Amazon EC2 執行個體的狀態檢查。
- `aws:executeScript` - 產生 Elastic Beanstalk 環境日誌套件的連結。
- `aws:executeScript` - 將日誌套件上傳至 支援。
- `aws:executeScript` - 輸出動作項目的報告，以協助您疑難排解可能影響 Elastic Beanstalk 環境狀態的問題。

Elastic Load Balancing

AWS Systems Manager 自動化為 Elastic Load Balancing 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)
- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS-UpdateALBDesyncMitigationMode](#)
- [AWS-UpdateCLBDesyncMitigationMode](#)

AWSConfigRemediation-DropInvalidHeadersForALB

Description

AWSConfigRemediation-DropInvalidHeadersForALB Runbook 可讓您指定的應用程式負載平衡器移除具有無效標頭的 HTTP 標頭。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- LoadBalancerArn

類型：字串

描述：（必要）您要捨棄無效標頭之負載平衡器的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文件步驟

- aws:executeAwsApi - 為您在 LoadBalancerArn 參數中指定的負載平衡器啟用捨棄無效標頭設定。

- `aws:executeScript` - 驗證已在參數中指定的負載平衡器上啟用捨棄無效標頭設定 `LoadBalancerArn`。

AWS-EnableCLBAccessLogs

Description

AWS-EnableCLBAccessLogs Runbook 會啟用 Classic Load Balancer 的存取日誌。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- `EmitInterval`

類型：整數

有效值：5 | 60

預設：60

描述：（選用）以分鐘為單位發佈存取日誌的間隔。

- `LoadBalancerNames`

類型：字串

描述：（必要）您要為其啟用存取日誌的 Classic Load Balancer 逗號分隔清單。

- S3BucketName

類型：字串

描述：（必要）存放存取日誌的 Amazon Simple Storage Service (Amazon S3) 儲存貯體名稱。

- S3BucketPrefix

類型：字串

描述：（選用）您為 Amazon S3 儲存貯體建立的邏輯階層，例如 my-bucket-prefix/prod。如不提供字首，則將日誌放置於儲存貯體根層級。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- elasticloadbalancing:ModifyLoadBalancerAttributes

文件步驟

- aws:executeAwsApi - 為您在 LoadBalancerNames 參數中指定的 Classic Load Balancer 啟用存取日誌。

輸出

EnableCLBAccessLogs.SuccessesLoadBalancers - 成功啟用存取日誌的負載平衡器名稱清單。

EnableCLBAccessLogs.FailedLoadBalancers - 啟用存取日誌失敗的負載平衡器名稱 MapList，以及失敗的原因。

AWS-EnableCLBConnectionDraining

Description

AWS-EnableCLBConnectionDraining Runbook 可讓 Classic Load Balancer (CLB) 上的連線耗盡至指定的逾時值。連線耗盡可讓 CLB 完成對取消註冊或運作狀態不佳的執行個體提出的傳輸中請求，

其指定的逾時是將執行個體報告為已取消註冊之前保持連線運作的時間。如需CLBs上耗盡連線的詳細資訊，請參閱 [Classic Load Balancer 使用者指南中的設定 Classic Load Balancer 的連接耗盡](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- LoadBalancerName

類型：字串

描述：（必要）您要啟用連線耗盡的負載平衡器名稱。

- ConnectionTimeout

類型：整數

有效值：1-3600

預設：300

描述：（必要）負載平衡器的連線逾時值。逾時值可以設定在 1 到 3600 秒之間。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文件步驟

- `ModifyLoadBalancerConnectionDraining` (aws : `executeAwsApi`) : 啟用連線耗盡，並為您指定的負載平衡器設定指定的逾時值。
- `VerifyLoadBalancerConnectionDrainingEnabled` (aws : `assertAwsResourceProperty`) : 確認負載平衡器已啟用連線耗盡。
- `VerifyLoadBalancerConnectionDrainingTimeout` (aws : `assertAwsResourceProperty`) : 驗證負載平衡器的連線逾時值是否符合您指定的值。

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Description

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing Runbook 會為您指定的 Classic Load Balancer (CLB) 啟用跨區域負載平衡。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN) , 允許 Systems Manager Automation 代表您執行動作。

- LoadBalancerName

類型：字串

描述：(必要) 您要啟用跨區域負載平衡的 CLB 名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elb:DescribeLoadBalancerAttributes
- elb:ModifyLoadBalancerAttributes

文件步驟

- aws:executeAwsApi - 為您在 LoadBalancerName 參數中指定的 CLB 啟用跨區域負載平衡。
- aws:assertAwsResourceProperty - 確認 CLB 上已啟用跨區域負載平衡。

AWSConfigRemediation-EnableELBDeletionProtection

Description

AWSConfigRemediation-EnableELBDeletionProtection Runbook 會為您指定的彈性負載平衡器 (ELB) 啟用刪除保護。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- LoadBalancerArn

類型：字串

描述：(必要) 您要啟用刪除保護之 ELB 的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:ModifyLoadBalancerAttributes

文件步驟

- aws:executeScript - 對您在 LoadBalancerArn 參數中指定的 ELB 啟用刪除保護。

AWSConfigRemediation-EnableLoggingForALBAndCLB

Description

AWSConfigRemediation-EnableLoggingForALBAndCLB Runbook 會啟用指定 AWS Application Load Balancer 或 Classic Load Balancer (CLB) 的記錄。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- LoadBalancerId

類型：字串

描述：（必要）Classic Load Balancer 名稱或 Application Load Balancer ARN。

- S3BucketName

類型：字串

描述：（必要）Amazon S3 儲存貯體名稱。

- S3BucketPrefix

類型：字串

描述：（選用）您為 Amazon Simple Storage Service (Amazon S3) 儲存貯體建立的邏輯階層，例如 my-bucket-prefix/prod。如不提供字首，則將日誌放置於儲存貯體根層級。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文件步驟

- `aws:executeScript` - 啟用並驗證 Classic Load Balancer 或 Application Load Balancer 的記錄。

AWSSupport-TroubleshootCLBConnectivity

Description

AWSSupport-TroubleshootCLBConnectivity Runbook 可協助您疑難排解 Classic Load Balancer (CLB) 和 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體之間的連線問題。此外，也會檢閱用戶端與 CLB 之間的連線問題。此 Runbook 也會檢閱 CLB 的運作狀態檢查、驗證是否遵循最佳實務，以及為您建立故障診斷儀表板。或者，您可以將自動化輸出上傳到 Amazon Simple Storage Service (Amazon S3) 儲存貯體。不過，此 Runbook 不支援將輸出上傳到可公開存取的 S3 儲存貯體。建議您為此自動化建立臨時 S3 儲存貯體。

Important

使用此 Runbook 可能會針對建立的儀表板產生費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#)

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InvestigationType

類型：字串

有效值：最佳實務 | 連線問題 | 疑難排解儀表板

描述：(必要) 您希望 Runbook 執行的操作。

- LoadBalancerName

類型：字串

描述：(必要) CLB 的名稱。

- S3Location

類型：字串

描述：(選用) 您要傳送自動化結果的 S3 儲存貯體名稱。不支援公開存取的儲存貯體。如果您的 S3 儲存貯體使用伺服器端加密，執行此自動化的使用者或角色必須具有 AWS KMS 金鑰的 `kms:GenerateDataKey` 許可。

- S3LocationPrefix

類型：字串

描述：(選用) 您要上傳自動化輸出的 Amazon S3 金鑰字首 (子資料夾)。

格式輸出會以下列格式儲存：`amzn-s3-demo-bucket/S3LocationPrefix/InvestigationType_{automation : EXECUTION_ID}.txt`。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:executeScript` - 驗證您在 `LoadBalancerName` 參數中指定的 CLB 是否存在。
- `aws:branch` - 根據為 `InvestigationType` 參數指定的值進行分支。
- `aws:executeScript` - 執行 CLB 的連線檢查。
- `aws:executeScript` - 驗證 CLB 組態是否符合 Elastic Load Balancing 最佳實務。
- `aws:executeScript` - 為您的 CLB 建立 Amazon CloudWatch 儀表板。
- `aws:executeScript` - 使用自動化結果建立文字檔案，並將其上傳至您在 `S3Location` 參數中指定的 Amazon S3 儲存貯體。

輸出

`RunBestPractices.Summary`

`RunConnectivityChecks.Summary`

`CreateTroubleshootingDashboard.Output`

`UploadOutputToS3.Output`

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Description

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing Runbook 會為您指定的網路負載平衡器 (NLB) 啟用跨區域負載平衡。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- LoadBalancerArn

類型：字串

描述：(必要) 您要啟用跨區域負載平衡之 NLB 的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文件步驟

- aws:executeAwsApi - 為您在 LoadBalancerArn 參數中指定的 NLB 啟用跨區域負載平衡。
- aws:executeScript - 確認 NLB 上已啟用跨區域負載平衡。

AWS-UpdateALBDesyncMitigationMode

Description

AWS-UpdateALBDesyncMitigationMode Runbook 會將 Application Load Balancer (ALB) 上的非同步緩解模式更新為指定的緩解模式。非同步緩解模式會決定負載平衡器如何處理可能對應用程式造成安全風險的請求。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- LoadBalancerArn

類型：字串

描述：（必要）您要修改其非同步緩解模式之 ALB 的 Amazon Resource Name (ARN)。

- DesyncMitigationMode

類型：字串

有效值：監控 | 防禦 | 最嚴格

描述：（必要）您希望 ALB 使用的緩解模式。如需有關取消同步緩解模式的資訊，請參閱《Application Load Balancer 使用者指南》中的[取消同步緩解模式](#)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文件步驟

- `VerifyLoadBalancerType` (aws : `assertAwsResourceProperty`) - 確認輸入 `LoadBalancerArn` 參數指定的值適用於應用程式負載平衡器，然後再繼續進行下一個步驟。
- `ModifyLoadBalancerDesyncMode` (aws : `executeAwsApi`) - 更新 ALB 以使用指定的 `DesyncMitigationMode`。
- `VerifyLoadBalancerDesyncMitigationMode` (aws : `executeScript`) - 驗證是否已針對目標 ALB 更新非同步緩解模式。

輸出

`VerifyLoadBalancerDesyncMitigationMode.ModificationResult` - 指令碼的訊息承載，驗證對 ALB 的修改。

AWS-UpdateCLBDesyncMitigationMode

Description

AWS-UpdateCLBDesyncMitigationMode Runbook 會將 Classic Load Balancer (CLB) 上的非同步緩解模式更新為指定的緩解模式。非同步緩解模式會決定負載平衡器如何處理可能對應用程式造成安全風險的請求。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- LoadBalancerName

類型：字串

描述：(必要) 您要修改其非同步緩解模式的 CLB 名稱。

- DesyncMitigationMode

類型：字串

有效值：監控 | 防禦 | 最嚴格

描述：(必要) 您希望 CLB 使用的緩解模式。如需有關取消同步緩解模式的資訊，請參閱《Application Load Balancer 使用者指南》中的[取消同步緩解模式](#)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

文件步驟

- `ModifyLoadBalancerDesyncMode` (aws : `executeAwsApi`) - 更新 CLB 以使用指定的 `DesyncMitigationMode`。
- `VerifyLoadBalancerDesyncMitigationMode` (aws : `executeScript`) - 驗證是否已針對目標 CLB 更新非同步緩解模式。

輸出

`VerifyLoadBalancerDesyncMitigationMode.ModificationResult` - 驗證 CLB 修改之指令碼的訊息承載。

Amazon EMR

AWS Systems Manager 自動化為 Amazon EMR 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-AnalyzeEMRLogs](#)
- [AWSSupport-DiagnoseEMRLogsWithAthena](#)

AWSSupport - AnalyzeEMRLogs

Description

此 Runbook 有助於識別在 Amazon EMR 叢集上執行任務時的錯誤。Runbook 會分析檔案系統上定義的日誌清單，並尋找預先定義的關鍵字清單。這些日誌項目用於建立 Amazon CloudWatch Events 事件，因此您可以根據事件採取任何必要的動作。或者，Runbook 會將日誌項目發佈至您選擇的 Amazon CloudWatch Logs 日誌群組。此 Runbook 目前會在日誌檔案中尋找下列錯誤和模式：

- `container_out_of_memory` – YARN 容器記憶體不足，執行中的任務可能會失敗。
- `yarn_nodemanager_health` : CORE 或 TASK 節點磁碟空間不足，無法執行任務。
- `node_state_change` : 主節點無法連線 CORE 或 TASK 節點。
- `step_failure` : EMR 步驟失敗。
- `no_core_nodes_running` : 目前沒有 CORE 節點正在執行，叢集運作狀態不佳。
- `hdfs_missing_blocks` : 缺少可能導致資料遺失的 HDFS 區塊。
- `hdfs_high_util` : HDFS 使用率很高，這可能會影響任務和叢集運作狀態。

- `instance_controller_restart` : Instance-Controller 程序已重新啟動。此程序對於叢集運作狀態至關重要。
- `instance_controller_restart_legacy` : Instance-Controller 程序已重新啟動。此程序對於叢集運作狀態至關重要。
- `high_load` : 偵測到高負載平均，可能會影響節點運作狀態報告，或導致逾時或速度變慢。
- `yarn_node_blacklisted` : YARN 已從執行中的任務將 CORE 或 TASK 節點列入黑名單。
- `yarn_node_lost` : YARN 已將 CORE 或 TASK 節點標記為 LOST，可能是連線問題。

與您指定的 `ClusterID` 相關聯的執行個體必須由 管理 AWS Systems Manager。您可以執行此自動化一次、排定自動化在特定時間間隔執行，或移除先前由自動化建立的排程。此 Runbook 支援 Amazon EMR 發行版本 5.20 到 6.30。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- `ClusterID` (`ClusterID`)

類型：字串

描述：（必要）您要分析其節點日誌的叢集 ID。

- 作業

類型：字串

有效值：執行一次 | 排程 | 移除排程

描述：（必要）在叢集上執行的操作。

- IntervalTime

類型：字串

有效值：5 分鐘 | 10 分鐘 | 15 分鐘

描述：（選用）執行自動化之間的持續時間。此參數僅適用於您Schedule為 Operation 參數指定的。

- LogToCloudWatchLogs

類型：字串

有效值：是 | 否

描述：（選用）如果您yes為此參數的值指定，自動化會使用 CloudWatchLogGroup 參數中指定的名稱來建立 CloudWatch Logs 日誌群組，以存放任何相符的日誌項目。

- CloudWatchLogGroup

類型：字串

描述：（選用）您要存放任何相符日誌項目的 CloudWatch Logs 日誌群組名稱。此參數僅適用於您yes為 LogToCloudWatchLogs 參數指定的。

- CreateLogInsightsDashboard

類型：字串

有效值：是 | 否

描述：（選用）如果您指定 yes，如果 CloudWatch 儀表板尚未存在，則會建立該儀表板。此參數僅適用於您yes為 LogToCloudWatchLogs 參數指定的。

- CreateMetricFilters

類型：字串

有效值：是 | 否

描述：(選用) 指定yes您是否要為 CloudWatch Logs 日誌群組建立指標篩選條件。此參數僅適用於您yes為 LogToCloudWatchLogs 參數指定的。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

- `aws:executeAwsApi` - 收集 `ClusterID` 參數中指定之 Amazon EMR 叢集的相關資訊。
- `aws:branch` - 以輸入為基礎的分支。
 - 如果提供的操作是 `Run Once` 或 `Schedule` :
 - `aws:assertAwsResourceProperty` - 驗證叢集是否可用。
 - `aws:executeAwsApi` - 收集叢集中執行之所有執行個體IDs。
 - `aws:assertAwsResourceProperty` - 驗證 SSM 代理程式是否在叢集中的所有執行個體上執行。
 - `aws:branch` - 根據您是否指定執行自動化一次或排程進行分支。
 - 如果提供的操作是 `Run Once` :
 - `aws:branch` - 根據 `LogToCloudWatchLogs` 參數中指定的值進行分支。
 - 如果 `LogToCloudWatchLogs` 值為 `yes` :
 - `aws:executeScript` - 檢查 參數中指定名稱的 CloudWatch Logs 日誌群組是否 `CloudWatchLogGroup` 已存在。如果沒有，則會使用指定的名稱建立群組。
 - `aws:branch` - 根據 `CreateMetricFilters` 參數中指定的值進行分支。
 - 如果 `CreateMetricFilters` 值為 `yes` :
 - `aws:executeAwsApi` - 每個指標篩選條件執行 12 個步驟
 - `aws:branch` - 根據 `CreateLogInsightsDashboard` 參數中指定的值進行分支。
 - 如果 `CreateLogInsightsDashboard` 值為 `yes` :
 - `aws:executeAwsApi` - 建立 CloudWatch 儀表板，如果其尚未存在，請使用 `CloudWatchLogGroup` 參數中指定的相同名稱。

- 如果CreateLogInsightsDashboard值為 no :
 - aws:runCommand - 執行 shell 指令碼來尋找叢集中每個執行個體的日誌模式。
- 如果CreateMetricFilters值為 no :
 - aws:branch - 根據CreateLogInsightsDashboard參數中指定的值進行分支。
- 如果CreateLogInsightsDashboard值為 yes :
 - aws:executeAwsApi - 建立 CloudWatch 儀表板，如果其尚未存在，請使用 CloudWatchLogGroup 參數中指定的相同名稱。
- 如果CreateLogInsightsDashboard值為 no :
 - aws:runCommand - 執行 shell 指令碼來尋找叢集中每個執行個體的日誌模式。
- 如果LogToCloudWatchLogs值為 no :
 - aws:executeAwsApi - 執行 shell 指令碼來尋找叢集中每個執行個體的日誌模式。
- 如果提供的操作是 Schedule :
 - aws:createStack - 建立以此 Runbook 為目標的 Amazon EventBridge 事件。
- 如果提供的操作是 Remove Schedule :
 - aws:executeAwsApi - 驗證叢集是否存在排程。
 - aws:deleteStack - 刪除排程。

輸出

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.InstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.output

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Description

AWSSupport-DiagnoseEMRLogsWithAthena Runbook 可協助診斷使用 Amazon Athena 與 Data Catalog 整合的 Amazon EMR 日誌。AWS Glue Amazon Athena 用於查詢容器、節點日誌或兩者的 Amazon EMR 日誌檔案，以及特定日期範圍或關鍵字搜尋的選用參數。

Runbook 可以自動擷取現有叢集的 Amazon EMR 日誌位置，也可以指定 Amazon S3 日誌位置。若要分析日誌，執行手冊：

- 在 Amazon EMR Amazon S3 日誌位置上建立 AWS Glue 資料庫並執行 Amazon Athena 資料定義語言 (DDL) 查詢，以建立叢集日誌的資料表和已知問題清單。Amazon Athena
- 執行資料處理語言 (DML) 查詢，以搜尋 Amazon EMR 日誌中的已知問題模式。查詢會傳回偵測到的問題清單、其發生計數，以及 Amazon S3 檔案路徑的相符關鍵字數量。
- 結果會上傳至您在字首下指定的 Amazon S3 儲存貯體 `saw_diagnose_EMR_known_issues`。
- Runbook 會傳回 Amazon Athena 查詢結果，並反白顯示從預先定義子集來源的 Amazon Knowledge Center (KC) 文章的調查結果、建議和參考。
- 完成或失敗時，會刪除 AWS Glue 資料庫和上傳至 Amazon S3 儲存貯體的已知問題檔案。

它如何運作？

使用 Amazon Athena AWSSupport-DiagnoseEMRLogsWithAthena 執行 Amazon EMR 日誌的分析，以偵測錯誤並反白顯示調查結果、建議和相關的知識中心文章。

Runbook 會執行下列步驟：

- 使用叢集 ID 或輸入 Amazon S3 位置取得 Amazon EMR 叢集日誌位置，以擷取日誌位置和大小。
- 根據日誌位置大小提供 Athena 成本估算。
- 在執行 Athena 查詢並繼續執行後續步驟之前，請求指定 IAM 主體的核准，以繼續取得核准。
- 將已知問題上傳至指定的 Amazon S3 儲存貯體，建立 AWS Glue 資料庫和資料表。
- 在 Amazon EMR 日誌資料上執行 Athena 查詢。查詢可以依日期範圍、關鍵字、兩個條件進行搜尋，或根據提供的輸入在沒有篩選條件的情況下執行。
- 分析結果以反白顯示調查結果、建議和相關的 KC 文章。
- Amazon Athena DML 查詢結果的輸出連結。
- 透過移除建立的資料庫、資料表和上傳的已知問題來清除環境。

文件類型

自動化

擁有者

Amazon

平台

/

AutomationAssumeRole 參數需要下列動作，才能成功使用 Runbook：

- athena:GetQueryExecution
- athena:StartQueryExecution
- athena:GetPreparedStatement
- athena:CreatePreparedStatement
- glue : GetDatabase
- glue : CreateDatabase
- glue : DeleteDatabase
- glue : CreateTable
- glue : GetTable
- glue : DeleteTable
- elasticmapreduce : DescribeCluster
- s3:ListBucket
- s3:GetBucketVersioning
- s3:ListBucketVersions
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetObject
- s3:GetBucketLocation
- pricing : GetProducts
- pricing : GetAttributeValues

- pricing : DescribeServices
- pricing : ListPriceLists

Important

若要限制僅存取此自動化所需的資源，請將下列政策連接至信任 SSM 服務的 IAM 角色。將分割區、區域和帳戶取代為執行執行手冊的分割區、區域和帳戶號碼的適當值。

```
{
  "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:{Partition}:s3::*/*/results/*",
        "arn:{partition}:s3::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Sid": "RestrictDeleteAccess",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
    ],
    "Resource": [
        "arn:{Partition}:s3::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
    ],
    "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:userDefinedFunction/saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "glue:CreateTable",
        "glue:GetTable",
        "glue:DeleteTable"
    ],
    "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/saw_diagnose_emr_known_issues",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/saw_diagnose_emr_logs_table",

```

```

        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
j_*",
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
    ]
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 在 文件 AWS Systems Manager 下導覽 [AWSSupport-DiagnoseEMRLogsWithAthena](#)。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，輸入以下內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ClusterID (必要)：

Amazon EMR 叢集 ID。

- S3LogLocation (選用)：

Amazon S3 Amazon EMR 日誌位置。輸入路徑樣式 URL Amazon S3 位置，例如：s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/。如果 Amazon EMR 叢集已終止超過 30 天，請提供此參數。

- S3BucketName (必要)：

要上傳已知問題清單的 Amazon S3 儲存貯體名稱，以及 Amazon Athena 查詢的輸出。儲存貯體應已啟用封鎖公開存取，且與 Amazon EMR 叢集位於相同的 AWS 區域和帳戶。

- 核准者 (必要)：

能夠核准或拒絕動作的已 AWS 驗證主體清單。您可以使用下列任何格式來指定委託人：使用者名稱、使用者 ARN、IAM 角色 ARN 或 IAM 擔任角色 ARN。核准者的數量上限為 10。

- FetchNodeLogsOnly (選用)：

如果設定為 `true`，自動化會診斷 Amazon EMR 應用程式容器日誌。預設值為 `false`。

- `FetchContainersLogsOnly`（選用）：

如果設定為 `true`，自動化會診斷 Amazon EMR 容器日誌。預設值為 `false`。

- `EndSearchDate`（選用）：

日誌搜尋的結束日期。如果提供，自動化將專門搜尋截至指定日期為止產生的日誌，格式為 YYYY-MM-DD（例如：2024-12-30）。

- `DaysToCheck`（選用）：

`EndSearchDate` 提供時，需要此參數來判斷從指定的回溯搜尋日誌的天數 `EndSearchDate`。最大值為 30 天。預設值為 1。

- `SearchKeywords`（選用）：

在日誌中搜尋的關鍵字清單，以逗號分隔。關鍵字不能包含單引號或雙引號。

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	ClusterID (Required) The Amazon EMR cluster ID. j-1K4BX00000HCB
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-1K4BX00000HCB/. String	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/bucket-public-access-control.html) and be in the same AWS region as the Amazon EMR cluster provided. 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	FetchNodeLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR node logs. false
FetchContainersLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster. 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
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	SearchKeywords (Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes. StringList

4. 選取執行。

5. 自動化會啟動。

6. 文件會執行下列步驟：

- `getLogLocation`：

透過查詢指定的 Amazon EMR 叢集 ID 來擷取 Amazon S3 日誌位置。如果自動化無法從 Amazon EMR 叢集 ID 查詢日誌位置，則 Runbook 會使用 `S3LogLocation` 輸入參數。

- `branchOnValidLog`：

驗證 Amazon EMR 日誌位置。如果位置有效，請繼續預估在 Amazon EMR 日誌上執行查詢時的 Amazon Athena 潛在成本。

- `estimateAthenaCosts` :

決定 Amazon EMR 日誌的大小，並提供在日誌資料集上執行 Athena 掃描的成本估算。對於非商業區域（非 AWS 分割區），此步驟只會提供日誌大小，而不會估算成本。您可以使用指定區域中的 Athena 定價文件來計算成本。

- `approveAutomation` :

等待指定的 IAM 主體核准，以繼續執行自動化的後續步驟。核准通知包含 Amazon EMR 日誌上 Amazon Athena 掃描的預估成本，以及自動化佈建之資源的詳細資訊。

- `uploadKnownIssuesExecuteAthenaQueries` :

將預先定義的已知問題上傳至 `S3BucketName` 參數中指定的 Amazon S3 儲存貯體。建立 AWS Glue 資料庫和資料表。根據輸入參數在 AWS Glue 資料庫中執行 Amazon Athena 查詢。

- `getQueryExecutionStatus` :

等待 Amazon Athena 查詢執行處於 `SUCCEEDED` 狀態。Amazon Athena DML 查詢會搜尋 Amazon EMR 叢集日誌中的錯誤和例外狀況。

- `analyzeAthenaResults` :

分析 Amazon Athena 結果，以提供源自預先定義映射集的調查結果、建議和知識中心 (KC) 文章。

- `getAnalyzeResultsQuery1ExecutionStatus` :

等待查詢執行處於 `SUCCEEDED` 狀態。Amazon Athena DML 查詢會分析先前 DML 查詢的結果。此分析查詢將傳回符合的例外狀況，以及解決方案和 KC 文章

- `getAnalyzeResultsQuery2ExecutionStatus` :

等待查詢執行處於 `SUCCEEDED` 狀態。Amazon Athena DML 查詢會分析先前 DML 查詢的結果。此分析查詢將傳回每個 Amazon S3 日誌路徑中偵測到的例外狀況/錯誤清單。

- `printAthenaQueriesMessage` :

列印 Amazon Athena DML 查詢結果的連結。

- `cleanupResources` :

刪除建立的 AWS Glue 資料庫並刪除在 Amazon EMR 日誌儲存貯體中建立的已知問題檔案，以清除資源。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

輸出為 Athena 查詢結果提供三個連結：

- 在 Amazon EMR 叢集日誌中找到的所有錯誤和經常發生的例外狀況清單，以及對應的日誌位置 (Amazon S3 字首)。
- Amazon EMR 日誌中符合的唯一已知例外狀況摘要，以及建議的解決方案和 KC 文章，以協助進行故障診斷。
- Amazon S3 日誌路徑中出現特定錯誤和例外狀況的詳細資訊，以支援進一步診斷。

▼ Outputs

```
printAthenaQueriesMessage QueriesLinkMessage
Log Devs Query Link: This link provides a comprehensive view of all the exceptions encountered within your EMR logs.
https://[REDACTED]

Analysis Query 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://[REDACTED]

Analysis Query 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://[REDACTED]
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- 如需詳細資訊，請參閱[疑難排解 Amazon EMR 叢集](#)

Amazon OpenSearch Service

AWS Systems Manager 自動化為 Amazon OpenSearch Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSONOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)

- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

AWSConfigRemediation-DeleteOpenSearchDomain

Description

AWSConfigRemediation-DeleteOpenSearchDomain Runbook 會使用 DeleteDomain API 刪除指定的 Amazon OpenSearch Service 網域。 [DeleteDomain](#)

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- DomainName

類型：字串

允許的值：(\d{12})/? 【a-z】 {1} 【a-z0-9-】 {2 , 28}

描述：（必要）您要刪除的 Amazon OpenSearch Service 網域名稱。

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DeleteDomain
- es:DescribeDomain

文件步驟

- aws:executeScript - 接受 Amazon OpenSearch Service 網域名稱做為輸入、將其刪除，並驗證刪除。

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Description

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain Runbook 會使用 [UpdateDomainConfig](#) API 在指定的 Amazon OpenSearch Service 網域EnforceHTTPS上啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- DomainName

類型：字串

允許的值：(\d{12})/? 【a-z】 {1} 【a-z0-9-】 {2 , 28}

描述：(必要) 您要用來強制執行 HTTPS 的 Amazon OpenSearch Service 網域名稱。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

文件步驟

- aws:executeScript - 在DomainName參數中指定的 Amazon OpenSearch Service 網域上啟用EnforceHTTPS端點選項。

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Description

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups Runbook 會使用 [UpdateDomainConfig](#) API 更新指定 Amazon OpenSearch Service 網域上的安全群組組態。

Note

AWS 安全群組只能套用至針對 Amazon Virtual Private Cloud (VPC) Access 設定的 Amazon OpenSearch Service 網域，而無法套用至針對公有存取設定的 Amazon OpenSearch Service 網域。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- DomainName

類型：字串

描述：（必要）您要用來更新安全群組的 Amazon OpenSearch Service 網域名稱。

- SecurityGroupList

類型：StringList

描述：（必要）您要指派給 Amazon OpenSearch Service 網域的安全群組 IDs。

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain

- `es:UpdateDomainConfig`

文件步驟

- `aws:executeScript` - 更新您在 `DomainName` 參數中指定的 Amazon OpenSearch Service 網域上的安全群組組態。

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Description

AWSSupport-TroubleshootOpenSearchRedYellowCluster 自動化 Runbook 用於識別紅色或黃色叢集運作狀態的原因，並引導您完成將叢集變更回綠色。

如何運作？

Runbook AWSSupport-TroubleshootOpenSearchRedYellowCluster 可協助您疑難排解紅色或黃色叢集的原因，並提供後續步驟，透過分析叢集組態和資源使用率來解決此問題。

Runbook 會執行下列步驟：

- 針對目標網域呼叫 [DescribeDomain](#) API，以取得叢集組態。
- 檢查 OpenSearch Service 網域是網際網路型（公有）還是 [Amazon Virtual Private Cloud \(VPC\) 型](#)。
- 根據叢集組態建立公有或 [Amazon VPC 型](#) AWS Lambda 函數。注意：Lambda 函數包含針對叢集執行 OpenSearch Service APIs 的疑難排解程式碼，以判斷叢集為何處於紅色或黃色狀態。
- 刪除 Lambda 函數。
- 顯示執行的檢查，以及解決紅色或黃色叢集問題的下一個建議步驟。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

LambdaExecutionRole 參數需要下列動作才能成功使用 Runbook：

- es:ESHttpGet

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

LambdaExecutionRole 政策概觀：

以下是 Lambda 函數執行角色 (AWS Identity and Access Management (IAM) 角色) 的範例，其授予函數存取此 Runbook 所需 AWS 服務和資源的許可。如需更多詳細資訊，請參閱 [Lambda 執行角色](#)。

Note

`ec2>DeleteNetworkInterface` 只有當您的 OpenSearch Service 叢集是以 [Amazon VPC 為基礎](#) 時 `ec2:DescribeNetworkInterfaces`，才需要 `ec2:CreateNetworkInterface`、和 `ec2:DeleteNetworkInterface`，以允許 Lambda 函數建立和管理 Amazon VPC 網路介面。如需詳細資訊，請參閱 [將傳出聯網連接到 Amazon VPC 和 Lambda 執行角色中的資源](#)。 <https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/_cluster/health",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/_cat/indices",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/_cat/allocation",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/_cluster/allocation/explain"
      ]
    },
    {
      "Condition": {
```

```

        "ArnLikeIfExists": {
            "ec2:Vpc": "arn:<partition>:ec2:<region>:<account-id>:vpc/
<vpc_id>"
        }
    },
    "Action": [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 導覽至主控台中的 [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#) AWS Systems Manager。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，輸入以下內容：
 - AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LambdaExecutionRole (必要)：

Lambda 用來簽署請求至 Amazon OpenSearch Service 叢集的 IAM 角色 ARN。

- DomainName (必要)：

具有紅色或黃色叢集運作狀態的 OpenSearch Service 網域名稱。

- UtilizationThreshold (選用)：

用於比較 CPUUtilization 和 JvmmemoryPressure 指標的使用率閾值百分比。預設值為 80。

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

AutomationAssumeRole
arn:aws:iam::[redacted]:role/AutomationAssumeRole

DomainName
(Required) The name of the Amazon OpenSearch Service domain is red or yellow status.

opensearch-red-yellow-sample

LambdaExecutionRole
(Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster.

Select an existing IAM Role

LambdaExecutionRole
arn:aws:iam::[redacted]:role/LambdaExecutionRole

UtilizationThreshold
(Optional) The utilization threshold in percentage used to compare the 'CPUUtilization' and 'JvmmemoryPressure' metrics. Default value is '80'.

80

4. 如果您已在 OpenSearch Service 叢集上啟用精細存取控制，請確定LambdaExecutionRole角色 Arn 已映射到至少具有cluster_monitor許可的角色。

Permissions Mapped users

Cluster permissions (1)
Cluster permissions specify how users in this role can access the cluster. You can specify permissions using both action groups or single permissions. An action group is a list of single permissions. [Learn more](#)

> • cluster_monitor

Backend roles
Use a backend role to directly map to roles through an external authentication system. [Learn more](#)

Backend roles

arn:aws:iam::123456789012:role/LambdaExecutionRole Remove

Add another backend role

Cancel Map

5. 選取執行。
6. 自動化啟動。
7. 自動化 Runbook 會執行下列步驟：

- GetClusterConfiguration：

擷取 OpenSearch Service 叢集組態。

- CreateAWSLambdaFunctionStack：

使用在帳戶中建立臨時 Lambda 函數 AWS CloudFormation。Lambda 函數用於執行 OpenSearch Service APIs。

- WaitForAWSLambdaFunctionStack：

等待 CloudFormation 堆疊完成。

- `GetClusterMetricsFromCloudWatch` :

取得 Amazon CloudWatch ClusterStatus、CPUUtilization 和 JVMMemoryPressure OpenSearch Service 叢集相關指標及其建立日期。

- `RunOpenSearchAPIs`

使用 Lambda 函數呼叫 OpenSearch Service APIs，並分析叢集指標資料，以診斷紅色或黃色叢集狀態的原因。

- `DeleteAWSLambdaFunctionStack` :

刪除您帳戶中此自動化建立的 Lambda 函數。

8. 完成後，請檢閱輸出區段以取得執行的詳細結果。

- `RootCause` :

提供叢集運作狀態為紅色或黃色的已識別原因概觀。

- `IssueDescription` :

提供叢集為何處於紅色或黃色狀態的詳細資訊，以及讓叢集返回綠色狀態的可能步驟。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- 如需詳細資訊，請參閱[疑難排解 Amazon OpenSearch Service](#)

AWSupport-TroubleshootOpenSearchHighCPU

Description

AWSupport-TroubleshootOpenSearchHighCPU Runbook 提供自動化解決方案，從 Amazon OpenSearch Service 網域收集診斷資料，以疑難排解[高 CPU](#) 問題。

如何運作？

AWSSupport-TroubleshootOpenSearchHighCPU Runbook 有助於疑難排解 Amazon OpenSearch Service 網域中的高 CPU 使用率。

Runbook 會執行下列步驟：

- 針對提供的 Amazon OpenSearch Service 網域執行 [DescribeDomain](#) API，以取得叢集中繼資料。
- 檢查 Amazon OpenSearch Service 網域是公有或 Amazon VPC 型 AWS CloudFormation，並在 的協助下建立公有或 [Amazon VPC 型](#) AWS Lambda 函數。
- Lambda 函數會從 Amazon OpenSearch Service 網域擷取診斷資料。
- 使用 AWS Step Functions 狀態機器來協調多個 Lambda 函數執行，以收集更全面的資料。
- 根據預設，會將收集的資料儲存在 Amazon CloudWatch 日誌群組中 24 小時。
- 刪除已建立的資源，但 CloudWatch 日誌群組除外。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

LambdaExecutionRole 參數需要下列動作才能成功使用 Runbook：

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2>DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

Lambda 執行角色會授予函數存取此 Runbook 所需 AWS 服務和資源的許可。如需更多詳細資訊，請參閱 [Lambda 執行角色](#)。

 Note

ec2>DeleteNetworkInterface 只有在您的 OpenSearch Service 叢集是以 [Amazon VPC 為基礎](#)時ec2:DescribeNetworkInterfaces，才需要 ec2:CreateNetworkInterface、和，以允許 Lambda 函數建立和管理 Amazon VPC 網路介面。如需詳細資訊，請參閱[將傳出聯網連接到 Amazon VPC 和 Lambda 執行角色中的資源](#)。 <https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

指示

請依照下列步驟設定自動化：

1. 導覽至主控台中的 [AWSSupport-TroubleshootOpenSearchHighCPU](#) AWS Systems Manager。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，輸入以下內容：
 - AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DomainName (必要)：

您想要針對高 CPU 問題進行故障診斷的 Amazon OpenSearch Service 網域名稱。

- **LambdaExecutionRoleForOpenSearch** (必要) :

要連接至 Lambda 函數之 IAM 角色的 ARN。Lambda 函數會使用此角色的登入資料來簽署對 Amazon OpenSearch Service 網域的請求。如果已在 Amazon OpenSearch Service 網域上啟用精細存取控制，您必須將此角色映射至 OpenSearch Service Dashboards 後端角色，並具有至少「cluster_monitor」許可。

- **DataRetentionDays** (選用) :

保留從 Amazon OpenSearch Service 網域收集之診斷資料的天數。根據預設，資料會保留 24 小時 (一天)。您可以選擇將資料保留最多 30 天。

- **NumberOfDataSamples** (選用) :

要從 Amazon OpenSearch Service 網域收集的資料範例數量。根據預設，會收集 5 個資料範例。您最多可以收集 10 個樣本，而且每個樣本收集都會叫用 Lambda 函數。

4. 如果您已在 OpenSearch Service 叢集上啟用精細存取控制，請確定**LambdaExecutionRole**角色 Arn 已映射到至少具有**cluster_monitor**許可的角色。

5. 選取執行。

6. 自動化會啟動。

7. 自動化 Runbook 會執行下列步驟：

- `checkConcurrency`：

確保只有一個針對指定 Amazon OpenSearch Service 網域的 Runbook 執行。如果 Runbook 找到另一個以相同網域名稱為目標的執行，則會傳回錯誤並結束。

- `getDomainConfig`：

取得目標 OpenSearch Service 網域的組態詳細資訊。

- `provisionResources`：

使用 佈建用於資料收集的資源 AWS CloudFormation。

- `waitForStackCreation`：

等待 AWS CloudFormation 堆疊完成。

- `describeStackResources`：

描述 AWS CloudFormation 堆疊並取得狀態機器的 ARN。

- `runStateMachine`：

執行 Step Functions 狀態機器，以叫用資料收集器 Lambda 函數一或多次。

- `describeErrorsFromStackEvents`：

描述堆疊中的錯誤 AWS CloudFormation。

- `unstageOpenSearchHighCPUAutomation`：

刪除 `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation 堆疊。

- `describeErrorsFromStackDeletion`：

描述刪除 AWS CloudFormation 堆疊時遇到的錯誤。

- `finalStatus`：

傳回 `AWSSupport-TroubleshootOpenSearchHighCPU` Runbook 的最終輸出。

8. 完成後，請檢閱輸出區段以取得執行的詳細結果。

- `finalStatus.FinalOutput`:

`AWSSupport-TroubleshootOpenSearchHighCPU` 提供存放診斷資料的 CloudWatch 日誌群組。

▼ Outputs

finalStatus.FinalOutput
Hot thread data collection completed. Please check the custom CloudWatch log group /aws/lambda/AWSSupport-HighCPU-df52ba5d-8773-4038-a908-b67ecd9c9d11 for more information.

