



使用者指南

# AWS Systems Manager 自動化手冊參考



# AWS Systems Manager 自動化手冊參考: 使用者指南

Copyright © 2024 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 參考 .....	1
檢視工作手冊內容 .....	3
API 閘道 .....	4
AWSConfigRemediation-DeleteAPIGatewayStage .....	4
AWSConfigRemediation-EnableAPIGatewayTracing .....	5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching .....	6
AWS Batch .....	8
AWSSupport-TroubleshootAWSBatchJob .....	8
AWS CloudFormation .....	13
AWS-DeleteCloudFormationStack .....	14
AWS-EnableCloudFormationSNSNotification .....	15
AWS-RunCfnLint .....	16
AWSSupport-TroubleshootCFNCustomResource .....	19
AWS-UpdateCloudFormationStack .....	20
CloudFront .....	21
AWSConfigRemediation-EnableCloudFrontDefaultRootObject .....	22
AWSConfigRemediation-EnableCloudFrontAccessLogs .....	23
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity .....	25
AWSConfigRemediation-EnableCloudFrontOriginFailover .....	26
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS .....	28
CloudTrail .....	29
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail .....	30
AWS-EnableCloudTrail .....	31
AWS-EnableCloudTrailCloudWatchLogs .....	33
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS .....	34
AWS-EnableCloudTrailKmsEncryption .....	35
AWSConfigRemediation-EnableCloudTrailLogFileValidation .....	37
AWS-EnableCloudTrailLogFileValidation .....	38
AWS-QueryCloudTrailLogs .....	39
CloudWatch .....	41
AWS-ConfigureCloudWatchOnEC2Instance .....	41
AWS-EnableCWAlarm .....	43
Amazon DocumentDB .....	45
AWS-EnableDocDbClusterBackupRetentionPeriod .....	45

CodeBuild .....	47
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK .....	47
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject .....	49
AWS CodeDeploy .....	50
AWSSupport-TroubleshootCodeDeploy .....	51
AWS Config .....	52
AWSSupport-SetupConfig .....	53
Amazon Connect .....	55
AWSSupport-AssociatePhoneNumbersToConnectContactFlows .....	55
AWSSupport-CollectAmazonConnectContactFlowLog .....	62
AWS Directory Service .....	67
AWS-CreateDSManagementInstance .....	68
AWSSupport-TroubleshootADConnectorConnectivity .....	72
AWSSupport-TroubleshootDirectoryTrust .....	75
AWS AppSync .....	79
AWS-EnableAppSyncGraphQLApiLogging .....	79
Amazon Athena .....	81
AWS-EnableAthenaWorkGroupEncryptionAtRest .....	81
DynamoDB .....	83
AWS-ChangeDDBRWCapacityMode .....	84
AWS-CreateDynamoDBBackup .....	86
AWS-DeleteDynamoDbBackup .....	87
AWSConfigRemediation-DeleteDynamoDbTable .....	88
AWS-DeleteDynamoDbTableBackups .....	89
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable .....	90
AWSConfigRemediation-EnablePITRForDynamoDbTable .....	92
AWS-EnableDynamoDbAutoscaling .....	93
AWS-RestoreDynamoDBTable .....	96
Amazon EBS .....	98
AWSSupport-AnalyzeEBSResourceUsage .....	99
AWS-ArchiveEBSSnapshots .....	105
AWS-AttachEBSVolume .....	107
AWSSupport-CalculateEBSPerformanceMetrics .....	108
AWS-CopySnapshot .....	115
AWS-CreateSnapshot .....	116
AWS-DeleteSnapshot .....	117

AWSConfigRemediation-DeleteUnusedEBSVolume .....	118
AWS-DeregisterAMIs .....	119
AWS-DetachEBSVolume .....	121
AWSConfigRemediation-EnableEbsEncryptionByDefault .....	122
AWS-ExtendEbsVolume .....	123
AWSSupport-ModifyEBSSnapshotPermission .....	125
AWSConfigRemediation-ModifyEBSVolumeType .....	127
Amazon EC2 .....	129
AWS-ASGEnterStandby .....	130
AWS-ASGExitStandby .....	131
AWS-CreateImage .....	132
AWS-DeleteImage .....	134
AWS-PatchAsgInstance .....	135
AWS-PatchInstanceWithRollback .....	137
AWS-QuarantineEC2Instance .....	140
AWS-ResizeInstance .....	142
AWS-RestartEC2Instance .....	143
AWS-SetupJupyter .....	144
AWS-StartEC2Instance .....	147
AWS-StopEC2Instance .....	148
AWS-TerminateEC2Instance .....	149
AWS-UpdateLinuxAmi .....	149
AWS-UpdateWindowsAmi .....	152
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck .....	155
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 .....	157
AWSEC2-CloneInstanceAndUpgradeSQLServer .....	158
AWSEC2-CloneInstanceAndUpgradeWindows .....	162
AWSEC2-ConfigureSTIG .....	165
AWSEC2-PatchLoadBalancerInstance .....	192
AWSEC2-SQLServerDBRestore .....	193
AWSSupport-ActivateWindowsWithAmazonLicense .....	198
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 .....	200
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD .....	204
AWSSupport-CheckXenToNitroMigrationRequirements .....	210
AWSSupport-ConfigureEC2Metadata .....	212
AWSSupport-CopyEC2Instance .....	215

AWSSupport-EnableWindowsEC2SerialConsole .....	220
AWSSupport-ExecuteEC2Rescue .....	228
AWSSupport-ListEC2Resources .....	231
AWSSupport-ManageRDPSettings .....	233
AWSSupport-ManageWindowsService .....	235
AWSSupport-MigrateEC2ClassicToVPC .....	237
AWSSupport-MigrateXenToNitroLinux .....	243
AWSSupport-ResetAccess .....	254
AWSSupport-ResetLinuxUserPassword .....	256
AWSPremiumSupport-ResizeNitroInstance .....	262
AWSSupport-RestoreEC2InstanceFromSnapshot .....	268
AWSSupport-SendLogBundleToS3Bucket .....	272
AWSSupport-StartEC2RescueWorkflow .....	274
AWSPremiumSupport-TroubleshootEC2DiskUsage .....	284
AWSSupport-TroubleshootEC2InstanceConnect .....	289
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs .....	294
AWSSupport-TroubleshootRDP .....	297
AWSSupport-TroubleshootSSH .....	303
AWSSupport-TroubleshootSUSERegistration .....	306
AWSSupport-TroubleshootWindowsPerformance .....	308
AWSSupport-TroubleshootWindowsUpdate .....	315
AWSSupport-UpgradeWindowsAWSDrivers .....	321
Amazon ECS .....	324
AWSSupport-CollectECSInstanceLogs .....	325
AWS-InstallAmazonECSAgent .....	327
AWS-ECSRunTask .....	329
AWSSupport-TroubleshootECSContainerInstance .....	332
AWSSupport-TroubleshootECSTaskFailedToStart .....	334
AWS-UpdateAmazonECSAgent .....	338
Amazon EFS .....	339
AWSSupport-CheckAndMountEFS .....	340
Amazon EKS .....	343
AWSSupport-CollectEKSIInstanceLogs .....	343
AWS-CreateEKSClusterWithFargateProfile .....	345
AWS-CreateEKSClusterWithNodegroup .....	348
AWS-DeleteEKSCluster .....	352

AWS-MigrateToNewEKSSelfManagedNodeGroup .....	354
AWSPremiumSupport-TroubleshootEKSCluster .....	360
AWSSupport-TroubleshootEKSWorkerNode .....	363
AWS-UpdateEKSCluster .....	366
AWS-UpdateEKSMangedNodeGroup .....	367
AWS-UpdateEKSSelfManagedLinuxNodeGroups .....	371
Elastic Beanstalk .....	374
AWSSupport-CollectElasticBeanstalkLogs .....	375
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	377
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications .....	379
AWSSupport-TroubleshootElasticBeanstalk .....	380
Elastic Load Balancing .....	383
AWSConfigRemediation-DropInvalidHeadersForALB .....	383
AWS-EnableCLBAccessLogs .....	385
AWS-EnableCLBConnectionDraining .....	386
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing .....	388
AWSConfigRemediation-EnableELBDeletionProtection .....	389
AWSConfigRemediation-EnableLoggingForALBAndCLB .....	390
AWSSupport-TroubleshootCLBConnectivity .....	392
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing .....	395
AWS-UpdateALBDesyncMitigationMode .....	396
AWS-UpdateCLBDesyncMitigationMode .....	398
Amazon EMR .....	400
AWSSupport-AnalyzeEMRLogs .....	400
AWSSupport-DiagnoseEMRLogsWithAthena .....	405
Amazon OpenSearch 服務 .....	413
AWSConfigRemediation-DeleteOpenSearchDomain .....	413
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain .....	414
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups .....	416
AWSSupport-TroubleshootOpenSearchRedYellowCluster .....	417
AWSSupport-TroubleshootOpenSearchHighCPU .....	423
EventBridge .....	429
AWS-AddOpsItemDedupStringToEventBridgeRule .....	429
AWS-DisableEventBridgeRule .....	430
Amazon FSx .....	432
AWSSupport-ValidateFSxWindowsADConfig .....	432