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- 如需詳細資訊，請參閱[疑難排解 Amazon OpenSearch Service](#)

EventBridge

AWS Systems Manager 自動化為 Amazon EventBridge 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

AWS-AddOpsItemDedupStringToEventBridgeRule

Description

AWS-AddOpsItemDedupStringToEventBridgeRule Runbook 新增與 Amazon EventBridge 規則相關聯的 all AWS Systems Manager OpsItems 重複資料刪除字串。如果已套用重複資料刪除字串，則 Runbook 不會將重複資料刪除字串新增至規則。若要進一步了解重複資料刪除字串和 OpsItems，請參閱 AWS Systems Manager 《使用者指南》中的 [減少重複 OpsItems](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DedupString

類型：字串

描述：(必要) 您要新增至規則的重複資料刪除字串。

- RuleName

類型：字串

描述：(必要) 您要新增重複資料刪除字串的規則名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:ListTargetsByRule
- events:PutTargets

文件步驟

- `aws:executeScript` - 將重複資料刪除字串新增至您在 `RuleName` 參數中指定的 EventBridge 規則。

AWS-DisableEventBridgeRule

Description

AWS-DisableEventBridgeRule Runbook 會停用您 `specify.To` 的 Amazon EventBridge 規則，進一步了解 EventBridge 規則，請參閱《[Amazon EventBridge 使用者指南](#)》中的 Amazon EventBridge 規則。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `EventBusName`

類型：字串

預設：預設

描述：(選用) 與您要停用的規則相關聯的事件匯流排。

- RuleName

類型：字串

描述：(必要) 您要停用的規則名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:DisableRule

文件步驟

- aws:executeAwsApi - 停用您在 RuleName 參數中指定的 EventBridge 規則。

AWS Glue

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Glue。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-TroubleshootGlueConnection](#)

AWSSupport-TroubleshootGlueConnection

Description

AWSSupport-TroubleshootGlueConnections Runbook 可協助疑難排解 AWS Glue 連線問題。測試連線的目標必須透過 JDBC 連線達到，並且可以是 Amazon Relational Database Service (Amazon RDS) 叢集/執行個體、Amazon Redshift 叢集，或可透過 JDBC 存取的任何其他目標。在前兩個案例

中，Reachability Analyzer 工具用於判斷是否授予來源 (AWS Glue) 和目標 (Amazon RDS 或 Amazon Redshift) 之間的連線。

如果連線的目標不是 Amazon RDS 或 Amazon Redshift，仍會透過在 AWS Glue 與連線相同的子網路中建立 AWS Lambda 函數（網路存在點）來測試連線，並檢查目標名稱是否可以解析，以及是否可在目標連接埠中連線。

Important

為了執行 [Reachability Analyzer](#) 檢查，彈性網路介面會在每個連線的資料來源子網路中建立。請確定您在這些子網路上有足夠的可用 IPs，而且在執行此自動化之前，一個 IP 的耗用不會影響您的工作負載。

Important

此自動化建立的所有資源都會加上標籤，以便輕鬆找到。使用的標籤為：

- `AWSSupport-TroubleshootGlueConnection : true`
- `AutomationExecutionId : Amazon EC2 Systems Manager ## ID`

如何運作？

Runbook 會執行下列步驟：

- 描述連線 AWS Glue 以取得連線檢查的來源資訊（子網路和安全群組）。
- 從 JDBC URL 中參考的資料來源擷取目標資訊（子網路和安全群組），如果存在，則從 `DatasourceSecurityGroups` 和 `DatasourceSubnets` 參數擷取目標資訊。
- 如果 JDBC URL 中存在的資料來源是 Amazon RDS 執行個體或叢集或 Amazon Redshift 叢集，則此自動化會使用先前步驟中收集的來源和目標資訊來建立 ENIs，並使用 Reachability Analyzer 來執行它們之間的連線檢查。
- Lambda 函數（在此自動化內容中為網路存在點）用於執行 L4 連線和名稱解析檢查。
- 相同的 Lambda 函數用於對 Amazon S3 端點執行檢查。
- 政策模擬器用於判斷連線中使用的 IAM 角色是否具有所需的許可。
- 自動化會檢查連線所使用的安全群組是否具有預期的組態。
- 產生的報告包含測試連線操作中失敗的可能原因，和/或成功執行的測試。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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

除了上述動作之外，AutomationAssumeRole還應該將 [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#) 做為 [連接的受管政策](#)，以便成功執行 [Reachability Analyzer](#) 測試。

以下是可授予的政策範例AutomationAssumeRole：

```
{
  "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"
        }
    }
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-TroubleshootGlueConnection](#) 中導覽至 。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- TestConnectionRole (必要)

在連線測試期間使用的 IAM 角色的 Amazon Resource Name (ARN)。

- **ConnectionName** (必要)

AWS Glue 您想要故障診斷的測試連線名稱失敗。

- **PersistReachabilityAnalyzerResults** (選用)

此旗標會通知是否應保留 Reachability Analyzer 執行的結果。預設：false。

- **PointOfPresenceLogRetentionPeriod** (選用)

Lambda 存在點的日誌將存放的天數。預設：7。

- **DatasourceSubnets** (選用)

如果無法使用原始資料來源，請使用此參數來提供使用的子網路，以便仍執行連線測試。必須搭配使用 DatasourceSecurityGroups。範例：subnet-1,subnet-2。

- **DatasourceSecurityGroups** (選用)

如果原始資料來源無法使用，請使用此參數來提供其使用的安全群組，以便仍執行連線測試。必須搭配使用 DatasourceSubnets。範例：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.	ConnectionName (Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt.
TestConnectionRole (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.	PersistReachabilityAnalyzerResults (Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false.
PointOfPresenceLogRetentionPeriod (Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7.	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.
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.	

4. 選取執行。

5. 自動化會啟動。

6. 自動化 Runbook 會執行下列步驟：

- ParseInputs：

此步驟會驗證輸入組合。如果同時提供 `DatasourceSubnets`、`DatasourceSecurityGroups` 和 `SecurityGroupIdList`，則它們有效並按原狀傳回。如果沒有提供，則會傳回兩個空白清單。如果只提供其中一個，步驟會引發 `ValueException`。

- `GetConnectionDetails` :

此步驟會傳回所提供 AWS Glue 連線的詳細資訊。

- `ParseSecurityGroupList` :

此步驟用於串連 `SecurityGroupIdList` 中的 `String`，以供此自動化的未來使用。

- `GetConnectionData` :

根據 JDBC URL 決定 `RedShift`、`RdsInstanceRdsCluster` 和 `Other` 之間的連線類型。此外，會傳回 JDBC 連線中使用的網域和連接埠、連線的 Amazon VPC 及其網域名稱伺服器。

- `GetNetworkDetails` :

從 Amazon RDS 或 Amazon Redshift 目標取得子網路和安全群組資訊。

- `CreateENITemplate` :

產生用於建立網路介面的 AWS CloudFormation 範本，用於測試連線。這是執行 `Reachability Analyzer` 工具的必要項目。

- `CreateENIStack` :

從上一個步驟中建立的範本建立 AWS CloudFormation 堆疊。

- `GetStackDetails` :

描述在上一個 AWS CloudFormation 堆疊中建立的堆疊，並擷取 `SourceNetworkInterfaceTargetNetworkInterfaces` 資訊。

- `RunSourceToTargetCheck` :

使用 `Reachability Analyzer` 工具，在上一個步驟中建立的來源和目標 ENIs 之間執行檢查。

- `DeleteENIStack` :

刪除建立網路介面的 AWS CloudFormation 堆疊

- `CreateNetworkPointOfPresence` :

AWS CloudFormation 會建立做為網路存在點的 Lambda 函數。

- `GetFunctionName` :

執行 AWS CloudFormation 描述堆疊 API 呼叫，以擷取在上一個步驟中建立的 Lambda 函數名稱。

- RunEndpointChecks :

使用網路存在點來判斷 JDBC 連線中存在的端點是否可解析，並可在宣告的連接埠中連線。

- CheckS3Connectivity :

檢查從連線至 Amazon S3 AWS Glue 服務的網路連線。

- DeletePointOfPresence :

刪除建立 Lambda 網路存在點的 AWS CloudFormation 堆疊。

- TestIAMRolePermissions :

檢查用於測試的 IAM 角色是否具有執行測試所需的許可。

- CheckConnectionSecurityGroupReferencingRule :

檢查 AWS Glue 連線中使用的安全群組是否允許來自其本身的所有傳入流量。如果有的話，它會傳回不含此規則的安全群組清單。

- GenerateReport :

產生包含清單 o 調查結果（連線測試失敗的可能原因）和後續步驟（嘗試解決連線測試失敗）的報告。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- 自動化結果

在本節中，您會找到描述測試連線操作失敗（尋找）可能原因的案例，以及如何修正這些原因（後續步驟）。如果自動化找不到測試失敗的原因，也會在本節中通知。

- 成功的測試

在本節中，您會找到通知此自動化成功測試項目的案例。如果自動化無法識別測試連線失敗的原因，則成功測試非常有用，因為它們會透過通知問題的原因來減少調查範圍。

- 自動化錯誤

在本節中，您將找到描述自動化期間發生的問題的案例，這些問題可能限制了自動化可執行的測試數量。案例的描述會通知哪個步驟失敗。

```

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-lLu7FYAp9bfi 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-lLu7FYAp9bfi 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-lLu7FYAp9bfi) 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-lLu7FYAp9bfi.

-----
✓ 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.

```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

Amazon FSx

AWS Systems Manager 自動化為 Amazon FSx 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSsupport-ValidateFSxWindowsADConfig](#)

AWSsupport-ValidateFSxWindowsADConfig

Description

AWSsupport-ValidateFSxWindowsADConfig Runbook 用於驗證 Amazon FSx for Windows File Server 的自我管理 Active Directory (AD) 組態

它如何運作？

Runbook 會在 Runbook 在 Amazon FSx 子網路上啟動AWSsupport-ValidateFSxWindowsADConfig的臨時 Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體上執行 Amazon FSx 驗證指令碼。指令碼會執行多次檢查，以驗證與自我管理 AD/DNS 伺服器的網路連線，以及 Amazon FSx 服務帳戶的許可。Runbook 可以驗證失敗或設定錯誤的 Amazon FSx for Windows File Server，或使用自我管理 AD 建立新的 Amazon FSx for Windows File Server。

根據預設，Runbook 會在 Amazon FSx 子網路上使用 建立 Amazon EC2 Windows 執行個體、AWS Systems Manager (SSM) 存取的安全群組、AWS Identity and Access Management (IAM) 角色和政策。AWS CloudFormation FSx 如果您想要在現有的 Amazon EC2 執行個體上執行指令碼，請在 參數中提供 IDInstanceId。成功執行時，它會刪除 CloudFormation 資源。不過，若要保留資源，請將 RetainCloudFormationStack 參數設定為 true。

CloudFormation 範本會代表您建立 IAM 角色，並具有必要的許可，以連接至 Amazon EC2 執行個體來執行 Amazon FSx 驗證指令碼。若要指定暫時執行個體的現有 IAM 執行個體設定檔，請使用 InstanceProfileName 參數。相關聯的 IAM 角色必須包含下列許可：

- ec2:DescribeSubnets 和 ec2:DescribeVpcs許可，以及 Amazon 受管政策 AmazonSSMManagedInstanceCore。
- 呼叫 GetSecretValue API，從 Systems Manager 取得 Amazon FSx 服務帳戶使用者名稱和密碼的許可。
- 將物件放入指令碼輸出的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的許可。

先決條件

建立臨時 Amazon EC2 執行個體（或 InstanceId 參數中提供的現有執行個體）的子網路必須允許存取 AWS Systems Manager、和 Amazon S3 端點 AWS Secrets Manager，才能使用 SSM Run Command 執行AmazonFSxADValidation指令碼。

AWS Secrets Manager 設定

驗證指令碼透過擷取 Amazon FSx 服務帳戶使用者名稱和密碼，並對 Secrets Manager 進行執行期呼叫，來連線至 Microsoft AD 網域。請依照[建立 AWS Secrets Manager 秘密](#)中的步驟建立新的 Secrets Manager 秘密。請確定使用者名稱和密碼是以格式使用金鑰/值對來存放{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}。如需保護秘密存取的相關資訊，請參閱[的身分驗證和存取控制 AWS Secrets Manager](#)。

如需工具的詳細資訊，請參閱 [AmazonFSxADValidation](#) README.md 檔案中的 TROUBLESHOOTING.md 和 檔案。

Runbook 執行

使用 Amazon FSx ID 或 AD 參數執行 Runbook。以下是 Runbook 工作流程：

- 從 Amazon FSx ID 取得參數，或使用輸入 AD 參數。
- 使用 CloudFormation 在 Amazon FSx 子網路、SSM 存取的安全群組、IAM 角色和政策（有條件）上建立臨時驗證 Amazon EC2 Windows 執行個體。FSx 如果指定參數，則會使用該 InstanceId 參數。
- 在 Amazon FSx 主要子網路中的目標 Amazon EC2 執行個體上下載並執行驗證指令碼。FSx
- 在自動化輸出中提供 AD 驗證結果代碼。此外，完整的指令碼輸出會上傳到 Amazon S3 儲存貯體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

自動化擔任角色的 IAM 政策範例

```
{
  "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"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [

```

```

        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
    ],
    "Resource": "*"
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-ValidateFSxWindowsADConfig](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 若要使用現有失敗或設定錯誤的 Amazon FSx 驗證自我管理 AD，請輸入下列參數：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- FSxId (條件式)：

Amazon FSx for Windows File Server ID。這是驗證現有失敗或設定錯誤的 Amazon FSx 的必要項目。

- SecretArn (必要)：

包含 Amazon FSx 服務帳戶使用者名稱和密碼之 Secrets Manager 秘密的 ARN。請確定使用者名稱和密碼是以格式使用金鑰/值對來存放{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}。CloudFormation 堆疊會建立具有GetSecretValue執行此 ARN 之許可的驗證執行個體。

- FSxSecurityGroupId (必要)：

Amazon FSx for Windows File Server 的安全群組 ID。

- BucketName (必要)：

要上傳驗證結果的 Amazon S3 儲存貯體。請確定儲存貯體已設定伺服器端加密 (SSE)，且儲存貯體政策不會將不必要的讀取/寫入許可授予不需要存取日誌的各方。此外，請確定 Amazon EC2 Windows 執行個體具有 Amazon S3 儲存貯體的必要存取權。

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. 若要驗證新 Amazon FSx 建立的自我管理 AD 組態，請輸入下列參數：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- SecretArn (必要)：

包含 Amazon FSx 服務帳戶使用者名稱和密碼之 Secrets Manager 秘密的 ARN。請確定使用者名稱和密碼是以格式使用金鑰/值對來存放 `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`。CloudFormation 堆疊會建立具有 GetSecretValue 執行此 ARN 之許可的驗證執行個體。

- FSxSecurityGroupId (必要)：

Amazon FSx for Windows File Server 的安全群組 ID。

- BucketName (必要)：

要上傳驗證結果的 Amazon S3 儲存貯體。請確定儲存貯體已設定伺服器端加密 (SSE)，且儲存貯體政策不會將不必要的讀取/寫入許可授予不需要存取日誌的各方。此外，請確定 Amazon EC2 Windows 執行個體具有 Amazon S3 儲存貯體的必要存取權。

- **FSxPreferredSubnetId** (條件式) :

Amazon FSx for Windows File Server 偏好的子網路。

- **DomainName** (條件式) :

自我管理 Microsoft AD 網域的完整網域名稱。

- **DnsIpAddresses** (條件式) :

自我管理 AD 網域中最多兩個 DNS 伺服器或網域控制器 IP 地址的清單。針對最多兩個 IPs，輸入它們，並以逗號分隔。

- **FSxAdminsGroup** (條件式) :

Amazon FSx for Windows File Server 委派檔案系統管理員群組。根據預設，此為 Domain Admins。

- **FSxOrganizationalUnit** (條件式) :

您要加入檔案系統的組織單位 (OU)。提供 OU 的辨別路徑名稱。範

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.

false

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.

true

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.

10.0.1.10

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.

String

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.

OU=testou,DC=example,DC=com

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.

String

DomainName

(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.

example.com

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.

subnet-test1234example

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`.

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.

String

5. 選取執行。

6. 自動化會啟動。

7. 文件會執行下列步驟：

- CheckBucketPublicStatus (aws : executeScript) :

檢查目標 Amazon S3 儲存貯體是否可能授予其物件的讀取和/或寫入公開存取權。

- BranchOnInputParameters (aws : branch) :

所提供輸入參數上的分支，例如 Amazon FSx ID 或 Amazon FSx 參數。

- AssertFileSystemTypelsWindows (aws : assertAwsResourceProperty) :

如果提供 Amazon FSx ID，會驗證檔案系統類型為 Amazon FSx for Windows File Server。

- GetValidationInputs (aws : executeScript) :

傳回 CloudFormation 範本建立 Amazon EC2 執行個體所需的自我管理 Microsoft AD 組態。

- BranchOnInstanceId (aws : branch) :

所提供輸入 上的分支InstanceId。如果InstanceId提供，驗證指令碼會從自動化 在目標 Amazon EC2 執行個體上執行step:RunValidationScript。

- CreateEC2InstanceStack (aws : createStack) :

使用 AmazonFSxADValidation工具的執行 AWS CloudFormation 位置，在偏好的子網路中建立 Amazon EC2 執行個體

- DescribeStackResources (aws : executeAwsApi) :

描述 CloudFormation 堆疊以取得臨時 Amazon EC2 執行個體 ID。

- WaitForEC2InstanceToBeManaged (aws : waitForAwsResourceProperty) :

等到 Systems Manager 管理 Amazon EC2 執行個體，才能使用 SSM Run Command 執行驗證指令碼。

- GetAmazonFSxADValidationAttachment (aws : executeAwsApi) :

從 Runbook 附件取得AmazonFSxADValidation工具 URL。

- RunValidationScript (aws : runCommand) :

在暫時 Amazon EC2 執行個體上執行AmazonFSxADValidation工具，並將結果存放在

BucketName 參數中指定的 Amazon S3 儲存貯體中。

- DescribeErrorsFromStackEvents (aws : executeScript) :

如果 Runbook 無法建立堆疊，則說明 CloudFormation 堆疊事件。

- BranchOnRetainCloudFormationStack (aws : branch) :

RetainCloudFormationStack 和 InstanceId 參數上的分支，以判斷是否應刪除 CloudFormation 堆疊。

- DeleteCloudFormationStack (aws : deleteStack) :

刪除 AWS CloudFormation 堆疊。

8. 完成後，請檢閱輸出區段以取得執行結果：

```

▼ Outputs

DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:3[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-0[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.

```

Runbook 會將驗證指令碼執行的結果上傳至 Amazon S3 儲存貯體。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [什麼是 Amazon FSx for Windows File Server ?](#)
- [驗證 Amazon FSx for Windows File Server 的自我管理 AD 組態](#)

GuardDuty

AWS Systems Manager 自動化為 Amazon GuardDuty 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

AWSConfigRemediation-CreateGuardDutyDetector

Description

AWSConfigRemediation-CreateGuardDutyDetector Runbook 會在您執行自動化 AWS 區域的中建立 Amazon GuardDuty (GuardDuty) 偵測器。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector
- guardduty:GetDetector

文件步驟

- aws:executeAwsApi - 建立 GuardDuty 偵測器。
- aws:assertAwsResourceProperty - 驗證偵測器Status的 為 ENABLED 。

IAM

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Identity and Access Management。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [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-TroubleshootIAMAccessDeniedEvents

Description

AWSSupport-TroubleshootIAMAccessDeniedEvents 自動化 Runbook 可協助疑難排解 AWS Identity and Access Management (IAM) 存取遭拒的問題。Runbook 會查詢 CloudTrail 是否有與指定 IAM 實體 AWS 和服務事件來源相關的最近存取遭拒事件。它會在最多 24 小時的可設定時段內分析事件，每次執行最多處理 10 個事件。系統會檢查每個已識別的存取遭拒事件，以協助了解拒絕的內容和嘗試的動作。自動化會分析身分型和資源型 IAM 政策。對於身分型政策，它會檢查連接到 IAM 實體的內嵌和受管政策。對於以資源為基礎的政策，它會評估多個 AWS 服務的政策，包括 Amazon Simple Storage Service (Amazon S3)、AWS Key Management Service (AWS KMS) AWS Lambda、Amazon Simple Notification Service (Amazon SNS)、Amazon Elastic Container Registry (Amazon ECR)、Amazon API Gateway、CodeArtifact、Amazon Elastic File System (Amazon EFS) AWS Serverless Application Repository、Amazon Simple Queue Service (Amazon SQS) AWS Cloud9、Amazon OpenSearch Service、AWS Signer 和 AWS Secrets Manager。

Runbook 利用 IAM 政策模擬功能，針對 CloudTrail 事件中含有的拒絕動作來評估這些政策。Runbook 透過適用於 IAM 使用者的 [SimulatePrincipalPolicy](#) 和適用於 IAM 角色的 [SimulateCustomPolicy](#)，利用 IAM 的政策模擬功能，針對 CloudTrail 事件中含有的拒絕動作來評估這些政策。自動化會輸出報告，以協助識別遭拒的特定動作、區分隱含和明確拒絕、列出負責存取拒絕的政策，並針對每個拒絕提供說明。報告也會建議潛在的解決方案，例如識別缺少的允許陳述式或衝突的拒絕陳述式。

如何運作？

Runbook 會執行下列步驟：

- 描述並驗證 RequesterARN (角色或使用者) 以取得 IAM 實體類型和 IAM ID 等資訊。
- 擷取與 RequesterARN、和相關聯的 CloudTrail 事件EventSource，ResourceARN如果提供的話。

- 分析 CloudTrail 事件以取得傳回存取遭拒錯誤時所執行的動作，然後檢查連接至 IAM 實體的所有 IAM 政策，例如內嵌和受管政策，以及資源型政策。然後，它會針對從有問題的 CloudTrail 事件存取遭拒錯誤中找到的動作來模擬這些政策，以判斷錯誤的原因。
- 輸出報告，判斷拒絕存取錯誤的類型、負責錯誤的政策，並針對錯誤提供潛在解決方案的建議。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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

範例政策：

```
{
  "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:GetFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:GetEnvironment",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-TroubleshootIAMAccessDeniedEvents](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：

- 描述：(選用) 允許 SSM Automation 代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。角色需要新增到您的 Amazon EKS 叢集存取項目或 RBAC 許可，以允許 Kubernetes API 呼叫。
- 類型：AWS::IAM::Role::Arn
- RequesterARN (必要)：
 - 描述：(必要) 您要調查特定 AWS 資源存取許可的 IAM 使用者或角色的 ARN。
 - 類型：字串
 - 允許模式：`^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/[\\w+\\.@-]+`
- ResourceARN (選用)：
 - 描述：(選用) 評估拒絕存取之 AWS 資源的 ARN。AWS 目標資源應存在於執行自動化 Runbook 的相同區域中。
 - 類型：字串
 - 允許模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:([a-zA-Z0-9\\-]{1,63}):([a-zA-Z0-9\\-]{0,63})?:([a-zA-Z0-9\\-]{1,1024})$`
- EventSource (必要)：
 - 描述：(必要) 產生 CloudTrail 事件的 Amazon API 端點。例如：`s3.amazonaws.com`。
 - 類型：字串
 - 允許模式：`^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (選用)：
 - 描述：(選用) 與 CloudTrail 事件相關聯的 Amazon API 動作名稱。例如：`s3:CreateBucket`。
 - 類型：字串
 - 允許模式：`^$|^([a-zA-Z0-9]+:[A-Za-z0-9]+)$`
- LookBackHours (選用)：
 - 描述：(選用) 搜尋事件時，在 CloudTrail Access Denied 事件中回顧的時數。有效範圍：1 到 24 小時。
 - 類型：整數
 - 允許模式：`^([1-9]|1[0-9]|2[0-4])$`
- 預設：12
- MaxEvents (選用)：

- 描述：(選用) 搜尋 Access Denied 事件時傳回的 CloudTrail 事件數目上限。有效範圍：1 至 5 事件。
- 類型：整數
- 允許模式：`^([1-9]|1[0-9]|2[0-4])$`
- 預設：3
- UseContextEntries (選用)：
 - 描述：(選用) 如果您指定 `true`，自動化會從 CloudTrail 事件擷取 API 請求內容的詳細資訊，並將其納入 IAM 政策模擬。
 - 類型：布林值
 - 允許模式：`^([1-9]|1[0-9]|2[0-4])$`
 - 預設：3

4. 選取執行。

5. 自動化會啟動。

6. 文件會執行下列步驟：

- ValidateRequesterArn

驗證和解構 RequesterArn ARN，擷取目標 IAM 使用者或角色的相關資訊。

- GetCloudTrailEventsWithAccessDeniedError

查詢 CloudTrail 事件，以取得與指定 IAM 實體 AWS 和服務 相關的最近 Access Denied 事件 EventSource。

- EvaluateIAMRequesterPolicies

根據 CloudTrail 事件的動作，評估請求者 IAM 實體的 IAM 許可。此評估包括分析與請求者相關聯的身分型和資源型政策。自動化利用 IAM 的政策模擬功能，在 CloudTrail 事件中識別的拒絕動作內容中評估這些政策。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- PermissionEvaluationResults

輸出報告，以協助識別遭拒的特定動作，區分隱含和明確拒絕。它還列出了負責存取拒絕的政策，並對每個拒絕提供說明。報告也會建議潛在的解決方案，例如識別缺少的允許陳述式或衝突的拒絕陳述式

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定 自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS-AttachIAMToInstance

Description

將 AWS Identity and Access Management (IAM) 角色連接至受管執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ForceReplace

類型：布林值

描述：（選用）指定是否取代現有 IAM 設定檔的旗標。

預設：true

- InstanceId

類型：字串

描述：（必要）您要為其指派 IAM 角色的執行個體 ID。

- RoleName

類型：字串

描述：（必要）要新增至受管執行個體的 IAM 角色名稱。

文件步驟

1. `aws:executeAwsApi - DescribeInstanceProfile` - 尋找連接至 EC2 執行個體的 IAM 執行個體描述檔。
2. `aws:branch - CheckInstanceProfileAssociations` - 檢查連接至 EC2 執行個體的 IAM 執行個體描述檔。
 - a. 如果已連接 IAM 執行個體描述檔，且 `ForceReplace` 設定為 `true`：
 - i. `aws:executeAwsApi - DisassociateIAMInstanceProfile` - 取消 IAM 執行個體描述檔與 EC2 執行個體的關聯。
 - b. `aws:executeAwsApi - ListInstanceProfilesForRole` - 列出所提供 IAM 角色的執行個體描述檔。
 - c. `aws:branch - CheckInstanceProfileCreated` - 檢查提供的 IAM 角色是否有相關聯的執行個體描述檔。
 - i. 如果 IAM 角色具有相關聯的執行個體描述檔：
 - A. `aws:executeAwsApi - DetachIAMProfileFromInstance` - 將 IAM 執行個體描述檔角色連接至 EC2 執行個體。
 - i. 如果 IAM 角色沒有相關聯的執行個體描述檔：
 - A. `aws:executeAwsApi - CreateInstanceProfileForRole` - 為指定的 IAM 角色建立執行個體描述檔角色。
 - B. `aws:executeAwsApi - AddRoleToInstanceProfile` - 將執行個體描述檔角色連接至指定的 IAM 角色。
 - C. `aws:executeAwsApi - GetInstanceProfile` - 取得指定 IAM 角色的執行個體設定檔資料。

D. `aws:executeAwsApi - AttachIAMProfileToInstanceWithRetry` - 將 IAM 執行個體描述檔角色連接至 EC2 執行個體。

輸出

`AttachIAMProfileToInstanceWithRetry.AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`AttachIAMProfileToInstance.AssociationId`

`ListInstanceProfilesForRole.InstanceProfileName`

`ListInstanceProfilesForRole.InstanceProfileArn`

AWS-DeleteIAMInlinePolicy

Description

AWS-DeleteIAMInlinePolicy Runbook 會刪除連接至您指定 IAM 身分的所有 AWS Identity and Access Management (IAM) 內嵌政策。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- iamArns

類型：字串

描述：(必要) 您要從中刪除內嵌政策之 IAM 身分ARNs逗號分隔清單。此清單可以包含 IAM 使用者、群組或角色。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

文件步驟

- aws:executeScript - 刪除連接到目標 IAM 身分的 IAM 內嵌政策。

AWSConfigRemediation-DeleteIAMRole

Description

AWSConfigRemediation-DeleteIAMRole Runbook 會 AWS Identity and Access Management 刪除您指定的 (IAM) 角色。此自動化不會刪除與 IAM 角色或服務連結角色相關聯的執行個體描述檔。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- IAMRoleID

類型：字串

描述：(必要) 您要刪除的 IAM 角色 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:GetRole
- iam>ListAttachedRolePolicies
- iam>ListInstanceProfilesForRole
- iam>ListRolePolicies
- iam>ListRoles
- iam:RemoveRoleFromInstanceProfile

文件步驟

- `aws:executeScript` - 收集您在 `IAMRoleID` 參數中指定的 IAM 角色名稱。
- `aws:executeScript` - 收集與 IAM 角色相關聯的政策和執行個體描述檔。
- `aws:executeScript` - 刪除連接的政策。
- `aws:executeScript` - 刪除 IAM 角色並驗證該角色已刪除。

AWSConfigRemediation-DeleteIAMUser

Description

AWSConfigRemediation-DeleteIAMUser Runbook 會 AWS Identity and Access Management 刪除您指定的 (IAM) 使用者。此自動化會刪除或分離與 IAM 使用者相關聯的下列資源：

- 存取金鑰
- 連接的受管政策
- Git 登入資料
- IAM 群組成員資格
- IAM 使用者密碼
- 內嵌政策
- 多重要素驗證 (MFA) 裝置
- 簽署憑證
- SSH 公有金鑰

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- IAMUserId

類型：字串

描述：(必要) 您要刪除的 IAM 使用者 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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:ListGroupsWithUser
- iam>ListMFADevices
- iam:ListServiceSpecificCredentials

- `iam:ListSigningCertificates`
- `iam:ListSSHPublicKeys`
- `iam:ListUserPolicies`
- `iam:ListUsers`
- `iam:RemoveUserFromGroup`

文件步驟

- `aws:executeScript` - 收集您在 `IAMUserId` 參數中指定的 IAM 使用者名稱。
- `aws:executeScript` - 收集與 IAM 使用者相關聯的存取金鑰、憑證、登入資料、MFA 裝置和 SSH 金鑰。
- `aws:executeScript` - 收集 IAM 使用者的群組成員資格和政策。
- `aws:executeScript` - 刪除與 IAM 使用者相關聯的存取金鑰、憑證、登入資料、MFA 裝置和 SSH 金鑰。
- `aws:executeScript` - 刪除 IAM 使用者的群組成員資格和政策。
- `aws:executeScript` - 刪除 IAM 使用者並確認已刪除使用者。

AWSConfigRemediation-DeleteUnusedIAMGroup

Description

AWSConfigRemediation-DeleteUnusedIAMGroup Runbook 會刪除不包含任何使用者的 IAM 群組。

AWSConfigRemediation-DeleteUnusedIAMGroup Runbook 會刪除不包含任何使用者的 IAM 群組。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- GroupName

類型：字串

描述：(必要) 您要刪除的 IAM 群組名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteGroup
- iam>DeleteGroupPolicy
- iam:DetachGroupPolicy

文件步驟

- aws:executeScript - 移除連接至目標 IAM 群組的受管和內嵌 IAM 政策，然後刪除 IAM 群組。

AWSConfigRemediation-DeleteUnusedIAMPolicy

Description

AWSConfigRemediation-DeleteUnusedIAMPolicy Runbook 會刪除未連接到任何使用者、群組或角色的 AWS Identity and Access Management (IAM) 政策。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- IAMResourceId

類型：字串

描述：(必要) 您要刪除之 IAM 政策的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DeletePolicy
- iam:DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

文件步驟

- `aws:executeScript` - 刪除您在 `IAMResourceId` 參數中指定的政策，並驗證政策已刪除。

AWSConfigRemediation-DetachIAMPolicy

Description

AWSConfigRemediation-DetachIAMPolicy Runbook 會分離您指定的 AWS Identity and Access Management (IAM) 政策。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- IAMResourceId

類型：字串

描述：（必要）您要分離的 IAM 政策 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

文件步驟

- `aws:executeScript` - 從所有資源分離 IAM 政策。

AWSConfigRemediation-EnableAccountAccessAnalyzer

Description

AWSConfigRemediation-EnableAccountAccessAnalyzer Runbook 會在您的 中建立 AWS Identity and Access Management (IAM) Access Analyzer AWS 帳戶。如需 Access Analyzer 的相關資訊，請參閱 [《AWS IAM 使用者指南》中的使用 IAM Access Analyzer](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AnalyzerName`

類型：字串

描述：(必要) 要建立的分析器名稱。

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- access-analyzer:CreateAnalyzer
- access-analyzer:GetAnalyzer

文件步驟

- aws:executeAwsApi - 為您的帳戶建立存取分析器。
- aws:waitForAwsResourceProperty - 等待存取分析器的狀態為 ACTIVE。
- aws:assertAwsResourceProperty - 確認存取分析器的狀態為 ACTIVE。

AWSSupport-GrantPermissionsToIAMUser

Description

此 Runbook 會將指定的許可授予 IAM 群組（新群組或現有群組），並將現有的 IAM 使用者新增至該群組。您可以選擇的政策：[Billing](#) 或 [Support](#)。若要為 IAM 啟用帳單存取，請記得也要啟用 [IAM 使用者和聯合身分使用者對帳單與成本管理頁面的存取](#)。

Important

如果您提供現有的 IAM 群組，群組中所有目前的 IAM 使用者都會收到新的許可。

執行此自動化 (主控台)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- IAMGroupName

類型：字串

預設：ExampleSupportAndBillingGroup

描述：(必要) 可以是新的或現有的群組。必須遵守 [IAM 實體名稱限制](#)。

- IAMUserName

類型：字串

預設：ExampleUser

描述：(必要) 必須是現有的使用者。

- LambdaAssumeRole

類型：字串

描述：(選用) 由 lambda 擔任之角色的 ARN。

- 許可

類型：字串

有效值：SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

預設：SupportAndBillingFullAccess

描述：(必要) 選擇其中一項：SupportFullAccess 授予支援中心的完整存取權。BillingFullAccess 授予帳單儀表板的完整存取權。SupportAndBillingFullAccess 授予支援中心和帳單儀表板的完整存取權。您可以在文件詳細資訊下的政策找到更多資訊。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

所需的許可取決於 AWSSupport-GrantPermissionsToIAMUser 的執行方式。

以目前登入的使用者或角色執行

建議您連接 AmazonSSMAutomationRole Amazon 受管政策，以及下列其他許可，以建立要傳遞給 Lambda 的 Lambda 函數和 IAM 角色：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda>DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
                "arn:aws:lambda:*:ACCOUNTID: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

使用者必須擁有 Runbook 上的 `ssm : StartAutomationExecution` 許可，以及傳遞為 `AutomationAssumeRole PassRoleLambdaAssumeRole`。以下為各 IAM 角色需要的許可：

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" : "*"
}
]
```

文件步驟

1. `aws:createStack` - 執行 AWS CloudFormation 範本以建立 Lambda 函數。
2. `aws:invokeLambdaFunction` - 執行 Lambda 以設定 IAM 許可。
3. `aws:deleteStack` - 刪除 CloudFormation 範本。

輸出

`configureIAM.Payload`

AWSConfigRemediation-RemoveUserPolicies

Description

AWSConfigRemediation-RemoveUserPolicies Runbook 會刪除 AWS Identity and Access Management (IAM) 內嵌政策，並分離連接到您指定使用者的任何受管政策。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- IAMUserID

類型：字串

描述：（必要）您要從中移除政策的使用者 ID。

- PolicyType

類型：字串

有效值：全部 | 內嵌 | 受管

預設：全部

描述：（必要）您要從使用者中移除的 IAM 政策類型。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteUserPolicy
- iam:DetachUserPolicy
- iam>ListAttachedUserPolicies

- `iam:ListUserPolicies`
- `iam:ListUsers`

文件步驟

- `aws:executeScript` - 刪除和分離您在 `IAMUserID` 參數中指定的使用者的 IAM 政策。

AWSConfigRemediation-ReplaceIAMInlinePolicy

Description

AWSConfigRemediation-ReplaceIAMInlinePolicy Runbook 會將內嵌 AWS Identity and Access Management (IAM) 政策取代為複寫的受管 IAM 政策。對於連接到使用者、群組或角色的內嵌政策，內嵌政策許可會複製到受管 IAM 政策。受管 IAM 政策會新增至 資源，並移除內嵌政策。AWS Config 必須在您執行此自動化的 AWS 區域 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `InlinePolicyName`

類型：StringList

描述：（必要）您要取代的內嵌 IAM 政策。

- ResourceId

類型：字串

描述：（必要）您要取代其內嵌政策的 IAM 使用者、群組或角色 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

文件步驟

- aws:executeScript - 將內嵌 IAM 政策取代為您指定的資源上的複 AWS 寫政策。

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Description

AWSConfigRemediation-RevokeUnusedIAMUserCredentials Runbook 會撤銷 unused AWS Identity and Access Management (IAM) 密碼和作用中的存取金鑰。此 Runbook 也會停用過期的存取金鑰，並刪除過期的登入設定檔。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- IAMResourceId

類型：字串

描述：（必要）您要撤銷未使用登入資料的 IAM 資源 ID。

- MaxCredentialUsageAge

類型：字串

預設：90

描述：（必要）必須已使用登入資料的天數。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam:DeleteAccessKey
- iam:DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

文件步驟

- aws:executeScript - 撤銷 IAMResourceId 參數中指定使用者的 IAM 登入資料。停用過期的存取金鑰，並刪除過期的登入設定檔。

Note

請務必設定此修復動作的 MaxCredentialUsageAge 參數，以符合您用來觸發此動作之 AWS Config 規則的 maxAccessKeyAge 參數：[access-keys-rotated](#)。

AWSConfigRemediation-SetIAMPasswordPolicy

Description

AWSConfigRemediation-SetIAMPasswordPolicy Runbook 會為您的 設定 AWS Identity and Access Management (IAM) 使用者密碼政策 AWS 帳戶。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- AllowUsersToChangePassword

類型：布林值

預設：false

描述：(選用) 如果設定為 true ，則 中的所有 IAM 使用者 AWS 帳戶 都可以使用 AWS Management Console 來變更其密碼。

- HardExpiry

類型：布林值

預設：false

描述：(選用) 如果設定為 true ，IAM 使用者在密碼過期後將無法重設密碼。

- MaxPasswordAge

類型：整數

預設：0

描述：(選用) IAM 使用者密碼有效的天數。

- MinimumPasswordLength

類型：整數

預設：6

描述：(選用) IAM 使用者密碼的最小字元數。

- PasswordReusePrevention

類型：整數

預設：0

描述：(選用) 阻止 IAM 使用者重複使用的先前密碼數目。

- RequireLowercaseCharacters

類型：布林值

預設：false

描述：(選用) 如果設定為 true，IAM 使用者的密碼必須包含 ISO 基本拉丁字母 (a 到 z) 中的小寫字元。

- RequireNumbers

類型：布林值

預設：false

描述：(選用) 如果設定為 true，IAM 使用者的密碼必須包含數字字元 (0-9)。

- RequireSymbols

類型：布林值

預設：false

描述：(選用) 如果設定為 true，IAM 使用者的密碼必須包含非英數字元 (! @ # \$ % ^ * () _ + - = [] { } | ')。

- RequireUppercaseCharacters

類型：布林值

預設：false

描述：(選用) 如果設定為 `true`，IAM 使用者的密碼必須包含 ISO 基本拉丁字母 (A 到 Z) 中的大寫字元。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

文件步驟

- `aws:executeScript` - 根據您為 Runbook 參數指定的值設定 IAM 使用者密碼政策 AWS 帳戶。

AWSSupport-ContainIAMPrincipal

Description

如果發生安全事件或疑似入侵 AWS Identity and Access Management (IAM) 使用者/角色或 AWS 身分中心 (IDC) 使用者，快速隔離受影響的身分至關重要，同時保留其組態以進行調查。AWSSupport-ContainIAMPrincipal Runbook 提供結構化、可復原的方法，以包含遭入侵的 IAM 或 IDC 身分，有效地封鎖其對 AWS 資源的存取，並防止入侵的潛在傳播。

此自動化程序可在不永久變更身分組態的情況下進行調查，並在認為適當時還原正常存取。遏制程序會維護 IAM 內的使用者或角色，或 IDC 內的使用者，同時有效地將其與所有網路活動隔離。此隔離可防止包含的身分資源與 Amazon Virtual Private Cloud 內的資源通訊，或存取網際網路資源。遏制的設計是可逆的，允許在認為適當時還原正常存取。

如何運作？

AWSSupport-ContainIAMPrincipal Runbook 為 IAM 使用者、角色和 Identity Center 使用者實作全面的遏制程序。在Contain模式下執行時，它會先驗證所有輸入參數，並對指定的 Amazon S3 儲存體執行安全檢查。然後，它會收集目標 IAM 主體的詳細資訊，並根據主體類型套用適當的遏制措施。對於 IAM 使用者，它會停用存取金鑰、移除主控台存取，以及連接拒絕政策。對於 IAM 角色，它會附加拒絕政策，以撤銷在遏制之前建立之工作階段的許可。對於 Identity Center 使用者，它會移除

許可集、群組成員資格，並套用拒絕政策。在整個過程中，Runbook 會將原始組態備份到 Amazon S3 儲存貯體，以便進行可能的還原。在 Restore 模式下執行時，它會嘗試使用備份組態將主體還原至其遏制前狀態。Runbook 包含預覽變更而不套用變更DryRun的選項，並提供成功操作和失敗案例的完整報告。

Important

- 使用提升權限：此 SSM 文件會執行需要提升權限的各種操作，例如修改 IAM 和 IDC 身分政策，以及套用隔離組態。這些動作可能會導致權限提升，或影響依賴目標身分的其他工作負載。您應該檢閱授予 AutomationAssumeRole 參數所指定角色的許可，並確保這些許可適用於預期的使用案例。如需 IAM 許可的詳細資訊，請參閱下列 AWS 文件：
 - [Identity and Access Management \(IAM\) 許可](#)
 - [AWS Systems Manager Automation 許可](#)
- 工作負載無法使用風險：此 Systems Manager 文件會執行隔離動作，這可能會導致工作負載無法使用或中斷。在安全事件期間執行時，它會從指定的 IAM 和 IDC 身分撤銷 AWS API 許可，防止他們進行任何 AWS API 呼叫或動作，以限制對受影響資源的存取。這可能會影響依賴這些身分的任何應用程式或服務。
- 建立其他資源：自動化文件可能會根據執行參數，有條件地建立其他資源，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體和存放在其中的 Amazon S3 物件。這些資源會根據您的 AWS 用量產生額外費用。
- 還原風險：如果動作參數設定為 Restore，此 SSM 文件會嘗試將 IAM 或 IDC 身分組態還原為其原始狀態。不過，還原程序可能會失敗，使 IAM 或 IDC 身分處於不一致的狀態。本文件提供在發生此類失敗時手動還原的說明，但您應該準備好在還原過程中處理潛在問題。

建議您徹底檢閱 Runbook、了解其潛在影響，並在非生產環境中進行測試，然後再在您的生產環境中執行。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列許可，才能成功使用 Runbook：

- s3:GetBucketLocation
- s3:GetBucket
- s3:ListBucket
- s3 : GetBucketPublicAccessBlocks
- s3 : GetAccountPublicAccessBlocks
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetObject
- s3:CreateBucket
- s3:PutObject
- 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
- organizations:ListAccounts
- sso : ListPermissionSetsProvisionedToAccount
- sso : GetInlinePolicyForPermissionSet
- sso : ListInstances
- sso-directory : SearchUsers
- sso : ListPermissionSets
- sso : ListAccountAssignments
- sso-directory : DescribeUser
- identitystore:ListUsers
- identitystore:ListGroups
- identitystore:IsMemberInGroups
- identitystore:ListGroupMemberships
- secretsmanager:CreateSecret
- secretsmanager>DeleteSecret