GuardDuty .....	445
AWSConfigRemediation-CreateGuardDutyDetector .....	446
IAM .....	447
AWS-AttachIAMToInstance .....	447
AWS-DeleteIAMInlinePolicy .....	449
AWSConfigRemediation-DeleteIAMRole .....	451
AWSConfigRemediation-DeleteIAMUser .....	452
AWSConfigRemediation-DeleteUnusedIAMGroup .....	455
AWSConfigRemediation-DeleteUnusedIAMPolicy .....	456
AWSConfigRemediation-DetachIAMPolicy .....	457
AWSConfigRemediation-EnableAccountAccessAnalyzer .....	459
AWSSupport-GrantPermissionsToIAMUser .....	460
AWSConfigRemediation-RemoveUserPolicies .....	465
AWSConfigRemediation-ReplaceIAMInlinePolicy .....	466
AWSConfigRemediation-RevokeUnusedIAMUserCredentials .....	468
AWSConfigRemediation-SetIAMPasswordPolicy .....	470
Amazon Kinesis Data Streams .....	473
AWS-EnableKinesisStreamEncryption .....	473
AWS KMS .....	475
AWSConfigRemediation-CancelKeyDeletion .....	475
AWSConfigRemediation-EnableKeyRotation .....	476
Lambda .....	477
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing .....	478
AWSConfigRemediation-DeleteLambdaFunction .....	479
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK .....	480
AWSConfigRemediation-MoveLambdaToVPC .....	482
AWSSupport-RemediateLambdaS3Event .....	483
AWSSupport-TroubleshootLambdaInternetAccess .....	486
AWSSupport-TroubleshootLambdaS3Event .....	489
Amazon Managed Workflows for Apache Airflow .....	491
AWSSupport-TroubleshootMWAAEnvironmentCreation .....	491
Neptune .....	497
AWS-EnableNeptuneDbAuditLogsToCloudWatch .....	497
AWS-EnableNeptuneDbBackupRetentionPeriod .....	498
AWS-EnableNeptuneClusterDeletionProtection .....	500
Amazon RDS .....	502



AWS-CreateEncryptedRdsSnapshot .....	503
AWS-CreateRdsSnapshot .....	505
AWSConfigRemediation-DeleteRDSCluster .....	506
AWSConfigRemediation-DeleteRDSClusterSnapshot .....	508
AWSConfigRemediation-DeleteRDSInstance .....	509
AWSConfigRemediation-DeleteRDSInstanceSnapshot .....	511
AWSConfigRemediation-DisablePublicAccessToRDSInstance .....	512
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster .....	513
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance .....	515
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance .....	517
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS .....	518
AWSConfigRemediation-EnableMultiAZOnRDSInstance .....	520
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance .....	521
AWSConfigRemediation-EnableRDSClusterDeletionProtection .....	523
AWSConfigRemediation-EnableRDSInstanceBackup .....	524
AWSConfigRemediation-EnableRDSInstanceDeletionProtection .....	526
AWSConfigRemediation-ModifyRDSInstancePortNumber .....	528
AWSSupport-ModifyRDSSnapshotPermission .....	529
AWSPremiumSupport-PostgreSQLWorkloadReview .....	531
AWS-RebootRdsInstance .....	546
AWSSupport-ShareRDSSnapshot .....	547
AWS-StartRdsInstance .....	550
AWS-StartStopAuroraCluster .....	551
AWS-StopRdsInstance .....	553
AWSSupport-TroubleshootConnectivityToRDS .....	553
AWSSupport-TroubleshootRDSIAMAuthentication .....	556
AWSSupport-ValidateRdsNetworkConfiguration .....	563
Amazon Redshift .....	568
AWSConfigRemediation-DeleteRedshiftCluster .....	569
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster .....	570
AWSConfigRemediation-EnableRedshiftClusterAuditLogging .....	572
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot .....	573
AWSConfigRemediation-EnableRedshiftClusterEncryption .....	575
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting .....	576
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster .....	577
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings .....	579