- sso : DeleteAccountAssignment
- sso : PutInlinePolicyToPermissionSet
- sso : CreateAccountAssignment
- sso : DeleteInlinePolicyFromPermissionSet
- sso : TagResource
- sso : UntagResource
- identitystore:DeleteGroupMembership
- identitystore:CreateGroupMembership

以下是授予 必要許可的 IAM 政策範例AutomationAssumeRole :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucket",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlocks",
        "s3:GetAccountPublicAccessBlocks",
        "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": "*"
}
]
}

```

指示

請依照下列步驟設定自動化：

1. 導覽至 AWS Systems Manager 主控台中的 [AWSSupport-ContainIAMPrincipal](#)。

2. 選擇 Execute automation (執行自動化)。

3. 針對輸入參數，輸入下列內容：

- AutomationAssumeRole (選用) :
 - 描述：(選用) Identity AWS and Access Management (IAM) 角色的 Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。
 - 類型：AWS::IAM::Role::Arn
- PrincipalType (必要) :
 - 描述：(必要) AWS IAM 主體類型：IAM 使用者、IAM 角色或 Identity Center 使用者。
 - 類型：字串
 - 允許的值：IAM user|IAM role|Identity Center user
- PrincipalName (必要) :
 - 描述：(必要) IAM 主體的名稱。對於 Identity Center 使用者，請提供使用者名稱。
 - 類型：字串
 - 允許模式：`^[a-zA-Z0-9\.\_\-\!\*'()/+ =, @]{1,1024}$`
- 動作 (必要) :
 - 描述：(必要) 選取 Contain 以隔離目標 IAM 主體 Restore，或嘗試從先前的備份將 IAM 主體還原為其原始組態。
 - 類型：字串
 - 允許的值：Contain|Restore
- DryRun (選用) :
 - 描述：(選用) 設為 `true`，自動化不會對目標 IAM 主體進行任何變更，而是輸出其嘗試變更的內容，詳細說明每個步驟。預設值：`true`。
 - 類型：布林值
 - 允許的值：`true|false`
- ActivateDisabledKeys (條件式) :
 - 描述：(條件式) 如果輸入參數動作設定為 `Restore` 且 `PrincipalType` 設定為 IAM 使用者，此選項會判斷此自動化是否應嘗試在停用時啟用相關聯的存取金鑰。請注意，無法驗證遭入侵存取金鑰的完整性。AWS 強烈建議您不要重新啟用遭入侵的金鑰。反之，建議您產生新的金鑰。預設值：`false`。
 - 類型：布林值

- BackupS3BucketName (條件式) :
 - 描述 : (條件式) 在動作設定為 時備份 IAM 主體組態的 Amazon S3 儲存貯體, Contain或在動作為 時從 還原組態Restore。請注意, 如果指定的動作為 , Contain且 Runbook 無法存取 儲存貯體, 或未提供 值, 則會在帳戶中建立新的儲存貯體, 名稱為 awssupport-containiamprincipal-`<random-string>`。如果 DryRun 設定為true此參數為必要。
 - 類型 : AWS::S3::Bucket::Name
 - BackupS3KeyName (條件式) :
 - 描述 : (條件式) 如果動作設定為 Restore, 這會指定自動化用來嘗試還原 IAM 主體組態的 Amazon S3 金鑰。Amazon Amazon S3 金鑰通常遵循此格式 : {year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json。金鑰可從先前的遏制自動化執行的輸出取得。
 - 類型 : 字串
 - 允許模式 : `^[a-zA-Z0-9\\.\_\-\_\!\*'()/]{0,1024}$`
 - BackupS3BucketAccess (條件式) :
 - 描述 : (條件式) 在執行遏制動作後, 允許存取備份 Amazon S3 儲存貯體的 IAM 使用者或角色 ARN。動作為 時, 需要此參數Contain。AutomationAssumeRole, 或在沒有AutomationAssumeRole 的情況下, 正在執行其內容的使用者會自動新增至清單中。
 - 類型 : StringList
 - 允許模式 : `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
 - TagIdentifier (選用) :
 - 描述 : (選用) 使用下列格式, 以您選擇的標籤標記 IAM 主體 : Key=<EXAMPLE_KEY>, Value=<EXAMPLE_VALUE>。此選項可讓您追蹤此 Runbook 的目標 IAM 主體。注意 : 標籤鍵和值區分大小寫。
 - 類型 : 字串
 - 允許模式 : `^$|^([Kk][Ee][Yy]=[\\+\\-\\|=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\|=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128})$`
4. 選取執行。
 5. 自動化會啟動。
 6. 文件會執行下列步驟 :
 - ValidateRequiredInputs

- CheckBackupS3BucketName

檢查目標 Amazon S3 儲存貯體是否可能授予read或write公開存取其物件。在遏制工作流程的情況下，如果儲存貯體不存在，則會建立新的 Amazon S3 儲存BackupS3BucketName貯體。

- BranchOnAction

根據指定的值來配置自動化Action。

- BranchOnPrincipalTypeAndDryRun

根據 IAM 主體的類型 (IAM 使用者、IAM 角色或 Identity Center 使用者)，以及它是否在 DryRun 模式下執行，來配置自動化。

- BranchOnPrincipalTypeForContain

為 Contain 動作型和輸入中指定的 IAM 委託人類型 (IAM 使用者、IAM 角色或 Identity Center 使用者) 分支自動化。

- GetIAMUser

取得目標 IAM 使用者的建立時間和使用者名稱。

- GetIAMUserDetails

取得和儲存目標 IAM 使用者的組態，包括內嵌政策、受管政策、存取金鑰、MFA 裝置和登入設定檔。

- UpdateS3KeyForUser

從步驟的輸出更新自動化 'S3Key' 變數GetIAMUserDetails。

- GetIAMRole

取得目標 IAM 角色的建立時間、角色名稱和路徑。

- GetIAMRoleDetails

取得和存放目標 IAM 角色的組態，包括內嵌政策和連接到角色的受管政策。

- UpdateS3KeyForRole

從步驟的輸出更新自動化 'S3Key' 變數GetIAMRoleDetails。

- GetIdentityStoreId

取得與 AWS 帳戶相關聯的 AWS IAM Identity Center 執行個體 ID。

使用 Identity Store ID 取得目標 Identity Center 使用者的使用者 ID。

- GatherIDCUserDetails

取得和儲存目標 Identity Center 使用者的組態，包括帳戶指派、相關聯的許可集和內嵌政策。

- UpdateS3KeyForIDCUser

從步驟的輸出更新自動化 'S3Key' 變數 GatherIDCUserDetails。

- BranchOnIdentityContain

根據的值 DryRun 和 Contain 動作的 IAM 主體類型來配置自動化。

- BranchOnDisableAccessKeys

根據 IAM 使用者是否具有需要停用的存取金鑰，來配置自動化。

- DisableAccessKeys

停用作用中的 IAM 使用者存取金鑰。

- BranchOnDisableConsoleAccess

根據 IAM 使用者是否已啟用 AWS 管理主控台存取的分支。

- DisableConsoleAccess

移除 IAM 使用者對 AWS 管理主控台的密碼型存取。

- AttachInlineDenyPolicyToUser

將拒絕政策連接至 IAM 使用者，以撤銷舊工作階段字符的許可。

- AttachInlineDenyPolicyToRole

將拒絕政策連接至 IAM 角色，以撤銷舊工作階段字符的許可。

- RemovePermissionSets

移除與 Identity Center 使用者相關聯的許可集。

- RemoveIDCUserFromIDCGroups

從 Identity Center 群組中移除 Identity Center 使用者。

- AttachInlineDenyPolicyToPermissionSet

將拒絕政策連接至與 Identity Center 使用者相關聯的許可集。

- BranchOnReactivateKeys

在還原程序期間，根據 ActivateDisabledKeys 參數分支自動化。

- DetachInlineDenyPolicy

在遏制過程中移除連接到 IAM 角色的拒絕政策。

- DetachInlineDenyPolicyFromPermissionSet

在遏制程序期間移除附加至許可集的拒絕政策。

- ReportContain

輸出有關 DryRun 設定為 時將執行的遏制動作的詳細資訊 True。

- ReportRestore

輸出在 DryRun 設定為 時將執行之還原動作的詳細資訊 True。

- ReportContainFailure

提供在遏制工作流程失敗情況下手動還原 IAM 主體原始組態的完整說明。

- ReportRestoreFailure

提供詳細說明，以在還原工作流程失敗案例期間手動完成 IAM 主體原始組態的還原。

7. 執行完成後，請檢閱輸出區段以取得執行的詳細結果：

- ContainIAMPrincipal.Output

提供當動作設定為「包含」且 DryRun 設定為「False」時所執行之遏制動作的詳細資訊。包括備份位置、套用的拒絕政策和修改組態的相關資訊。

- RestoreIAMPrincipal.Output

提供當動作設定為 Restore 且 DryRun 設定為 False 時所執行還原動作的詳細資訊。包括還原組態的相關資訊，以及在還原期間遇到的任何問題。

- ReportContain.Output

輸出有關當動作設定為「包含」且 DryRun 設定為「True」時將執行之遏制動作的詳細資訊。包括目前和遏制後組態的比較。

- ReportRestore.Output

輸出當動作設定為 Restore 且 DryRun 設定為 True 時，將執行之還原動作的詳細資訊。顯示目前的組態和要還原的原始組態。

- `ReportContainFailure.Output`

提供在遏制工作流程失敗情況下手動還原 IAM 主體原始組態的完整說明。

- `ReportRestoreFailure.Output`

提供詳細說明，以在還原工作流程失敗案例期間手動完成 IAM 主體原始組態的還原。

輸出

執行完成後，請檢閱輸出區段以取得詳細結果：

- `ContainIAMPrincipal.Output`

提供當動作設定為「包含」且 `DryRun` 設定為「False」時所執行之遏制動作的詳細資訊。包括備份位置、套用的拒絕政策和修改組態的相關資訊。

- `RestoreIAMPrincipal.Output`

提供當動作設定為 `Restore` 且 `DryRun` 設定為 `False` 時所執行還原動作的詳細資訊。包括還原組態的相關資訊，以及在還原期間遇到的任何問題。

- `ReportContain.Output`

輸出有關當動作設定為「包含」且 `DryRun` 設定為「True」時將執行之遏制動作的詳細資訊。包括目前和遏制後組態的比較。

- `ReportRestore.Output`

輸出當動作設定為 `Restore` 且 `DryRun` 設定為 `True` 時，將執行之還原動作的詳細資訊。顯示目前的組態和要還原的原始組態。

- `ReportContainFailure.Output`

提供在遏制工作流程失敗情況下手動還原 IAM 主體原始組態的完整指示。

- `ReportRestoreFailure.Output`

提供詳細說明，以在還原工作流程失敗案例期間手動完成 IAM 主體原始組態的還原。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)

- [執行簡易自動化](#)
- [設定自動化](#)
- [支援自動化工作流程](#)

Amazon Kinesis Data Streams

AWS Systems Manager 自動化為 Amazon Kinesis Data Streams 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableKinesisStreamEncryption](#)

AWS-EnableKinesisStreamEncryption

Description

AWS-EnableKinesisStreamEncryption Runbook 會在 Amazon Kinesis Data Streams (Kinesis Data Streams) 上啟用加密。如果寫入加密串流的生產者應用程式無法存取 AWS Key Management Service (AWS KMS) 金鑰，將會發生錯誤。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- KinesisStreamName

類型：字串

描述：(必要) 您要啟用加密的串流名稱。

- KeyId

類型：字串

預設：alias/aws/kinesis

描述：(必要) 您要用於加密的客戶受管 AWS KMS 金鑰。此值可以是全域唯一識別符、別名或金鑰的 ARN，或是以 "alias/" 開頭的別名名稱。您也可以使用 參數的預設值來使用 AWS 受管金鑰。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- kinesis:DescribeStream
- kinesis:StartStreamEncryption
- kms:DescribeKey

文件步驟

- VerifyKinesisStreamStatus (aws:waitForAwsResourceProperty) - 檢查 Kinesis Data Streams 的狀態。
- EnableKinesisStreamEncryption (aws:executeAwsApi) - 啟用 Kinesis Data Streams 的加密。
- VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty) - 等待 Kinesis Data Streams 狀態傳回 ACTIVE。
- VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty) - 驗證 Kinesis Data Streams 已啟用加密。

AWS KMS

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Key Management Service。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

AWSConfigRemediation-CancelKeyDeletion

Description

AWSConfigRemediation-CancelKeyDeletion Runbook 會取消刪除您指定的 AWS Key Management Service (AWS KMS) 客戶受管金鑰。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KeyId

類型：字串

描述：（必要）您要取消刪除的客戶受管金鑰 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion
- kms:DescribeKey

文件步驟

- aws:executeAwsApi - 取消刪除您在 KeyId 參數中指定的客戶受管金鑰。
- aws:assertAwsResourceProperty - 確認您的客戶受管金鑰已停用金鑰刪除。

AWSConfigRemediation-EnableKeyRotation

Description

AWSConfigRemediation-EnableKeyRotation Runbook 會啟用對稱 AWS Key Management Service (AWS KMS) 客戶受管金鑰的自動金鑰輪換。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KeyId

類型：字串

描述：(必要) 您要啟用自動金鑰輪換的客戶受管金鑰 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:EnableKeyRotation
- kms:GetKeyRotationStatus

文件步驟

- aws:executeAwsApi - 針對您在 KeyId 參數中指定的客戶受管金鑰啟用自動金鑰輪換。
- aws:assertAwsResourceProperty - 確認您的客戶受管金鑰已啟用自動金鑰輪換。

Lambda

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Lambda。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)

- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

Description

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing Runbook 會在您在 FunctionName 參數中指定的 AWS Lambda 函數上啟用 AWS X-Ray 即時追蹤。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- FunctionName

類型：字串

描述：（必要）要啟用追蹤的 Lambda 函數名稱或 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

文件步驟

- `aws:executeAwsApi` - 在 `FunctionName` 參數中指定的 Lambda 函數上啟用 X-Ray 追蹤。
- `aws:assertAwsResourceProperty` - 驗證已在 Lambda 函數上啟用 X-Ray 追蹤。

輸出

`UpdateLambdaConfig.UpdateFunctionConfigurationResponse` - 來自 `UpdateFunctionConfiguration` API 呼叫的回應。

AWSConfigRemediation-DeleteLambdaFunction

Description

AWSConfigRemediation-DeleteLambdaFunction Runbook 會刪除您指定的 AWS Lambda 函數。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- LambdaFunctionName

類型：字串

描述：(必要) 您要刪除的 Lambda 函數名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:DeleteFunction
- lambda:GetFunction

文件步驟

- aws:executeAwsApi - 刪除 LambdaFunctionName 參數中指定的 Lambda 函數。
- aws:executeScript - 驗證 Lambda 函數已刪除。

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Description

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK Runbook 會靜態加密您使用 AWS Lambda () 客戶受管金鑰所指定 AWS Key Management Service (Lambda AWS KMS) 函數的環境變數。此 Runbook 應僅用作基準，以確保您 Lambda 函數的環境變數根據最低建議的安全最佳實務進行加密。我們建議使用不同的客戶受管金鑰加密多個函數。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- FunctionName

類型：字串

描述：（必要）您要加密其環境變數的 Lambda 函數名稱或 ARN。

- KMSKeyArn

類型：字串

描述：（必要）您要用來加密 Lambda 函數環境變數 AWS KMS 的客戶受管金鑰 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文件步驟

- `aws:waitForAwsResourceProperty` - 等待 `LastUpdateStatus` 屬性為 `Successful`。
- `aws:executeAwsApi` - 使用您在 `FunctionName` 參數中指定的 AWS KMS 客戶受管金鑰，加密您在 `KMSKeyArn` 參數中指定的 Lambda 函數的環境變數。
- `aws:assertAwsResourceProperty` - 確認您的 Lambda 函數的環境變數已啟用加密。

AWSConfigRemediation-MoveLambdaToVPC

Description

AWSConfigRemediation-MoveLambdaToVPC Runbook 會將 AWS Lambda (Lambda) 函數移至 Amazon Virtual Private Cloud (Amazon VPC)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `FunctionName`

類型：字串

描述：（必要）要移至 Amazon VPC 的 Lambda 函數名稱。

- SecurityGroupIds

類型：字串

描述：(必要) 您要指派給與 Lambda 函數相關聯的彈性網路介面 (ENIs) 的安全群組 IDs。

- SubnetIds

類型：字串

描述：(必要) 您要建立與 Lambda 函數相關聯之彈性網路介面 (ENIs)子網路 IDs。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunction
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文件步驟

- aws:executeAwsApi - 更新您在 FunctionName 參數中指定的 Lambda 函數的 Amazon VPC 組態。
- aws:waitForAwsResourceProperty - 等待 Lambda 函數LastUpdateStatus成為 successful 。
- aws:executeScript - 驗證 Lambda 函數 Amazon VPC 組態已成功更新。

AWSSupport-RemediateLambdaS3Event

Description

AWSSupport-TroubleshootLambdaS3Event 執行手冊為 AWS 知識中心文章中概述的程序提供自動化解決方案。[為什麼我的 Amazon S3 事件通知不會觸發我的 Lambda 函數？](#) 以及 [為什麼我在建立 Amazon S3 事件通知以觸發我的 Lambda 函數時收到錯誤「無法驗證下列目的地組態」？](#) 此 Runbook 可協助您識別並修復 Amazon Simple Storage Service (Amazon S3) 事件通知為何無法觸發

您指定的 AWS Lambda 函數。如果 Runbook 輸出建議驗證和設定 Lambda 函數並行，請參閱[非同步調用](#)和[AWS Lambda 函數擴展](#)。

 Note

「無法驗證下列目的地組態」錯誤也可能因為不正確的 Amazon Simple Notification Service (Amazon SNS) 和 Amazon Simple Queue Service (Amazon SQS) Amazon S3 事件組態而發生。此 Runbook 只會檢查 Lambda 函數組態。如果使用 Runbook 後，您仍然收到「無法驗證下列目的地組態」錯誤，請檢閱任何現有的 Amazon SNS 和 Amazon SQS Amazon S3 事件組態。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LambdaFunctionArn

類型：字串

描述：（必要）Lambda 函數的 ARN。

- S3BucketName

類型：字串

描述：(必要) 事件通知觸發 Lambda 函數的 Amazon S3 儲存貯體名稱。

- 動作

類型：字串

有效值：故障診斷 | 修復

描述：(必要) 您希望 Runbook 執行的動作。Troubleshoot 選項有助於識別任何問題，但不執行任何變動動作來解決問題。Remediate 選項有助於識別和嘗試為您解決問題。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

文件步驟

- `aws:branch` - 根據為 Action 參數指定的輸入進行分支。

如果指定的值為 Troubleshoot：

- `aws:executeAutomation` - 執行 `AWSSupport-TroubleshootLambdaS3Event` Runbook。
- `aws:executeAwsApi` - 檢查在上一個步驟中執行的 `AWSSupport-TroubleshootLambdaS3Event` Runbook 輸出。

如果指定的值為 Remediate：

- `aws:executeScript` - 執行指令碼以修復[為什麼我的 Amazon S3 事件通知不會觸發我的 Lambda 函數中概述的問題？](#)以及[為什麼我在建立 Amazon S3 事件通知以觸發我的 Lambda 函數時收到錯誤「無法驗證下列目的地組態」？](#) 知識中心文章。

輸出

`checkoutput.Output`

`remediatelambdas3event.Output`

AWSSupport-TroubleshootLambdaInternetAccess

Description

AWSSupport-TroubleshootLambdaInternetAccess Runbook 可協助您疑難排解在 Amazon Virtual Private Cloud (Amazon VPC) 中啟動之 AWS Lambda 函數的網際網路存取問題。會檢閱子網路路由、安全群組規則和網路存取控制清單 (ACL) 規則等資源，以確認允許傳出網際網路存取。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `FunctionName`

類型：字串

描述：(必要) 您要疑難排解網際網路存取的 Lambda 函數名稱。

- destinationIp

類型：字串

描述：(必要) 您要建立傳出連線的目的地 IP 地址。

- destinationPort

類型：字串

預設：443

描述：(選用) 您要建立傳出連線的目的地連接埠。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- lambda:GetFunction
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls

文件步驟

- aws:executeScript - 驗證啟動 Lambda 函數之 VPC 中各種資源的組態。
- aws:branch - 根據指定的 Lambda 函數是否在 VPC 中進行分支。
- aws:executeScript - 檢閱啟動 Lambda 函數之子網路的路由表路由，並驗證網路位址轉譯 (NAT) 閘道和網際網路閘道的路由是否存在。確認 Lambda 函數不在公有子網路中。
- aws:executeScript - 驗證與 Lambda 函數相關聯的安全群組，允許根據 destinationIp 和 destinationPort 參數指定的值進行傳出網際網路存取。
- aws:executeScript - 驗證與 Lambda 函數子網路相關聯的 ACL 規則，且 NAT 閘道允許根據 destinationIp 和 destinationPort 參數指定的值進行傳出網際網路存取。

輸出

checkVpc.vpc - 啟動 Lambda 函數的 VPC ID。

checkVpc.subnet - 啟動 Lambda 函數的子網路 IDs。

checkVpc.securityGroups - 與 Lambda 函數相關聯的安全群組。

checkNACL.NACL - 具有資源名稱的分析訊息。LambdaIp是指 Lambda 函數彈性網路界面的私有 IP 地址。LambdaIpRules 物件只會針對具有 NAT 閘道路由的子網路產生。下列內容是輸出的範例。

```
{
  "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"
  }
}
```

checkSecurityGroups.secgrps - 分析與您的 Lambda 函數相關聯的安全群組。下列內容是輸出的範例。

```
{
  "sg-123456789":{
    "Status":"Allowed",
```

```

    "Analysis": "This security group has allowed destination IP and port in its
outbuond rule."
  }
}

```

checkSubnet.subnets - 分析與 Lambda 函數相關聯的 VPC 中的子網路。下列內容是輸出的範例。

```

{
  "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

Description

AWSsupport-TroubleshootLambdaS3Event 執行手冊為 AWS 知識中心文章中概述的程序提供自動化解決方案。[為什麼我的 Amazon S3 事件通知不會觸發我的 Lambda 函數？](#) 以及 [為什麼我在建立 Amazon S3 事件通知以觸發我的 Lambda 函數時收到錯誤「無法驗證下列目的地組態」？](#) 此 Runbook 可協助您識別 Amazon Simple Storage Service (Amazon S3) 事件通知為何無法觸發您指定的 AWS Lambda 函數。如果 Runbook 輸出建議驗證和設定 Lambda 函數並行，請參閱[非同步調用](#)和[AWS Lambda 函數擴展](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LambdaFunctionArn

類型：字串

描述：(必要) Amazon S3 事件通知觸發的 Lambda 函數 ARN。

- S3BucketName

類型：字串

描述：(必要) 事件通知觸發 Lambda 函數的 Amazon S3 儲存貯體名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- lambda:GetPolicy
- s3:GetBucketNotification

文件步驟

- aws:executeScript - 執行指令碼以驗證 Amazon S3 事件通知的組態設定。驗證 Lambda 函數的資源型 IAM 政策，並產生 AWS Command Line Interface (AWS CLI) 命令，以在政策缺少所需的許可時新增所需的許可。驗證屬於相同 S3 儲存貯體事件通知一部分的其他 Lambda 函數資源政策，並在缺少必要許可時產生 AWS CLI 命令做為輸出。

輸出

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager 自動化為 Amazon Managed Workflows for Apache Airflow 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSsupport-TroubleshootMWAAEnvironmentCreation](#)

AWSsupport-TroubleshootMWAAEnvironmentCreation

Description

AWSsupport-TroubleshootMWAAEnvironmentCreation Runbook 提供偵錯 Amazon Managed Workflows for Apache Airflow (Amazon MWAA) 環境建立問題的資訊，並盡最大努力執行檢查以及記錄的原因，以協助識別故障。

如何運作？

Runbook 會執行下列步驟：

- 擷取 Amazon MWAA 環境的詳細資訊。
- 驗證執行角色許可。
- 檢查環境是否具有使用所提供 AWS KMS 金鑰進行記錄的許可，以及是否存在所需的 CloudWatch 日誌群組。
- 剖析所提供日誌群組中的日誌，以找出任何錯誤。
- 檢查網路組態，以驗證 Amazon MWAA 環境是否可以存取所需的端點。
- 產生包含調查結果的報告。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-TroubleshootMWAAEnvironmentCreation](#) 中導覽至。
2. 選擇 **Execute automation** (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - `AutomationAssumeRole` (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `EnvironmentName` (必要)：

您要評估的 Amazon MWAA 環境名稱。

Input parameters

AutomationAssumeRole	EnvironmentName
(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.	(Required) Name of the MWAA environment you wish to evaluate.
	String

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- **GetMWAAEnvironmentDetails:**

擷取 Amazon MWAA 環境的詳細資訊。如果此步驟失敗，自動化程序將停止並顯示為 **Failed**。

- **CheckIAMPermissionsOnExecutionRole:**

驗證執行角色是否具有 Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch 和 Amazon SQS 資源所需的許可。如果偵測到客戶受管 AWS Key Management Service (AWS KMS) 金鑰，自動化會驗證金鑰的必要許可。此步驟使用 `iam:SimulateCustomPolicy` API 來確定自動化執行角色是否符合所有必要的許可。

- **CheckKMSPolicyOnKMSKey:**

檢查 AWS KMS 金鑰政策是否允許 Amazon MWAA 環境使用金鑰來加密 CloudWatch Logs。如果已 AWS 管理 AWS KMS 金鑰，自動化會略過此檢查。

- **CheckIfRequiredLogGroupsExists:**

檢查是否存在 Amazon MWAA 環境所需的 CloudWatch 日誌群組。如果沒有，自動化會檢查 CloudTrail 是否有 CreateLogGroup 和 DeleteLogGroup 事件。此步驟也會檢查 CreateLogGroup 事件。

- **BranchOnLogGroupsFindings:**

根據與 Amazon MWAA 環境相關的 CloudWatch 日誌群組存在的分支。如果至少有一個日誌群組存在，自動化會剖析它以尋找錯誤。如果沒有日誌群組，自動化會略過下一個步驟。

- **CheckForErrorsInLogGroups:**

剖析 CloudWatch 日誌群組以找出錯誤。

- **GetRequiredEndpointsDetails:**

擷取 Amazon MWAA 環境使用的服務端點。

- **CheckNetworkConfiguration:**

驗證 Amazon MWAA 環境的網路組態是否符合要求，包括檢查安全群組、網路 ACLs、子網路和路由表組態。

- **CheckEndpointsConnectivity:**

調用 AWS Support-Connectivity Troubleshooter 子自動化，以驗證 Amazon MWAA 與所需端點的連線。

- **CheckS3BlockPublicAccess:**

檢查 Amazon MWAA 環境的 Amazon S3 儲存貯體是否 Block Public Access 已啟用，並檢閱帳戶的整體 Amazon S3 Block Public Access 設定。

- **GenerateReport:**

從自動化收集資訊，並列印每個步驟的結果或輸出。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- 檢查 Amazon MWAA 環境執行角色許可：

驗證執行角色是否具有 Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch 和 Amazon SQS 資源的必要許可。如果偵測到客戶受管 AWS KMS 金鑰，自動化會驗證金鑰的必要許可。

- 檢查 Amazon MWAA 環境 AWS KMS 金鑰政策：

驗證執行角色是否擁有 Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch 和 Amazon SQS 資源的必要許可。此外，如果偵測到客戶受管 AWS KMS 金鑰，自動化會檢查金鑰的必要許可。

- 檢查 Amazon MWAA 環境 CloudWatch 日誌群組：

檢查是否存在 Amazon MWAA 環境所需的 CloudWatch Log Groups。如果沒有，自動化接著會檢查 CloudTrail 以尋找 CreateLogGroup 和 DeleteLogGroup 事件。

- 檢查 Amazon MWAA 環境路由表：

檢查 Amazon MWAA 環境中的 Amazon VPC 路由表是否已正確設定。

- 檢查 Amazon MWAA 環境安全群組：

檢查 Amazon MWAA 環境 Amazon VPC 安全群組是否已正確設定。

- 檢查 Amazon MWAA 環境網路 ACLs：

檢查 Amazon MWAA 環境中的 Amazon VPC 安全群組是否已正確設定。

- 檢查 Amazon MWAA 環境子網路：

驗證 Amazon MWAA 環境的子網路是否為私有。

- 檢查 Amazon MWAA 環境所需的端點連線：

驗證 Amazon MWAA 環境是否可以存取所需的端點。為此，自動化會叫用 AWS Support-ConnectivityTroubleshooter 自動化。

- 檢查 Amazon MWAA 環境 Amazon S3 儲存貯體：

檢查 Amazon MWAA 環境的 Amazon S3 儲存貯體是否 Block Public Access 已啟用，並檢閱帳戶的 Amazon S3 Block Public Access 設定。

- 檢查 Amazon MWAA 環境 CloudWatch 日誌群組錯誤：

剖析 Amazon MWAA 環境的現有 CloudWatch 日誌群組以找出錯誤。

▼ 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 [REDACTED] is 5. This suggests that all log groups were created successfully ✓

🔗 Checking the MWAA environment Route Tables
NAT GW [REDACTED] has Internet route: subnet-[REDACTED] > nat-[REDACTED] -> igw-[REDACTED] ✓
NAT GW [REDACTED] has Internet route: subnet-[REDACTED] > nat-[REDACTED] -> igw-[REDACTED] ✓

🔗 Checking the MWAA environment Security Groups
Security group [REDACTED] has self-referencing rules for all traffic. ✓

🔗 Checking the MWAA environment Network ACLs
NACL [REDACTED] allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔗 Checking the MWAA environment Subnets
Subnet: subnet-[REDACTED] is private ✓
Subnet: subnet-[REDACTED] is private ✓

🔗 Checking the MWAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?region=eu-west-1