AWSConfigRemediation-ModifyRedshiftClusterNodeType .....	580
Amazon S3 .....	582
AWS-ArchiveS3BucketToIntelligentTiering .....	583
AWS-ConfigureS3BucketLogging .....	585
AWS-ConfigureS3BucketVersioning .....	587
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock .....	588
AWSConfigRemediation-ConfigureS3PublicAccessBlock .....	590
AWS-CreateS3PolicyToExpireMultipartUploads .....	592
AWS-DisableS3BucketPublicReadWrite .....	594
AWS-EnableS3BucketEncryption .....	595
AWS-EnableS3BucketKeys .....	596
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy .....	597
AWSConfigRemediation-RestrictBucketSSLRequestsOnly .....	599
AWSSupport-TroubleshootS3PublicRead .....	600
SageMaker .....	605
AWS-DisableSageMakerNotebookRootAccess .....	605
Secrets Manager .....	607
AWSConfigRemediation-DeleteSecret .....	608
AWSConfigRemediation-RotateSecret .....	609
安全中樞 .....	611
AWSConfigRemediation-EnableSecurityHub .....	611
AWS Shield .....	612
AWSPremiumSupport-DDoSResiliencyAssessment .....	612
Amazon SNS .....	621
AWS-EnableSNSTopicDeliveryStatusLogging .....	621
AWSConfigRemediation-EncryptSNSTopic .....	623
AWS-PublishSNSNotification .....	625
Amazon SQS .....	626
AWS-EnableSQSEncryption .....	626
Step Functions .....	628
AWS-EnableStepFunctionsStateMachineLogging .....	628
Systems Manager .....	630
AWS-BulkDeleteAssociation .....	631
AWS-BulkEditOpsItems .....	632
AWS-BulkResolveOpsItems .....	635
AWS-ConfigureMaintenanceWindows .....	637

AWS-CreateManagedLinuxInstance .....	638
AWS-CreateManagedWindowsInstance .....	641
AWSConfigRemediation-EnableCWLoggingForSessionManager .....	643
AWS-ExportOpsDataToS3 .....	645
AWS-ExportPatchReportToS3 .....	646
AWS-SetupInventory .....	648
AWS-SetupManagedInstance .....	652
AWS-SetupManagedRoleOnEC2Instance .....	653
AWSSupport-TroubleshootManagedInstance .....	654
AWSSupport-TroubleshootPatchManagerLinux .....	657
AWSSupport-TroubleshootSessionManager .....	660
第三方 .....	665
AWS-CreateJiraIssue .....	665
AWS-CreateServiceNowIncident .....	667
AWS-RunPacker .....	670
Amazon VPC .....	671
AWS-CloseSecurityGroup .....	672
AWSSupport-ConfigureDNSQueryLogging .....	674
AWSSupport-ConfigureTrafficMirroring .....	677
AWSSupport-ConnectivityTroubleshooter .....	679
AWSSupport-TroubleshootVPN .....	682
AWSConfigRemediation-DeleteEgressOnlyInternetGateway .....	688
AWSConfigRemediation-DeleteUnusedENI .....	689
AWSConfigRemediation-DeleteUnusedSecurityGroup .....	690
AWSConfigRemediation-DeleteUnusedVPCNetworkACL .....	691
AWSConfigRemediation-DeleteVPCFlowLog .....	693
AWSConfigRemediation-DetachAndDeleteInternetGateway .....	694
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway .....	696
AWS-DisableIncomingSSHOnPort22 .....	697
AWS-DisablePublicAccessForSecurityGroup .....	699
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP .....	700
AWSSupport-EnableVPCFlowLogs .....	701
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch .....	707
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket .....	709
AWS-ReleaseElasticIP .....	711
AWS-RemoveNetworkACLUnrestrictedSSHRDP .....	712