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] 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/[REDACTED]?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 [REDACTED] DAGProcessing - no errors found ✓
Parsed log group [REDACTED] Scheduler - no errors found ✓
Parsed log group [REDACTED] Task - no errors found ✓
Parsed log group [REDACTED] WebServer - no errors found ✓
Parsed log group [REDACTED] Worker - no errors found ✓

```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

Neptune

AWS Systems Manager 自動化為 Amazon Neptune 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Description

AWS-EnableNeptuneDbAuditLogsToCloudWatch Runbook 可協助您將 Amazon Neptune 資料庫叢集的稽核日誌傳送至 Amazon CloudWatch Logs。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `DbClusterResourceId`

類型：字串

描述：（必要）您要為其啟用稽核日誌的 Neptune 資料庫叢集的資源 ID。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文件步驟

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - 傳回 Neptune 資料庫叢集的 ID。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - 驗證 Neptune 資料庫引擎類型為 `neptune`。
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`) - 允許傳送 Neptune 資料庫叢集的稽核日誌 CloudWatch Logs。
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - 驗證 Neptune 資料庫叢集狀態為 `available`。
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`) - 驗證稽核日誌已成功設定為傳送至 CloudWatch Logs。

AWS-EnableNeptuneDbBackupRetentionPeriod

Description

AWS-EnableNeptuneDbBackupRetentionPeriod Runbook 可協助您為 Amazon Neptune 資料庫叢集啟用備份保留期介於 7 到 35 天的自動備份。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DbClusterResourceId

類型：字串

描述：（必要）您要為其啟用備份的 Neptune 資料庫叢集的資源 ID。

- BackupRetentionPeriod

類型：整數

有效值：7-35

描述：（必要）備份保留的天數。

- PreferredBackupWindow

類型：字串

描述：（選用）進行備份時，每天至少 30 分鐘的時段。該值必須是國際標準時間座標 (UTC)，並使用格式：hh24:mm-hh24:mm。備份保留期不能與偏好的維護時段衝突。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文件步驟

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - 傳回 Neptune 資料庫叢集的 ID。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - 驗證 Neptune 資料庫引擎類型為 `neptune`。
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - 驗證 Neptune 資料庫叢集狀態為 `available`。
- `ModifyNeptuneDbRetentionPeriod` (`aws:executeAwsApi`) - 設定 Neptune 資料庫叢集的保留期間。
- `VerifyNeptuneDbBackupsEnabled` (`aws:executeScript`) - 驗證保留期間和備份時段已成功設定。

AWS-EnableNeptuneClusterDeletionProtection

Description

AWS-EnableNeptuneClusterDeletionProtection Runbook 會為您指定的 Amazon Neptune 叢集啟用刪除保護。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DbClusterResourceId

類型：字串

描述：(必要) 您要啟用刪除保護的 Neptune 叢集 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文件步驟

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - 傳回 Neptune 資料庫叢集的 ID。
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - 驗證指定資料庫叢集的引擎類型為 neptune。
- VerifyNeptuneStatus (aws:waitForAwsResourceProperty) - 驗證叢集的狀態為 available。
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi) - 在 Neptune 資料庫叢集上啟用刪除保護。

- `VerifyNeptuneDbDeletionProtection (aws:assertAwsResourceProperty)` - 驗證資料庫叢集上已啟用刪除保護。

輸出

- `EnableNeptuneDbDeletionProtection.EnableNeptuneDbDeletionProtectionResponse` - API 操作的輸出。

Amazon RDS

AWS Systems Manager 自動化為 Amazon Relational Database Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-CreateEncryptedRdsSnapshot](#)
- [AWS-CreateRdsSnapshot](#)
- [AWSConfigRemediation-DeleteRDSCluster](#)
- [AWSConfigRemediation-DeleteRDSClusterSnapshot](#)
- [AWSConfigRemediation-DeleteRDSInstance](#)
- [AWSConfigRemediation-DeleteRDSInstanceSnapshot](#)
- [AWSConfigRemediation-DisablePublicAccessToRDSInstance](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance](#)
- [AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS](#)
- [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

Description

AWS-CreateEncryptedRdsSnapshot Runbook 會從未加密的 Amazon Relational Database Service (Amazon RDS) 執行個體建立加密快照。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DBInstanceIdentifier

類型：字串

描述：(必要) 您要建立快照的 Amazon RDS 執行個體 ID。

- DBSnapshotIdentifier

類型：字串

描述：(選用) Amazon RDS 快照的名稱範本。預設名稱範本為 *DBInstanceIdentifier-yyyymmddhhmmss*。

- EncryptedDBSnapshotIdentifier

類型：字串

描述：(選用) 加密快照的名稱。預設名稱是您為附加的 DBSnapshotIdentifier 參數指定的值-encrypted。

- InstanceTags

類型：字串

描述：(選用) 要新增至資料庫執行個體的標籤。(範例：Key=tagKey1，Value=tagValue1；Key=tagKey2，Value=tagValue2)'

- KmsKeyId

類型：字串

預設：alias/aws/rds

描述：(選用) 您要用來加密快照之客戶受管金鑰的 ARN、金鑰 ID 或金鑰別名。

- SnapshotTags

類型：字串

描述：(選用) 要新增至快照的標籤。(範例：Key=tagKey1，Value=tagValue1；Key=tagKey2，Value=tagValue2)'

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- rds:AddTagsToResource
- rds:CopyDBSnapshot
- rds:CreateDBSnapshot
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

文件步驟

- aws:executeScript - 建立您在 DBInstanceIdentifier 參數中指定的資料庫執行個體快照。
- aws:executeScript - 驗證在上一個步驟中建立的快照是否存在，且為 available。
- aws:executeScript - 將先前建立的快照複製到加密的快照。
- aws:executeScript - 驗證上一個步驟中建立的加密快照是否存在。

輸出

CopyRdsSnapshotToEncryptedRdsSnapshot.EncryptedSnapshotId - 加密 Amazon RDS 快照的 ID。

AWS-CreateRdsSnapshot

Description

為 Amazon RDS 執行個體建立 Amazon Relational Database Service (Amazon RDS) 快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DBInstanceIdentifier

類型：字串

描述：(必要) 要從中建立快照的 RDS 執行個體的 DBInstanceID ID。

- DBSnapshotIdentifier

類型：字串

描述：(選用) 要建立的 RDS 快照集 DBSnapshotIdentifier ID。

- InstanceTags

類型：字串

描述：(選用) 要為執行個體建立的標籤。

- SnapshotTags

類型：字串

描述：(選用) 要為快照建立的標籤。

文件步驟

createRDSSnapshot – 建立 RDS 快照並傳回快照 ID。

verifyRDSSnapshot – 檢查上一個步驟中建立的快照是否存在。

輸出

createRDSSnapshot.SnapshotId – 已建立快照的 ID。

AWSConfigRemediation-DeleteRDSCluster

Description

AWSConfigRemediation-DeleteRDSCluster Runbook 會刪除您指定的 Amazon Relational Database Service (Amazon RDS) 叢集。AWS Config 必須在您執行此自動化的 AWS 區域 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DBClusterId

類型：字串

描述：（必要）您要啟用刪除保護之資料庫叢集的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds>DeleteDBInstance`
- `rds:DescribeDBClusters`

文件步驟

- `aws:executeScript` - 刪除您在 `DBClusterId` 參數中指定的資料庫叢集。

AWSConfigRemediation-DeleteRDSClusterSnapshot

Description

AWSConfigRemediation-DeleteRDSClusterSnapshot Runbook 會刪除指定的 Amazon Relational Database Service (Amazon RDS) 叢集快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `DBClusterSnapshotId`

類型：字串

描述：(必要) 要刪除的 Amazon RDS 叢集快照識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

文件步驟

- `aws:branch` - 檢查叢集快照是否處於 `available` 狀態。如果無法使用，流程會結束。
- `aws:executeAwsApi` - 使用資料庫 (DB) 叢集快照識別符刪除指定的 Amazon RDS 叢集快照。
- `aws:executeScript` - 確認已刪除指定的 Amazon RDS 叢集快照。

AWSConfigRemediation-DeleteRDSInstance

Description

AWSConfigRemediation-DeleteRDSInstance Runbook 會刪除您指定的 Amazon Relational Database Service (Amazon RDS) 執行個體。當您刪除資料庫 (DB) 執行個體時，該執行個體的所有自動備份都會遭到刪除，而且無法復原。手動資料庫快照不會刪除。如果您要刪除的資料庫執行個體處於 `failed`、`incompatible-network` 或 `incompatible-restore` 狀態，您必須將 `SkipFinalSnapshot` 參數設定為 `true`。

Note

如果您想要刪除的資料庫執行個體位於 Amazon Aurora 資料庫叢集中，如果資料庫執行個體是僅供讀取複本和資料庫叢集中唯一的執行個體，則 Runbook 不會刪除資料庫執行個體。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- DbiResourceId

類型：字串

描述：（必要）您要刪除之資料庫執行個體的資源識別符。

- SkipFinalSnapshot

類型：布林值

預設：false

描述：（選用）如果設定為 true，則在刪除資料庫執行個體之前不會建立最終快照。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBInstance

- `rds:DescribeDBInstances`

文件步驟

- `aws:executeAwsApi` - 從您在 `DbiResourceId` 參數中指定的值收集資料庫執行個體名稱。
- `aws:branch` - 根據您在 `SkipFinalSnapshot` 參數中指定的值進行分支。
- `aws:executeAwsApi` - 刪除您在 `DbiResourceId` 參數中指定的資料庫執行個體。
- `aws:executeAwsApi` - 建立最終快照後，刪除您在 `DbiResourceId` 參數中指定的資料庫執行個體。
- `aws:assertAwsResourceProperty` - 驗證資料庫執行個體已刪除。

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Description

AWSConfigRemediation-DeleteRDSInstanceSnapshot Runbook 會刪除您指定的 Amazon Relational Database Service (Amazon RDS) 執行個體快照。只會刪除 `available` 處於 狀態的快照。此 Runbook 不支援從 Amazon Aurora 資料庫執行個體刪除快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- DbSnapshotId

類型：字串

描述：(必要) 您要刪除的快照 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

文件步驟

- aws:executeAwsApi - 收集 DbSnapshotId 參數中指定的快照狀態。
- aws:assertAwsResourceProperty - 確認快照的狀態為 available 。
- aws:executeAwsApi - 刪除 DbSnapshotId 參數中指定的快照。
- aws:executeScript - 驗證已刪除快照。

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Description

AWSConfigRemediation-DisablePublicAccessToRDSInstance Runbook 會停用您指定之 Amazon Relational Database Service (Amazon RDS) 資料庫 (DB) 執行個體的公有可存取性。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- DbiResourceId

類型：字串

描述：（必要）您要停用公開可存取性之資料庫執行個體的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文件步驟

- aws:executeAwsApi - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- aws:assertAwsResourceProperty - 驗證資料庫執行個體處於 AVAILABLE 狀態。
- aws:executeAwsApi - 停用資料庫執行個體上的公有可存取性。
- aws:waitForAwsResourceProperty - 等待資料庫執行個體變更為 MODIFYING 狀態。
- aws:waitForAwsResourceProperty - 等待資料庫執行個體變更為 AVAILABLE 狀態。

- `aws:assertAwsResourceProperty` - 確認已停用資料庫執行個體上的公有可存取性。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Description

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster Runbook 會在您指定的 Amazon Relational Database Service (Amazon RDS) 叢集上啟用 CopyTagsToSnapshot 設定。啟用此設定會將資料庫叢集的所有標籤複製到資料庫叢集的快照。預設為不複製它們。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- 立即套用

類型：布林值

預設：false

描述：（選用）如果您 `true` 為此參數指定，無論資料庫叢集 PreferredMaintenanceWindow 的設定為何，都會盡快以非同步方式套用此請求中的修改和任何待定修改。

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `DbClusterResourceId`

類型：字串

描述：(必要) 您要啟用CopyTagsToSnapshot設定之資料庫叢集的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文件步驟

- `aws:executeAwsApi` - 從資料庫叢集資源識別符收集資料庫叢集識別符。
- `aws:assertAwsResourceProperty` - 確認資料庫叢集處於 AVAILABLE 狀態。
- `aws:executeAwsApi` - 在資料庫叢集上啟用 CopyTagsToSnapshot設定。
- `aws:assertAwsResourceProperty` - 確認已在資料庫叢集上啟用CopyTagsToSnapshot設定。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Description

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance Runbook 會在您指定的 Amazon Relational Database Service (Amazon RDS) 執行個體上啟用 CopyTagsToSnapshot設定。啟用此設定會將資料庫執行個體的所有標籤複製到資料庫執行個體的快照。預設為不複製它們。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- 立即套用

類型：布林值

預設：false

描述：(選用) 如果您true為此參數指定，無論資料庫執行個體PreferredMaintenanceWindow的設定為何，都會盡快以非同步方式套用此請求中的修改和任何待定修改。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- DbiResourceId

類型：字串

描述：(必要) 您要啟用CopyTagsToSnapshot設定之資料庫執行個體的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文件步驟

- `aws:executeAwsApi` - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- `aws:assertAwsResourceProperty` - 確認資料庫執行個體處於 AVAILABLE 狀態。
- `aws:executeAwsApi` - 在資料庫執行個體上啟用 CopyTagsToSnapshot 設定。
- `aws:assertAwsResourceProperty` - 確認已在資料庫執行個體上啟用 CopyTagsToSnapshot 設定。

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Description

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance Runbook 會在您指定的 Amazon RDS 資料庫執行個體上啟用增強型監控。如需增強型監控的資訊，請參閱《Amazon RDS 使用者指南》中的 [增強型監控](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `MonitoringInterval`

類型：整數

有效值：1 | 5 | 10 | 15 | 30 | 60

描述：(必要) 從資料庫執行個體收集增強型監控指標的間隔，以秒為單位。

- `MonitoringRoleArn`

類型：字串

描述：(必要) 允許 Amazon RDS 將增強型監控指標傳送至 Amazon CloudWatch Logs 的 IAM 角色的 Amazon Resource Name (ARN)。

- `ResourceId`

類型：字串

描述：(必要) 您要啟用增強型監控之資料庫執行個體的資源識別符。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文件步驟

- `aws:executeAwsApi` - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- `aws:assertAwsResourceProperty` - 確認資料庫執行個體處於 AVAILABLE 狀態。
- `aws:executeAwsApi` - 在您的資料庫執行個體上啟用增強型監控。
- `aws:executeScript` - 確認已在資料庫執行個體上啟用增強型監控。

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Description

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS Runbook 會在您指定的 Amazon RDS 資料庫執行個體上啟用 AutoMinorVersionUpgrade 設定。啟用此設定表示次要版本升級會在維護時段期間自動套用至資料庫執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- DbiResourceId

類型：字串

描述：（必要）您要 AutoMinorVersionUpgrade 設定之資料庫執行個體的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文件步驟

- `aws:executeAwsApi` - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- `aws:assertAwsResourceProperty` - 確認資料庫執行個體處於 AVAILABLE 狀態。
- `aws:executeAwsApi` - 在資料庫執行個體上啟用 `AutoMinorVersionUpgrade` 設定。
- `aws:executeScript` - 確認已在資料庫執行個體上啟用 `AutoMinorVersionUpgrade` 設定。

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Description

AWSConfigRemediation-EnableMultiAZOnRDSInstance Runbook 會將您的 Amazon Relational Database Service (Amazon RDS) 資料庫 (DB) 執行個體變更為異地同步備份部署。變更此設定不會導致中斷。除非您將 `ApplyImmediately` 參數設定為 `true`，否則變更會在下一個維護時段套用 `true`。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- 立即套用

類型：布林值

預設：false

描述：(選用) 如果您true為此參數指定，無論資料庫執行個體PreferredMaintenanceWindow的設定為何，都會盡快以非同步方式套用此請求中的修改和任何待定修改。

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DbiResourceId

類型：字串

描述：(必要) 資料庫執行個體的唯一不 AWS 區域可變識別符，以啟用 MultiAZ設定。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- rds:DescribeDBInstances
- rds:ModifyDBInstance
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文件步驟

- aws:executeAwsApi - 使用 DBInstanceId 參數中提供的值擷取資料庫執行個體名稱。
- aws:executeAwsApi - 驗證 DBInstanceStatus為 available。
- aws:branch - 檢查是否已在您在 DbiResourceId 參數中指定的資料庫執行個體true上MultiAZ將設定為。
- aws:executeAwsApi - 在您於 DbiResourceId 參數中指定的資料庫執行個體true上，將 MultiAZ 設定變更為。
- aws:assertAwsResourceProperty - 確認您在 DbiResourceId 參數中指定的資料庫執行個體true上，MultiAZ設定為。

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Description

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance Runbook 會在您指定的 Amazon RDS 資料庫執行個體上啟用績效詳情。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DbiResourceId

類型：字串

描述：（必要）您要啟用績效詳情之資料庫執行個體的資源識別符。

- PerformanceInsightsKMSKeyId

類型：字串

預設：alias/aws/rds

描述：（選用）您希望 Performance Insights 用來加密所有潛在敏感資料的 Amazon Resource Name (ARN)、金鑰 ID 或 AWS Key Management Service (AWS KMS) 客戶受管金鑰的金鑰別名。

如果您輸入此參數的金鑰別名，請在值前面加上 **alias/**。如果您未指定此參數的值，AWS 受管金鑰 則會使用。

- PerformanceInsightsRetentionPeriod

類型：整數

有效值：7，731

預設：7

描述：（選用）您想要保留績效詳情資料的天數。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CreateGrant
- kms:DescribeKey
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文件步驟

- aws:executeAwsApi - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- aws:assertAwsResourceProperty - 確認資料庫執行個體狀態為 available。
- aws:executeAwsApi - 收集 PerformanceInsightsKMSKeyId 參數中指定之 AWS KMS 客戶受管金鑰的 ARN。
- aws:branch - 檢查是否已將值指派給資料庫執行個體的 PerformanceInsightsKMSKeyId 屬性。
- aws:executeAwsApi - 在您於 DbInstanceResourceId 參數中指定的資料庫執行個體上啟用績效詳情。
- aws:assertAwsResourceProperty - 確認為 PerformanceInsightsKMSKeyId 參數指定的值已用於在資料庫執行個體上啟用 Performance Insights 的加密。
- aws:assertAwsResourceProperty - 確認已在資料庫執行個體上啟用績效詳情。

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Description

AWSConfigRemediation-EnableRDSClusterDeletionProtection Runbook 會在您指定的 Amazon Relational Database Service (Amazon RDS) 叢集上啟用刪除保護。AWS Config 必須在您執行此自動化 AWS 區域 的 中啟用。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterId

類型：字串

描述：（必要）您要啟用刪除保護之資料庫叢集的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文件步驟

- `aws:executeAwsApi` - 從資料庫叢集資源識別符收集資料庫叢集名稱。
- `aws:assertAwsResourceProperty` - 驗證資料庫叢集狀態為 `available`。
- `aws:executeAwsApi` - 對您在 `ClusterId` 參數中指定的資料庫叢集啟用刪除保護。
- `aws:assertAwsResourceProperty` - 驗證資料庫叢集上已啟用刪除保護。

AWSConfigRemediation-EnableRDSInstanceBackup

Description

AWSConfigRemediation-EnableRDSInstanceBackup Runbook 會為您指定的 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體啟用備份。此 Runbook 不支援啟用 Amazon Aurora 資料庫執行個體的備份。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- 立即套用

類型：布林值

預設：false

描述：(選用) 如果您 `true` 為此參數指定，無論資料庫執行個體 PreferredMaintenanceWindow 的設定為何，都會盡快以非同步方式套用此請求中的修改和任何待定修改。

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- BackupRetentionPeriod

類型：整數

有效值：1-35

描述：(必要) 備份保留的天數。

- DbiResourceId

類型：字串

描述：(必要) 您要為其啟用備份之資料庫執行個體的資源識別符。

- PreferredBackupWindow

類型：字串

描述：(選用) 建立備份的每日時間範圍 (UTC)。

約束：

- 必須為 格式 hh24:mi-hh24:mi
- 必須為國際標準時間 (UTC)
- 不得和慣用的維護時段衝突
- 必須至少 30 分鐘

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文件步驟

- `aws:executeScript` - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。啟用資料庫執行個體的備份。確認已在資料庫執行個體上啟用備份。

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Description

AWSConfigRemediation-EnableRDSInstanceDeletionProtection Runbook 會在您指定的 Amazon RDS 資料庫執行個體上啟用刪除保護。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- 立即套用

類型：布林值

預設：false

描述：（選用）如果您true為此參數指定，無論資料庫執行個體PreferredMaintenanceWindow的設定為何，都會盡快以非同步方式套用此請求中的修改和任何待定修改。

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DbInstanceResourceId

類型：字串

描述：(必要) 您要啟用刪除保護之資料庫執行個體的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文件步驟

- aws:executeAwsApi - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- aws:executeAwsApi - 在資料庫執行個體上啟用刪除保護。
- aws:assertAwsResourceProperty - 確認已在資料庫執行個體上啟用刪除保護。

AWSConfigRemediation-ModifyRDSInstancePortNumber

Description

AWSConfigRemediation-ModifyRDSInstancePortNumber Runbook 會修改 Amazon Relational Database Service (Amazon RDS) 執行個體接受連線的連接埠號碼。執行此自動化將會重新啟動資料庫。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- PortNumber

類型：字串

描述：(選用) 您希望資料庫執行個體接受連線的連接埠號碼。

- RDSDBInstanceResourceId

類型：字串

描述：(必要) 您要修改其傳入連接埠號碼之資料庫執行個體的資源識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文件步驟

- `aws:executeAwsApi` - 從資料庫執行個體資源識別符收集資料庫執行個體識別符。
- `aws:assertAwsResourceProperty` - 確認資料庫執行個體處於 AVAILABLE 狀態。
- `aws:executeAwsApi` - 修改資料庫執行個體接受連線的傳入連接埠號碼。
- `aws:waitForAwsResourceProperty` - 等待資料庫執行個體處於 MODIFYING 狀態。
- `aws:waitForAwsResourceProperty` - 等待資料庫執行個體處於 AVAILABLE 狀態。

AWSsupport-ModifyRDSnapshotPermission

Description

AWSsupport-ModifyRDSnapshotPermission Runbook 可協助您修改多個 Amazon Relational Database Service (Amazon RDS) 快照的許可。使用此 Runbook，您可以建立快照 Public 或 Private，並與其他 共用 AWS 帳戶。使用此 Runbook 無法與其他帳戶共用使用預設 KMS 金鑰加密的快照。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- AccountIds

類型：StringList

預設：none

描述：（選用）您要與其共用快照的帳戶 IDs。如果您No輸入 參數的值，則需要此Private參數。

- AccountPermissionOperation

類型：字串

有效值：新增 | 移除

預設：none

描述：（選用）要執行的操作類型。

- 私有

類型：字串

有效值：是 | 否

描述：（必要）如果您想要與特定帳戶共用快照，請輸入 No 作為值。

- SnapshotIdentifiers

類型：StringList

描述：（必要）您要修改其許可的 Amazon RDS 快照名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBSnapshots
- rds:ModifyDBSnapshotAttribute

文件步驟

1. `aws:executeScript` - 驗證 `SnapshotIdentifiers` 參數中提供的快照 IDs。驗證 IDs 之後，指令碼會檢查加密快照，並在找到任何快照時輸出清單。
2. `aws:branch` - 根據您為 `Private` 參數輸入的值來配置自動化。
3. `aws:executeScript` - 修改指定快照的許可，以與指定的帳戶共用快照。
4. `aws:executeScript` - 修改快照的許可，將快照從 `變更為 Public Private`。

輸出

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Result`

`MakePrivate.Result`

`MakePrivate.Commands`

AWSPremiumSupport-PostgreSQLWorkloadReview

Description

AWSPremiumSupport-PostgreSQLWorkloadReview Runbook 會擷取 Amazon Relational Database Service (Amazon RDS) PostgreSQL 資料庫用量統計資料的多個快照。An 支援 [Proactive Services](#) 專家需要擷取的統計資料，才能執行操作審查。系統會使用一組自訂 SQL 和 shell 指令碼來收集統計資料。這些指令碼會下載到 中由此 Runbook 建立 AWS 帳戶 的臨時 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。Runbook 要求您使用包含使用者名稱和密碼金鑰/值對的 AWS Secrets Manager 秘密來提供登入資料。使用者名稱必須具有查詢標準 PostgreSQL 統計資料檢視和函數的許可。

此 Runbook 會自動 AWS 帳戶 使用 AWS CloudFormation 堆疊在 中建立下列 AWS 資源。您可以使用 AWS CloudFormation 主控台監控堆疊建立。

- 在 VPC 的私有子網路中啟動的虛擬私有雲端 (VPC) 和 Amazon EC2 執行個體，可使用 NAT 閘道選擇性連線至網際網路。
- 連接至暫時 Amazon EC2 執行個體的 AWS Identity and Access Management (IAM) 角色，具有擷取 Secrets Manager 秘密值的許可。此角色也提供許可，以將檔案上傳至您選擇的 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以及選擇性地上傳至 支援 案例。
- 允許資料庫執行個體與暫時 Amazon EC2 執行個體之間連線的 VPC 對等互連。
- Systems Manager、Secrets Manager 和連接到暫時 VPC 的 Amazon S3 VPC 端點。

- 具有已註冊任務的維護時段，可定期啟動和停止暫時 Amazon EC2 執行個體、執行資料收集指令碼，以及將檔案上傳至 Amazon S3 儲存貯體。維護時段也會建立 IAM 角色，提供執行已註冊任務的許可。

當 Runbook 完成時，會刪除用於建立必要 AWS 資源的 AWS CloudFormation 堆疊，並將報告上傳到您選擇的 Amazon S3 儲存貯體，以及選擇性的支援案例。

Note

根據預設，會保留暫時 Amazon EC2 執行個體的根 Amazon EBS 磁碟區。您可以將 `EbsVolumeDeleteOnTermination` 參數設定為 `true` 來覆寫此選項。

先決條件

- Enterprise Support 訂閱 此 Runbook 和 Proactive Services 工作負載診斷和檢閱需要 Enterprise Support 訂閱。使用此 Runbook 之前，請聯絡您的技術客戶經理 (TAM) 或專家 TAM (STAM) 以取得指示。如需詳細資訊，請參閱 [支援 Proactive Services](#)。
- 帳戶和 AWS 區域 配額 請確定您尚未達到在此執行手冊的帳戶和區域中可建立的 Amazon EC2 執行個體或 VPCs 數量上限。如果您需要請求提高限制，請參閱 [服務提高限制表單](#)。
- 資料庫組態
 1. 您在 `DatabaseName` 參數中指定的資料庫應設定 `pg_stat_statements` 延伸模組。如果您尚未在 `pg_stat_statements` 中設定 `shared_preload_libraries`，則必須編輯資料庫參數群組中的值，並套用變更。變更參數 `shared_preload_libraries` 需要重新啟動資料庫執行個體。如需詳細資訊，請參閱 [使用參數群組](#)。`pg_stat_statements` 將新增至 `shared_preload_libraries` 會新增一些效能額外負荷。不過，這對於追蹤個別陳述式的效能很有用。如需 `pg_stat_statements` 延伸模組的詳細資訊，請參閱 [PostgreSQL 文件](#)。如果您未設定 `pg_stat_statements` 延伸模組，或延伸模組不存在於用於統計資料收集的資料庫中，則陳述式層級分析將不會出現在操作審查中。
 2. 確定 `track_counts` 和 `track_activities` 參數未關閉。如果在資料庫參數群組中關閉這些參數，則無法使用有意義的統計資料。變更這些參數需要您重新啟動資料庫執行個體。如需詳細資訊，請參閱 [在 Amazon RDS for PostgreSQL 資料庫執行個體上使用參數](#)。
 3. 如果 `track_io_timing` 參數已關閉，則操作檢閱中不會包含 I/O 層級統計資料。變更 `track_io_timing` 需要重新啟動資料庫執行個體，而且會根據資料庫執行個體工作負載產生額外的效能額外負荷。儘管關鍵工作負載的效能額外負荷，但此參數仍提供有關每個查詢的 I/O 時間的有用資訊。

帳單和費用 此自動化執行期間，AWS 帳戶 將針對暫時 Amazon EC2 執行個體、相關聯的 Amazon EBS 磁碟區、NAT 閘道和傳輸的資料，向您收取相關費用。根據預設，此 Runbook 會建立 t3.micro Amazon Linux 2 執行個體來收集統計資料。Runbook 會在步驟之間啟動和停止執行個體，以降低成本。

資料安全和控管 此 Runbook 會透過查詢 [PostgreSQL 統計資料檢視和函數來收集統計資料](#)。請確定 SecretId 參數中提供的登入資料僅允許對統計資料檢視和函數的唯讀許可。在自動化過程中，集合指令碼會上傳到您的 Amazon S3 儲存貯體，並且可以位於 `s3://amzn-s3-demo-bucket/automation execution id/queries/`。

這些指令碼會收集 AWS 專家用來檢閱物件層級關鍵效能指標的資料。指令碼會收集資料表名稱、結構描述名稱和索引名稱等資訊。如果其中任何一種資訊包含敏感資訊，例如收入指標、使用者名稱、電子郵件地址或任何其他個人身分識別資訊，我們建議您停止此工作負載檢閱。請聯絡您的 AWS TAM 以討論工作負載檢閱的替代方法。

請確定您擁有必要的核准和許可，以共用此自動化所收集的統計資料和中繼資料 AWS。

安全考量 如果您將 UpdateRdsSecurityGroup 參數設定為 yes，則 Runbook 會更新與資料庫執行個體相關聯的安全群組，以允許來自暫時 Amazon EC2 執行個體私有 IP 地址的傳入流量。

如果您將 UpdateRdsRouteTable 參數設定為 yes，則 Runbook 會更新與資料庫執行個體正在執行之子網路相關聯的路由表，以允許透過 VPC 對等互連至暫時 Amazon EC2 執行個體的流量。

使用者建立 若要允許集合指令碼連線至 Amazon RDS 資料庫，您必須設定具有讀取統計資料檢視許可的使用者。然後，您必須將登入資料存放在 Secrets Manager 中。建議您為此自動化建立新的專用使用者。建立個別使用者可讓您稽核和追蹤此自動化執行的活動。

1. 建立新的使用者。

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. 請確定此使用者只能進行唯讀連線。

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. 設定使用者層級限制。

```
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;"
```

- 將 `pg_monitor` 許可授予新使用者，使其可以存取資料庫統計資料。(此 `pg_monitor` 角色是 `pg_read_all_settings`、`pg_read_all_stats` 和 `pg_stat_scan_table` 的成員。)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

此 Systems Manager Automation 新增至暫時 Amazon EC2 執行個體描述檔的許可。下列許可會新增至與暫時 Amazon EC2 執行個體相關聯的 IAM 角色。AmazonSSMManagedInstanceCore 受管政策也會與 IAM 角色建立關聯，以允許 Systems Manager 管理 Amazon EC2 執行個體。

```
{
  "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:region:account id:secret:secret id",
  "Effect": "Allow"
},
{
  "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:DescribeCases"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
]
}

```

此 Systems Manager Automation 新增至暫時維護時段的許可。下列許可會自動新增至與維護 Windows 任務相關聯的 IAM 角色。維護 Windows 任務會啟動、停止命令，並將命令傳送至暫時 Amazon EC2 執行個體。

```

{
  "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:region:account id:instance/temporary instance id",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
    ],
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ssm.amazonaws.com"
        }
    },
    "Action": "iam:PassRole",
    "Resource": "*",
    "Effect": "Allow"
}
]
```

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- DBInstanceIdentifier

類型：字串

描述：(必要) 資料庫執行個體的 ID。

- DatabaseName

類型：字串

描述：(必要) 資料庫執行個體上託管的資料庫名稱。

- SecretId

類型：字串

描述：(必要) 包含使用者名稱和密碼金鑰值對之 Secrets Manager 秘密的 ARN。AWS CloudFormation 堆疊會建立具有此 ARN GetSecretValue 操作許可的 IAM 政策。登入資料用於允許臨時執行個體收集資料庫統計資料。請聯絡您的 TAM 或 STAM 以討論最低必要許可。

- 確認

類型：字串

描述：(必要) **yes** 如果您確認此 Runbook 會在您的帳戶中建立臨時資源，以從資料庫執行個體收集統計資料，請輸入。我們建議您先聯絡您的 TAM 或 STAM，再執行此自動化。

- SupportCase

類型：字串

描述：(選用) TAM 或 STAM 提供的 支援 案例編號。如果提供，則 Runbook 會更新案例並連接收集的資料。此選項需要暫時 Amazon EC2 執行個體具備網際網路連線，才能存取 支援 API 端點。您必須將 AllowVpcInternetAccess 參數設定為 true。案例主旨必須包含片語 AWSPremiumSupport-PostgreSQLWorkloadReview。

- S3BucketName

類型：字串

描述：(必要) 帳戶中您要上傳自動化所收集的資料的 Amazon S3 儲存貯體名稱。確認儲存貯體政策不會將任何不必要的讀取或寫入許可授予不需要存取儲存貯體內容的主體。基於此自動化的目的，我們建議您建立新的暫時 Amazon S3 儲存貯體。Runbook 提供 `s3:PutObject` API 操作的許可給連接到暫時 Amazon EC2 執行個體的 IAM 角色。上傳的檔案將位於 `s3://bucket name/automation execution id`。

- InstanceType

類型：字串

描述：(選用) 將執行自訂 SQL 和 shell 指令碼的暫時 Amazon EC2 執行個體類型。

有效值：t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

預設：t3.micro

- VpcCidr

類型：字串

描述：(選用) 新 VPC CIDR 表示法中的 IP 地址範圍 (例如 172.31.0.0/16)。請確定您選取的 CIDR 不重疊或符合任何與資料庫執行個體連線的現有 VPC。您可以建立的最小 VPC 使用 /28 子網路遮罩，而最大的 VPC 使用 /16 子網路遮罩。

預設：172.31.0.0/16

- StackResourcesNamePrefix

類型：字串

描述：(選用) AWS CloudFormation 堆疊資源名稱字首和標籤。Runbook 會使用此字首建立 AWS CloudFormation 堆疊資源，做為套用至資源的名稱和標籤的一部分。標籤鍵/值對的結構為 `StackResourcesNamePrefix:{{automation:EXECUTION_ID}}`。

預設：AWSPostgreSQLWorkloadReview

- 排程

類型：字串

描述：(選用) 維護時段排程。指定維護時段執行任務的頻率。預設值為每個 1 hour。

有效值：15 分鐘 | 30 分鐘 | 1 小時 | 2 小時 | 4 小時 | 6 小時 | 12 小時 | 1 天 | 2 天 | 4 天

預設：1 小時

- 持續時間

類型：整數

描述：(選用) 您希望允許自動化執行的最長持續時間，以分鐘為單位。支援的持續時間上限為 8,640 分鐘 (6 天)。預設值為 4,320 分鐘 (3 天)。

有效值：30-8640

預設：4320

- UpdateRdsRouteTable

類型：字串

描述：(選用) 如果設定為 true，則 Runbook 會更新與資料庫執行個體執行所在子網路相關聯的路由表。新增 IPv4 路由，透過新建立的 VPC 對等互連，將流量路由到暫時 Amazon EC2 執行個體私有 IPV4 地址。

有效值：true | false

預設：false

- AllowVpcInternetAccess

類型：字串

描述：(選用) 如果設定為 true，則 Runbook 會建立 NAT 閘道，以提供暫時 Amazon EC2 執行個體的網際網路連線，以便與支援 API 端點通訊。您可以保留此參數，就像只希望 Runbook 將輸出上傳到 Amazon S3 儲存貯體 false 一樣。

有效值：true | false

預設：false

- UpdateRdsSecurityGroup

類型：字串

描述：(選用) 如果設定為 true，則 Runbook 會更新與資料庫執行個體相關聯的安全群組，以允許來自暫時執行個體私有 IP 地址的流量。

有效值：false | true

預設：false

- EbsVolumeDeleteOnTermination

類型：字串

描述：(選用) 如果設定為 true，則臨時 Amazon EC2 執行個體的根磁碟區會在 Runbook 完成並刪除 AWS CloudFormation 堆疊後刪除。

有效值：false | true

預設：false

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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:RemoveTagsFromResource`
- `ssm:SendCommand`
- `support:AddAttachmentsToSet`
- `support:AddCommunicationToCase`
- `support:DescribeCases`

文件步驟

1. `aws:assertAwsResourceProperty` - 確認資料庫執行個體處於 `available` 狀態。
2. `aws:executeAwsApi` - 收集資料庫執行個體的詳細資訊。
3. `aws:executeScript` - 檢查 中指定的 Amazon S3 儲存貯體是否 `S3BucketName` 允許匿名或公有讀取或寫入存取許可。
4. `aws:executeScript` - 從用來在 中建立臨時 AWS 資源的 Automation Runbook 附件取得 AWS CloudFormation 範本內容 AWS 帳戶。
5. `aws:createStack` - 建立 AWS CloudFormation 堆疊資源。
6. `aws:waitForAwsResourceProperty` - 等待範本建立的 Amazon EC2 執行個體 AWS CloudFormation 執行。
7. `aws:executeAwsApi` - 取得由 建立的臨時 Amazon EC2 執行個體和 VPC 對等互連的 IDs AWS CloudFormation。
8. `aws:executeAwsApi` - 取得暫時 Amazon EC2 執行個體的 IP 地址，以設定與資料庫執行個體的連線。
9. `aws:executeAwsApi` - 標記連接到暫時 Amazon EC2 執行個體的 Amazon EBS 磁碟區。
10. `aws:waitForAwsResourceProperty` - 等到暫時 Amazon EC2 執行個體通過狀態檢查。
11. `aws:waitForAwsResourceProperty` - 等到暫時 Amazon EC2 執行個體由 Systems Manager 管理。如果此步驟逾時或失敗，則 Runbook 會重新啟動執行個體。
 - a. `aws:executeAwsApi` - 如果上一個步驟失敗或逾時，則重新啟動暫時 Amazon EC2 執行個體。
 - b. `aws:waitForAwsResourceProperty` - 等到暫時 Amazon EC2 執行個體在重新啟動後由 Systems Manager 管理。
12. `aws:runCommand` - 在暫時 Amazon EC2 執行個體上安裝中繼資料收集器應用程式需求。
13. `aws:runCommand` - 透過在臨時 Amazon EC2 執行個體上建立組態檔案來設定資料庫執行個體的存取權。
14. `aws:executeAwsApi` - 建立維護時段，以使用 Run Command 定期執行中繼資料收集器應用程式。維護時段會在命令之間啟動和停止執行個體。
15. `aws:waitForAwsResourceProperty` - 等待範本建立的維護時段 AWS CloudFormation 就緒。
16. `aws:executeAwsApi` - 取得維護時段 IDs，並變更 建立的行事曆 AWS CloudFormation。
17. `aws:sleep` - 等到維護時段的結束日期。
18. `aws:executeAwsApi` - 關閉維護時段。
19. `aws:executeScript` - 取得在維護時段期間執行的任務結果。

20aws:waitForAwsResourceProperty - 等待維護時段完成最後一個任務，然後再繼續。

21aws:branch - 根據您是否為 SupportCase 參數提供值來配置工作流程。

- a. aws:changeInstanceState - 啟動暫時 Amazon EC2 執行個體，並等待狀態檢查通過，再上傳報告。
- b. aws:waitForAwsResourceProperty - 等到暫時 Amazon EC2 執行個體由 Systems Manager 管理。如果此步驟逾時或失敗，則 Runbook 會重新啟動執行個體。
 - i. aws:executeAwsApi - 如果上一個步驟失敗或逾時，則重新啟動暫時 Amazon EC2 執行個體。
 - ii. aws:waitForAwsResourceProperty - 等到暫時 Amazon EC2 執行個體在重新啟動後由 Systems Manager 管理。
- c. aws:runCommand - 如果您提供 SupportCase 參數的值，請將中繼資料報告連接至 支援 案例。指令碼會壓縮報告並將其分割為 5 MB 檔案。指令碼連接至 支援 案例的檔案數目上限為 12。

22aws:changeInstanceState - 在 AWS CloudFormation 堆疊無法刪除時停止暫時 Amazon EC2 執行個體。

23aws:executeAwsApi - 說明 Runbook 無法建立或更新 AWS CloudFormation 堆疊時的 AWS CloudFormation 堆疊事件。

24aws:waitForAwsResourceProperty - 等到 AWS CloudFormation 堆疊處於終端機狀態後再刪除。

25aws:executeAwsApi - 刪除不包含維護時段的 AWS CloudFormation 堆疊。如果 EbsVolumeDeleteOnTermination 參數值設定為 `false`，則會保留與暫時 Amazon EC2 執行個體相關聯的根 Amazon EBS 磁碟區。

AWS-RebootRdsInstance

Description

如果尚未重新啟動，AWS-RebootRdsInstance 則 Runbook 會重新啟動 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 您要重新啟動的 Amazon RDS 資料庫執行個體 ID。

文件步驟

RebootInstance - 如果資料庫執行個體尚未重新啟動，請將其重新啟動。

WaitForAvailableState - 等待資料庫執行個體完成重新啟動程序。

輸出

此自動化沒有輸出。

AWSupport-ShareRDSSnapshot

Description

AWSupport-ShareRDSSnapshot Runbook 為 知識中心文章中概述的程序提供自動化解決方案 [如何與其他帳戶共用加密的 Amazon RDS 資料庫快照？](#) 如果您的 Amazon Relational Database Service (Amazon RDS) 快照是使用預設值加密 AWS 受管金鑰，則無法共用快照。在這種情況下，您必須使用客戶受管金鑰複製快照，然後與目標帳戶共用快照。此自動化會使用您在 SnapshotName 參數中指定的值，或所選 Amazon RDS 資料庫執行個體或叢集的最近快照來執行這些步驟。

Note

如果您未指定 KMSKey 參數的值，自動化會在您的帳戶中建立新的 AWS KMS 客戶受管金鑰，用來加密快照。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AccountIds

類型：StringList

描述：（必要）共用快照的帳戶 IDs 逗號分隔清單。

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- 資料庫

類型：字串

描述：（必要）您要共用其快照的 Amazon RDS 資料庫執行個體或叢集名稱。如果您指定 參數的值，則此SnapshotName參數為選用。

- KMSKey

類型：字串

描述：(選用) 用於加密快照的客戶受管金鑰的完整 Amazon Resource Name (ARN) AWS KMS。

- SnapshotName

類型：字串

描述：(選用) 您要使用的資料庫叢集或執行個體快照 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- rds:DescribeDBInstances
- rds:DescribeDBSnapshots
- rds:CopyDBSnapshot
- rds:ModifyDBSnapshotAttribute

AutomationAssumeRole 需要下列動作，才能成功啟動資料庫叢集的 Runbook。

- ssm:StartAutomationExecution
- rds:DescribeDBClusters
- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

用來執行自動化的 IAM 角色必須新增為金鑰使用者，才能使用 ARNKmsKey 參數中指定的 KMS 金鑰。如需有關將金鑰使用者新增至 KMS 金鑰的資訊，請參閱《AWS Key Management Service 開發人員指南》中的[變更金鑰政策](#)。

如果您未指定 KMSKey 參數的值，AutomationAssumeRole需要下列其他動作才能成功啟動 Runbook。

- kms:CreateKey

- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

文件步驟

1. aws:executeScript - 檢查是否為 KMSKey 參數提供值，如果找不到值，則建立 AWS KMS 客戶受管金鑰。
2. aws:branch - 檢查是否已相應地為 SnapshotName 參數和分支提供值。
3. aws:executeAwsApi - 檢查提供的快照是否來自資料庫執行個體。
4. aws:executeScript - 格式化SnapshotName參數，以連字號取代冒號。
5. aws:executeAwsApi - 使用指定的 KMSKey 複製快照。
6. aws:waitForAwsResourceProperty - 等待複製快照操作完成。
7. aws:executeAwsApi - 與AccountIds指定的 共用新的快照。
8. aws:executeAwsApi - 檢查提供的快照是否來自資料庫叢集。
9. aws:executeScript - 格式化SnapshotName參數，以連字號取代冒號。
- 10aws:executeAwsApi - 使用指定的 KMSKey 複製快照。
- 11aws:waitForAwsResourceProperty - 等待複製快照操作完成。
- 12aws:executeAwsApi - 與AccountIds指定的 共用新的快照。
- 13aws:executeAwsApi - 檢查為 Database 參數提供的值是否為資料庫執行個體。
- 14aws:executeAwsApi - 檢查為 Database 參數提供的值是否為資料庫叢集。
- 15aws:executeAwsApi - 擷取指定 的快照清單Database。
- 16aws:executeScript - 從上一個步驟中組合的清單中確定可用的最新快照。
- 17aws:executeAwsApi - 使用指定的 複製資料庫執行個體快照KMSKey。
- 18aws:waitForAwsResourceProperty - 等待複製快照操作完成。
- 19aws:executeAwsApi - 與AccountIds指定的 共用新的快照。
- 20aws:executeAwsApi - 擷取指定 的快照清單Database。
- 21aws:executeScript - 從上一個步驟中組合的清單中確定可用的最新快照。
- 22aws:executeAwsApi - 使用指定的 複製資料庫執行個體快照KMSKey。
- 23aws:waitForAwsResourceProperty - 等待複製快照操作完成。
- 24aws:executeAwsApi - 與AccountIds指定的 共用新的快照。

`25.aws:executeScript` - 如果您未指定 `KMSKey` 參數的值且自動化失敗，則刪除自動化建立 AWS KMS 的客戶受管金鑰。

AWS-StartRdsInstance

Description

啟動 Amazon Relational Database Service (Amazon RDS) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：（必要）要啟動的 Amazon RDS 執行個體 ID。

AWS-StartStopAuroraCluster

Description

此 Runbook 會啟動或停止 Amazon Aurora 叢集。

Note

若要啟動叢集，它必須處於 stopped 狀態。若要停止叢集，它必須處於 available 狀態。此 Runbook 無法用來啟動或停止 Aurora Serverless 叢集、Aurora 多主機叢集、Aurora 全域資料庫的一部分，或使用 Aurora 平行查詢的叢集。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- ClusterName

類型：字串

描述：（必要）您要停止或啟動的 Aurora 叢集名稱。

- 動作

類型：字串

有效值：開始 | 停止

預設：開始

描述：（必要）您要停止或啟動的 Aurora 叢集名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

文件步驟

- `aws:executeScript` - 根據您為 指定的值啟動或停止叢集。

輸出

`StartStopAuroraCluster.ClusterName` - Aurora 叢集的名稱

`StartStopAuroraCluster.CurrentStatus` - Aurora 叢集的目前狀態

`StartStopAuroraCluster.Message` - 自動化的詳細資訊

AWS-StopRdsInstance

Description

停止 Amazon Relational Database Service (Amazon RDS) 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：（必要）要停止的 Amazon RDS 執行個體 ID。

AWSSupport-TroubleshootConnectivityToRDS

Description

AWSSupport-TroubleshootConnectivityToRDS Runbook 會診斷 EC2 執行個體與 Amazon Relational Database Service 執行個體之間的連線問題。自動化會確認資料庫執行個體可用，然後會檢查關聯的安全群組規則、網路存取控制清單 (網路 ACL)，以及路由表來檢查是否有潛在的連線能力問題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DBInstanceIdentifier

類型：字串

描述：(必要) 要測試連線能力的目標資料庫執行個體 ID。

- SourceInstance

類型：字串

允許的模式：`^[a-z0-9]{8,17}$`

描述：(必要) 要測試連線能力的來源 EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- rds:DescribeDBInstances

文件步驟

- aws:assertAwsResourceProperty - 確認資料庫執行個體狀態為 available。
- aws:executeAwsApi - 取得資料庫執行個體的相關資訊。
- aws:executeAwsApi - 取得資料庫執行個體網路 ACLs 的相關資訊。

- `aws:executeAwsApi` - 取得資料庫執行個體子網路 CIDR。
- `aws:executeAwsApi` - 取得 EC2 執行個體的相關資訊。
- `aws:executeAwsApi` - 取得 EC2 執行個體網路 ACLs 的相關資訊。
- `aws:executeAwsApi` - 取得與 EC2 執行個體相關聯之安全群組的相關資訊。
- `aws:executeAwsApi` - 取得與資料庫執行個體相關聯之安全群組的相關資訊。
- `aws:executeAwsApi` - 取得與 EC2 執行個體相關聯之路由表的相關資訊。
- `aws:executeAwsApi` - 取得與 EC2 執行個體的 Amazon VPC 相關聯的主要路由表相關資訊。
- `aws:executeAwsApi` - 取得與資料庫執行個體相關聯之路由表的相關資訊。
- `aws:executeAwsApi` - 取得與資料庫執行個體的 Amazon VPC 相關聯之主要路由表的相關資訊。
- `aws:executeScript` - 評估安全群組規則。
- `aws:executeScript` - 評估網路 ACLs。
- `aws:executeScript` - 評估路由表。
- `aws:sleep` - 結束自動化。

輸出

`getRDSInstanceProperties.DBInstanceIdentifier` - 自動化中使用的資料庫執行個體。

`getRDSInstanceProperties.DBInstanceStatus` – 資料庫執行個體目前的狀態。

`evalSecurityGroupRules.SecurityGroupEvaluation` – 比較 `SourceInstance` 安全群組規則與資料庫執行個體安全群組規則的結果。

`evalNetworkAclRules.NetworkAclEvaluation` – 比較 `SourceInstance` 網路 ACL 與資料庫執行個體網路 ACL 的結果。

`evalRouteTableEntries.RouteTableEvaluation` – 比較 `SourceInstance` 路由表與資料庫執行個體路由的結果。

AWSSupport-TroubleshootRDSIAMAuthentication

Description

`AWSSupport-TroubleshootRDSIAMAuthentication` 有助於對 Amazon RDS for PostgreSQL、Amazon RDS for MySQL、Amazon RDS for MariaDB、Amazon Aurora PostgreSQL

和 Amazon Aurora MySQL 執行個體進行故障診斷 AWS Identity and Access Management (IAM) 身分驗證。使用此 Runbook 來驗證使用 Amazon RDS 執行個體或 Aurora 叢集進行 IAM 身分驗證所需的組態。它也提供步驟來修正 Amazon RDS 執行個體或 Aurora 叢集的連線問題。

 Important

此 Runbook 不支援 Amazon RDS for Oracle 或 Amazon RDS for Microsoft SQL Server。

 Important

如果提供來源 Amazon EC2 執行個體且目標資料庫為 Amazon RDS，AWSsupport-TroubleshootConnectivityToRDS 則會叫用子自動化來疑難排解 TCP 連線。輸出也提供可在 Amazon EC2 執行個體或來源機器上執行的命令，以使用 IAM 身分驗證連線至 Amazon RDS 執行個體。

如何運作？

此 Runbook 包含六個步驟：

- 步驟 1：validateInputs：驗證自動化的輸入。
- 步驟 2：branchOnSourceEC2Provided：驗證輸入參數中是否提供來源 Amazon EC2 執行個體 ID。
- 步驟 3：validateRDSConnectivity：如果提供，則從來源 Amazon EC2 執行個體驗證 Amazon RDS 連線。
- 步驟 4：validateRDSIAMAuthentication：驗證 IAM Authentication 功能是否已啟用。
- 步驟 5：validateIAMPolicies：驗證所提供的 IAM 使用者/角色中是否存在所需的 IAM 許可。
- 步驟 6：generateReport：產生先前執行步驟結果的報告。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- RDSType

類型：字串

描述：(必要)：選取您嘗試連線和驗證的關聯式資料庫類型。

允許的值：Amazon RDS 或 Amazon Aurora Cluster。

- DBInstanceIdentifier

類型：字串

描述：(必要) 目標 Amazon RDS 資料庫執行個體或 Aurora 資料庫叢集的識別符。

允許模式：`^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

最大字元數：63

- SourceEc2InstanceIdentifier

類型：`AWS::EC2::Instance::Id`

描述：(選用) 如果您要從在相同帳戶和區域中執行的 Amazon EC2 執行個體連線至 Amazon RDS 資料庫執行個體，則為 Amazon EC2 執行個體 ID。如果來源不是 Amazon EC2 執行個體或目標 Amazon RDS 類型是 Aurora 資料庫叢集，請勿指定此參數。

預設：""

- DBIAMRoleName

類型：字串

描述：(選用) 用於 IAM 型身分驗證的 IAM 角色名稱。僅在 DBIAMUserName 未提供 參數時提供，否則請保留空白。DBIAMUserName 必須提供 DBIAMRoleName 或。

允許模式：`^[a-zA-Z0-9+=,.\@_-]{1,64}$|^$`

最大字元數：64

預設：""

- DBIAMUserName

類型：字串

描述：(選用) 用於 IAM 型身分驗證的 IAM 使用者名稱。只有在未提供 DBIAMRoleName 參數時才提供，否則請保留空白。DBIAMUserName 必須提供 DBIAMRoleName 或。

允許模式：`^[a-zA-Z0-9+=,.\@_-]{1,64}$|^$`

最大字元數：64

預設：""

- DBUserName

類型：字串

描述：(選用) 映射至 IAM 角色/使用者的資料庫使用者名稱，以在資料庫中進行 IAM 型身分驗證。預設選項會*評估資料庫中所有使用者是否允許 `rds-db:connect` 許可。

允許模式：`^[a-zA-Z0-9+=,.\@*_]{1,64}$`

最大字元數：64

預設：*

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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`

指示

1. 導覽至 AWS Systems Manager 主控台中的 [AWSSupport-TroubleshootRDSIAMAuthentication](#)。
2. 選取執行自動化
3. 針對輸入參數，輸入下列內容：
 - `AutomationAssumeRole`（選用）：

(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `RDSType`（必要）：

選取您嘗試連線和驗證的 Amazon RDS 類型。從兩個允許的值中選擇：Amazon RDS 或 Amazon Aurora Cluster。

- `DBInstanceIdentifier`（必要）：

輸入您要連線的目標 Amazon RDS 資料庫執行個體或 Aurora 叢集的識別符，並使用 IAM 登入資料進行身分驗證。

- SourceEc2InstanceIdentifier (選用)：

如果您要從相同帳戶和區域中存在的 Amazon EC2 執行個體連線至 Amazon RDS 資料庫執行個體，請提供 Amazon EC2 執行個體 ID。如果來源不是 Amazon EC2 或目標 Amazon RDS 類型是 Aurora 叢集，請保留空白。

- DBIAMRoleName (選用)：

輸入用於 IAM 型身分驗證的 IAM 角色名稱。只有在DBIAMUserName未提供時才提供；否則，請保留空白。DBIAMUserName 必須提供 DBIAMRoleName或。

- DBIAMUserName (選用)：

輸入用於 IAM 型身分驗證的 IAM 使用者。只有在DBIAMRoleName未提供時才提供，否則請保留空白。DBIAMUserName 必須提供 DBIAMRoleName或。

- DBUserName (選用)：

輸入對應至 IAM 角色/使用者的資料庫使用者，以在資料庫中進行 IAM 型身分驗證。預設選項*用於評估；此欄位未提供任何內容。

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. 選取執行。

5. 請注意，自動化會啟動。

6. 文件會執行下列步驟：

- 步驟 1：validateInputs：

驗證自動化的輸入 - `SourceEC2InstanceIdentifier` (選用)、`DBInstanceIdentifier`或`ClusterID`，以及`DBIAMRoleName`或`DBIAMUserName`。它會驗證輸入的輸入參數是否存在於您的帳戶和區域中。它也會驗證使用者是否輸入其中一個 IAM 參數 (例如 `DBIAMRoleName`或`DBIAMUserName`)。此外，它會執行其他驗證，例如，如果提及的資料庫處於可用狀態。

- 步驟 2 : `branchOnSourceEC2Provided` :

驗證來源 Amazon EC2 是否在輸入參數中提供，且資料庫為 Amazon RDS。如果是，它會繼續進行步驟 3。如果沒有，它會略過步驟 3，即 Amazon EC2-Amazon RDS Connectivity 驗證，並繼續進行步驟 4。

- 步驟 3 : `validateRDSConnectivity` :

如果在輸入參數中提供來源 Amazon EC2，且資料庫是 Amazon RDS，則步驟 2 會啟動步驟 3。在此步驟中，`AWSSupport-TroubleshootConnectivityToRDS`會叫用子自動化來驗證來源 Amazon EC2 的 Amazon RDS 連線。子自動化 `Runbook AWSSupport-TroubleshootConnectivityToRDS` 會驗證是否已備妥所需的網路組態 (Amazon Virtual Private Cloud 【Amazon VPC】、安全群組、網路存取控制清單 【NACL】、Amazon RDS 可用性)，以便您可以從 Amazon EC2 執行個體連線至 Amazon RDS 執行個體。

- 步驟 4 : `validateRDSIAMAuthentication` :

驗證是否已在 Amazon RDS 執行個體或 Aurora 叢集上啟用 IAM 身分驗證功能。

- 步驟 5 : `validateIAMPolicies` :

驗證傳遞的 IAM 使用者/角色中是否存在所需的 IAM 許可，以讓 IAM 登入資料能夠驗證指定資料庫使用者的 Amazon RDS 執行個體 (如果有的話)。

- 步驟 6 : `generateReport` :

取得先前步驟的所有資訊，並列印每個步驟的結果或輸出。它還列出了使用 IAM 登入資料連接到 Amazon RDS 執行個體的參考和執行步驟。

7. 當自動化完成時，請檢閱輸出區段以取得詳細結果：

- 檢查連線至資料庫的 IAM 使用者/角色許可：

驗證傳遞的 IAM 使用者/角色中是否存在所需的 IAM 許可，以讓 IAM 登入資料能夠驗證指定資料庫使用者的 Amazon RDS 執行個體 (如果有的話)。

- 檢查資料庫的 IAM 型身分驗證屬性：

驗證是否已為指定的 Amazon RDS 資料庫/Aurora 叢集啟用 IAM 身分驗證功能。

- 檢查從 Amazon EC2 執行個體到 Amazon RDS 執行個體的連線：

驗證所需的網路組態 (Amazon VPC、安全群組、NACL、Amazon RDS 可用性) 是否已到位，以便從 Amazon EC2 執行個體連線到 Amazon RDS 執行個體。

- 後續步驟:

列出使用 IAM 登入資料連接到 Amazon RDS 執行個體的參考和執行命令和步驟。

Outputs

ScriptExecutionId

Ze1d[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>

參考

Systems Manager Automation

- [執行此自動化 \(主控台 \)](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSsupport-ValidateRdsNetworkConfiguration

Description

`AWSSupport-ValidateRdsNetworkConfiguration` 自動化有助於避免在執行 `ModifyDBInstance` 或 `StartDBInstance` 操作之前，您現有 Amazon Relational Database Service (Amazon RDS) / Amazon Aurora / Amazon DocumentDB 執行個體的網路狀態不相容。如果執行個體已處於不相容的網路狀態，則 Runbook 將提供原因。

如何運作？

此 Runbook 會判斷您的 Amazon RDS 資料庫執行個體是否會進入不相容的網路狀態，或者，如果它具有，則判斷它是否處於不相容的網路狀態。

Runbook 會對 Amazon RDS 資料庫執行個體執行下列檢查：

- 每個區域的 Amazon Elastic Network Interface (ENI) 配額。
- 資料庫子網路群組中的所有子網路都存在。
- 子網路有足夠的可用 IP 地址（可供）。
- （適用於可公開存取的 Amazon RDS 執行個體）VPC 屬性的設定 (`enableDnsSupport` 和 `enableDnsHostnames`)。

Important

將本文件用於 Amazon Aurora / Amazon DocumentDB 叢集時，請務必使用 `DBInstanceIdentifier` 而非 `ClusterIdentifier`。否則，文件會在第一個步驟失敗。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- rds:DescribeDBInstances
- servicequotas:GetServiceQuota
- ec2:DescribeNetworkInterfaces
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets

範例政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
      ]
    }
  ]
}
```

指示

1. 在 AWS Systems Manager 主控台中導覽至 [AWSSupport-ValidateRdsNetworkConfiguration](#)。
2. 選取執行自動化
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：

(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DBInstanceIdentifier (必要)：

輸入 Amazon Relational Database Service 執行個體識別符。

The screenshot shows the 'Input parameters' section of an AWS Systems Manager Automation console. It contains two input fields: 'AutomationAssumeRole' and 'DBInstanceIdentifier'. The 'AutomationAssumeRole' field is a dropdown menu with the selected value 'arn:aws:iam::123456789012:role/AutomationAssumeRoleSSM'. The 'DBInstanceIdentifier' field is a text input containing the value 'my-rds-instance-01'.