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules .....	713
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules .....	714
AWSSupport-SetupIPMonitoringFromVPC .....	716
AWSSupport-TerminateIPMonitoringFromVPC .....	727
AWS WAF .....	730
AWS-AddWAFRegionalRuleToRuleGroup .....	730
AWS-AddWAFRegionalRuleToWebAcl .....	732
AWSConfigRemediation-EnableWAFClassicLogging .....	735
AWSConfigRemediation-EnableWAFClassicRegionalLogging .....	736
AWSConfigRemediation-EnableWAFV2Logging .....	738
Amazon WorkSpaces .....	739
AWS-CreateWorkSpace .....	740
AWSSupport-RecoverWorkSpace .....	743
X-Ray .....	746
AWSConfigRemediation-UpdateXRayKMSKey .....	747
.....	cccxlx

# Systems Manager Automation Runbook 參考

為了協助您快速開始使用，請 AWS Systems Manager 提供預先定義的 Runbook。這些手冊是由 Amazon Web Services 維護 AWS Support, 和 AWS Config. runbook 參考說明 Systems Manager、AWS Support和所提供的每個預先定義的 Runbook。AWS Config

## Important

如果您執行使用 AWS Identity and Access Management (IAM) 服務角色呼叫其他服務的自動化工作流程，請注意服務角色必須具有叫用這些服務的權限來設定服務角色。此要求適用於所有 AWS Automation Runbook (AWS-\* Runbook)，例如 AWS-ConfigureS3BucketLogging、AWS-CreateDynamoDBBackup 和 AWS-RestartEC2Instance Runbook 等。此需求也適用於您建立的任何自訂 Automation Runbook，以呼叫其他 AWS 服務的動作呼叫其他服務。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內嵌原則新增至角色，以啟用其他 AWS 服務的權限。如需詳細資訊，請參閱[新增自動化內嵌原則以叫用其他 AWS 服務](#)。

本參考文獻包含描述 AWS、AWS Support和 AWS Config所擁有之每個 Systems Manager 手冊的主題。手冊由相關 AWS 服務組織。每個頁面都提供了使用 runbook 時可以指定的必要和可選參數的說明。每個頁面還列出了 runbook 中的步驟和自動化的輸出（如果有的話）。

此參考資料不包含需要核准 (例如AWS-CreateManagedLinuxInstanceWithApproval或 runbook) 之類的 R AWS-StopEC2InstanceWithApproval unbook 的個別頁面。任何 runbook 名稱包括WithApproval, 意味著手冊包括行動 [aws:approve](#). 此動作會暫時暫停自動化操作，直到指定的主參與者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。

如需執行自動化的相關資訊，請參閱[執行簡單自動化操作](#)。如需在多個目標上執行自動化的相關資訊，請參閱[執行使用目標和費率控制的自動化](#)。

## 主題

- [檢視工作手冊內容](#)
- [API 闡道](#)
- [AWS Batch](#)
- [AWS CloudFormation](#)

- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)
- [Amazon OpenSearch 服務](#)
- [EventBridge](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow](#)
- [Neptune](#)

- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [SageMaker](#)
- [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](#)

## 檢視工作手冊內容

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

若要檢視工作手冊內容

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

-或-

如果 AWS Systems Manager 首頁首頁開啟，請選擇功能表圖示

(☰

) 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 閘道

AWS Systems Manager 自動化為 Amazon API 閘道提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

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

## AWSConfigRemediation-DeleteAPIGatewayStage

### Description (描述)

該手AWSConfigRemediation-DeleteAPIGatewayStage冊刪除了亞馬遜 API 網關 (API 網關) 階段。AWS Config 必須在您執行此自動化操作的AWS 區域位置啟用。

### [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- StageArn



類型：字串

描述：(必填) 您要刪除之 API 閘道階段的 Amazon 資源名稱 (ARN)。

必要的 IAM 許可

此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 閘道階段。

## AWSConfigRemediation-EnableAPIGatewayTracing

Description (描述)

AWSConfigRemediation-EnableAPIGatewayTracing執行手冊可在亞馬遜 API 閘道 (API 閘道) 階段上進行追蹤。AWS Config必須在您執行此自動化操作的AWS 區域位置啟用。