4. 選取執行。

5. 請注意，自動化會啟動。

6. 文件會執行下列步驟：

- 步驟 1：assertRdsState：

檢查提供的執行個體識別符是否存在，並具有下列任何狀態：available、stopped 或 incompatible-network。

- 步驟 2：gatherRdsInformation：

收集有關 Amazon RDS 執行個體的必要資訊，以供稍後在自動化中使用。

- 步驟 3：checkEniQuota：

檢查區域的 Amazon ENI 目前可用配額。

- 步驟 4：validateVpcAttributes：

驗證 Amazon VPC 的 DNS 參數 (enableDnsSupport 和 enableDnsHostnames) 是否設為 true (如果 Amazon RDS 執行個體為則不是 PubliclyAccessible)。

- 步驟 5：validateSubnetAttributes：

驗證中是否存在子網路，DBSubnetGroup 並檢查每個子網路的可用 IPs。

- 步驟 6：generateReport：

取得先前步驟的所有資訊，並列印每個步驟的結果或輸出。它還列出了使用 IAM 登入資料連接到 Amazon RDS 執行個體的參考和執行步驟。

7. 當自動化完成時，請檢閱輸出區段以取得詳細結果：

具有有效網路組態的 Amazon RDS 執行個體：

▼ 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.
```

網路組態不正確的 Amazon RDS 執行個體 (VPC 屬性 enableDnsHostnames 設定為 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.

```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [如何解決網路狀態不相容的 Amazon RDS 資料庫問題？](#)
- [如何解決網路狀態不相容的 Amazon DocumentDB 執行個體問題？](#)

Amazon Redshift

AWS Systems Manager 自動化為 Amazon Redshift 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

AWSConfigRemediation-DeleteRedshiftCluster

Description

AWSConfigRemediation-DeleteRedshiftCluster Runbook 會刪除您指定的 Amazon Redshift 叢集。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterIdentifier

類型：字串

描述：(必要) 您要刪除的 Amazon Redshift 叢集 ID。

- SkipFinalClusterSnapshot

類型：布林值

預設：false

描述：(選用) 如果設定為 false ，自動化會在刪除 Amazon Redshift 叢集之前建立快照。如果設定為 true ，則不會建立最終叢集快照。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift>DeleteCluster
- redshift:DescribeClusters

文件步驟

- aws:branch - 根據您為 SkipFinalClusterSnapshot 參數指定的值進行分支。
- aws:executeAwsApi - 刪除 ClusterIdentifier 參數中指定的 Amazon Redshift 叢集。
- aws:assertAwsResourceProperty - 驗證已刪除 Amazon Redshift 叢集。

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Description

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster Runbook 會停用您指定之 Amazon Redshift 叢集的公有可存取性。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterIdentifier

類型：字串

描述：(必要) 您要停用公開可存取性之叢集的唯一識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文件步驟

- aws:executeAwsApi - 停用 ClusterIdentifier 參數中指定之叢集的公有可存取性。
- aws:waitForAwsResourceProperty - 等待叢集的狀態變更為 available 。
- aws:assertAwsResourceProperty - 確認叢集上已停用公有可存取性設定。

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Description

AWSConfigRemediation-EnableRedshiftClusterAuditLogging Runbook 會為您指定的 Amazon Redshift 叢集啟用稽核記錄。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- BucketName

類型：字串

描述：（必要）您要上傳日誌的 Amazon Simple Storage Service (Amazon S3) 儲存貯體名稱。

- ClusterIdentifier

類型：字串

描述：（必要）您要啟用稽核記錄之叢集的唯一識別符。

- S3KeyPrefix

類型：字串

描述：(選用) 您要上傳日誌的 Amazon S3 金鑰字首 (子資料夾)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeLoggingStatus
- redshift:EnableLogging
- s3:GetBucketAcl
- s3:PutObject

文件步驟

- aws:branch - 根據是否為 S3KeyPrefix 參數指定值進行分支。
- aws:executeAwsApi - 在 ClusterIdentifier 參數中指定的叢集上啟用稽核記錄。
- aws:assertAwsResourceProperty - 驗證是否已在叢集上啟用稽核記錄。

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Description

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot Runbook 會為您指定的 Amazon Redshift 叢集啟用自動快照。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- AutomatedSnapshotRetentionPeriod

類型：整數

有效值：1-35

描述：(必要) 自動化快照保留的天數。

- ClusterIdentifier

類型：字串

描述：(必要) 您要啟用自動快照之叢集的唯一識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文件步驟

- aws:executeAwsApi - 在 ClusterIdentifier 參數中指定的叢集上啟用自動化快照。
- aws:waitForAwsResourceProperty - 等待叢集的狀態變更為 available 。
- aws:executeScript - 確認叢集上已啟用自動快照。

AWSConfigRemediation-EnableRedshiftClusterEncryption

Description

AWSConfigRemediation-EnableRedshiftClusterEncryption Runbook 會在您使用 AWS Key Management Service (AWS KMS) 客戶受管金鑰指定的 Amazon Redshift 叢集上啟用加密。此 Runbook 應僅用作基準，以確保您的 Amazon Redshift 叢集根據最低建議的安全最佳實務進行加密。我們建議使用不同的客戶受管金鑰加密多個叢集。此 Runbook 無法變更已加密叢集上使用 AWS KMS 的客戶受管金鑰。若要變更用於加密叢集 AWS KMS 的客戶受管金鑰，您必須先停用叢集上的加密。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterIdentifier

類型：字串

描述：（必要）您要啟用加密之叢集的唯一識別符。

- KMSKeyARN

類型：字串

描述：（必要）您要用來加密叢集資料的 客戶受管金鑰的 AWS KMS Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文件步驟

- aws:executeAwsApi - 在 ClusterIdentifier 參數中指定的 Amazon Redshift 叢集上啟用加密。
- aws:assertAwsResourceProperty - 驗證叢集上已啟用加密。

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Description

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting Runbook 會為您指定的 Amazon Redshift 叢集啟用增強型虛擬私有雲端 (VPC) 路由。如需增強型 VPC 路由的相關資訊，請參閱 [《Amazon Redshift 管理指南》中的 Amazon Redshift 增強型 VPC 路由](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterIdentifier

類型：字串

描述：(必要) 您要啟用增強型 VPC 路由之叢集的唯一識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文件步驟

- aws:executeAwsApi - 在 ClusterIdentifier 參數中指定的叢集上啟用增強型 VPC 路由。
- assertAwsResourceProperty - 確認叢集上已啟用增強型 VPC 路由。

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Description

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster Runbook 需要傳入連線，才能為您指定的 Amazon Redshift 叢集使用 SSL。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- ClusterIdentifier

類型：字串

描述：(必要) 您要啟用增強型 VPC 路由之叢集的唯一識別符。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:DescribeClusterParameters
- redshift:ModifyClusterParameterGroup

文件步驟

- aws:executeAwsApi - 從 參數中指定的叢集收集ClusterIdentifier參數詳細資訊。
- aws:executeAwsApi - 在 ClusterIdentifier 參數中指定的叢集上啟用 require_ssl設定。
- aws:assertAwsResourceProperty - 確認已在叢集上啟用require_ssl設定。
- aws:executeScript - 驗證叢集require_ssl的設定。

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Description

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings Runbook 會修改您指定的 Amazon Redshift 叢集的維護設定。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AllowVersionUpgrade

類型：布林值

描述：（必要）如果設定為 true，主要版本升級會在維護時段期間自動套用至叢集。

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- AutomatedSnapshotRetentionPeriod

類型：整數

有效值：1-35

描述：（必要）保留自動快照的天數。

- **ClusterIdentifier**

類型：字串

描述：（必要）您要啟用增強型 VPC 路由之叢集的唯一識別符。

- **PreferredMaintenanceWindow**

類型：字串

描述：（必要）可進行系統維護的每週時間範圍 (UTC)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

文件步驟

- `aws:executeAwsApi` - 修改 `ClusterIdentifier` 參數中指定之叢集的維護設定。
- `aws:assertAwsResourceProperty` - 確認已為叢集設定修改後的維護設定。

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Description

AWSConfigRemediation-ModifyRedshiftClusterNodeType Runbook 會修改您指定之 Amazon Redshift 叢集的節點類型和節點數量。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- 傳統

類型：布林值

描述：(選用) 如果設定為 true，調整大小操作會使用傳統調整大小程序。

- ClusterIdentifier

類型：字串

描述：(必要) 您要修改其節點類型之叢集的唯一識別符。

- ClusterType

類型：字串

有效值：單一節點 | 多節點

描述：(必要) 您要指派給叢集的叢集類型。

- NodeType

類型：字串

有效值：ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

描述：(必要) 您要指派給叢集的節點類型。

- NumberOfNodes

類型：整數

有效值：2-100

描述：(選用) 您要指派給叢集的節點數量。如果您的叢集是 single-node 類型，請勿為此參數指定值。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ResizeCluster

文件步驟

- aws:executeScript - 修改 ClusterIdentifier 參數中指定之叢集的節點類型和節點數量。

Amazon S3

AWS Systems Manager 自動化為 Amazon Simple Storage Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [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-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)
- [AWSSupport-ContainS3Resource](#)

AWS-ArchiveS3BucketToIntelligentTiering

Description

AWS-ArchiveS3BucketToIntelligentTiering Runbook 會為您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體建立或取代智慧型分層組態。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName

類型：字串

描述：(必要) 您要為其建立智慧型分層組態的 S3 儲存貯體名稱。

- ConfigurationId

類型：字串

描述：(必要) 智慧型分層組態的 ID。這可以是新的組態 ID 或現有組態的 ID。

- NumberOfDaysToArchive

類型：字串

有效值：90-730

描述：(必要) 儲存貯體中物件有資格轉換為 Archive Access 層的連續天數。

- NumberOfDaysToDeepArchive

類型：字串

有效值：180-730

描述：(必要) 儲存貯體中物件有資格轉換為 Deep Archive Access 層的連續天數。

- S3Prefix

類型：字串

描述：(選用) 您要套用組態之物件的金鑰名稱字首。

- 標籤

類型：MapList

描述：(選用) 指派給您要套用組態之物件的中繼資料。標籤由使用者定義的索引鍵和值組成。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetIntelligentTieringConfiguration
- s3:PutIntelligentTieringConfiguration

文件步驟

- `PutsBucketIntelligentTieringConfiguration` (aws : `executeScript`) - 建立或更新指定儲存貯體的 Amazon S3 Intelligent-Tiering 組態。
- `VerifyBucketIntelligentTieringConfiguration` (aws : `assertAwsResourceProperty`) - 驗證 S3 儲存貯體智慧型組態已套用至指定的儲存貯體。

AWS-ConfigureS3BucketLogging

Description

在 Amazon Simple Storage Service (Amazon S3) 儲存貯體上啟用記錄。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- `BucketName`

類型：字串

描述：（必要）您要為其設定記錄的 Amazon S3 儲存貯體名稱。

- **GrantedPermission**

類型：字串

有效值：FULL_CONTROL | READ | WRITE

描述：(選用) 指派給儲存貯體之被授予者的記錄許可。

- **GranteeEmailAddress**

類型：字串

(選用) 被授予者的電子郵件地址。

- **GranteeId**

類型：字串

描述：(選用) 被授予者的正式使用者 ID。

- **GranteeType**

類型：字串

有效值：CanonicalUser | AmazonCustomerByEmail | 群組

描述：(必要) 被授予者的類型。

- **GranteeUri**

類型：字串

描述：(選用) 被授予者群組的 URI。

- **TargetBucket**

類型：字串

描述：(必要) 指定您希望 Amazon S3 存放伺服器存取日誌的儲存貯體。您可以將日誌傳送到您擁有的任何儲存貯體。您也可以設定多個儲存貯體，以將其日誌傳送至相同的目標儲存貯體。在此情況下，您應該針對各個來源儲存貯體選擇不同的 TargetPrefix，讓傳送的日誌檔案能夠以索引鍵區分。

- **TargetPrefix**

類型：字串

預設：/

描述：(選用) 為索引鍵指定字首，而日誌檔案將會存放於索引鍵之下。

AWS-ConfigureS3BucketVersioning

Description

設定 Amazon Simple Storage Service (Amazon S3) 儲存貯體的版本控制。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName

類型：字串

描述：(必要) 您要設定版本控制的 Amazon S3 儲存貯體名稱。

- VersioningState

類型：字串

有效值：已啟用 | 已暫停

預設：Enabled

描述：(選用) 套用至 VersioningConfiguration.Status。設為「Enabled」(啟用) 時，此程序會啟用儲存貯體之物件的版本控制，而所有新增至儲存貯體的物件都會收到唯一的版本 ID。設定為 Suspended 時，此程序會停用儲存貯體中物件的版本控制。新增至儲存貯體的所有物件都會收到版本 ID null。

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Description

Runbook 會根據您在 AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock Runbook 參數中指定的值，設定 Amazon S3 儲存貯體的 Amazon Simple Storage Service (Amazon S3) 公有存取區塊設定。Amazon S3

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- BlockPublicAcls

類型：布林值

預設：true

描述：(選用) 如果設定為 `true`，Amazon S3 會封鎖 S3 儲存貯體的公有存取控制清單 (ACLs)，以及存放在您在 `BucketName` 參數中指定的 S3 儲存貯體中的物件。

- `BlockPublicPolicy`

類型：布林值

預設：`true`

描述：(選用) 如果設定為 `true`，Amazon S3 會封鎖您在 `BucketName` 參數中指定的 S3 儲存貯體的公有儲存貯體政策。

- `BucketName`

類型：字串

描述：(必要) 您要設定的 S3 儲存貯體名稱。

- `IgnorePublicAcls`

類型：布林值

預設：`true`

描述：(選用) 如果設定為 `true`，Amazon S3 會忽略您在 `BucketName` 參數中指定的 S3 儲存貯體的所有公有 ACLs。

- `RestrictPublicBuckets`

類型：布林值

預設：`true`

描述：(選用) 如果設定為 `true`，Amazon S3 會限制您在 `BucketName` 參數中指定的 S3 儲存貯體的公有儲存貯體政策。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`

- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

文件步驟

- `aws:executeAwsApi` - 建立或修改 `BucketName` 參數中指定之 S3 儲存貯體的 `PublicAccessBlock` 組態。
- `aws:executeScript` - 傳回 `BucketName` 參數中指定的 S3 儲存貯體 `PublicAccessBlock` 組態，並根據 Runbook 參數中指定的值驗證已成功進行變更。

AWSConfigRemediation-ConfigureS3PublicAccessBlock

Description

Runbook 會根據您在 `AWSConfigRemediation-ConfigureS3PublicAccessBlock` Runbook 參數中指定的值，設定 AWS 帳戶的 Amazon Simple Storage Service (Amazon S3) 公有存取區塊設定。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AccountId`

類型：字串

描述：（必要）AWS 帳戶 擁有您正在設定的 S3 儲存貯體的 ID。

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- BlockPublicAcls

類型：布林值

預設：true

描述：(選用) 如果設定為 true，Amazon S3 會封鎖 AWS 帳戶 您在 AccountId 參數中指定之擁有的 S3 儲存貯體的公有存取控制清單 (ACLs)。

- BlockPublicPolicy

類型：布林值

預設：true

描述：(選用) 如果設定為 true，Amazon S3 會針對 AWS 帳戶 您在 AccountId 參數中指定的所擁有的 S3 儲存貯體封鎖公有儲存貯體政策。

- IgnorePublicAcls

類型：布林值

預設：true

描述：(選用) 如果設定為 true，Amazon S3 會忽略 AWS 帳戶 您在 AccountId 參數中指定之擁有的 S3 儲存貯體的所有公有 ACLs。

- RestrictPublicBuckets

類型：布林值

預設：true

描述：(選用) 如果設定為 true，Amazon S3 會限制 AWS 帳戶 您在 AccountId 參數中指定之擁有的 S3 儲存貯體的公有儲存貯體政策。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock

文件步驟

- aws:executeAwsApi - 建立或修改 AccountId 參數中指定 AWS 帳戶的PublicAccessBlock組態。
- aws:executeScript - 傳回 AccountId 參數中 AWS 帳戶 指定的PublicAccessBlock組態，並根據 Runbook 參數中指定的值驗證已成功進行變更。

AWS-CreateS3PolicyToExpireMultipartUploads

Description

AWS-CreateS3PolicyToExpireMultipartUploads Runbook 會為指定的儲存貯體建立生命週期政策，以在定義的天數後過期未完成的分段上傳進行中。此 Runbook 會將新的生命週期政策與已存在的任何現有生命週期儲存貯體政策合併。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName

類型：字串

描述：(必要) 您要設定的 S3 儲存貯體名稱。

- DaysUntilExpire

類型：整數

描述：(必要) Amazon S3 在永久移除上傳的所有部分之前等待的天數。

- RuleId

類型：字串

描述：(必要) 用來識別生命週期儲存貯體規則的 ID。這必須是唯一的值。

- S3Prefix

類型：字串

描述：(選用) 您要套用組態之物件的金鑰名稱字首。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration

文件步驟

- ConfigureExpireMultipartUploads (aws : executeScript) - 設定儲存貯體的生命週期政策。

- VerifyExpireMultipartUploads (aws : executeScript) - 驗證已為儲存貯體設定生命週期政策。

輸出

- VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse
- VerifyExpireMultipartUploads.LifecycleConfigurationRule

AWS-DisableS3BucketPublicReadWrite

Description

使用 Amazon Simple Storage Service (Amazon S3) Block Public Access 停用公有 S3 儲存貯體的讀取和寫入存取權。如需詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的使用 Amazon S3 封鎖公開存取](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName

類型：字串

描述：(必要) 您想要限制存取的 S3 儲存貯體。

AWS-EnableS3BucketEncryption

Description

設定 Amazon Simple Storage Service (Amazon S3) 儲存貯體的預設加密。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- BucketName

類型：字串

描述：(必要) 您想要加密內容的 S3 儲存貯體之名稱。

- SSEAlgorithm

類型：字串

預設：AES256

描述：(選用) 用於預設加密的伺服器端加密演算法。

AWS-EnableS3BucketKeys

Description

AWS-EnableS3BucketKeys Runbook 會在您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體上啟用儲存貯體金鑰。此儲存貯體層級金鑰會在其生命週期期間為新物件建立資料金鑰。如果您未指定 KmsKeyId 參數的值，則使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密會用於預設加密組態。

Note

使用 AWS Key Management Service (AWS KMS) 金鑰 (DSSE-KMS) 的雙層伺服器端加密不支援 Amazon S3 儲存貯體金鑰。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- BucketName

類型：字串

描述：(必要) 您要為其啟用儲存貯體金鑰的 S3 儲存貯體名稱。

- KMSKeyId

類型：字串

描述：(選用) 要用於伺服器端加密的 Amazon Resource Name (ARN)、金鑰 ID 或 AWS Key Management Service (AWS KMS) 客戶受管金鑰的金鑰別名。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetEncryptionConfiguration
- s3:PutEncryptionConfiguration

文件步驟

- ChooseEncryptionType (aws : branch) - 評估為 KmsKeyId 參數提供的值，以判斷是否將使用 SSE-S3 (AES256) 或 SSE-KMS。
- PutBucketKeysKMS (aws : executeAwsApi) - 使用指定的，將指定 S3 儲存貯體的 BucketKeyEnabled 屬性設定為 KmsKeyId。
- PutBucketKeysAES256 (aws : executeAwsApi) - 使用 AES256 加密將指定 S3 儲存貯體的 BucketKeyEnabled 屬性設定為。
- VerifyS3BucketKeysEnabled (aws : assertAwsResourceProperty) - 驗證已在目標 S3 儲存貯體上啟用儲存貯體金鑰。

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Description

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy Runbook 會從 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策中移除具有萬用字元 (Principal: * 或 Principal: "AWS": *) Allow動作的主體政策陳述式。也會移除具有條件的政策陳述式。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- BucketName

類型：字串

描述：(必要) 您要修改其政策的 Amazon S3 儲存貯體名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy

- `s3:PutBucketPolicy`

文件步驟

- `aws:executeScript` - 修改儲存貯體政策，並驗證使用萬用字元的主體政策陳述式已從您在 `BucketName` 參數中指定的 Amazon S3 儲存貯體中移除。

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Description

AWSConfigRemediation-RestrictBucketSSLRequestsOnly Runbook 會建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策陳述式，明確拒絕對您所指定 Amazon S3 儲存貯體的 HTTP 請求。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `BucketName`

類型：字串

描述：（必要）您要拒絕 HTTP 請求的 S3 儲存貯體名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

文件步驟

- `aws:executeScript` - 為明確拒絕 HTTP 請求的 BucketName 參數中指定的 S3 儲存貯體建立儲存貯體政策。

AWSSupport-TroubleshootS3PublicRead

Description

AWSSupport-TroubleshootS3PublicRead Runbook 會診斷從您在 S3BucketName 參數中指定的公有 Amazon Simple Storage Service (Amazon S3) 儲存貯體讀取物件的問題。也會分析 S3 儲存貯體中物件的設定子集。

[執行此自動化（主控台）](#)

限制

- 此自動化不會檢查允許公開存取物件的存取點。
- 此自動化不會評估 S3 儲存貯體政策中的條件索引鍵。
- 如果您使用的是 AWS Organizations，則此自動化不會評估服務控制政策，以確認允許存取 Amazon S3。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- CloudWatchLogGroupName

類型：字串

描述：(選用) 您要傳送自動化輸出的 Amazon CloudWatch Logs 日誌群組。如果找不到符合您指定值的日誌群組，自動化將會使用此參數值建立日誌群組。此自動化所建立之日誌群組的保留期間為 14 天。

- CloudWatchLogStreamName

類型：字串

描述：(選用) 您要傳送自動化輸出的 CloudWatch Logs 日誌串流。如果找不到符合您指定值的日誌串流，自動化將會使用此參數值建立日誌串流。如果您未指定此參數的值，自動化將使用 ExecutionId 做為日誌串流的名稱。

- HttpGet

類型：布林值

有效值：true | false

預設：true

描述：(選用) 如果此參數設定為 true，自動化會對 S3BucketName 您指定的 中的物件提出部分 HTTP 請求。使用 Range HTTP 標頭只會傳回物件的第一個位元組。

- IgnoreBlockPublicAccess

類型：布林值

有效值：true | false

預設：false

描述：（選用）如果此參數設為 true，自動化會忽略您在 S3BucketName 參數中指定的 S3 儲存貯體的公有存取區塊設定。不建議從預設值變更此參數。

- MaxObjects

類型：整數

有效值：1-25

預設：5

描述：（選用）您在 S3BucketName 參數中指定的 S3 儲存貯體中要分析的物件數量。

- S3BucketName

類型：字串

描述：（必要）要故障診斷的 S3 儲存貯體名稱。

- S3PrefixName

類型：字串

描述：（選用）您要在 S3 儲存貯體中分析之物件的金鑰名稱字首。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[物件金鑰](#)。

- StartAfter

類型：字串

描述：（選用）您希望自動化開始分析 S3 儲存貯體中物件的物件金鑰名稱。

- ResourcePartition

類型：字串

有效值：aws | aws-us-gov | aws-cn

預設：aws

描述：(必要) S3 儲存貯體所在的分割區。

- 詳細資訊

類型：布林值

有效值：true | false

預設：false

描述：(選用) 若要在自動化期間傳回更多詳細資訊，請將此參數設定為 true 。如果 參數設定為 false ，則只會傳回警告和錯誤訊息。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

只有在您希望自動化將日誌資料傳送至 CloudWatch Logs 時，才需要 logs:CreateLogGroup logs:CreateLogStream、和 logs:PutLogEvents許可。

```
{
  "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"
  }
]
}

```

文件步驟

- `aws:assertAwsResourceProperty` - 確認 S3 儲存貯體存在且可存取。
- `aws:executeScript` - 傳回 S3 儲存貯體位置和正式使用者 ID。
- `aws:executeScript` - 傳回您帳戶的公有存取區塊設定和 S3 儲存貯體。
- `aws:assertAwsResourceProperty` - 確認 S3 儲存貯體付款人設定為 `BucketOwner`。如果在 S3 儲存貯體上啟用 `Requester Pays`，則自動化會結束。
- `aws:executeScript` - 傳回 S3 儲存貯體政策狀態，並判斷是否被視為公有。如需公有 S3 儲存貯體的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》](#) 中的「公」意義。
- `aws:executeAwsApi` - 傳回 S3 儲存貯體政策。
- `aws:executeAwsApi` - 傳回 S3 儲存貯體政策中找到的所有內容索引鍵。
- `aws:assertAwsResourceProperty` - 確認 `GetObject` API 動作的 S3 儲存貯體政策中是否有明確拒絕。
- `aws:executeAwsApi` - 傳回 S3 儲存貯體的存取控制清單 (ACL)。
- `aws:executeScript` - 如果您指定 `CloudWatchLogGroupName` 參數的值，則建立 `CloudWatch Logs` 日誌群組和日誌串流。
- `aws:executeScript` - 根據您在 Runbook 輸入參數中指定的值，會評估自動化期間收集的任何 S3 儲存貯體設定是否阻止公有存取物件。此指令碼會執行下列函數：

- 評估公有存取區塊設定
- 根據您在 `S3PrefixName` 和 `StartAfter` 參數中指定的值，從 `S3 MaxObjects` 儲存貯體傳回物件。
- 傳回 `S3` 儲存貯體政策，以模擬從 `S3` 儲存貯體傳回之物件的自訂 IAM 政策。
- 如果 `HttpGet` 參數設定為 `true`，則對傳回的物件執行部分 HTTP `range` 請求。使用 `Range` HTTP 標頭只會傳回物件的第一個位元組。
- 檢查傳回物件的金鑰名稱，以確認其結尾是一或兩個句點。無法從 Amazon S3 主控台下載以句點結尾的物件金鑰名稱。
- 檢查傳回物件的擁有者是否與 `S3` 儲存貯體的擁有者相符。
- 檢查物件的 ACL 是否授予匿名使用者 `READ` 或 `FULL_CONTROL` 許可。
- 傳回與物件相關聯的標籤。
- 使用模擬的 IAM 政策來確認 `GetObject` API 動作的 `S3` 儲存貯體政策中是否明確拒絕此物件。
- 傳回物件的中繼資料，以確認支援儲存體方案。
- 檢查物件的伺服器端加密設定，以確認是否使用 a AWS Key Management Service (AWS KMS) 客戶受管金鑰來加密物件。

輸出

`AnalyzeObjects.bucket`

`AnalyzeObjects.object`

AWSsupport-EmptyS3Bucket

Description

`AWSsupport-EmptyS3Bucket` 自動化 Runbook 會使用生命週期過期組態規則來清空現有的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

Important

- 不支援啟用多重要素驗證 (MFA) 的 Amazon S3 儲存貯體。
- 此 Runbook 修改的生命週期規則會永久刪除指定 Amazon S3 儲存貯體中的所有物件及其版本。您無法復原永久刪除的物件。如需詳細資訊，請參閱[即將過期的物件](#)。

如何運作？

Runbook 會 `AWSSupport-EmptyS3Bucket` 執行下列高階步驟：

- 如果啟用，則暫停儲存貯體版本控制。
- 更新儲存貯體政策以拒絕任何 `s3:PutObject` API 呼叫（以防止清空時重新上傳）。
- 更新生命週期規則，根據輸入參數中指定的過期日刪除所有物件。

Note

- 以 Amazon S3 物件鎖定保護的物件版本不會遭到生命週期組態刪除或覆寫。
- 刪除程序是非同步的，在執行手冊執行完成後可能需要一些時間才能完成。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

`AutomationAssumeRole` 參數需要下列動作，才能成功使用 Runbook：

- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`
- `s3:GetBucketVersioning`
- `s3:PutBucketVersioning`
- `s3:GetBucketPolicy`
- `s3:GetBucketLifecycleConfiguration`

- s3:GetLifecycleConfiguration
- s3:PutBucketPolicy
- s3 : PutBucketLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:DeleteBucketPolicy
- s3 : DeleteBucketLifecycle

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-EmptyS3Bucket](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列項目：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN) ，可讓 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- S3BucketName：

您要清空的 Amazon S3 儲存貯體名稱。

- SNSTopicArn：

提供 Amazon SNS 主題的 ARN 以進行核准通知。此 Amazon SNS 主題用於在自動化執行期間，於必要期間傳送核准通知。

- ApproverIAM：

提供能夠核准或拒絕動作的 AWS 驗證主體清單。核准者數目上限為 10。您可以使用任何這些格式、AWS Identity and Access Management (IAM) 使用者名稱、IAM 使用者 ARN、IAM 角色 ARN 或 IAM 擔任角色使用者 ARN 來指定主體。

- MinimumRequiredApprovals (選用)：

繼續自動化所需的核准數量下限。如果您未指定值，系統會預設為 1。此參數的值必須為正數。此參數的值不能超過核准者IAM 參數定義的ApproverIAM數目。

- NoncurrentVersionExpirationDays (選用)：

指定非目前物件版本過期的天數。過期時，Amazon S3 會永久刪除非目前的物件版本。

- 預設：1
- 最大值：365
- ExpirationDays（選用）：

以天數的形式指定物件生命週期的過期時間。

- 預設：1
- 最大值：365
- AbortIncompleteMultipartUpload（選用）：

指定自啟動未完成分段上傳後，Amazon S3 將等待的天數，然後再永久移除上傳的所有部分。

- 預設：1
- 最大值：365
- 確認：

請閱讀此自動化執行手冊所執行動作的完整詳細資訊，並在您確認步驟 Yes, I understand and acknowledge 時提供同意。

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. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- **checkConcurrency:**

確保只有一個針對指定 Amazon S3 儲存貯體的執行此 Runbook。如果 Runbook 找到另一個以相同儲存貯體名稱為目標的進行中執行，則會傳回錯誤並結束。

- **getBucketVersioningConfiguration:**

擷取指定 Amazon S3 儲存貯體的版本控制狀態。

- **branchOnStoppingIfMFADeleteEnabled** (條件式)：

如果在指定的 Amazon S3 儲存貯體上啟用多重要素驗證 (MFA)，則停止自動化。

- **approvalToMakeChangesToTheProvidedS3Bucket:**

等待指定的主體核准，以停用儲存貯體版本控制，並更新指定 Amazon S3 儲存貯體的儲存貯體政策和生命週期規則組態。

- **branchOnBucketVersioningStatus** (條件式)：

如果在指定的 Amazon S3 儲存貯體上啟用版本控制，請將其停用，否則請繼續更新儲存貯體政策和生命週期組態。

- **suspendBucketVersioning:**

暫停指定 Amazon S3 儲存貯體的版本控制狀態。

- **updateBucketPolicyAndLifeCycleConfiguration:**

新增或更新儲存貯體政策，以拒絕所有 `s3:PutObject` 請求，並根據使用者提供的輸入參數更新生命週期組態以使物件過期。

- **branchOnFailingIfBucketPropertiesNotUpdated** (條件式)：

檢查 `updateBucketPolicyAndLifeCycleConfiguration` 步驟的狀態，如果自動化變更，會嘗試還原原始儲存貯體版本控制狀態。

- **branchOnFailureOriginalVersioningStatus** (條件式)：

失敗時，分支會判斷原始版本控制狀態。如果已由此自動化啟用和暫停，會嘗試再次啟用它。

- **onFailureRestoreBucketVersioning**

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

✓ 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)

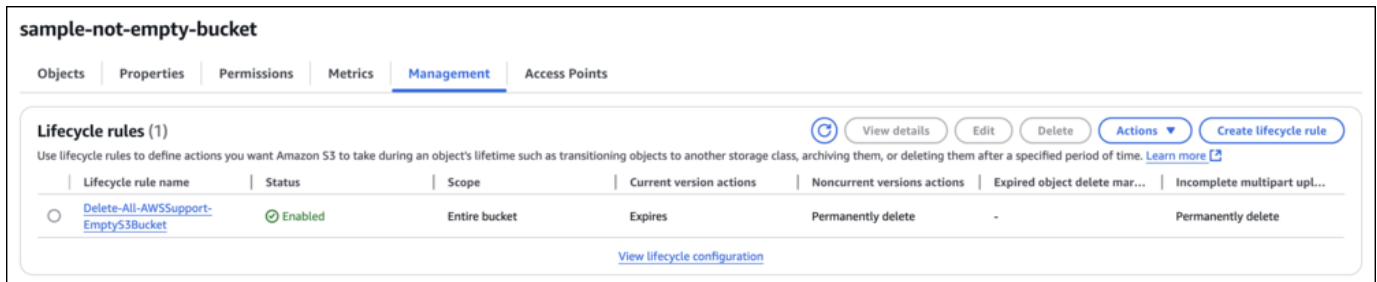
Q Find Steps

< 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	-

- 成功執行

此工作流程會更新儲存貯體的生命週期規則。物件將根據Delete-All-AWSSupport-EmptyS3-Bucket生命週期政策刪除。



- 失敗執行

不會執行部分刪除。如果執行失敗，生命週期和其他儲存貯體設定會復原。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程](#)

如需管理 Amazon S3 儲存貯體和物件的詳細資訊，請參閱[清空儲存貯體](#)。

AWSSupport-TroubleshootS3EventNotifications

Description

AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager 自動化 Runbook 可協助疑難排解使用 AWS Lambda 函數、Amazon Simple Notification Service (Amazon SNS) 儲存貯體事件通知。Amazon SNS Amazon SQS 它提供使用 Amazon S3 儲存貯體設定為目的地事件通知之不同資源的組態設定報告。

它如何運作？

Runbook 會執行下列步驟：

- 檢查 Amazon S3 儲存貯體是否存在於執行 AWSSupport-TroubleshootS3EventNotifications 的相同帳戶中。
- 使用 [GetBucketNotificationConfiguration](#) API，擷取設定為 Amazon S3 儲存貯體事件通知的目的地資源 (AWS Lambda 函數或 Amazon SNS 主題或 Amazon SQS 佇列)。Amazon S3

- 驗證目的地資源是否存在，然後檢閱目的地資源的資源型政策，以判斷是否允許 Amazon S3 發佈至目的地。
- 如果您使用 AWS Key Management Service (AWS KMS) 金鑰加密目的地，則會檢查金鑰政策，以判斷是否允許 Amazon S3 存取。
- 產生所有目的地資源檢查的報告。

Important

- 此 Runbook 只有在 Amazon S3 儲存貯體擁有者與執行自動化 Runbook 的 AWS 帳戶 擁有者相同時，才能評估事件通知組態。
- 此外，此 Runbook 無法評估在另一個 中託管的目的地資源上的政策 AWS 帳戶。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName

類型：AWS::S3::Bucket::Name

描述：（必要）使用事件通知設定的 Amazon S3 儲存貯體名稱（含）。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

自動化擔任角色的 IAM 政策範例

```
{
  "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:::<bucket-name>"
    },
    {
        "Sid": "SQSPermission",
        "Effect": "Allow",
        "Action": [
            "sqs:GetQueueAttributes",
            "sqs:GetQueueUrl"
        ],
        "Resource": "arn:aws:sqs:<region>:123456789012:*"
    },
    {
        "Sid": "SNSPermission",
        "Effect": "Allow",
        "Action": [
            "sns:GetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:<region>:123456789012:*"
    },
    {
        "Sid": "KMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey",
            "kms:ListAliases"
        ],
        "Resource": "arn:aws:kms:<region>:123456789012:key/
<key-id>"
    },
    {
        "Sid": "LambdaPermission",
        "Effect": "Allow",
        "Action": [
            "lambda:GetPolicy",
            "lambda:GetFunction"
        ]
    }

```

```

        ],
        "Resource":
"arn:aws:lambda:<region>:123456789012:function:*"
    },
    {
        "Sid": "IAMPermission",
        "Effect": "Allow",
        "Action": [
            "iam:GetContextKeysForCustomPolicy",
            "iam:SimulateCustomPolicy",
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermission",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationStepExecutions"
        ],
        "Resource": "*"
    }
]
}

```

指示

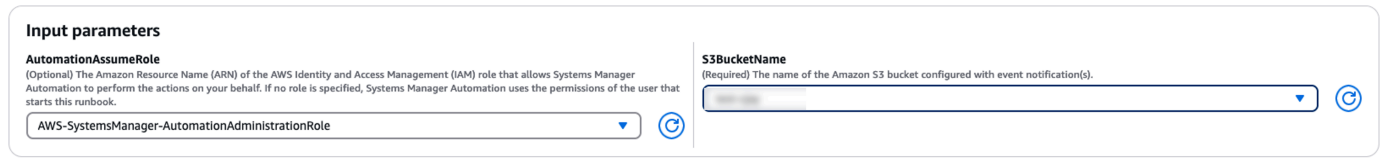
請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-TroubleshootS3EventNotifications](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- S3BucketName (必要)：

使用事件通知設定的 Amazon S3 儲存貯體名稱 (Amazon S3)。



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).

AWS-SystemsManager-AutomationAdministrationRole

4. 選取執行。
5. 自動化會啟動。
6. 文件會執行下列步驟：

- ValidateInputs

驗證提供的 Amazon S3 儲存貯體屬於執行自動化的相同帳戶，並擷取儲存貯體託管的區域。

- GetBucketNotificationConfiguration

呼叫 GetBucketNotificationConfiguration API 來檢閱使用 Amazon S3 儲存貯體和格式輸出設定的事件通知。

- BranchOnSQSResourcePolicy

有關事件通知中是否有 Amazon SQS 資源的分支。

- ValidateSQSResourcePolicy

驗證 Amazon SQS 佇列屬性上的資源政策具有 Amazon S3 的 `sqs:SendMessage` 許可。如果 Amazon SQS 資源已加密，會檢查加密是否未使用預設 AWS KMS 金鑰，即 `aws/sqs` 並檢查 AWS KMS 金鑰政策是否具有 Amazon S3 的許可。

- BranchOnSNSResourcePolicy

有關事件通知中是否有 Amazon SNS 資源的分支。

- ValidateSNSResourcePolicy

驗證 Amazon SNS 主題屬性上的資源政策具有 Amazon S3 的 `sns:Publish` 許可。如果 Amazon SNS 資源已加密，會檢查加密是否未使用預設 AWS KMS 金鑰，即 `aws/sns` 並檢查 AWS KMS 金鑰政策是否具有 Amazon S3 的許可。

- BranchOnLambdaFunctionResourcePolicy

有關事件通知中是否有 AWS Lambda 函數的分支。

- ValidateLambdaFunctionResourcePolicy

驗證 AWS Lambda 函數上的資源政策具有 Amazon S3 的 `lambda:InvokeFunction` 許可。

- GenerateReport

傳回 Runbook 步驟輸出的詳細資訊，以及解決使用 Amazon S3 儲存貯體設定之事件通知的任何問題的建議。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- Amazon SQS 事件通知

如果使用 Amazon SQS Amazon S3 目的地通知，Amazon SQS 佇列的清單會與檢查結果一起顯示。報告包含 Amazon SQS 資源檢查、Amazon SQS 存取政策檢查、AWS KMS 金鑰檢查、AWS KMS 金鑰狀態檢查和 AWS KMS 金鑰政策檢查。

- Amazon SNS 事件通知

如果使用 Amazon S3 儲存貯體設定了 Amazon SNS 目的地通知，Amazon SNS 主題的清單會與檢查結果一起顯示。Amazon S3 報告包含 Amazon SNS 資源檢查、Amazon SNS 存取政策檢查、AWS KMS 金鑰檢查、AWS KMS 金鑰狀態檢查和 AWS KMS 金鑰政策檢查。

- AWS Lambda 事件通知

如果使用 Amazon S3 儲存貯體設定了 AWS Lambda 目的地通知，則 Lambda 函數的清單會與檢查結果一起顯示。報告包含 Lambda 資源檢查和 Lambda 存取政策檢查。

```

▼ 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: 12345678901234567890123456789012
| 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:SAW-Core-TroubleshootS3EventNotification-EncryptedTopic | 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
|-----

```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSSupport-ContainS3Resource

Description

AWSSupport-ContainS3Resource Runbook 為 [支援自動化工作流程 \(SAW\) Runbook：包含遭入侵的 AWS Amazon S3 儲存貯體](#) 中所述的程序提供自動化解決方案

Important

- 此 Runbook 會執行需要提升權限的各種操作，例如修改 Amazon S3 儲存貯體政策、標籤和公有存取組態。這些動作可能會導致權限提升，或影響依賴目標 Amazon S3 儲存貯體的其他工作負載。您應該檢閱授予 AutomationAssumeRole 參數所指定角色的許可，並確保這些許可適用於預期的使用案例。如需 IAM 許可的詳細資訊，請參閱下列 AWS 文件：[Identity and Access Management \(IAM\) PermissionsAWS AWS Systems Manager Automation Permissions](#)。
- 此 Runbook 會執行可能導致工作負載無法使用或中斷的變動動作。具體而言，Contain動作會封鎖對指定 Amazon S3 儲存貯體的所有存取，SecureRoles 參數中指定的角色除外。這可能會影響依賴目標 Amazon S3 儲存貯體的任何應用程式或服務。
- 在Contain動作期間，如果原始儲存貯體的組態尚未存在，此 Runbook 可能會建立額外的 Amazon S3 儲存貯體（由 BackupS3BucketName 參數指定）來存放其備份。
- 如果 Action 參數設定為 Restore，此 Runbook 會嘗試根據存放在儲存貯體中的備份，將 Amazon S3 儲存BackupS3BucketName貯體的組態還原為其原始狀態。不過，還原程序可能會失敗，使 Amazon S3 儲存貯體處於不一致的狀態。Runbook 提供在發生此類失敗時手動還原的說明，但您應該準備好在還原過程中處理潛在問題。

建議您徹底檢閱 Runbook、了解其潛在影響，並在非生產環境中進行測試，然後再在您的生產環境中執行。

如何運作？

此 Runbook 的運作方式會根據資源類型和動作而有所不同：

- 對於 Amazon S3 一般用途儲存貯體 Containment：自動化會封鎖對儲存貯體的公開存取、停用 ACL 組態、強制執行儲存貯體擁有者物件擁有權，並將拒絕所有 Amazon S3 動作的限制儲存貯體政策放入儲存貯體，但允許列出的 IAM 角色除外。
- 對於 Amazon S3 一般用途物件 Containment：自動化會封鎖對儲存貯體的公開存取、停用 ACL 組態、強制執行儲存貯體擁有者物件擁有權，並將限制性儲存貯體政策放在物件上拒絕所有 Amazon S3 動作，但允許列出的 IAM 角色除外。
- 對於 Amazon S3 Directory Bucket Containment：自動化會將拒絕所有 Amazon S3 動作的限制儲存貯體政策放入儲存貯體，但允許列出的 IAM 角色除外。
- 對於 Amazon S3 一般用途儲存貯體 Restore：自動化會在遏制之前將封鎖公開存取組態、儲存貯體 ACL 組態、儲存貯體擁有者物件擁有權和儲存貯體政策還原為初始組態。
- 對於 Amazon S3 一般用途物件 Restore：自動化會在遏制之前，將封鎖公開存取組態、儲存貯體 ACL 組態、物件 ACL 組態、儲存貯體擁有者物件擁有權和儲存貯體政策還原至初始組態。
- 對於 Amazon S3 Directory Bucket Restore：自動化會在遏制之前將儲存貯體政策還原至初始組態。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

/

所需的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

以下是授予 必要許可的 IAM 政策範例AutomationAssumeRole：

```
{
  "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": "*"
  }
]
}

```

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSSupport-ContainS3Resource](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - BucketName (必要)：
 - 描述：(必要) Amazon S3 儲存貯體的名稱。
 - 類型：AWS::S3::Bucket::Name
 - 動作 (必要)：
 - 描述：(必要) 選取 Contain 以隔離 Amazon S3 資源 Restore，或嘗試從先前的備份將資源組態還原至其原始狀態。
 - 類型：字串
 - 允許的值：Contain|Restore
 - DryRun (選用)：
 - 描述：(選用) 當設定為 true 時，自動化不會對目標 Amazon S3 資源進行任何變更，而是輸出其嘗試變更的內容。預設值：true。
 - 類型：布林值
 - 允許的值：true|false
 - BucketKeyName (選用)：
 - 描述：(選用) 您要包含或還原之 Amazon S3 物件的金鑰。在物件層級遏制期間使用。

- 類型：字串
- 允許模式：`^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}$`
- BucketRestrictAccess (條件式)：
 - 描述：(條件式) 在執行遏制動作後，允許存取目標 Amazon S3 資源的 IAM 使用者或角色 ARN。當 Action 設為 時，需要此參數 Contain。
 - 類型：StringList
 - 允許模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- TagIdentifier (選用)：
 - 描述：(選用) Key=BatchId, Value=78925 格式的標籤，將在遏制工作流程期間新增至此 Runbook 建立或修改的資源。
 - 類型：字串
 - 允許模式：`^$|^([Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/\\@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/\\@a-zA-Z0-9]{0,128})$`
- BackupS3BucketName (條件式)：
 - 描述：(條件式) 將 Action 設定為 時要備份目標資源組態的 Amazon S3 儲存貯體，Contain 或將 Action 設定為 時要從 還原組態 Restore。
 - 類型：AWS::S3::Bucket::Name
- BackupS3KeyName (條件式)：
 - 描述：(條件式) 如果 Action 設定為 Restore，這會指定自動化用來嘗試還原目標資源組態的 Amazon S3 金鑰。
 - 類型：字串
 - 允許模式：`^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}$`
- BackupS3BucketAccess (條件式)：
 - 描述：(條件式) 在執行遏制動作後，允許存取備份 Amazon S3 儲存貯體的 IAM 使用者或角色 ARN。當 Action 為 時，此參數為必要 Contain。
 - 類型：StringList
 - 允許模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- AutomationAssumeRole (選用)：

- 描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 IAM 角色的 Amazon Resource Name (ARN)。
- 類型：AWS::IAM::Role::Arn

4. 選取執行。

5. 自動化會啟動。

6. 文件會執行下列步驟：

- validateRequiredInputs

根據指定的動作驗證所需的自動化輸入參數。

- assertBucketExists

檢查目標 Amazon S3 儲存貯體是否存在並可存取。

- backupBucketPreChecks

檢查備份 Amazon S3 儲存貯體是否可能授予對其物件的公開讀取或寫入存取權。

- backupTargetBucketMetadata

描述目標 Amazon S3 儲存貯體的目前組態，並將備份上傳至指定的備份 Amazon S3 儲存貯體。

- containBucket

執行儲存貯體層級操作，以包含目標 Amazon S3 儲存貯體。

- BranchOnActionAndMode

根據輸入參數 Action 和 DryRun 分支自動化。

- RestoreInstanceConfiguration

從備份還原 Amazon S3 儲存貯體組態。

- containFinalOutput

以可讀取的格式整合遏制活動。

- ReportContain

輸出遏制動作的試轉詳細資訊。

- ReportRestore

輸出還原動作的試轉詳細資訊。

- ReportRestoreFailure

提供在還原工作流程失敗案例期間還原 Amazon S3 儲存貯體原始組態的說明。

- `ReportContainmentFailure`

提供在遏制工作流程失敗情況下還原 Amazon S3 儲存貯體原始組態的說明。

- `FinalOutput`

輸出遏制動作的詳細資訊。

7. 執行完成後，請檢閱輸出區段以取得執行的詳細結果：

- `ContainFinalOutput.Output`

當 `DryRun` 設定為 `False` 時，輸出此 Runbook 所執行之遏制動作的詳細資訊。

- `RestoreFinalOutput.Output`

當 `DryRun` 設定為 `False` 時，輸出此 Runbook 所執行還原動作的詳細資訊。

- `ContainS3ResourceDryRun.Output`

當 `DryRun` 設定為 `True` 時，輸出此 Runbook 所執行之遏制動作的詳細資訊。

- `RestoreS3ResourceDryRun.Output`

將 `DryRun` 設定為 `True` 時，輸出此 Runbook 所執行還原動作的詳細資訊。

- `ReportContainmentFailure.Output`

提供在遏制工作流程失敗案例期間還原目標 Amazon S3 資源原始組態的說明。

- `ReportRestoreFailure.Output`

提供在還原工作流程失敗案例期間還原目標 Amazon S3 資源原始組態的說明。

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定 自動化](#)
- [支援自動化工作流程](#)

Amazon SES

AWS Systems Manager 自動化為 Amazon Simple Email Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSSupport-AnalyzeSESMessageSendingStatus](#)

AWSSupport-AnalyzeSESMessageSendingStatus

描述

AWSSupport-AnalyzeSESMessageSendingStatus 自動化 Runbook 摘要未傳遞電子郵件訊息的電子郵件交付狀態，並為您提供建議，以解決未交付的原因。Runbook 會擷取存放在 Amazon SES 發佈的 Amazon CloudWatch Logs 群組中的 Amazon Simple Email Service (Amazon SES 電子郵件傳送事件。如需 Amazon SES 事件發佈詳細資訊，請參閱[使用 Amazon Simple Email Service 事件發佈進行監控](#)。Runbook 也提供摘要和電子郵件傳遞的時間軸，以及可能影響未傳遞電子郵件訊息的建議。您可以在每個執行的輸出區段中找到這些訊息。請注意，此 Runbook 只能在事件存放區部署之後對事件進行疑難排解。

如何運作？

Runbook 會執行下列步驟：

- 檢查相同 CloudWatch Logs 群組的並行自動化執行。
- 分析與自動化參數提供的訊息 IDs 對應的 Amazon SES 事件。
- 輸出交付摘要至自動化執行的輸出區段。

Important

- 執行此 Runbook 之前，您必須將已發佈的 Amazon SES 事件存放至自動化參數指定的 CloudWatch Logs 日誌群組。此 Runbook 只會分析存放在日誌群組中的 Amazon SES 事件。

執行此自動化 (主控台)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- logs:StartQuery
- logs:GetQueryResults
- ses:GetIdentityMailFromDomainAttributes
- ses:GetSendQuota
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

指示

請依照下列步驟設定自動化：

1. 在文件下的 Systems Manager [AWSsupport-AnalyzeSESMessagesSendingStatus](#) 中導覽至 。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：
(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN) ，
允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager
Automation 會使用啟動此 Runbook 之使用者的許可。
 - MessageIds (必要)

您想要分析的 Amazon Simple Email Service 事件的逗號分隔 Amazon Simple Email Service 訊息 IDs。

- CloudWatchLogsGroup (選用)

存放 Amazon Simple Email Service 事件的 Amazon CloudWatch Logs 群組。預設日誌群組名稱為 `/ses/sending_event_logs`。如果您想要使用預設日誌群組以外的其他日誌群組，請在此欄位輸入您的日誌群組名稱。」，

- QueryStartTime (選用)

事件分析時間範圍的開始時間。有效時間格式為 ISO8601 (例如 ``yyyy-MM-ddTHH:mm:ss``、``1970-01-01T00:00:00``)。預設日期時間為 30 天前。

- QueryEndTime (選用)

事件分析時間範圍的結束時間。有效時間格式為 ISO8601 (例如 ``yyyy-MM-ddTHH:mm:ss``、``1970-01-01T00:00:00``)。預設日期時間是目前時間。

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.



MessageIds

(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

StringList

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

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. 選取執行。
5. 自動化會啟動。
6. 文件會執行下列步驟：

- **CheckConcurrency:**

確保只有一個以 Amazon CloudWatch Logs 群組為目標的 Runbook 執行。如果 Runbook 找到另一個以相同日誌群組為目標的執行，則會傳回錯誤並結束。

- **AnalyzeSesEvents:**

分析存放在自動化參數所指定 Amazon CloudWatch Logs 群組中的 Amazon Simple Email Service 事件。

- **OutputFailureReason:**

步驟失敗時的輸出執行AnalyzeSESMessagesSendingStatus步驟失敗訊息。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

- 因退信而未交付電子郵件訊息的分析輸出

電子郵件訊息因退信而無法到達目的地信箱的自動化執行輸出。

```
▼ 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
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定 自動化](#)
- [支援自動化工作流程登陸頁面](#)

SageMaker AI

AWS Systems Manager 自動化為 Amazon SageMaker AI 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-DisableSageMakerNotebookRootAccess](#)

AWS-DisableSageMakerNotebookRootAccess

Description

AWS-DisableSageMakerNotebookRootAccess Runbook 會停用 Amazon SageMaker AI 筆記本執行個體的根存取權。在自動化期間，筆記本執行個體會停止以進行必要的變更。不支援 SageMaker AI Studio 筆記本執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- NotebookInstanceName

類型：字串

描述：(必要) 要停用根存取的 SageMaker AI 筆記本執行個體名稱。

- StartInstanceAfterUpdate

類型：布林值

預設：true

描述：(選用) 決定筆記本執行個體是否在停用根存取後啟動。此參數的預設設定為 true。如果設定為 true，執行個體會在停用根存取後啟動。如果設定為 false，則停用根存取後，執行個體會保持 stopped 狀態。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- sagemaker:DescribeNotebookInstance
- sagemaker:StartNotebookInstance
- sagemaker:StopNotebookInstance
- sagemaker:UpdateNotebookInstance

文件步驟

- CheckNotebookInstanceStatus (aws : executeAwsApi)：檢查筆記本執行個體的目前狀態。
- StopOrUpdateNotebookInstance (aws : branch)：根據筆記本執行個體狀態的分支。
- StopNotebookInstance (aws : executeAwsApi)：如果狀態為 `Running`，則啟動執行個體 `stopped`。
- WaitForInstanceToStop (aws : waitForAwsResourceProperty)：驗證執行個體為 `stopped`。
- UpdateNotebookInstance (aws : executeAwsApi)：停用筆記本執行個體的根存取權。
- WaitForNotebookUpdate (aws : waitForAwsResourceProperty)：確認根存取已停用且執行個體的狀態 `stopped`。
- ChooseInstanceStart (aws : branch)：根據執行個體是否應啟動的分支。

- StartNotebookInstance (aws : executeAwsApi) : 啟動筆記本執行個體。
- VerifyNotebookInstanceStatus (aws : waitForAwsResourceProperty) : 驗證執行個體是否在停用根存取available之前。
- VerifyNotebookInstanceRootAccess (aws : assertAwsResourceProperty) : 確認筆記本執行個體根存取設定已成功停用。

Secrets Manager

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Secrets Manager。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

AWSConfigRemediation-DeleteSecret

Description

AWSConfigRemediation-DeleteSecret Runbook 會刪除秘密和存放於 的所有版本 AWS Secrets Manager。您可以選擇性地指定復原時段，在此期間可以還原秘密。如果您未指定 RecoveryWindowInDays 參數的值，則操作預設為 30 天。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- RecoveryWindowInDays

類型：整數

有效值：7-30

預設：30

描述：(選用) 您可以還原秘密的天數。

- SecretId

類型：字串

描述：(必要) 您要刪除之秘密的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- secretsmanager:DeleteSecret
- secretsmanager:DescribeSecret

文件步驟

- aws:executeAwsApi - 刪除您在 SecretId 參數中指定的秘密。
- aws:executeScript - 確認秘密已排定刪除。

AWSConfigRemediation-RotateSecret

Description

AWSConfigRemediation-RotateSecret Runbook 會輪換存放在其中的秘密 AWS Secrets Manager。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- RotationInterval

類型：間隔

有效值：1-365

描述：（必要）秘密輪換之間的天數。

- RotationLambdaArn

類型：字串

描述：（必要）可輪換秘密之函數的 AWS Lambda Amazon Resource Name (ARN)。

- SecretId

類型：字串

描述：（必要）您要輪換之秘密的 Amazon Resource Name (ARN)。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

文件步驟

- `aws:executeAwsApi` - 輪換您在 `SecretId` 參數中指定的秘密。
- `aws:executeScript` - 驗證已在秘密上啟用輪換。

安全中樞

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Security Hub。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-EnableSecurityHub](#)

AWSConfigRemediation-EnableSecurityHub

Description

AWSConfigRemediation-EnableSecurityHub Runbook 會為您執行自動化 AWS 區域 的 AWS 帳戶 和 啟用 AWS Security Hub (Security Hub)。如需 Security Hub 的相關資訊，請參閱AWS Security Hub 《使用者指南》中的[什麼是 AWS Security Hub ?](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- EnableDefaultStandards

類型：布林值

預設：true

描述：(必要) 如果設定為 true ，則會啟用 Security Hub 指定的預設安全標準。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- securityhub:DescribeHub
- securityhub:EnableSecurityHub
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文件步驟

- aws:executeAwsApi - 在目前帳戶和區域中啟用 Security Hub。
- aws:executeAwsApi - 驗證 Security Hub 已啟用。

AWS Shield

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS Shield。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

AWSPremiumSupport-DDoSResiliencyAssessment

Description

AWSPremiumSupport-DDoSResiliencyAssessment、AWS Systems Manager automation Runbook 可協助您檢查 DDoS 漏洞，並根據的 AWS Shield Advanced 保護來設定資源 AWS 帳戶。它為容易遭受分散式阻斷服務 (DDoS) 攻擊的資源提供組態設定報告。它用於收集、分析和評估下列資源：Amazon Route 53、Amazon Load Balancer、Amazon CloudFront 分佈 AWS Global Accelerator 和 AWS 彈性 IPs 以根據建議的 AWS Shield Advanced 保護最佳實務進行組態設定。最終組態報告可在您選擇的 Amazon S3 儲存貯體中作為 HTML 檔案提供。

如何運作？

此 Runbook 包含一系列針對已啟用公開存取的各種資源類型的檢查，以及它們是否已根據 [AWS DDoS 最佳實務白皮書](#) 中的建議設定保護。Runbook 會執行下列動作：

- 檢查 AWS Shield Advanced 的訂閱是否已啟用。
- 如果啟用，它會尋找是否有任何 Shield Advanced 受保護的資源。
- 它會尋找 中的所有全域和區域資源，AWS 帳戶 並檢查這些資源是否受到 Shield 保護。
- 它需要評估的資源類型參數、Amazon S3 儲存貯體名稱和 Amazon S3 儲存貯體 AWS 帳戶 ID (S3BucketOwner)。
- 它會將調查結果傳回為存放在提供的 Amazon S3 儲存貯體中的 HTML 報告。

輸入參數會 AssessmentType 決定是否對所有資源執行檢查。根據預設，Runbook 會檢查所有類型的資源。如果只選取 GlobalResources 或 RegionalResources 參數，則 Runbook 只會對選取的資源類型執行檢查。

Important

- 存取 AWSPremiumSupport-* Runbook 需要 Enterprise 或 Business Support 訂閱。如需詳細資訊，請參閱[比較 支援 計劃](#)。
- 此 Runbook 需要 ACTIVE [AWS Shield Advanced 訂閱](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- AssessmentType

類型：字串

描述：（選用）決定要評估 DDoS 彈性評估的資源類型。根據預設，Runbook 將評估全域和區域資源。對於區域資源，Runbook 會描述所有應用程式 (ALB) 和網路 (NLB) 負載平衡器，以及您 AWS 帳戶/區域中的所有 Auto Scaling 群組。

有效值：['Global Resources', 'Regional Resources', 'Global and Regional Resources']

預設：全域和區域資源

- S3BucketName

類型：AWS::S3::Bucket::Name

描述：(必要) 將上傳報告的 Amazon S3 儲存貯體名稱。

允許模式：`^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3BucketOwnerAccount

類型：字串

描述：(選用) AWS 帳戶 擁有 Amazon S3 儲存貯體的 。如果 Amazon S3 儲存貯體屬於不同的 ，請指定此參數 AWS 帳戶，否則您可以將此參數保留空白。

允許模式：`^$|^[0-9]{12,13}$`

- S3BucketOwnerRoleArn

類型：AWS::IAM::Role::Arn

描述：(選用) IAM 角色的 ARN，具有描述 Amazon S3 儲存貯體和 AWS 帳戶 封鎖公有存取組態的許可 AWS 帳戶。如果未指定此參數，則 Runbook 會使用啟動此 Runbook 的 AutomationAssumeRole 或 IAM 使用者 (如果 AutomationAssumeRole 未指定)。請參閱 Runbook 描述中的必要許可區段。

允許模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12,13}:role/.*$`

- S3BucketPrefix

類型：字串

描述：(選用) Amazon S3 內儲存結果之路徑的字首。

允許模式：`^[a-zA-Z0-9][-\./a-zA-Z0-9]{0,255}$|^$`

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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

自動化擔任角色的 IAM 政策範例

```
{
  "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::123456789012:role/
<AutomationAssumeRole-Name>",
    "Effect": "Allow"
  }
]
}

```

指示

1. 導覽至 AWS Systems Manager 主控台中的 [AWSPremiumSupport-DDoSResiliencyAssessment](#)。
2. 選取執行自動化
3. 針對輸入參數，輸入下列內容：
 - AutomationAssumeRole (選用)：

(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- **AssessmentType** (選用)：

決定要評估 DDoS 彈性評估的資源類型。根據預設，Runbook 會評估全域和區域資源。

- **S3BucketName** (必要)：

以 HTML 格式儲存評估報告的 Amazon S3 儲存貯體名稱。

- **S3BucketOwner** (選用)：

用於所有權驗證的 Amazon S3 儲存貯體 AWS 帳戶 ID。如果報告需要發佈到跨帳戶 Amazon S3 儲存貯體，則需要 AWS 帳戶 ID，如果 Amazon S3 儲存貯體與自動化啟動 AWS 帳戶相同，則為選用。

- **S3BucketPrefix** (選用)：

Amazon S3 內儲存結果之路徑的任何字首。

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::[redacted]: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

[redacted]

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.

[redacted]

4. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- **CheckShieldAdvancedState**：

驗證 是否已訂閱 AWS 帳戶 AWS Shield Advanced，以及 Runbook 是否可存取 Amazon S3 儲存貯體。

- **S3BucketSecurityChecks**：

檢查「S3BucketName」中指定的 Amazon S3 儲存貯體是否允許匿名或公有讀取或寫入存取許可、儲存貯體是否已啟用靜態加密，以及「S3BucketOwner」中提供的 ID AWS 帳戶 是否為 Amazon S3 儲存貯體的擁有者。

- BranchOnShieldAdvancedStatus :

根據 AWS Shield Advanced 訂閱狀態和/或 Amazon S3 儲存貯體擁有權狀態分支文件步驟。

- ShieldAdvancedConfigurationReview :

檢閱 Shield Advanced 組態，以確保有最少的必要詳細資訊。例如：AWS Shield 回應團隊 (SRT) 的 IAM 存取團隊、聯絡人清單詳細資訊和 SRT 主動參與狀態。

- ListShieldAdvancedProtections :

列出 Shield Protected Resources，並為每個服務建立一組受保護的資源。

- BranchOnResourceTypeAndCount :

根據資源類型參數的值和 Shield 保護的全域資源數目，分支文件步驟。

- ReviewGlobalResources :

檢閱 Shield Advanced 保護的全域資源，例如 Route 53 Hosted Zones、CloudFront Distributions 和 Global Accelerators。

- BranchOnResourceType :

如果為全域、區域或兩者，根據資源類型選擇分支文件步驟。

- ReviewRegionalResources :

檢閱 Shield Advanced 受保護的區域資源，例如 Application Load Balancer、Network Load Balancer、Classic Load Balancer、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體 (彈性 IPs)。

- SendReportToS3 :

將 DDoS 評估報告詳細資訊上傳至 Amazon S3 儲存貯體。

7. 完成後，評估報告 HTML 檔案的 URI 會在 Amazon S3 儲存貯體中提供：

報告成功執行 Runbook 的 S3 主控台連結和 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 ✔ Success	All executed steps 9	# Succeeded 9
# Failed 0	# Cancelled 0	# TimedOut 0

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [AWS Shield Advanced](#)

Amazon SNS

AWS Systems Manager 自動化為 Amazon Simple Notification Service 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)
- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

AWS-EnableSNSTopicDeliveryStatusLogging

Description

AWS-EnableSNSTopicDeliveryStatusLogging Runbook 會設定 HTTP、Amazon Data Firehose、LambdaPlatform application、或 Amazon Simple Queue Service (Amazon SQS) 端點的交付狀態記錄。這可讓 Amazon SNS 將失敗的提醒和成功提醒通知的範例百分比記錄到 Amazon CloudWatch。如果已針對主題設定交付狀態記錄，則 Runbook 會將現有的組態取代為您為輸入參數指定的新值。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- EndpointType

類型：字串

有效值：

- HTTP
- Firehose
- Lambda
- 應用程式
- SQS

描述：(必要) 您要記錄交付狀態通知訊息的 Amazon SNS 主題端點類型。

- TopicArn

類型：字串

描述：(必要) 您要為其設定交付狀態記錄的 Amazon SNS 主題 ARN。

- SuccessFeedbackRoleArn

類型：字串

描述：(必要) Amazon SNS 用來將日誌成功通知訊息傳送至 CloudWatch 的 IAM 角色 ARN。

- SuccessFeedbackSampleRate

類型：字串

有效值：0-100

描述：(必要) 指定 Amazon SNS 主題要取樣的成功訊息百分比。

- FailureFeedbackRoleArn

類型：字串

描述：(必要) Amazon SNS 用來將失敗通知訊息日誌傳送至 CloudWatch 的 IAM 角色 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:PassRole
- sns:GetTopicAttributes
- sns:SetTopicAttributes

文件步驟

- aws:executeAwsApi - 將 SuccessFeedbackRoleArn 參數的值套用至 Amazon SNS 主題。

- `aws:executeAwsApi` - 將 `SuccessFeedbackSampleRate` 參數的值套用至 Amazon SNS 主題。
- `aws:executeAwsApi` - 將 `FailureFeedbackRoleArn` 參數的值套用至 Amazon SNS 主題。
- `aws:executeScript` - 確認已在 Amazon SNS 主題上啟用交付狀態記錄。

輸出

`VerifyDeliveryStatusLoggingEnabled.GetTopicAttributesResponse` - `GetTopicAttributes` API 操作的回應。

`VerifyDeliveryStatusLoggingEnabled.VerifyDeliveryStatusLoggingEnabled` - 指出成功驗證交付狀態記錄的訊息。

AWSConfigRemediation-EncryptSNSTopic

Description

`AWSConfigRemediation-EncryptSNSTopic` Runbook 會在您使用 () 客戶受管金鑰指定的 Amazon Simple Notification Service AWS Key Management Service (Amazon SNS AWS KMS) 主題上啟用加密。此 Runbook 應僅用作基準，以確保您的 Amazon SNS 主題根據最低建議的安全最佳實務進行加密。我們建議使用不同的客戶受管金鑰加密多個主題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- KmsKeyArn

類型：字串

描述：(必要) 您要用來加密 Amazon SNS 主題之客戶受管金鑰的 AWS KMS Amazon Resource Name (ARN)。Amazon SNS

- TopicArn

類型：字串

描述：(必要) 您要加密之 Amazon SNS 主題的 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- sns:GetTopicAttributes
- sns:SetTopicAttributes

文件步驟

- aws:executeAwsApi - 加密您在 TopicArn 參數中指定的 Amazon SNS 主題。
- aws:assertAwsResourceProperty - 確認加密已在 Amazon SNS 主題上啟用。

AWS-PublishSNSNotification

Description

發佈通知至 Amazon SNS。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 訊息

類型：字串

描述：(必要) 要包含在 SNS 通知的訊息。

- TopicArn

類型：字串

描述：(必要) 要發佈通知之 SNS 主題的 ARN。

Amazon SQS

AWS Systems Manager 自動化為 Amazon Simple Queue Service (Amazon SQS) 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableSQSEncryption](#)

AWS-EnableSQSEncryption

Description

AWS-EnableSQSEncryption Runbook 可為 Amazon Simple Queue Service (Amazon SQS) 佇列啟用靜態加密。Amazon SQS 佇列可以使用 Amazon SQS 受管金鑰 (SSE-SQS) 或使用 AWS Key Management Service (AWS KMS) 受管金鑰 (SSE-KMS) 加密。您指派給佇列的金鑰必須具有金鑰政策，其中包含授權使用該佇列的所有主體的許可。啟用加密後，匿名SendMessage和對加密佇列的ReceiveMessage請求會遭到拒絕。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- QueueUrl

類型：字串

描述：（必要）您要啟用加密的 Amazon SQS 佇列 URL。

- KmsKeyId

類型：字串

描述：(選用) 用於加密的 AWS KMS 金鑰。此值可以是全域唯一識別符、別名或金鑰的 ARN，或是以 "alias/" 開頭的別名名稱。您也可以透過指定別名 `aws/sqs` 來使用 AWS 受管金鑰。

- `KmsDataKeyReusePeriodSeconds`

類型：字串

有效值：60-86400

預設：300

描述：(選用) Amazon SQS 佇列可以重複使用資料金鑰來加密或解密訊息的時間長度，然後再 AWS KMS 再次呼叫。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

文件步驟

- `SelectKeyType (aws:branch)`：根據指定金鑰的分支。
- `PutAttributeSseKms (aws:executeAwsApi)` - 更新 Amazon SQS 佇列以使用為加密指定的 AWS KMS 金鑰。
- `PutAttributeSseSqs (aws:executeAwsApi)` - 更新 Amazon SQS 佇列以使用預設金鑰進行加密。
- `VerifySqsEncryptionKms (aws:assertAwsResourceProperty)` - 驗證 Amazon SQS 佇列上已啟用加密。
- `VerifySqsEncryptionDefault (aws:assertAwsResourceProperty)` - 驗證 Amazon SQS 佇列上已啟用加密。

Step Functions

AWS Systems Manager 自動化為 AWS Step Functions（步驟函數）提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-EnableStepFunctionsStateMachineLogging](#)

AWS-EnableStepFunctionsStateMachineLogging

Description

AWS-EnableStepFunctionsStateMachineLogging Runbook 會在您指定的 AWS Step Functions 狀態機器上啟用或更新記錄。最低記錄層級必須設定為 ALL、ERROR 或 FATAL。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- Level

類型：字串

有效值：ALL | ERROR | FATAL

描述：（必要）您要啟用加密的 Amazon SQS 佇列 URL。

- LogGroupArn

類型：字串

描述：（必要）您要傳送狀態機器日誌的 Amazon CloudWatch Logs 日誌群組 ARN。

- StateMachineArn

類型：字串

描述：（必要）您要啟用登入之狀態機器的 ARN。

- IncludeExecutionData

類型：布林值

預設：False

描述：（選用）判斷日誌中是否包含執行資料。

- TracingConfiguration

類型：布林值

預設：False

描述：（選用）判斷是否啟用 AWS X-Ray 追蹤。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine
- states:UpdateStateMachine

文件步驟

- `EnableStepFunctionsStateMachineLogging` (`aws:executeAwsApi`) - 使用指定的記錄組態更新指定的狀態機器。
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`) - 確認已為指定的狀態機器啟用記錄。

輸出

- `EnableStepFunctionsStateMachineLogging.Response` - `UpdateStateMachine` API 呼叫的回應。

Systems Manager

AWS Systems Manager 自動化為 Systems Manager 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [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

Description

AWS-BulkDeleteAssociation Runbook 可協助您一次刪除最多 50 個 Systems Manager State Manager 關聯。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- AssociationIds

類型：StringList

描述：（必要）以逗號分隔的清單，列出您要刪除的關聯 IDs。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:DeleteAssociation`

文件步驟

- `aws:executeScript` - 刪除您在 `AssociationIds` 參數中指定的關聯。

AWS-BulkEditOpsItems

Description

AWS-BulkEditOpsItems Runbook 可協助您編輯 AWS Systems Manager OpsItems 的狀態、嚴重性、類別或優先順序。此自動化一次最多可以編輯 50 OpsItems。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 類別

類型：字串

有效值：

- 可用性
- 成本
- 未變更
- 效能
- 復原
- 安全

預設：無變更

描述：(選用) 您要為已編輯 OpsItems 指定的新類別。

- OpsItemIds

類型：StringList

描述：(必要) 您想要編輯的 OpsItems IDs 逗號分隔清單 (例如 oi-XXXXXXXXXXXXX , oi-XXXXXXXXXXXXX)。

- 優先順序

類型：字串

有效值：

- 未變更
- 1
- 2
- 3
- 4
- 5

預設：無變更

描述：(選用) 已編輯 OpsItems 相對於系統中其他 OpsItems 的重要性。

- 嚴重性

類型：字串

有效值：

- 未變更

- 1
- 2
- 3
- 4

預設：無變更

描述：(選用) 已編輯 OpsItems 的嚴重性。

- WaitTimeBetweenEditsInSecs

類型：字串

有效值：0.0-2.0

預設：0.8

描述：(選用) 自動化在呼叫 UpdateOpsItems 操作之間等待的時間。

- Status

類型：字串

有效值：

- InProgress
- 未變更
- 開啟
- Resolved (已解決)

預設：無變更

描述：(選用) 已編輯 OpsItems 的新狀態。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文件步驟

- `aws:executeScript` - 根據您為 `Category`、`OpsItemIds` 參數指定的 `PrioritySeverity`，編輯您在 `Status` 參數中指定的 `OpsItems`。

AWS-BulkResolveOpsItems

Description

AWS-BulkResolveOpsItems Runbook resolves AWS Systems Manager OpsItems 符合您指定的篩選條件。您也可以指定 `OpsItemId`，以使用 `OpsInsightsId` 參數新增至解析的 `OpsItems`。如果您指定 `S3BucketName` 參數的值，結果摘要會傳送至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。若要在結果摘要傳送到 Amazon S3 儲存貯體後收到通知，請指定 `SnsTopicArn` 參數的值。此自動化一次最多可解析 1,000 `OpsItems`。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 篩選條件

類型：字串

描述：（必要）傳回您要解析之 OpsItems 的篩選條件鍵值對。例如，`[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`。若要進一步了解可用於篩選 OpsItems 回應的選項，請參閱 AWS Systems Manager API 參考 中的 [OpsItemFilters](#)。

- OpsInsightId

類型：字串

描述：（選用）您要新增至解析 OpsItems 的相關資源識別符。

- S3BucketName

類型：字串

描述：（選用）您要傳送結果摘要的 Amazon S3 儲存貯體名稱。

- SnsMessage

類型：字串

描述：（選用）您希望 Amazon Simple Notification Service (Amazon SNS) 在自動化完成時傳送的通知。

- SnsTopicArn

類型：字串

描述：（選用）當結果摘要傳送到 Amazon S3 時，您要通知的 Amazon SNS 主題 ARN。Amazon S3

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文件步驟

- `aws:executeScript` - 根據您指定的篩選條件收集並解析 OpsItems。如果您為 `OpsInsightId` 參數指定值，則會將該值新增為相關資源。
- `aws:executeScript` - 如果您為 `S3BucketName` 參數指定值，則結果摘要會傳送至 Amazon S3 儲存貯體。
- `aws:executeScript` - 如果您為 `SnsTopicArn` 參數指定了值，則結果摘要傳送至 Amazon S3 後，系統會傳送通知至 Amazon SNS 主題，如果指定，則會包含 `SnsMessage` 參數值。Amazon S3

AWS-ConfigureMaintenanceWindows

Description

AWS-ConfigureMaintenanceWindows Runbook 可協助您啟用或停用多個 Systems Manager 維護時段。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- MaintenanceWindows

類型：StringList

描述：（必要）您想要啟用或停用的維護時段 IDs 的逗號分隔清單。

- MaintenanceWindowsStatus

類型：字串

有效值："True" | "False"

預設：「False」

描述：（必要）判斷是否啟用或停用維護時段。指定「True」以啟用維護時段，並指定「False」以停用它們。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:GetMaintenanceWindow
- ssm:UpdateMaintenanceWindow

文件步驟

- aws:executeScript - 收集您在 MaintenanceWindows 參數中指定的維護時段狀態，並啟用或停用維護時段。

AWS-CreateManagedLinuxInstance

Description

建立針對 Systems Manager 設定的 Linux EC2 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- Amild

類型：字串

描述：用來啟動執行個體的（必要）AMI ID。

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- GroupName

類型：字串

預設：SSMSecurityGroupForLinuxInstances

描述：(必要) 要建立的安全群組之名稱。

- HttpTokens

類型：字串

有效值：選用 | 必要

預設：選用

描述：（選用）IMDSv2 使用字符支援的工作階段。將 HTTP 字符的使用設定為 optional 或 required，以判斷 IMDSv2 是選用還是必要。

- InstanceType

類型：字串

預設：t2.medium

描述：(必要) 要啟動的執行個體類型。預設為 t2.medium。

- KeyPairName

類型：字串

描述：(必要) 建立執行個體時要使用的金鑰對。

- RemoteAccessCidr

類型：字串

預設：0.0.0.0/0

描述：(必要) 建立安全群組，並將 SSH 連接埠 (連接埠範圍 22) 開放給 CIDR 指定的 IP (預設為 0.0.0.0/0)。如果安全群組已存在，則不會修改，規則也不會變更。

- RoleName

類型：字串

預設：SSMManagedInstanceProfileRole

描述：(必要) 要建立的角色之名稱。

- StackName

類型：字串

預設：CreateManagedInstanceStack{{automation:EXECUTION_ID}}

描述：(選用) 指定此 Runbook 使用的堆疊名稱

- SubnetId

類型：字串

預設：Default

描述：(必要) 新的執行個體會部署至此子網路或預設子網路 (若未指定)。

- VpcId

類型：字串

預設：Default

描述：（必要）如果未指定，新的執行個體將部署到此 Amazon Virtual Private Cloud (Amazon VPC) 或預設 Amazon VPC。

AWS-CreateManagedWindowsInstance

Description

為針對 Systems Manager Windows Server 設定的 建立 EC2 執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

參數

- Amild

類型：字串

預設：{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}

描述：用來啟動執行個體的（必要）AMI ID。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- **GroupName**

類型：字串

預設：SSMSecurityGroupForLinuxInstances

描述：(必要) 要建立的安全群組之名稱。

- **HttpTokens**

類型：字串

有效值：選用 | 必要

預設：選用

描述：(選用) IMDSv2 使用字符支援的工作階段。將 HTTP 字符的使用設定為 `optional` 或 `required`，以判斷 IMDSv2 是選用還是必要。

- **InstanceType**

類型：字串

預設：t2.medium

描述：(必要) 要啟動的執行個體類型。預設為 t2.medium。

- **KeyPairName**

類型：字串

描述：(必要) 建立執行個體時要使用的金鑰對。

- **RemoteAccessCidr**

類型：字串

預設：0.0.0.0/0

描述：(必要) 建立安全群組，並將 RDP 連接埠 (連接埠範圍 3389) 開放給 CIDR 指定的 IP (預設為 0.0.0.0/0)。如果安全群組已存在，則不會修改，規則也不會變更。

- RoleName

類型：字串

預設：SSMManagedInstanceProfileRole

描述：(必要) 要建立的角色之名稱。

- StackName

類型：字串

預設：CreateManagedInstanceStack{{automation:EXECUTION_ID}}

描述：(選用) 指定此 Runbook 使用的堆疊名稱

- SubnetId

類型：字串

預設：Default

描述：(必要) 新的執行個體會部署至此子網路或預設子網路 (若未指定)。

- VpcId

類型：字串

預設：Default

描述：(必要) 如果未指定，新的執行個體將部署到此 Amazon Virtual Private Cloud (Amazon VPC) 或預設 Amazon VPC。

AWSConfigRemediation-EnableCWLoggingForSessionManager

Description

AWSConfigRemediation-EnableCWLoggingForSessionManager Runbook 可讓 AWS Systems Manager Session Manager (Session Manager) 工作階段將輸出日誌儲存到 Amazon CloudWatch (CloudWatch) 日誌群組。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DestinationLogGroup

類型：字串

描述：(必要) CloudWatch 日誌群組的名稱。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm>CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

文件步驟

- `aws:executeScript` - 接受 CloudWatch 日誌群組，以更新存放 Session Manager 工作階段輸出日誌偏好設定的文件，或在不存在時建立一個。

AWS-ExportOpsDataToS3

Description

此 Runbook 會擷取 AWS Systems Manager Explorer 中的 OpsData 摘要清單，並將其匯出至指定 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的物件。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- columnFields

類型：StringList

描述：(必要) 要寫入輸出檔案的資料行欄位。

- 篩選條件

類型：字串

描述：(選用) 篩選 getOpsSummary 要求。

- resultAttribute

類型：字串

描述：(選用) getOpsSummary 要求的結果屬性。

- s3BucketName

類型：字串

描述：(必要) 要下載輸出檔案的 S3 儲存貯體。

- snsSuccessMessage

類型：字串

描述：(選用) 執行手冊完成時要傳送的訊息。

- snsTopicArn

類型：字串

描述：(必要) 下載完成時要通知的 Amazon Simple Notification Service (Amazon SNS) 主題 ARN。

- syncName

類型：字串

描述：(選用) 資源資料同步的名稱。

文件步驟

getOpsSummaryStep – 立即擷取最多 5,000 個 ops 摘要以匯出至 CSV 檔案。

輸出

OpsData 物件 – 如果執行手冊成功執行，您會在目標 S3 儲存貯體中找到匯出的 OpsData 物件。

AWS-ExportPatchReportToS3

Description

此 Runbook 會擷取修補程式管理員中的 AWS Systems Manager 修補程式摘要資料和修補程式詳細資訊清單，並將其匯出至指定 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的 .csv 檔案。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- assumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用執行本文件之使用者的許可。

- s3BucketName

類型：字串

描述：（必要）您要下載輸出檔案的 S3 儲存貯體。

- snsTopicArn

類型：字串

描述：（選用）下載完成時要通知的 Amazon Simple Notification Service (Amazon SNS) 主題 Amazon Resource Name (ARN)。

- snsSuccessMessage

類型：字串

描述：（選用）執行手冊完成時要傳送的訊息文字。

- targets

類型：字串

描述：（必要）執行個體 ID 或萬用字元 (*)，指出要報告特定執行個體或所有執行個體的修補程式資料。

文件步驟

ExportReportStep – 此步驟的動作取決於 targets 參數的值。如果 targets 格式為 instanceids=*，則步驟會擷取您帳戶中執行個體最多 10,000 個修補程式摘要，並將資料匯出至 .csv 檔案。

如果 targets 格式為 instanceids=<instance-id>，則步驟會擷取您帳戶中指定執行個體的修補程式摘要和所有修補程式，並將其匯出至 .csv 檔案。

輸出

PatchSummary/Patches 物件 – 如果執行手冊成功執行，匯出的修補程式報告物件會下載到您的目標 S3 儲存貯體。

AWS-SetupInventory

Description

為一或多個受管執行個體建立 Systems Manager 庫存關聯。系統會根據關聯中的排程，從您的執行個體收集中繼資料。如需詳細資訊，請參閱[AWS Systems Manager 庫存](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- 應用程式

類型：字串

預設：Enabled

描述：(選用) 收集已安裝之應用程式的中繼資料。

- AssociatedDocName

類型：字串

預設：AWS-GatherSoftwareInventory

描述：(選用) 用於從受管執行個體收集庫存的 Runbook 名稱。

- AssociationName

類型：字串

描述：(選用) 要指派給執行個體的庫存關聯名稱。

- AssocWaitTime

類型：字串

預設：PT5M

描述：(選用) 庫存收集在庫存關聯開始時間到達時應暫停的時間量。時間使用 ISO 8601 格式。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- AwsComponents

類型：字串

預設：Enabled

描述：(選用) 收集 amazon-ssm-agent 等 AWS 元件的中繼資料。

- CustomInventory

類型：字串

預設：Enabled

描述：(選用) 收集自訂庫存中繼資料。

- 檔案

類型：字串

描述：(選用) 收集執行個體之檔案的中繼資料。如需如何收集此類庫存資料的詳細資訊，請參閱[使用檔案和 Windows 登錄庫存](#)。需要 SSMAgent 2.2.64.0 或更新版本。Linux 範例：
`[{"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

類型：字串

預設：Enabled

描述：(選用) 收集執行個體的其他資訊，包括 CPU 型號、速度和核心數量等。

- InstanceIds

類型：字串

預設：*

描述：(必要) 您想要清查的 EC2 執行個體。

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- NetworkConfig

類型：字串

預設：Enabled

描述：(選用) 收集網路組態的中繼資料。

- OutputS3BucketName

類型：字串

描述：(選用) 您要寫入庫存日誌資料的 Amazon S3 儲存貯體名稱。

- OutputS3KeyPrefix

類型：字串

描述：(選用) 您要寫入庫存日誌資料的 Amazon S3 金鑰字首 (子資料夾)。

- OutputS3Region

類型：字串

描述：(選用) Amazon S3 AWS 區域 所在的 名稱。

- 排程

類型：字串

預設：cron(0 */30 * * * ? *)

描述：(選用) 庫存關聯排程的 Cron 運算式。預設為每 30 分鐘。

- 服務

類型：字串

預設：Enabled

描述：(選用，僅 Windows 作業系統，需要 SSMAgent 2.2.64.0 及更新版本) 收集服務組態的資料。

- WindowsRegistry

類型：字串

描述：(選用) 收集 Microsoft Windows 登錄機碼的中繼資料。如需如何收集此類庫存資料的詳細資訊，請參閱[使用檔案和 Windows 登錄庫存](#)。需要 SSM 代理程式 2.2.64.0 或更新版本。範例：[{"Path":"HKEY_CURRENT_CONFIG\System","Recursive":true},