[運行此自動化 \(控制台\)](#)

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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- StageArn

類型：字串

描述：(必填) 您要啟用追蹤之 API 閘道階段的 Amazon 資源名稱 (ARN)。

### 必要的 IAM 許可

此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 閘道階段啟用追蹤。

## AWSConfigRemediation-UpdateAPIGatewayMethodCaching

### Description (描述)

AWSConfigRemediation-UpdateAPIGatewayMethodCaching執行手冊會更新 Amazon API 閘道階段資源的快取方法設定。

### [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- CachingAuthorizedMethods

類型:StringList

說明：(必要) 授權啟用快取的方法。清單必須

是DELETE、、、GETHEADOPTIONSPATCH、POST和的某些組合PUT。快取會針對選取的方法啟用，而非選取的方法則會停用快取。如果已選取，則會啟用所有方法ANY的快取，如果已選取，則NONE會停用所有方法的快取。

- StageArn

類型：字串

說明：(必要) API 的 API 閘道階段 ARN。REST

### 必要的 IAM 許可

此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 作為輸入，使用 API 動作更新 API 閘道階段的快取方法設定，並驗證更新。`UpdateStage`

## AWS Batch

AWS Systems Manager 自動化提供預先定義的 AWS Batch 執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

- [AWSSupport-TroubleshootAWSBatchJob](#)

## AWSSupport-TroubleshootAWSBatchJob

### Description

`AWSSupport-TroubleshootAWSBatchJob` runbook 可協助您疑難排解阻止 AWS Batch 工作從狀態進行的問題。`RUNNABLE STARTING`

它是如何工作的？

此 Runbook 執行以下檢查：

- 如果運算環境處於`INVALID`或`DISABLED`狀態。
- 如果計算環境的`Max vCPU`參數大到足以容納工作佇列中的工作量。
- 如果工作所需的記憶體 `vCPUs` 資源超過運算環境的執行個體類型所能提供的資源。
- 如果作業應在執行個體 GPU 上執行，但運算環境未設定 GPU 為使用型執行個體。
- 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 彈性容器服務 (Amazon ECS) 叢集；如果沒有，則會執行 [AWSSupport-TroubleshootECSContainer](#) 執行手冊。
- 如果有任何權限問題封鎖執行工作所需的特定動作。

### Important

- 這個 runbook 必須在相同的 AWS 地區啟動，因為你的工作被卡在`RUNNABLE`狀態。

- 可以針 AWS Batch 對在 Amazon AWS Fargate 或 Amazon 彈性運算雲端 (Amazon EC2) 執行個體上排定的任務啟動此執行手冊。如果在 Amazon 彈性 Kubernetes 服務 (亞馬遜EKS) 上啟動某 AWS Batch 個任務的自動化，則啟動會停止。
- 如果執行個體可用於執行任務，但無法註冊 Amazon ECS 叢集，則此 runbook 會啟AWSsupport-TroubleshootECSContainerInstance動自動化執行手冊，以嘗試判斷原因。如需詳細資訊，請參考 [AWSsupport-T roubleshootECSContainer 執行個體執行手冊](#)。

## 運行此自動化 (控制台)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- JobId

類型：字串

描述：(必要) 卡在RUNNABLE狀態中的 AWS Batch Job ID。

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

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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. 瀏覽至主 AWS Systems Manager 控制台中的 [AWSSupport-TroubleshootAWSBatchJob](#)。
2. 選擇執行自動化
3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole(選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- JobId ( 必填 )：

停留在RUNNABLE狀態中的 AWS Batch Job ID。

**Input parameters**

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Choose an option

**JobId**  
(Required) The ID of the AWS Batch Job that is stuck in RUNNABLE status.

b9[REDACTED]e32

4. 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/角色執行預檢IAM權限檢查。如果有任何遺失權限，此步驟會提供全域輸出區段中遺失的API動作。

- ProceedOnlyIfUserHasPermission:

基於你是否有權限為 runbook 的所有必要操作的分支。

- `AWSBatchJobEvaluation`:

對 AWS Batch Job 執行檢查，確認工作是否存在且處於RUNNABLE狀態。

- `ProceedOnlyIfBatchJobExistsAndIsinRunnableState`:

根據工作是否存在且處於RUNNABLE狀態進行分支。

- `BatchComputeEnvironmentEvaluation`:

對 AWS Batch 計算環境執行檢查。

- `ProceedOnlyIfComputeEnvironmentChecksAreOK` :

以計算環境檢查是否成功為基礎的分支。

- `UnderlyingInfraEvaluation`:

對基礎 Auto Scaling 群組或競價型叢集請求執行檢查。

- `ProceedOnlyIfInstancesNotJoiningEcsCluster`:

根據是否有執行個體未加入 Amazon ECS 叢集而定的分支。

- `EcsAutomationRunner`:

針對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URI供評估報告HTML檔案的：

S3 控制台鏈接和 Amazon S3，URI用於成功執行手冊的報告



## ▼ Outputs

ExecutionResults.message

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

```

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0EEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0EEWmt8eY" 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-egMKn0EEWmt8eY".
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[REDACTED]606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

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

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0EEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0EEWmt8eY" 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-egMKn0EEWmt8eY".
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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化工作流登陸頁](#)

## AWS CloudFormation

AWS Systems Manager 自動化提供預先定義的 AWS CloudFormation 執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWS-DeleteCloudFormationStack](#)
- [AWS-EnableCloudFormationSNSNotification](#)

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

## AWS-DeleteCloudFormationStack

### Description (描述)

刪除 AWS CloudFormation 堆疊。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux, macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- StackNameOrId

類型：字串

描述：(必填) 要刪除之 CloudFormation 堆疊的名稱或唯一 ID

# AWS-EnableCloudFormationSNSNotification

## Description

該 AWS-EnableCloudFormationSNSNotification runbook 為您指定的 ( SNS ) 堆棧啟用 Amazon 簡單通知服務 AWS CloudFormation ( Amazon AWS CloudFormation ) 通知。

## [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- StackArn

類型：字串

說明：(必填) 您要啟用 Amazon SNS 通知的 AWS CloudFormation 堆疊名稱 ARN 或名稱。

- NotificationArn

類型：字串

說明：( 必填 ) 您要與 AWS CloudFormation 堆棧關聯的 Amazon SNS 主題。ARN

### 所需 IAM 權限

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

- SSM : GetAutomationExecution
- SSM : StartAutomationExecution
- 雲形 : DescribeStacks
- 雲形 : UpdateStack
- kms:解密
- 公里 : GenerateDataKey
- sns:Publish
- 平方 : GetQueueAttributes

### 文件步驟

- CheckCfnSnsLimits ( aws:executeScript ) -驗證尚未與您指定的 AWS CloudFormation 堆棧相關聯的 Amazon SNS 主題的最大數量。
- EnableCfnSnsNotification ( aws:executeAwsApi ) -為 AWS CloudFormation 堆棧啟用 Amazon SNS 通知。
- VerificationCfnSnsNotification (aws:executeScript)-驗證是否已為 AWS CloudFormation 堆疊啟用 Amazon SNS 通知。

### 輸出

CheckCfnSnsLimits。 NotificationArnList -接收 Amazon AWS CloudFormation 堆棧SNS通知的列表。 ARNs

VerificationCfnSnsNotification。 VerifySnsTopicsResponse -確認已為 AWS CloudFormation 堆疊啟用 Amazon SNS 通知的API作業回應。

## AWS-RunCfnLint

### Description (描述)

此手冊使用一個[AWS CloudFormation林特](#) ( cfn-python-lint ) 來驗證 YAML 和 JSON 模板對資源規範。AWS CloudFormationAWS-RunCfnLintrunbook 會執行額外的檢查，例如確保已為資源屬性輸入有效值。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。

## 運行此自動化 (控制台)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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：默認 | 安靜 | 可解析 | 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。

- 範本 3 BucketName

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

說明：(選擇性) 要傳遞給 `--regions` 參數的值，以根據指定的範本測試範本AWS 區域。

範例：us-east-1、us-west-1

## 文件步驟

RunCfnLintAgainstTemplate— 針對指定的AWS CloudFormation範本執行 `cfn-python-lint` 工具。