```
{"Path": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Amazon\\MachineImage", "ValueNames":  
  ["AMIName"]}]
```

- WindowsRoles

類型：字串

預設：Enabled

描述：(選用) 收集執行個體上的 Windows 角色相關資訊。僅適用於 Windows 作業系統。需要 SSMAgent 2.2.64.0 或更新版本。

- WindowsUpdates

類型：字串

預設：Enabled

描述：(選用) 收集執行個體上所有 Windows Update 的資料。

AWS-SetupManagedInstance

Description

使用 Systems Manager 存取的 AWS Identity and Access Management (IAM) 角色設定執行個體。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InstanceId

類型：字串

描述：(必要) 要設定的 EC2 執行個體之 ID

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- RoleName

類型：字串

預設：SSMRoleForManagedInstance

描述：(選用) EC2 執行個體的 IAM 角色名稱。如果此角色不存在，則會建立此角色。指定此值時，請確認角色包含 AmazonSSMManagedInstanceCore 受管政策。

AWS-SetupManagedRoleOnEC2Instance

Description

使用 SSMRoleForManagedInstance 受管 IAM 角色設定執行個體，以進行 Systems Manager 存取。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InstanceId

類型：字串

描述：(必要) 要設定的 EC2 執行個體之 ID

- LambdaAssumeRole

類型：字串

描述：(選用) 角色的 ARN，允許由自動化建立的 Lambda 代您執行動作。如果未指定，則會建立暫時性角色來執行 Lambda 函數。

- RoleName

類型：字串

預設：SSMRoleForManagedInstance

描述：(選用) EC2 執行個體的 IAM 角色名稱。如果此角色不存在，則會建立此角色。指定此值時，請確認角色包含 AmazonSSMManagedInstanceCore 受管政策。

AWSsupport-TroubleshootManagedInstance

Description

AWSsupport-TroubleshootManagedInstance Runbook 可協助您判斷 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體為何未報告由 管理 AWS Systems Manager。此 Runbook 會檢閱執行個體的 VPC 組態，包括安全群組規則、VPC 端點、網路存取控制清單 (ACL) 規則和路由表。它也會

確認包含所需許可的 AWS Identity and Access Management (IAM) 執行個體設定檔已連接至執行個體。

 Important

此自動化 Runbook 不會評估 IPv6 規則。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- InstanceId

類型：字串

描述：(必要) 未報告為 Systems Manager 所管理的 Amazon EC2 執行個體 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `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`

文件步驟

- `aws:executeScript` - 收集執行個體PingStatus的。
- `aws:branch` - 根據執行個體是否已報告為 Systems Manager 管理的分支。
- `aws:executeAwsApi` - 收集執行個體的詳細資訊，包括 VPC 組態。
- `aws:executeScript` - 如果適用，會收集已部署以搭配 Systems Manager 使用的 VPC 端點相關其他詳細資訊，並確認連接到 VPC 端點的安全群組允許從執行個體的 TCP 連接埠 443 上的傳入流量。
- `aws:executeScript` - 檢查路由表是否允許流量流向 VPC 端點或公有 Systems Manager 端點。
- `aws:executeScript` - 檢查網路 ACL 規則是否允許流量流向 VPC 端點或公有 Systems Manager 端點。
- `aws:executeScript` - 檢查與執行個體相關聯的安全群組是否允許傳出流量到 VPC 端點或公有 Systems Manager 端點。

- `aws:executeScript` - 檢查連接至執行個體的執行個體描述檔是否包含提供必要許可的受管政策。
- `aws:branch` - 根據執行個體的作業系統進行分支。
- `aws:executeScript` - 提供 `ssmagent-toolkit-linux` shell 指令碼的參考。
- `aws:executeScript` - 提供 `ssmagent-toolkit-windows` PowerShell 指令碼的參考。
- `aws:executeScript` - 產生自動化的最終輸出。
- `aws:executeScript` - 如果執行個體 `PingStatus` 的是 `Online`，會傳回執行個體已由 Systems Manager 管理。

AWSSupport-TroubleshootPatchManagerLinux

Description

AWSSupport-TroubleshootPatchManagerLinux Runbook 會使用 中的工具 Patch Manager，針對可能導致 Linux 受管節點修補程式失敗的常見問題進行故障診斷 AWS Systems Manager。此 Runbook 的主要目標是識別修補程式命令失敗根本原因，並建議修補計畫。

如何運作？

AWSSupport-TroubleshootPatchManagerLinux Runbook 會考慮您提供的兩個執行個體 ID/命令 ID 進行故障診斷。如果未提供命令 ID，它會在提供的執行個體上選取過去 30 天內最新的失敗修補程式命令。檢查命令狀態、先決條件履行和作業系統分佈後，執行手冊會下載並執行日誌分析器套件。輸出包含問題根本原因，以及修正問題所需的動作。

文件類型

自動化

擁有者

Amazon

平台

- Amazon Linux 2 和 AL2023
- Red Hat Enterprise Linux 8.X 和 9.X
- Centos 8.X 和 9.X

- SUSE 15.X

參數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:SendCommand
- ssm:DescribeDocument
- ssm:GetCommandInvocation
- ssm:ListCommands
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:GetDocument
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

指示

請依照下列步驟設定自動化：

1. 在 AWS Systems Manager 主控台 [AWSsupport-TroubleshootPatchManagerLinux](#) 中導覽至。
2. 選擇 Execute automation (執行自動化)。
3. 針對輸入參數，輸入下列項目：

- InstanceId (必要)：

使用互動式執行個體選擇器，選擇修補程式命令失敗的 Linux 型 SSM 受管節點 (Amazon Elastic Compute Cloud (Amazon EC2) 或混合啟動伺服器) ID，或手動輸入 SSM 受管執行個體的 ID。

- AutomationAssumeRole (選用)：

輸入允許自動化代表您執行動作的 IAM 角色 ARN。如果未指定角色，Automation 會使用啟動此 Runbook 的使用者許可。

- RunCommandId (選用)：

輸入AWS-RunPatchBaseline文件的失敗執行命令 ID。如果您未提供命令 ID，則 Runbook 會在所選執行個體上尋找過去 30 天內最新的失敗修補程式命令。

Input parameters

InstanceId
 (Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.

☒ Show interactive instance picker

i-0

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.

42e

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- CheckConcurrency：

確保只有一個針對相同執行個體的此 Runbook 執行。如果 Runbook 找到另一個以相同執行個體為目標的進行中執行，則會傳回錯誤並結束。

- ValidateCommandID：

驗證是否為 AWS-RunPatchBaseline SSM 文件執行提供的命令 ID 做為輸入參數。如果未提供命令 ID，則 Runbook 會考慮AWS-RunPatchBaseline過去 30 天內所選執行個體上的最新失敗執行。

- BranchOnCommandStatus：

確認提供的命令的狀態失敗。否則，執行手冊會結束執行，並產生報告，指出提供的命令已成功執行。

- VerifyPrerequisites：

確認符合上述先決條件。

- GetPlatformDetails：

擷取作業系統 (OS) 分佈和版本。

- GetDownloadURL：

擷取 PatchManager Log Analyzer 套件的下載 URL。

- EvaluatePatchManagerLogs：

下載並執行執行個體上的 PatchManager Log Analyzer python 套件，以評估日誌檔案。

- GenerateReport :

產生 Runbook 執行的最終報告，其中包含已識別的問題和建議的解決方案。

7. 完成後，請檢閱輸出區段以取得執行的詳細結果：

```
▼ Outputs

GenerateReportOutput
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
```

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWSsupport-TroubleshootSessionManager

Description

AWSsupport-TroubleshootSessionManager Runbook 可協助您疑難排解常見問題，這些常見問題會讓您無法使用 Session Manager 連線至受管 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。Session Manager 是 中的工具 AWS Systems Manager。此 Runbook 會檢查下列項目：

- 檢查執行個體是否在 Systems Manager 管理的情況下執行和報告。
- 如果執行個體未報告為由 Systems Manager 管理，則執行 AWSsupport-TroubleshootManagedInstance Runbook。

- 檢查執行個體上安裝的 SSM Agent 版本。
- 檢查包含 Session Manager 建議 AWS Identity and Access Management (IAM) 政策的執行個體描述檔是否連接到 Amazon EC2 執行個體。
- 從執行個體收集 SSM Agent 日誌。
- 分析您的 Session Manager 偏好設定。
- 執行 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook 以分析執行個體與 Session Manager、AWS Key Management Service (AWS KMS)、Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs (CloudWatch Logs) 端點的連線。

考量

- 不支援混合受管節點。
- 此 Runbook 只會檢查建議的受管 IAM 政策是否連接到執行個體描述檔。它不會分析執行個體描述檔中包含的 IAM 或 AWS KMS 許可。

Important

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook 使用 [VPC Reachability Analyzer](#) 來分析來源和服務端點之間的網路連線。每個來源和目的地之間的分析執行都會向您收取費用。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- InstanceId

類型：字串

描述：(必要) 您使用 Session Manager 無法連線的 Amazon EC2 執行個體 ID。

- SessionPreferenceDocument

類型：字串

預設：SSM-SessionManagerRunShell

描述：(選用) 工作階段偏好設定文件的名稱。如果您在啟動工作階段時未指定自訂工作階段偏好設定文件，請使用預設值。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

文件步驟

1. `aws:waitForAwsResourceProperty`：最多等待 6 分鐘，讓目標執行個體通過狀態檢查。
2. `aws:executeScript`：剖析工作階段偏好設定文件。
3. `aws:executeAwsApi`：取得連接至執行個體之執行個體描述檔的 ARN。
4. `aws:executeAwsApi`：檢查您的執行個體是否報告為由 Systems Manager 管理。
5. `aws:branch`：根據執行個體是否報告為 Systems Manager 管理的分支。
6. `aws:executeScript`：檢查安裝在執行個體上的 SSM 代理程式是否支援 Session Manager。
7. `aws:branch`：根據執行個體的平台進行分支，以收集 `ssm-cli` 日誌。
8. `aws:runCommand`：`ssm-cli` 從 Linux 或 macOS 執行個體收集日誌輸出。
9. `aws:runCommand`：`ssm-cli` 從 Windows 執行個體收集日誌輸出。
10. `aws:executeScript`：剖析 `ssm-cli` 日誌。
11. `aws:executeScript`：檢查建議的 IAM 政策是否連接到執行個體描述檔。

- 12aws:branch : 決定是否根據ssm-cli日誌評估ssmmessages端點連線能力。
- 13aws:executeAutomation : 評估執行個體是否可以連線至ssmmessages端點。
- 14aws:branch : 決定是否根據ssm-cli日誌和工作階段偏好設定評估 Amazon S3 端點連線能力。
- 15aws:executeAutomation : 評估執行個體是否可以連線至 Amazon S3 端點。
- 16aws:branch : 決定是否根據ssm-cli日誌和工作階段偏好設定評估 AWS KMS 端點連線能力。
- 17aws:executeAutomation : 評估執行個體是否可以連線至 AWS KMS 端點。
- 18aws:branch : 決定是否根據ssm-cli日誌和工作階段偏好設定評估 CloudWatch Logs 端點連線能力。
- 19aws:executeAutomation : 評估執行個體是否可以連線至 CloudWatch Logs 端點。
- 20aws:executeAutomation : 執行 AWSSupport-TroubleshootManagedInstance Runbook。
- 21aws:executeScript : 編譯先前步驟的輸出並輸出報告。

Outputs

- generateReport.EvalReport - Runbook 以純文字執行的檢查結果。

第三方

AWS Systems Manager 自動化為第三方產品和服務提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

AWS-CreateJiraIssue

Description

在 Jira 建立問題。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AssigneeName

類型：字串

描述：(選用) 應指派問題之人員的使用者名稱。

- DueDate

類型：字串

描述：(選用) 問題的到期日，格式為 yyyy-mm-dd。

- IssueDescription

類型：字串

描述：(必要) 問題的詳細說明。

- IssueSummary

類型：字串

描述：(必要) 問題的簡要說明。

- IssueTypeName

類型：字串

描述：(必要) 您要建立的問題類型名稱 (例如，任務、子任務、錯誤等)。

- JiraURL

類型：字串

描述：(必要) Jira 執行個體的 URL。

- JiraUsername

類型：字串

描述：(必要) 要建立問題的使用者名稱。

- PriorityName

類型：字串

描述：(選用) 問題優先順序的名稱。

- ProjectKey

類型：字串

描述：(必要) 應該在其中建立問題之專案的金鑰。

- SSMPParameterName

類型：字串

描述：(必要) 包含 Jira 使用者 API 金鑰或密碼之加密 SSM 參數的名稱。

文件步驟

`aws:createStack` - 建立 CloudFormation 堆疊以建立 Lambda IAM 角色和函數。

`aws:invokeLambdaFunction` - 叫用 Lambda 函數來建立 Jira 問題

`aws:deleteStack` - 刪除已建立的 CloudFormation 堆疊。

輸出

Issued：新建立的 Jira 問題 ID

AWS-CreateServiceNowIncident

Description

在 ServiceNow 事件表格中建立事件。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 類別

類型：字串

描述：(選用) 事件的類別。

有效值：無 | 查詢/說明 | 軟體 | 硬體 | 網路 | 資料庫

預設值：無

- 描述

類型：字串

描述：(必要) 有關事件的詳細說明。

- 影響

類型：字串

摘要：(選用) 事件對業務造成的影響。

有效值：高 | 中 | 低

預設值：低

- ServiceNowInstanceUsername

類型：字串

描述：(必要) 要建立事件的使用者名稱。

- ServiceNowInstancePassword

類型：字串

描述：(必要) 包含 ServiceNow 使用者密碼之加密 SSM 參數的名稱。

- ServiceNowInstanceURL

類型：字串

描述：(必要) ServiceNow 執行個體的 URL

- ShortDescription

類型：字串

描述：(必要) 事件的簡短描述。

- Subcategory

類型：字串

描述：(選用) 事件的子類別。

有效值：無 | 防毒 | 電子郵件 | 內部應用程式 | 作業系統 | CPU | 磁碟 | 鍵盤 | 硬體 | 記憶體 | 監視器 | 滑鼠 | DHCP | DNS | IP 地址 | VPN | 無線 | DB2 | MS SQL Server | Oracle

預設值：無

文件步驟

Push_incident – 將事件資訊推送至 ServiceNow。

輸出

Push_incident.incidentID – 建立的事件 ID。

AWS-RunPacker

Description

此 Runbook 使用 HashiCorp [Packer](#) 工具來驗證、修正或建置用於建立機器映像的套件範本。此 Runbook 使用 Packer v1.7.2。

Note

如果您指定 `vpc_id` 值，也必須指定公用子網路的 `subnet_id` 值。除非您修改子網路的 IPv4 公用定址屬性，否則您也必須將 `associate_public_ip_address` 設定為 `true`。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- Force

類型：布林值

描述：一個 Packer 選項，以強制建置器在成品來自舊版建置時執行，否則防止建置執行。

- Mode

類型：字串

描述：對範本進行驗證時要使用 Packer 的模式或命令。選項包括 Build、Validate 和 Fix。

- TemplateFileName

類型：字串

描述：S3 儲存貯體中範本檔案的名稱或鍵。

- TemplateS3BucketName

類型：字串

描述：包含套件程式範本的 S3 儲存貯體名稱。

文件步驟

RunPackerProcessTemplate – 使用 Packer 工具針對範本執行選取的模式。

輸出

RunPackerProcessTemplate.output – Packer 工具中的 stdout。

RunPackerProcessTemplate.fixed_template_key – 存放在 S3 儲存貯體中的範本名稱，僅在「固定」模式下執行時使用。

RunPackerProcessTemplate.s3_bucket – S3 儲存貯體的名稱，其中包含僅在「固定」模式下執行時使用的固定範本。

Amazon VPC

AWS Systems Manager 自動化為 Amazon Virtual Private Cloud 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [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

Description

此 Runbook 會從您指定的安全群組中移除所有輸入和輸出規則。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- SecurityGroupId

類型：字串

描述：(必要) 您要關閉的安全群組 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文件步驟

- aws:executeScript - 從您在 SecurityGroupId 參數中指定的安全群組移除所有輸入和輸出規則。

AWSSupport-ConfigureDNSQueryLogging

Description

AWSSupport-ConfigureDNSQueryLogging Runbook 會為源自於您虛擬私有雲端 (VPC) 的 DNS 查詢或 Amazon Route 53 託管區域的 DNS 查詢設定記錄。您可以選擇將查詢日誌發佈至 Amazon CloudWatch Logs、Amazon Simple Storage Service (Amazon S3) 或 Amazon Data Firehose。如需查詢記錄和解析程式查詢日誌的詳細資訊，請參閱[公有 DNS 查詢記錄](#)和[解析程式查詢記錄](#)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- LogDestinationArn

類型：字串

描述：（選用）您要傳送查詢日誌的 CloudWatch Logs 群組、Amazon S3 儲存貯體或 Firehose 串流的 ARN。請注意，Route 53 公有 DNS 查詢記錄僅支援 CloudWatch Logs 群組。如果您未指定此參數的值，自動化會建立格式為 `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID}` 的 CloudWatch Logs 群組，以及發佈查詢日誌的 IAM 資源政策。自動化建立的 CloudWatch Logs 群組的保留期間為 14 天。

- QueryLogType

類型：字串

描述：（選用）您要記錄的查詢類型。

有效值：公有 | Resolver/Private

預設：公有

- ResourceId

類型：字串

描述：(必要) 您要記錄其查詢的資源 ID。如果您Public為 QueryLogType 參數指定，資源必須是 Route 53 私有託管區域的 ID。如果您Resolver/Private為 QueryLogType 參數指定，資源必須是 VPC 的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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

文件步驟

- aws:executeScript - 驗證您為ResourceId參數指定的資源是否存在，並檢查資源類型是否符合所需的QueryLogType選項。
- aws:executeScript - 驗證您為 LogDestinationArn 參數指定的值是否符合所需的QueryLogType。
- aws:executeScript - 驗證 Route 53 發佈日誌至 CloudWatch Logs 日誌群組所需的許可，並在日誌不存在時建立所需的 IAM 資源政策。
- aws:executeScript - 啟用所選目的地上的 DNS 查詢記錄。

AWSSupport-ConfigureTrafficMirroring

Description

AWSSupport-ConfigureTrafficMirroring Runbook 會設定流量鏡像，以協助您疑難排解負載平衡器與 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體之間的連線問題。流量鏡像會從連接至執行個體的網路界面複製傳入和傳出流量。若要設定流量鏡像，此 Runbook 會建立所需的目標、篩選條件和工作階段。根據預設，Runbook 會針對 Amazon DNS 以外的所有通訊協定，設定所有傳入和傳出流量的鏡像。如果您想要鏡像來自特定來源和目的地的流量，您可以在自動化完成後修改傳入和傳出規則。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- SourceENI

類型：字串

描述：（必要）您要設定流量鏡像的彈性網路介面。

- 目標

類型：字串

描述：（必要）鏡像流量的目的地。您必須指定網路界面、Network Load Balancer 或 Gateway Load Balancer 端點的 ID。如果您指定 Network Load Balancer，連接埠 4789 上必須有 UDP 接聽程式。

- SessionNumber

類型：字串

有效值：1-32766

描述：（必要）您要使用的鏡像工作階段數量。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:CreateTrafficMirrorTarget
- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilter
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

文件步驟

- aws:executeScript - 執行指令碼來建立目標。
- aws:executeAwsApi - 建立篩選規則。
- aws:executeAwsApi - 為所有傳入流量建立鏡像篩選規則。
- aws:executeAwsApi - 為所有傳出流量建立鏡像篩選規則。
- aws:executeAwsApi - 建立流量鏡像工作階段。
- aws:executeAwsApi - 在篩選條件或工作階段建立失敗時刪除篩選條件。
- aws:executeAwsApi - 在篩選條件或工作階段建立失敗時刪除目標。

輸出

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.TargetIDOutput

AWSsupport-ConnectivityTroubleshooter

Description

AWSsupport-ConnectivityTroubleshooter Runbook 會診斷下列項目之間的連線問題：

- AWS Amazon Virtual Private Cloud (Amazon VPC) 內的資源
- AWS 使用 VPCs 對等互連連線 AWS 區域 之相同 內不同 Amazon VPC 中的 資源
- AWS Amazon VPC 中的 資源，以及使用網際網路閘道的網際網路資源
- AWS Amazon VPC 中的 資源，以及使用網路位址轉譯 (NAT) 閘道的網際網路資源

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- DestinationIP

類型：字串

描述：（必要）您要連線之資源的 IPv4 地址。

- DestinationPort

類型：字串

預設：true

描述：（必要）您要在目的地資源上連線的連接埠號碼。

- DestinationVpc

類型：字串

預設：全部

描述：（選用）您要測試連線的 Amazon VPC ID。

- SourceIP

類型：字串

描述：（必要）您要測試連線之 Amazon VPC 中 AWS 資源的私有 IPv4 地址。

- SourcePortRange

類型：字串

描述：（選用）您要測試連線的 Amazon VPC 中 AWS 資源所使用的連接埠範圍。

- SourceVpc

類型：字串

預設：全部

描述：（選用）您要測試連線的 Amazon VPC ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DescribeNatGateways

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

文件步驟

- `aws:executeScript` - 收集您在 `SourceIP` 參數中指定之 AWS 資源的詳細資訊。
- `aws:executeScript` - 使用從上一個步驟收集的路由，判斷來自 AWS 資源的網路流量目的地。
- `aws:branch` - 根據網路流量的目的地進行分支。
- `aws:executeAwsApi` - 收集目的地資源的詳細資訊。
- `aws:executeScript` - 確認目的地 Amazon VPC 傳回的 ID 符合 `DestinationVpc` 參數中指定的值，如果有的話。
- `aws:executeAwsApi` - 收集來源和目的地資源的安全群組規則。
- `aws:executeScript` - 確認安全群組規則是否允許來源和目的地資源之間的所需流量。
- `aws:executeAwsApi` - 收集與來源和目的地資源子網路相關聯的網路存取控制清單 (NACLs)。
- `aws:executeScript` - 確認 NACLs 是否允許來源和目的地資源之間的所需流量。
- `aws:executeScript` - 確認來源是否具有與資源相關聯的公有 IP 地址，如果路由目的地是網際網路閘道。
- `aws:executeAwsApi` - 收集來源資源的安全群組規則。
- `aws:executeScript` - 確認安全群組規則是否允許從來源到目的地資源所需的流量。
- `aws:executeAwsApi` - 收集與來源資源子網路相關聯的 NACLs。
- `aws:executeScript` - 確認 NACLs 是否允許來源資源所需的流量。
- `aws:executeAwsApi` - 收集 NAT 閘道的詳細資訊。
- `aws:executeAwsApi` - 收集與 NAT 閘道子網路相關聯的 NACLs。
- `aws:executeScript` - 確認 NACLs 是否允許來自 NAT 閘道子網路所需的流量。
- `aws:executeScript` - 收集與 NAT 閘道子網路相關聯的路由。
- `aws:executeScript` - 確認 NAT 閘道是否有網際網路閘道的路由。
- `aws:executeAwsApi` - 收集 VPC 互連連線的詳細資訊。

- `aws:executeScript` - 確認兩個 VPCs 位於相同區域，且目的地 VPC 傳回的 ID 符合 `DestinationVpc` 參數中指定的值，如果有的話。
- `aws:executeAwsApi` - 傳回目的地資源的子網路。
- `aws:executeScript` - 收集與對等 VPC 子網路相關聯的路由。
- `aws:executeScript` - 確認對等 VPC 是否有對等連線的路由。
- `aws:executeScript` - 確認如果自動化不支援目的地，是否允許來自來源資源的流量。

AWSSupport-TroubleshootVPN

Description

AWSSupport-TroubleshootVPN Runbook 可協助您追蹤和解決 AWS Site-to-Site VPN 連線中的錯誤。自動化包含數個自動檢查，旨在追蹤與 AWS Site-to-Site VPN 連線通道相關的 IKEv1 或 IKEv2 錯誤。自動化會嘗試比對特定錯誤，其對應的解決方案會形成常見問題清單。

注意：此自動化無法修正錯誤。它會在指定的時間範圍執行，並掃描日誌群組是否有 [VPN CloudWatch 日誌群組](#) 中的錯誤。

如何運作？

Runbook 會執行參數驗證，以確認輸入參數中包含的 Amazon CloudWatch 日誌群組是否存在、日誌群組中是否有任何日誌串流對應至 VPN 通道記錄、VPN 連線 ID 是否存在，以及通道 IP 地址是否存在。它會在為 VPN 記錄設定的 CloudWatch 日誌群組上進行 Logs Insights API 呼叫。

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LogGroupName

類型：字串

描述：(必要) 為 AWS Site-to-Site VPN 連線記錄設定的 Amazon CloudWatch 日誌群組名稱

允許模式：`^[\\.\-_\/#A-Za-z0-9]{1,512}`

- VpnConnectionId

類型：字串

描述：(必要) 要故障診斷的 AWS Site-to-Site VPN 連線 ID。

允許模式：`^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

類型：字串

描述：(必要) 與您的 相關聯的通道編號 1 IPv4 地址 AWS Site-to-Site VPN。

允許模式：`^((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

類型：字串

描述：(選用) 與 相關聯的通道編號 2 IPv4 地址 AWS Site-to-Site VPN。

允許模式：`^((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

類型：字串

描述：(必要) 選取您使用的 IKE 版本。允許的值：IKEv1, IKEv2

有效值：`['IKEv1', 'IKEv2']`

- StartTimeinEpoch

類型：字串

描述：(選用) 日誌分析的開始時間。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 進行日誌分析

允許模式：`^\d{10}|^$`

- EndTimeinEpoch

類型：字串

描述：(選用) 日誌分析的結束時間。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 進行日誌分析。如果同時指定 StartTimeinEpoch/EndTimeinEpoch 和 LookBackPeriod，則 LookBackPeriod 優先

允許模式：`^\d{10}|^$`

- LookBackPeriod

類型：字串

描述：(選用) 兩位數時間，以小時為單位，來回顧日誌分析。有效範圍：01 - 99。如果您也提供 StartTimeinEpoch 和 EndTime，則此值優先

允許模式：`^(\d?[1-9]|[1-9]0)|^$`

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- logs:DescribeLogGroups
- logs:GetQueryResults
- logs:DescribeLogStreams
- logs:StartQuery
- ec2:DescribeVpnConnections

指示

注意：當記錄輸出格式為 JSON 時，此自動化適用於為 VPN 通道記錄設定的 CloudWatch 日誌群組。

請依照下列步驟設定自動化：

1. 導覽至 AWS Systems Manager 主控台中的 [AWSSupport-TroubleshootVPN](#)。

2. 對於輸入參數，輸入以下內容：

- AutomationAssumeRole (選用)：

(IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)，允許 Systems Manager Automation 代表您執行動作。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- LogGroupName (必要)：

要驗證的 Amazon CloudWatch 日誌群組名稱。這必須是設定為 VPN 傳送日誌的 CloudWatch 日誌群組。

- VpnConnectionId (必要)：

追蹤其日誌群組的 AWS Site-to-Site VPN 連線 ID 是否有 VPN 錯誤。

- TunnelAIPAddress (必要)：

通道與您的 AWS Site-to-Site VPN 連線相關聯的 IP 地址。

- TunnelBIPAddress (選用)：

與您的 AWS Site-to-Site VPN 連線相關聯的通道 B IP 地址。

- IKEVersion (必要)：

選取您使用的 IKEVersion。允許的值：IKEv1, IKEv2。

- StartTimeinEpoch (選用)：

要查詢錯誤的時間範圍開始。範圍包含，因此指定的開始時間會包含在查詢中。指定為 epoch 時間，自 1970 年 1 月 1 日起的秒數，00:00:00 UTC。

- EndTimeinEpoch (選用)：

要查詢錯誤的時間範圍結束。範圍包含，因此指定的結束時間會包含在查詢中。指定為 epoch 時間，自 1970 年 1 月 1 日起的秒數，00:00:00 UTC。

- LookBackPeriod (必要)：

以小時為單位的時間，以查詢錯誤。

注意：設定 `StartTimeinEpoch`、`EndTimeinEpoch` 或 `LookBackPeriod` 來修正日誌分析的時間範圍。提供以小時為單位的兩位數號碼，以檢查從自動化開始時間開始的過去錯誤。或者，如果錯誤是過去在特定時間範圍內，請包含 `StartTimeinEpoch` 和 `EndTimeinEpoch`，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-123abc456xyz	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 <code>StartTimeEpoch/EndTimeEpoch</code> or <code>LookBackPeriod</code> for logs analysis. String	EndTimeEpoch (Optional) End time for log analysis. You can either use <code>StartTimeEpoch/EndTimeEpoch</code> or <code>LookBackPeriod</code> for logs analysis. String
LookBackPeriod (Required) Time in hours to look back for log analysis. 05	

3. 選取執行。

4. 自動化會啟動。

5. 自動化 Runbook 會執行下列步驟：

- `parameterValidation`：

對自動化中包含的輸入參數執行一系列驗證。

- `branchOnValidationOfLogGroup`：

檢查 參數中提及的日誌群組是否有效。如果無效，它會停止進一步啟動自動化步驟。

- `branchOnValidationOfLogStream`：

檢查日誌串流是否存在於包含的 CloudWatch 日誌群組中。如果無效，它會停止進一步啟動自動化步驟。

- `branchOnValidationOfVpnConnectionId`：

檢查 參數中包含的 VPN 連線 ID 是否有效。如果無效，它會停止進一步啟動自動化步驟。

- `branchOnValidationOfVpnIp`：

檢查參數中提及的通道 IP 地址是否有效。如果無效，則會停止進一步執行自動化步驟。

- `traceError`：

在包含的 CloudWatch 日誌群組中進行日誌洞見 API 呼叫，並搜尋與 IKEv1/IKEv2 相關的錯誤，以及相關的建議解析。

6. 完成後，請檢閱輸出區段以取得執行的詳細結果。

▼ Outputs	
parameterValidation.LogGroupName LogGroupvalid parameterValidation.VpnConnection validVPNconnection traceError.Tunnel1IKEv2 ("IKEv2ErrorCount":0) traceError.Tunnel2IKEv2 ("IKEv2ErrorCount":0) traceError.Tunnel1IKEv1 ("IKEv1ErrorCount":0) [{"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.	parameterValidation.LogStream validLogStream parameterValidation.VpnIpAddress validVPNIP traceError.Tunnel2IKEv1 ("IKEv1ErrorCount":0)

參考

Systems Manager Automation

- [執行此自動化（主控台）](#)
- [執行自動化](#)
- [設定自動化](#)
- [支援自動化工作流程登陸頁面](#)

AWS 服務文件

- [Site-to-Site日誌的內容](#)

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Description

AWSConfigRemediation-DeleteEgressOnlyInternetGateway Runbook 會刪除您指定的輸出
限定網際網路閘道。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- EgressOnlyInternetGatewayId

類型：字串

描述：(必要) 您要刪除的僅輸出網際網路閘道 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

文件步驟

- aws:executeScript - 刪除 EgressOnlyInternetGatewayId 參數中指定的輸出限定網際網路閘道。
- aws:executeScript - 驗證已刪除輸出限定網際網路閘道。

AWSConfigRemediation-DeleteUnusedENI

Description

AWSConfigRemediation-DeleteUnusedENI Runbook 會刪除連接狀態為 detached (ENI)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- NetworkInterfaceId

類型：字串

描述：(必要) 您要刪除的 ENI ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkInterface

- `ec2:DescribeNetworkInterfaces`

文件步驟

- `aws:executeAwsApi` - 刪除您在 `NetworkInterfaceId` 參數中指定的 ENI。
- `aws:executeScript` - 驗證 ENI 已刪除。

AWSConfigRemediation-DeleteUnusedSecurityGroup

Description

AWSConfigRemediation-DeleteUnusedSecurityGroup Runbook 會刪除您在 `GroupId` 參數中指定的安全群組。如果您嘗試刪除與 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體相關聯的安全群組，或由另一個安全群組參考，則自動化會失敗。此自動化不會刪除預設安全群組。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `GroupId`

類型：字串

描述：（必要）您要刪除的安全群組 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

文件步驟

- `aws:executeAwsApi` - 使用您在 `GroupId` 參數中提供的值傳回安全群組名稱。
- `aws:branch` - 確認群組名稱不是「預設」。
- `aws:executeAwsApi` - 刪除 `GroupId` 參數中指定的安全群組。
- `aws:executeScript` - 確認已刪除安全群組。

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Description

AWSConfigRemediation-DeleteUnusedVPCNetworkACL Runbook 會刪除未與子網路相關聯的網路存取控制清單 (ACL)。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN) , 允許 Systems Manager Automation 代表您執行動作。

- NetworkAcId

類型：字串

描述：(必要) 您要刪除的網路 ACL ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAcl
- ec2:DescribeNetworkAcls

文件步驟

- aws:executeAwsApi - 刪除 NetworkAcId 參數中指定的網路 ACL。
- aws:executeScript - 確認已刪除 NetworkAcId 參數中指定的網路 ACL。

AWSConfigRemediation-DeleteVPCFlowLog

Description

AWSConfigRemediation-DeleteVPCFlowLog Runbook 會刪除您指定的虛擬私有雲端 (VPC) 流程日誌。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- FlowLogId

類型：字串

描述：(必要) 您要刪除之流程日誌的 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs

文件步驟

- aws:executeAwsApi - 刪除您在 FlowLogId 參數中指定的流程日誌。
- aws:executeScript - 驗證流程日誌已刪除。

AWSConfigRemediation-DetachAndDeleteInternetGateway

Description

AWSConfigRemediation-DetachAndDeleteInternetGateway Runbook 會分離並刪除您指定的網際網路閘道。如果虛擬私有雲端 (VPC) 中的任何 Amazon EC2 執行個體具有與其相關聯的彈性 IP 地址或公有 IPv4 地址，則 Runbook 會失敗。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- InternetGatewayId

類型：字串

描述：（必要）您要刪除的網際網路閘道 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteInternetGateway
- ec2:DescribeInternetGateways

- `ec2:DetachInternetGateway`

文件步驟

- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的狀態屬性變更為 `available` 或逾時。
- `aws:executeAwsApi` - 擷取指定的虛擬私有閘道組態。
- `aws:branch` - 根據 `VpcAttachments.state` 參數值的分支。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的 `VpcAttachments.state's` 屬性變更為 `attached` 或逾時。
- `aws:executeAwsApi` - 接受虛擬私有閘道的 ID 和 Amazon VPC 的 ID 做為輸入，並從 Amazon VPC 分離虛擬私有閘道。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的 `VpcAttachments.state's` 屬性變更為 `detached` 或逾時。
- `aws:executeAwsApi` - 接受虛擬私有閘道的 ID 做為輸入，並將其刪除。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID 做為輸入，並驗證其刪除。
- `aws:executeAwsApi` - 從網際網路閘道 ID 收集 VPC ID。
- `aws:executeAwsApi` - 從 VPC 分離網際網路閘道 ID。
- `aws:executeAwsApi` - 刪除網際網路閘道。

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Description

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway Runbook 會分離和刪除連接至使用 Amazon Virtual Private Cloud (Amazon EC2 Amazon Virtual Private Cloud) 閘道。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- VpnGatewayId

類型：字串

描述：(必要) 要刪除的虛擬私有閘道 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteVpnGateway
- ec2:DetachVpnGateway
- ec2:DescribeVpnGateways

文件步驟

- aws:waitForAwsResourceProperty - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的狀態屬性變更為 available 或 逾時。
- aws:executeAwsApi - 擷取指定的虛擬私有閘道組態。

- `aws:branch` - 根據 `VpcAttachments.state` 參數值的分支。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的 `VpcAttachments.state`'s 屬性變更為 `attached`或逾時。
- `aws:executeAwsApi` - 接受虛擬私有閘道的 ID 和 Amazon VPC 的 ID 做為輸入，並從 Amazon VPC 分離虛擬私有閘道。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID，並等待虛擬私有閘道的 `VpcAttachments.state`'s 屬性變更為 `detached`或逾時。
- `aws:executeAwsApi` - 接受虛擬私有閘道的 ID 做為輸入，並將其刪除。
- `aws:waitForAwsResourceProperty` - 接受虛擬私有閘道的 ID 做為輸入，並驗證其刪除。

AWS-DisableIncomingSSHOnPort22

Description

AWS-DisableIncomingSSHOnPort22 Runbook 會移除規則，允許安全群組在 TCP 連接埠 22 上不受限制的傳入 SSH 流量。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- SecurityGroupIds

類型：字串

描述：(必要) 您希望限制 SSH 流量之安全群組 IDs 的逗號分隔清單。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

文件步驟

- aws:executeAwsApi - 從您在 SecurityGroupIds 參數中指定的安全群組移除允許 TCP 連接埠 22 上傳入 SSH 流量的所有規則。

輸出

DisableIncomingSSTemplate.RestrictedSecurityGroupIds - 已移除傳入 SSH 規則的安全群組 IDs 清單。

AWS-DisablePublicAccessForSecurityGroup

Description

此 Runbook 會停用對所有 IP 地址開啟的預設 SSH 和 RDP 連接埠。

Important

此 Runbook 對於符合下列兩項條件的安全群組失敗，並出現「InvalidPermission.NotFound」錯誤：1) 安全群組位於非預設 VPC；以及 2) 安全群組的傳入規則並未使用下列四種模式指定開放連接埠：

- 0.0.0.0/0
- ::/0
- SSH or RDP port + 0.0.0.0/0
- SSH or RDP port + ::/0

 Note

此 Runbook 不適用於 AWS 區域 位於中國的 。

執行此自動化 (主控台)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- GroupId

類型：字串

描述：(必要) 應該停用連接埠的安全群組 ID。

- `IpAddressToBlock`

類型：字串

描述：（選用）應封鎖其存取權的其他 IPv4 地址，格式為 1.2.3.4/32。

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Description

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP Runbook 會停用您指定之子網路的 IPv4 公有定址屬性。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（必要）(IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `SubnetId`

類型：字串

描述：（必要）您要停用自動指派公有 IPv4 地址屬性的子網路 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSubnets
- ec2:ModifySubnetAttribute

文件步驟

- aws:executeAwsApi - 停用您在 SubnetId 參數中指定之子網路的自動指派公有 IPv4 地址屬性。
- aws:assertAwsResourceProperty - 確認屬性已停用。

AWSSupport-EnableVPCFlowLogs

Description

AWSSupport-EnableVPCFlowLogs Runbook 會為 中的子網路、網路介面和 VPCs 建立 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌 AWS 帳戶。如果您為子網路或 VPC 建立流程日誌，則會監控該子網路或 Amazon VPC 中的每個彈性網路介面。流程日誌資料會發佈至您指定的 Amazon CloudWatch Logs 日誌群組或 Amazon Simple Storage Service (Amazon S3) 儲存貯體。如需流程日誌的詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的 [VPC 流程日誌](#)。

Important

當您將流程記錄發佈到或發佈到 CloudWatch Logs 或 Amazon S3 時，會套用付費日誌的資料擷取和存檔費用。如需詳細資訊，請參閱[流程日誌定價](#)

[執行此自動化（主控台）](#)

Note

選取 s3 做為日誌目的地時，請確定儲存貯體政策允許日誌交付服務存取儲存貯體。如需詳細資訊，請參閱[流程日誌的 Amazon S3 儲存貯體許可](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 的使用者許可。

- DeliverLogsPermissionArn

類型：字串

描述：(選用) 允許 Amazon Elastic Compute Cloud (Amazon EC2) 將流程日誌發佈至您帳戶中 CloudWatch Logs 日誌群組的 IAM 角色 ARN。如果您 s3 為 LogDestinationType 參數指定，請勿為此參數提供值。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的將[流程日誌發佈至 CloudWatch Logs](#)。

- LogDestinationARN

類型：字串

描述：(選用) 發佈流程日誌資料的資源 ARN。如果為 LogDestinationType 參數 cloud-watch-logs 指定，請提供您要發佈流程日誌資料的 CloudWatch Logs 日誌群組 ARN。或者，請改用 LogGroupName。如果 s3 已針對 LogDestinationType 參數指定，您必須指定您要為此參數發佈流程日誌資料的 Amazon S3 儲存貯體 ARN。您也可以在儲存貯體中指定資料夾。

Important

選擇 s3 做為 LogDestinationType，您應確保選取的儲存貯體遵循 [Amazon S3 儲存貯體安全最佳實務](#)，並遵循組織和地理區域的資料隱私權法律。

- LogDestinationType

類型：字串

有效值：cloud-watch-logs | s3

描述：（必要）決定流程日誌資料的發佈位置。如果您將 指定LogDestinationType為 s3 ，請勿指定 DeliverLogsPermissionArn或 LogGroupName 。

- LogFormat

類型：字串

描述：（選用）要包含在流程日誌中的欄位，以及它們應該出現在記錄中的順序。如需可用欄位的清單，請參閱《Amazon VPC 使用者指南》中的[流程日誌記錄](#)。如果您未提供此參數的值，則會使用預設格式建立流程日誌。如果您指定此參數，則必須至少指定一個欄位。

- LogGroupName

類型：字串

描述：（選用）發佈流程日誌資料的 CloudWatch Logs 日誌群組名稱。如果您s3為 LogDestinationType 參數指定，請勿為此參數提供 值。

- ResourceIds

類型：StringList

描述：（必要）以逗號分隔的清單，列出您要為其建立流量日誌的子網路、彈性網路介面或 VPC IDs。

- TrafficType

類型：字串

有效值：接受 | 拒絕 | ALL

描述：（必要）要記錄的流量類型。您可以記錄資源接受或拒絕的流量，或所有流量的日誌。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- 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`

範例政策

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSM Execution Permissions",
      "Effect": "Allow",
      "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2 FlowLogs Permissions",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFlowLogs",
        "ec2>DeleteFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "arn:{partition}:ec2:{region}:{account-id}:{instance|
subnet|vpc|transit-gateway|transit-gateway-attachment}/{resource ID}"
    },
    {
      "Sid": "IAM CreateRole Permissions",
      "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:{partition}:iam::{account-id}:role/{role name}",
        "arn:{partition}:iam::{account-id}:role/
AWSsupportCreateFlowLogsRole"
    ]
  },
  {
    "Sid": "CloudWatch Logs Permissions",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogDelivery",
      "logs:CreateLogGroup",
      "logs>DeleteLogDelivery",
      "logs>DeleteLogGroup",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource": [
      "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}",
      "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}:*"
    ]
  },
  {
    "Sid": "S3 Permissions",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetAccountPublicAccessBlock",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketAcl",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:{partition}:s3::{bucket name}",
      "arn:{partition}:s3::{bucket name}/*"
    ]
  }
]
}

```

文件步驟

- `aws:branch` - 根據為 `LogDestinationType` 參數指定的值進行分支。
- `aws:executeScript` - 檢查目標 Amazon Simple Storage Service (Amazon S3) 是否可能授予其物件的讀取或寫入 `public` 存取權。
- `aws:executeScript` - 如果未為 `LogDestinationARN` 參數指定值，且為 `LogDestinationType` 參數指定值，`cloud-watch-logs` 則建立日誌群組。
- `aws:executeScript` - 根據 Runbook 參數中指定的值建立流程日誌。

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Description

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch Runbook 會將將流程日誌資料發佈至 Amazon Simple Storage Service (Amazon S3) 的現有 Amazon VPC 流程日誌取代為將流程日誌資料發佈至您指定的 Amazon CloudWatch Logs (CloudWatch Logs) 日誌群組的流程日誌。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- `DestinationLogGroup`

類型：字串

描述：（必要）您要發佈流程日誌資料的 CloudWatch Logs 日誌群組名稱。

- DeliverLogsPermissionArn

類型：字串

描述：（必要）您要使用的 AWS Identity and Access Management (IAM) 角色 ARN，可提供 Amazon Elastic Compute Cloud (Amazon EC2) 將流程日誌資料發佈至 CloudWatch Logs 的必要許可。

- FlowLogId

類型：字串

描述：（必要）發佈至您要取代之 Amazon S3 的流程日誌 ID。

- MaxAggregationInterval

類型：整數

有效值：60 | 600

描述：（選用）最長時間間隔，以秒為單位，在此期間會擷取封包流程並彙總到流程日誌記錄中。

- TrafficType

類型：字串

有效值：接受 | 拒絕 | ALL

描述：（必要）您要記錄和發佈的流程日誌資料類型。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2>DeleteFlowLogs

- `ec2:DescribeFlowLogs`

文件步驟

- `aws:executeAwsApi` - 從您在 `FlowLogId` 參數中指定的值收集 VPC 的詳細資訊。
- `aws:executeAwsApi` - 根據您為 Runbook 參數指定的值建立流程日誌。
- `aws:assertAwsResourceProperty` - 驗證新建立的流程日誌發佈至 CloudWatch Logs。
- `aws:executeAwsApi` - 刪除發佈至 Amazon S3 的流程日誌。
- `aws:executeScript` - 確認發佈至 Amazon S3 的流程日誌已刪除。

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Description

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket Runbook 會使用將流程日誌資料發佈至您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的流程日誌，取代將流程日誌資料發佈至 Amazon CloudWatch Logs (CloudWatch Logs) 的現有 Amazon VPC 流程日誌。Amazon S3

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- DestinationS3BucketArn

類型：字串

描述：(必要) 您要發佈流程日誌資料的 Amazon S3 儲存貯體 ARN。

- FlowLogId

類型：字串

描述：(必要) 發佈至您要取代之 CloudWatch Logs 的流程日誌 ID。

- MaxAggregationInterval

類型：整數

有效值：60 | 600

描述：(選用) 最長時間間隔，以秒為單位，在此期間會擷取封包流程並彙總到流程日誌記錄中。

- TrafficType

類型：字串

有效值：接受 | 拒絕 | ALL

描述：(必要) 您要記錄和發佈的流程日誌資料類型。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs

文件步驟

- `aws:executeAwsApi` - 從您在 `FlowLogId` 參數中指定的值收集 VPC 的詳細資訊。
- `aws:executeAwsApi` - 根據您為 `Runbook` 參數指定的值建立流程日誌。
- `aws:assertAwsResourceProperty` - 驗證新建立的流程日誌發佈至 Amazon S3。
- `aws:executeAwsApi` - 刪除發佈至 CloudWatch Logs 的流程日誌。
- `aws:executeScript` - 確認發佈至 CloudWatch Logs 的流程日誌已刪除。

AWS-ReleaseElasticIP

Description

使用分配 ID 釋出指定的彈性 IP 地址。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- `AllocationId`

類型：字串

描述：(必要) 彈性 IP 地址的分配 ID。

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Description

AWS-RemoveNetworkACLUnrestrictedSSHRDP Runbook 會從指定的網路 ACL 移除所有網路存取控制清單 (ACL) 規則，允許從所有來源地址傳入流量到預設 SSH 和 RDP 連接埠。不會移除包含與預設 SSH 和 RDP 連接埠重疊之連接埠範圍的規則。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- NetworkAcId

類型：字串

描述：（必要）您要移除無限制規則的網路 ACL ID，允許從所有來源地址傳入流量到預設 SSH 和 RDP 連接埠。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

文件步驟

- `aws:executeScript` - 移除允許來自您在 `SecurityGroupId` 參數中指定之安全群組之所有來源地址流量的所有輸入規則。

輸出

`RemoveNACLEntriesAndVerify.VerificationMessage` - 驗證成功刪除網路 ACL 規則的訊息。

`RemoveNACLEntriesAndVerify.RulesDeletedAndApiResponses` - 已刪除的網路 ACL 規則，以及 `DeleteNetworkAclEntry` API 操作回應。

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Description

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules Runbook 會從您指定的安全群組中移除所有輸入規則，以允許來自所有來源地址的流量。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- SecurityGroupId

類型：字串

描述：(必要) 您要移除允許來自所有來源地址流量之傳入規則的安全群組 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

文件步驟

- aws:executeScript - 移除允許來自您在 SecurityGroupId 參數中指定之安全群組之所有來源地址流量的所有輸入規則。

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Description

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules Runbook 會從您指定的虛擬私有雲端 (VPC) 的預設安全群組中移除所有規則。

[執行此自動化 \(主控台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)，允許 Systems Manager Automation 代表您執行動作。

- GroupId

類型：字串

描述：(必要) 您要從中移除所有規則的安全群組 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文件步驟

- aws:assertAwsResourceProperty - 確認您在 GroupId 參數中指定的安全群組已命名為預設值。
- aws:executeScript - 從您在 GroupId 參數中指定的安全群組移除所有規則。

AWSSupport-SetupIPMonitoringFromVPC

Description

AWSSupport-SetupIPMonitoringFromVPC 會在指定的子網路中建立 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，並透過持續執行 ping、MTR、traceroute 和 tracetcp 測試來監控選取的目標 IPs (IPv4 或 IPv6)。結果會儲存在 Amazon CloudWatch Logs 日誌中，並套用指標篩選條件，以在 CloudWatch 儀表板中快速視覺化延遲和封包遺失統計資料。

其他資訊

CloudWatch Logs 資料可用於網路故障診斷和分析模式/趨勢。此外，您可以在封包遺失和/或延遲達到閾值時，使用 Amazon SNS 通知設定 CloudWatch 警示。使用 開啟案例時，也可以使用資料 AWS 支援，以協助快速隔離問題，並在調查網路問題時縮短解決時間。

Note

若要清除 建立的資源AWSSupport-SetupIPMonitoringFromVPC，您可以使用 Runbook AWSSupport-TerminateIPMonitoringFromVPC。如需詳細資訊，請參閱 [AWSSupport-TerminateIPMonitoringFromVPC](#)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- CloudWatchLogGroupNamePrefix

類型：字串

預設：/AWSSupport-SetupIPMonitoringFromVPC

描述：(選用) 用於為測試結果建立之每個 CloudWatch 日誌群組的字首。

- CloudWatchLogGroupRetentionInDays

類型：字串

有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

預設：7

描述：(選用) 您想要保留網路監控結果的天數。

- InstanceType

類型：字串

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

預設：t3.micro

描述：(選用) EC2Rescue 執行個體的 EC2 執行個體類型。建議大小：t3.micro。

- SubnetId

類型：字串

描述：(必要) 監控執行個體的子網路 ID。請注意，如果您指定私有子網路，則必須確保有網際網路存取權，以允許監控執行個體設定測試（表示、安裝 CloudWatch Logs 代理程式、與 Systems Manager 和 CloudWatch 互動）。

- TargetIPs

類型：字串

描述：(必要) 要監控的 IPv4 及/或 IPv6 逗號分隔清單。不可使用空格。大小上限為 255 字元。請注意，如果您提供無效的 IP，則自動化會失敗並轉返測試設定。

- TestInstanceSecurityGroupId

類型：字串

描述：(選用) 測試執行個體的安全群組 ID。如果未指定，自動化會在執行個體建立期間建立一個。確定安全群組允許對監控 IPs 傳出存取。

- `TestInstanceProfileName`

類型：字串

描述：(選用) 測試執行個體的現有 IAM 執行個體描述檔名稱。如果未指定，自動化會在執行個體建立期間建立一個。角色必須具有下列許可：`logs:CreateLogStream`、`logs:DescribeLogStreams`、`logs:DescribeLogGroups`、`logs:PutLogEvents` 和 AWS 受管政策 `AmazonSSMManagedInstanceCore`。

- `TestInterval`

類型：字串

描述：(選用) 測試間隔之間的分鐘數。預設值為 1 分鐘，最大值為 10 分鐘。

- `RetainDashboardAndLogsOnDeletion`

類型：字串

描述：(選用) `False` 指定在刪除 AWS CloudFormation 堆疊時刪除 Amazon CloudWatch 儀表板和日誌。預設值為 `True`。根據預設，儀表板和日誌會保留，而且不再需要時需要手動刪除。

必要的 IAM 許可

`AutomationAssumeRole` 參數需要下列動作才能成功使用 Runbook。

Warning

建議傳遞 `TestInstanceProfileName` 參數或確保已設置安全護欄，以防止濫用可變 IAM 許可。

建議執行自動化的使用者連接 `AmazonSSMAutomationRole` IAM 受管政策。此外，使用者必須將以下政策連接至其使用者帳戶、群組或角色：

```
{
```

```

"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:<partition>:iam:<account-id>:role/SetupIPMonitoringFromVPC*",
      "arn:<partition>:iam:<account-id>: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 `TestInstanceProfileName` 參數，則不需要下列 IAM 許可來執行 Runbook：

- `iam:CreateRole`
- `iam:CreateInstanceProfile`
- `iam:DetachRolePolicy`
- `iam:AttachRolePolicy`
- `iam:AddRoleToInstanceProfile`
- `iam:RemoveRoleFromInstanceProfile`

- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:DeleteInstanceProfile`

文件步驟

1. **`aws:executeAwsApi`** - 描述提供的子網路。
2. **`aws:branch`** - 評估 `TargetIPs` 輸入。

(IPv6) 若 `TargetIPs` 包含 IPv6：

`aws:assertAwsResourceProperty` - 檢查提供的子網路是否有關聯的 IPv6 集區

3. **`aws:executeScript`** - 取得最新 Amazon Linux 2 的執行個體類型架構和公有參數路徑 AMI。
4. **`aws:executeAwsApi`** - AMI 從參數存放區取得最新的 Amazon Linux 2。
5. **`aws:executeAwsApi`** - 在子網路的 VPC 中建立測試的安全群組。

(清除) 如果安全群組建立失敗：

`aws:executeAwsApi` - 如果存在，請刪除自動化建立的安全群組。

6. **`aws:executeAwsApi`** - 允許測試安全群組中的所有傳出流量。

(清除) 如果安全群組輸出規則建立失敗：

`aws:executeAwsApi` - 如果存在，請刪除自動化建立的安全群組。

7. **`aws:executeAwsApi`** - 為測試 EC2 執行個體建立 IAM 角色

(清除) 如果角色建立失敗：

- a. **`aws:executeAwsApi`** - 刪除自動化建立的 IAM 角色，如果有的話。
- b. **`aws:executeAwsApi`** - 如果存在，請刪除自動化建立的安全群組。

8. **`aws:executeAwsApi`** - 連接 `AmazonSSMManagedInstanceCore` 受管政策

(清除) 若政策連接失敗：

- a. **`aws:executeAwsApi`** - 如果連接，請從自動化建立的角色分離 `AmazonSSMManagedInstanceCore` 受管政策。
- b. **`aws:executeAwsApi`** - 刪除自動化建立的 IAM 角色。
- c. **`aws:executeAwsApi`** - 刪除自動化建立的安全群組，如果存在的話。

9. **aws:executeAwsApi** - 連接內嵌政策，以允許設定 CloudWatch 日誌群組保留和建立 CloudWatch 儀表板

(清除) 若內嵌政策連接失敗：

- a. **aws:executeAwsApi** - 如果已建立，請從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- b. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- d. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果有的話。

10 **aws:executeAwsApi** - 建立 IAM 執行個體描述檔。

(清除) 如果執行個體描述檔建立失敗：

- a. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔，如果有的話。
- b. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- c. **aws:executeAwsApi** - 從自動化建立的角色中刪除 AmazonSSMManagedInstanceCore 受管政策。
- d. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- e. **aws:executeAwsApi** - 如果存在，請刪除自動化建立的安全群組。

11 **aws:executeAwsApi** - 將 IAM 執行個體描述檔與 IAM 角色建立關聯。

(清除) 如果執行個體描述檔和角色關聯失敗：

- a. **aws:executeAwsApi** - 若有關聯，請從角色移除 IAM 執行個體描述檔。
- b. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- d. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- e. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- f. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

12 **aws:sleep** - 等待執行個體描述檔變成可用。

13 **aws:runInstances** - 在指定的子網路中建立測試執行個體，並使用先前連接的執行個體描述檔建立測試執行個體。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。

- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

14 **aws:branch** - 評估 TargetIPs 輸入。

(IPv6) 若 TargetIPs 包含 IPv6：

aws:executeAwsApi - 將 IPv6 指派給測試執行個體。

15 **aws:waitForAwsResourceProperty** - 等待測試執行個體成為受管執行個體。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 如果存在，請刪除自動化建立的安全群組。

16 **aws:runCommand** - 安裝測試先決條件：

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。

g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

17 **aws:runCommand** - 驗證提供的 IPs 在語法上是正確的 IPv4 和/或 IPv6 地址：

(清除) 如果步驟失敗：

a. **aws:changeInstanceState** - 終止測試執行個體。

b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。

c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。

d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。

e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。

f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。

g. **aws:executeAwsApi** - 如果存在，請刪除自動化建立的安全群組。

18 **aws:runCommand** - 為每個提供的 IPs 定義 MTR 測試。

(清除) 如果步驟失敗：

a. **aws:changeInstanceState** - 終止測試執行個體。

b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。

c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。

d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。

e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。

f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。

g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

19 **aws:runCommand** - 為每個提供的 IPs 定義第一個 ping 測試。

(清除) 如果步驟失敗：

a. **aws:changeInstanceState** - 終止測試執行個體。

b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。

c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。

d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。

e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。

- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

20**aws:runCommand** - 為每個提供的 IPs 定義第二個 ping 測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

21**aws:runCommand** - 定義每個所提供 IPs 的追蹤路徑測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 如果存在，請刪除自動化建立的安全群組。

22**aws:runCommand** - 為每個提供的 IPs 定義追蹤路由測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。

- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

23**aws:runCommand** - 設定 CloudWatch 日誌。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

24**aws:runCommand** - 排程 cronjobs 每分鐘執行一次測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

25**aws:sleep** - 等待測試產生一些資料。

26**aws:runCommand** - 設定所需的 CloudWatch 日誌群組保留。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。

b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。

- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

27 **aws:runCommand** - 設定 CloudWatch 日誌群組指標篩選條件。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState** - 終止測試執行個體。
- b. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- c. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- f. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- g. **aws:executeAwsApi** - 刪除自動化建立的安全群組，如果存在的話。

28 **aws:runCommand** - 建立 CloudWatch 儀表板。

(清除) 如果步驟失敗：

- a. **aws:executeAwsApi** - 刪除存在的 CloudWatch 儀表板。
- b. **aws:changeInstanceState** - 終止測試執行個體。
- c. **aws:executeAwsApi** - 從角色移除 IAM 執行個體描述檔。
- d. **aws:executeAwsApi** - 刪除自動化建立的 IAM 執行個體描述檔。
- e. **aws:executeAwsApi** - 從自動化建立的角色刪除 CloudWatch 內嵌政策。
- f. **aws:executeAwsApi** - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
- g. **aws:executeAwsApi** - 刪除自動化建立的 IAM 角色。
- h. **aws:executeAwsApi** - 如果存在，請刪除自動化建立的安全群組。

輸出

`createCloudWatchDashboards.Output` - CloudWatch 儀表板的 URL。

`createManagedInstance.InstanceIds` - 測試執行個體 ID。

AWSSupport-TerminateIPMonitoringFromVPC

Description

AWSSupport-TerminateIPMonitoringFromVPC 會終止先前由 啟動的 IP AWSSupport-SetupIPMonitoringFromVPC 監控測試。與指定測試 ID 相關的資料都會刪除。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- AutomationExecutionId

類型：字串

描述：（必要）您先前執行 AWSSupport-SetupIPMonitoringFromVPC Runbook 時來自的自動化執行 ID。與此執行 ID 相關聯的所有資源都會遭到刪除。

- InstanceId

類型：字串

描述：(必要) 監控執行個體的執行個體 ID。

- SubnetId

類型：字串

描述：(必要) 監控執行個體的字網路 ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

建議執行自動化的使用者連接 AmazonSSMAutomationRole IAM 受管政策。此外，使用者必須將下列政策連接至其使用者、群組或角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteInstanceProfile",
        "iam>DeleteRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport/SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::An-AWS-Account-ID: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"
}
]
}

```

文件步驟

1. `aws:assertAwsResourceProperty` - 檢查 `AutomationExecutionId` 和 `InstanceId` 是否與相同的測試相關。
2. `aws:assertAwsResourceProperty` - 檢查 `SubnetId` 和 `InstanceId` 是否與相同的測試相關。
3. `aws:executeAwsApi` - 擷取測試安全群組。
4. `aws:executeAwsApi` - 刪除 CloudWatch 儀表板。
5. `aws:changeInstanceState` - 終止測試執行個體。
6. `aws:executeAwsApi` - 從角色移除 IAM 執行個體描述檔。
7. `aws:executeAwsApi` - 刪除自動化建立的 IAM 執行個體描述檔。
8. `aws:executeAwsApi` - 從自動化建立的角色中刪除 CloudWatch 內嵌政策。
9. `aws:executeAwsApi` - 從自動化建立的角色分離 AmazonSSMManagedInstanceCore 受管政策。
10. `aws:executeAwsApi` - 刪除自動化建立的 IAM 角色。
11. `aws:executeAwsApi` - 如果存在，請刪除自動化建立的安全群組。

輸出

無

AWS WAF

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS WAF。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-AddWAFRegionalRuleToRuleGroup](#)
- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

AWS-AddWAFRegionalRuleToRuleGroup

Description

AWS-AddWAFRegionalRuleToRuleGroup Runbook 會將現有的 AWS WAF 區域規則新增至 AWS WAF 區域規則群組。僅支援 AWS WAF 傳統區域規則群組。AWS WAF 傳統區域規則群組最多可有 10 個規則。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- RuleGroupId

類型：字串

描述：(必要) 您要更新的規則群組 ID。

- RulePriority

類型：整數

描述：(必要) 新規則的優先順序。規則優先順序會決定區域群組中規則的評估順序。值較低的規則優先順序高於值較高的規則。值必須是唯一的整數。如果您將多個規則新增至區域規則群組，則值不必是連續的。

- RuleId

類型：字串

描述：(必要) 您要新增至區域規則群組的規則 ID。

- RuleAction

類型：字串

描述：(必要) 指定 Web 請求符合規則條件時所 AWS WAF 採取的動作。

有效值：允許 | 封鎖 | 計數

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

文件步驟

- `GetWAFChangeToken` (aws : `executeAwsApi`) - 擷取 AWS WAF 變更字符，以確保 Runbook 不會向服務提交衝突的請求。
- `AddWAFRuleToWAFRegionalRuleGroup` (aws : `executeScript`) - 將指定的規則新增至 AWS WAF 區域規則群組。
- `VerifyChangeTokenPropagating` (aws : `waitForAwsResourceProperty`) - 驗證變更字符的狀態為 `PENDING` 或 `INSYNC`。
- `VerifyRuleAddedToRuleGroup` (aws : `executeScript`) - 驗證指定的 AWS WAF 規則已新增至目標區域規則群組。

輸出

- `VerifyRuleAddedToRuleGroup.VerifyRuleAddedToRuleGroupResponse` - 步驟的輸出，驗證新規則已新增至區域規則群組。
- `VerifyRuleAddedToRuleGroup.ListActivatedRulesInRuleGroupResponse` - `ListActivatedRulesInRuleGroup` API 操作的輸出。

AWS-AddWAFRegionalRuleToWebAcl

Description

`AWS-AddWAFRegionalRuleToWebAcl` Runbook 會將現有的 AWS WAF 區域規則、規則群組或速率型規則新增至 AWS WAF Classic 區域 Web 存取控制清單 (ACL)。此 Runbook 不會更新由管理的現有 AWS WAF Classic 區域 Web ACL AWS Firewall Manager。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- WebACLId

類型：字串

描述：(必要) 您要更新的 Web ACL ID。

- ActivatedRulePriority

類型：整數

描述：(必要) 新規則的優先順序。規則優先順序決定 Web ACL 中規則的評估順序。值較低的規則優先順序高於值較高的規則。值必須是唯一的整數。如果您將多個規則新增至區域 Web ACL，則值不必是連續的。

- ActivatedRuleRuleId

類型：字串

描述：(必要) 您要新增至 Web ACL 的規則、速率型規則或群組的 ID。

- ActivatedRuleAction

類型：字串

有效值：允許 | 封鎖 | 計數

描述：(選用) 指定 Web 請求符合規則條件時所 AWS WAF 採取的動作。

- **ActivatedRuleType**

類型：字串

有效值：REGULAR | RATE_BASED | GROUP

預設：REGULAR

描述：(選用) 您要新增至 Web ACL 的規則類型。雖然此欄位是選用的，但請注意，如果您嘗試在不設定類型的情況下將RATE_BASED規則新增至 Web ACL，則請求會失敗，因為請求預設為REGULAR規則。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

文件步驟

- `DetermineWebACLNotInFMSAndRulePriority` (aws : `executeScript`) - 驗證 AWS WAF Web ACL 是否在 Firewall Manager 安全政策中，並確認優先順序 ID 不會與現有的 ACL 衝突。
- `AddRuleOrRuleGroupToWebACL` (aws : `executeScript`) - 將指定的規則新增至 AWS WAF Web ACL。
- `VerifyRuleOrRuleGroupAddedToWebAcl` (aws : `executeScript`) - 驗證指定的 AWS WAF 規則已新增至目標 Web ACL。

輸出

- `DetermineWebACLNotInFMSAndRulePriority.PrereqResponse`: 步驟的輸出 `DetermineWebACLNotInFMSAndRulePriority`。
- `VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse`: 步驟的輸出 `AddRuleOrRuleGroupToWebACL`。

- `VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse.VerifyRuleOrRuleGroupAddedToWebAcl` 的輸出。

AWSConfigRemediation-EnableWAFCClassicLogging

Description

AWSConfigRemediation-EnableWAFCClassicLogging Runbook 可讓您記錄您指定的 AWS WAF Web 存取控制清單 (Web ACL) 的 Amazon Data Firehose (Firehose)。

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、 macOS、 Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- `DeliveryStreamName`

類型：字串

描述：（必要）您要傳送日誌的 Firehose 交付串流名稱。

- WebACId

類型：字串

描述：（必要）您要启用登入的 AWS WAF Web ACL ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

文件步驟

- `aws:executeAwsApi` - 確認您在 中指定的交付串流DeliveryStreamName存在。
- `aws:executeAwsApi` - 收集 WebACLIId 參數中指定的 AWS WAF Web ACL ARN。
- `aws:executeAwsApi` - 啟用 Web ACL 的記錄。
- `aws:assertAwsResourceProperty` - 確認已在 AWS WAF Web ACL 上啟用記錄。

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Description

AWSConfigRemediation-EnableWAFClassicRegionalLogging Runbook 可讓您針對指定的 AWS WAF Web 存取控制清單 (ACL) 記錄到 Amazon Data Firehose (Firehose)。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（必要）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- LogDestinationConfigs

類型：字串

描述：（必要）您要傳送日誌的 Firehose 交付串流的 Amazon Resource Name (ARN)。

- WebACLId

類型：字串

描述：（必要）您要啟用登入的 AWS WAF Web ACL ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf-regional:GetLoggingConfiguration
- waf-regional:GetWebAcl
- waf-regional:PutLoggingConfiguration

文件步驟

- aws:executeAwsApi - 收集 WebACLId 參數中指定的 AWS WAF Web ACL ARN。
- aws:executeAwsApi - 啟用 Web ACL 的記錄。
- aws:assertAwsResourceProperty - 確認已在 AWS WAF Web ACL 上啟用記錄。

AWSConfigRemediation-EnableWAFV2Logging

Description

AWSConfigRemediation-EnableWAFV2Logging Runbook 允許使用指定的 Amazon Data Firehose AWS WAF (Firehose) 交付串流記錄 (AWS WAF V2) Web 存取控制清單 (Web ACL)。

[執行此自動化 \(主控台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- LogDestinationConfigs

類型：字串

描述：(必要) 您要與 Web ACL 建立關聯的 Firehose 交付串流 ARN。

Note

Firehose 交付串流 ARN 必須以字首 `aws-waf-logs-` 開頭。例如，`aws-waf-logs-us-east-2-analytics`。如需詳細資訊，請參閱 [Amazon Data Firehose](#)。

- WebAclArn

類型：字串

描述：(必要) 將啟用日誌記錄之 Web ACL 的 ARN。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`

- `wafv2:GetLoggingConfiguration`

文件步驟

- `aws:executeScript` - 啟用 AWS WAF V2 Web ACL 的記錄，並驗證記錄是否具有指定的組態。

Amazon WorkSpaces

AWS Systems Manager 自動化為 Amazon WorkSpaces 提供預先定義的 Runbook。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

AWS-CreateWorkSpace

Description

AWS-CreateWorkSpace Runbook 會根據您為輸入參數指定的值，建立新的 Amazon WorkSpaces 虛擬桌面，稱為 WorkSpace。如需 WorkSpaces 的相關資訊，請參閱《[Amazon WorkSpaces 管理指南](#)》中的什麼是 [Amazon WorkSpaces](#)？。 Amazon WorkSpaces

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- BundleId

類型：字串

描述：(必要) 用於 Workspace 的套件 ID。

- ComputeTypeName

類型：字串

有效值：VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

描述：(選用) Workspace 的運算類型。

- DirectoryId

類型：字串

描述：(必要) 要新增 Workspace 的目錄 ID。

- RootVolumeEncryptionEnabled

類型：布林值

有效值：true | false

預設：false

描述：（選用）判斷 Workspace 的根磁碟區是否已加密。

- RootVolumeSizeGib

類型：整數

描述：（必要）Workspace 根磁碟區的大小。

- RunningMode

類型：字串

有效值：ALWAYS_ON | AUTO_STOP

描述：（必要）Workspace 的執行模式。

- RunningModeAutoStopTimeoutInMinutes

類型：整數

描述：（選用）使用者在 WorkSpaces 停止時登出後的時間。以 60 分鐘的間隔指定值。

- 標籤

類型：字串

描述：（選用）您要套用至 Workspace 的標籤。

- UserName

類型：字串

描述：（必要）要與 Workspace 建立關聯的使用者名稱。

- UserVolumeEncryptionEnabled

類型：布林值

有效值：true | false

預設：false

描述：（選用）判斷 Workspace 的使用者磁碟區是否已加密。

- UserVolumeSizeGib

類型：整數

描述：（必要）WorkSpace 的使用者磁碟區大小。

- VolumeEncryptionKey

類型：字串

描述：（選用）您要用來加密 WorkSpace 上存放資料的對稱 AWS Key Management Service 金鑰。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

文件步驟

- aws:executeScript - 根據您為輸入參數指定的值建立 WorkSpace。
- aws:waitForAwsResourceProperty - 驗證 WorkSpace 的狀態為 AVAILABLE。

輸出

CreateWorkspace.WorkspaceId

AWSsupport-RecoverWorkSpace

Description

AWSsupport-RecoverWorkSpace Runbook 會在您指定的 Amazon WorkSpaces 虛擬桌面上執行復原步驟，稱為 WorkSpace。Runbook 會重新啟動 WorkSpace，如果狀態仍然為 UNHEALTHY，會根據您為輸入參數指定的值來還原或重建 WorkSpace。使用此 Runbook 之前，建議您檢閱《[Amazon WorkSpaces 管理指南](#)》中的對 [WorkSpaces 問題進行故障診斷](#)。Amazon WorkSpaces

⚠ Important

還原或重建 Workspace 是可能導致資料遺失的潛在破壞性動作。這是因為 Workspace 從最後一個可用的快照還原，而從快照復原的資料可能長達 12 小時。

還原選項會根據最新的快照重新建立根磁碟區和使用者磁碟區。重建選項會從最新的快照重新建立使用者磁碟區，並從與建立 Workspace 之套件相關聯的映像重新建立 Workspace。

已安裝的應用程式或在建立 Workspace 後變更的系統設定將會遺失。如需還原和重建 WorkSpaces 的詳細資訊，請參閱《Amazon [WorkSpaces 管理指南](#)》中的[還原 Workspace](#)和[重建 Workspace](#) Workspace。Amazon WorkSpaces

執行此自動化（主控台）

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：（選用）允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。如果未指定角色，Systems Manager Automation 會使用啟動此 Runbook 之使用者的許可。

- 確認

類型：字串

有效值：是

描述：（必要）輸入 yes 表示您了解還原和重建動作會嘗試從最新的快照復原 Workspace，而且從這些快照還原的資料可能長達 12 小時。

- 重新開機

類型：字串

有效值：是 | 否

預設：是

描述：(必要) 判斷 Workspace 是否重新啟動。

- 重建

類型：字串

有效值：是 | 否

預設：否

描述：(必要) 判斷 Workspace 是否重建。

- 還原

類型：字串

有效值：是 | 否

預設：否

描述：(必要) 決定是否還原 Workspace。

- WorkspaceId

類型：字串

描述：(必要) 您要復原的 Workspace ID。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

workspaces:DescribeWorkspaces

- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

文件步驟

- `aws:executeAwsApi` - 收集您在 `WorkspaceId` 參數中指定的 `WorkSpace` 狀態。
- `aws:assertAwsResourceProperty` - 驗證 `WorkSpace` 的狀態為 `AVAILABLE`、`ERROR`、`IMPAIRED` `STOPPED` 或 `UNHEALTHY`。
- `aws:branch` - 根據 `WorkSpace` 狀態的分支。
- `aws:executeAwsApi` - 啟動 `WorkSpace`。
- `aws:branch` - 根據您為 `Action` 參數指定的值進行分支。
- `aws:waitForAwsResourceProperty` - 在啟動後等待 `WorkSpace` 狀態。
- `aws:waitForAwsResourceProperty` - 等待 `WorkSpace` 狀態在啟動 `UNHEALTHY` 後變更為 `AVAILABLE`、`ERROR` `IMPAIRED` 或。
- `aws:executeAwsApi` - 開始後收集 `WorkSpace` 的狀態。
- `aws:branch` - 啟動後根據 `WorkSpace` 狀態進行分支。
- `aws:executeAwsApi` - 收集可用於還原或重建 `WorkSpace` 的快照。
- `aws:branch` - 根據您為 `Reboot` 參數指定的值進行分支。
- `aws:executeAwsApi` - 重新啟動 `WorkSpace`。
- `aws:executeAwsApi` - 開始後收集 `WorkSpace` 的狀態。
- `aws:waitForAwsResourceProperty` - 等待 `WorkSpace` 的狀態變更為 `REBOOTING`。
- `aws:waitForAwsResourceProperty` - 等待 `WorkSpace` 狀態在重新啟動 `UNHEALTHY` 後變更為 `AVAILABLE`、`ERROR` 或。
- `aws:executeAwsApi` - 在重新啟動後收集 `WorkSpace` 的狀態。
- `aws:branch` - 重新啟動後，根據 `WorkSpace` 狀態進行分支。
- `aws:branch` - 根據您為 `Restore` 參數指定的值進行分支。
- `aws:executeAwsApi` - 還原 `WorkSpace`。如果還原失敗，Runbook 會嘗試重建 `WorkSpace`。
- `aws:waitForAwsResourceProperty` - 等待 `WorkSpace` 的狀態變更為 `RESTORING`。

- `aws:waitForAwsResourceProperty` - 等待 WorkSpace 狀態在還原UNHEALTHY後變更為 AVAILABLE 、 ERROR 或 。
- `aws:executeAwsApi` - 在還原後收集 WorkSpace 的狀態。
- `aws:branch` - 還原後根據 WorkSpace 狀態進行分支。
- `aws:branch` - 根據您為 Rebuild 參數指定的值進行分支。
- `aws:executeAwsApi` - 重建 WorkSpace。
- `aws:waitForAwsResourceProperty` - 等待 WorkSpace 的狀態變更為 REBUILDING 。
- `aws:waitForAwsResourceProperty` - 等待 WorkSpace 狀態在重建UNHEALTHY後變更為 AVAILABLE 、 ERROR 或 。
- `aws:executeAwsApi` - 在重建後收集 WorkSpace 的狀態。
- `aws:assertAwsResourceProperty` - 確認 WorkSpace 的狀態為 AVAILABLE 。

X-Ray

AWS Systems Manager 自動化為 提供預先定義的 Runbook AWS X-Ray。如需有關執行手冊的詳細資訊，請參閱 [Working with runbooks](#)。如需如何檢視 Runbook 內容的詳細資訊，請參閱 [檢視 Runbook 內容](#)。

主題

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

AWSConfigRemediation-UpdateXRayKMSKey

Description

AWSConfigRemediation-UpdateXRayKMSKey Runbook 會使用 AWS Key Management Service (AWS KMS) 金鑰啟用 AWS X-Ray 資料加密。此 Runbook 應僅用作基準，以確保 AWS X-Ray 根據最低建議的安全性最佳實務加密您的資料。我們建議您使用不同的 KMS 金鑰加密多組資料。

[執行此自動化（主控台）](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、macOS、Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager Automation 代表您執行動作的 (IAM) 角色的 AWS Identity and Access Management Amazon Resource Name (ARN)。

- KeyId

類型：字串

描述：(必要) AWS X-Ray 要用來加密資料的 KMS 金鑰的 Amazon Resource Name (ARN)、金鑰 ID 或金鑰別名。

必要的 IAM 許可

AutomationAssumeRole 參數需要下列動作才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:DescribeKey
- xray:GetEncryptionConfig
- xray:PutEncryptionConfig

文件步驟

- aws:executeAwsApi - 使用您在 KeyId 參數中指定的 KMS 金鑰啟用 X-Ray 資料的加密。
- aws:waitForAwsResourceProperty - 等待 X-Ray 的加密組態狀態為 ACTIVE 。
- aws:executeAwsApi - 收集您在 KeyId 參數中指定的金鑰 ARN。
- aws:assertAwsResourceProperty - 驗證已在您的 X-Ray 上啟用加密。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。