## 輸出

RunCfnLintAgainstTemplate輸出 — 工具的標準輸出。cfn-python-lint

## AWSsupport-TroubleshootCFNCustomResource

### Description (描述)

AWSsupport-TroubleshootCFNCustomResource 有助於診斷為什麼AWS CloudFormation堆疊在建立、更新或刪除自訂資源失敗。runbook 會檢查用於自訂資源的服務Token，以及傳回的錯誤訊息。檢閱自訂資源的詳細資料之後，runbook 輸出會提供堆疊行為的說明，以及自訂資源的疑難排解步驟。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux, macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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

此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，並輸出有關如何疑難排解失敗的自訂資源的資訊。

## AWS-UpdateCloudFormationStack

### Description

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

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LambdaAssumeRole

類型：字串

描述：(必要) Lambda 所承擔的角色

- StackNameOrId

類型：字串

說明：(必填) 要更新之 AWS CloudFormation 堆疊的名稱或唯一 ID

- TemplateUrl

類型：字串

說明：(必填) 包含更新 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 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

### 主題

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

# AWSConfigRemediation-EnableCloudFrontDefaultRootObject

## Description (描述)

AWSConfigRemediation-EnableCloudFrontDefaultRootObject 執行手冊會為您指定的 Amazon CloudFront (CloudFront) 分發設定預設根物件。

## [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- CloudFrontDistributionId

類型：字串

描述：(必要) 您要為其 CloudFront 配置預設根物件的發佈 ID。

- DefaultRootObject

類型：字串

描述：(必要) 當檢視者要求指 CloudFront 向您的根 URL 時，您要傳回的物件。

### 必要的 IAM 許可

此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-為您在參數中指定的CloudFront分佈配置預設根物件。CloudFrontDistributionId

## AWSConfigRemediation-EnableCloudFrontAccessLogs

### Description

AWSConfigRemediation-EnableCloudFrontAccessLogs執行手冊會為您指定的 Amazon CloudFront (CloudFront) 分發啟用存取記錄。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux 系統macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- BucketName

類型：字串

說明：(必填) 您要存放存取日誌的 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體的名稱。不支援遠南 -1、AP-東 1、歐南 -1 和我-南 -1 中的值區。AWS 區域

- CloudFrontId

類型：字串

描述：( 必填 ) 您要啟用存取記錄的 CloudFront 分發 ID。

- IncludeCookies

類型：布林值

有效值：true | false

說明：(必要) 如果您想要在存取記錄中包含 Cookie>true，請將此參數設定為。

- 字首

類型：字串

描述：(選用) 您想要 CloudFront filenames 為發行版之存取記錄前置詞的選擇性字串，例如，myprefix/。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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:GetBucketLocationAPI 只能用於同一帳戶中的 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-針對您在CloudFrontDistributionId參數中指定的 CloudFront 散佈啟用存取記錄。

## AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

## Description (描述)

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity執行手冊會為您指定的 Amazon CloudFront (CloudFront) 分發啟用來源存取身分。此自動化會為所有 Amazon 簡單儲存服務 (Amazon S3) CloudFront 原始類型的來源類型指派相同的來源存取身分識別，而不會為您指定的 CloudFront分發提供原始存取身分。此自動化不會授與存取 Amazon S3 儲存貯體中物件的CloudFront 原始存取身分的讀取權限。您必須更新 Amazon S3 儲存貯體許可以允許存取。

[運行此自動化 \(控制台\)](#)

## 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- CloudFrontDistributionId

類型：字串

描述：(必要) 您要啟用來源容錯移轉的CloudFront發行版 ID。

- OriginAccessIdentityId

類型：字串

描述：(必要) 要與CloudFront來源建立關聯的來源存取身分識別碼。

### 必要的 IAM 許可

此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發佈啟用原始存取身分識別，並驗證原始存取身分是否已指派。

## AWSConfigRemediation-EnableCloudFrontOriginFailover

### Description (描述)

AWSConfigRemediation-EnableCloudFrontOriginFailover執行手冊可為您指定的 Amazon CloudFront (CloudFront) 分發啟用來源容錯移轉。

[運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- CloudFrontDistributionId

類型：字串

描述：(必要) 您要在其上啟用來源容錯移轉的 CloudFront 發行版 ID。

- OriginGroupId

類型：字串

描述：(必要) 原始群組的 ID。

- PrimaryOriginId

類型：字串

描述：(必要) 原點群組中主要原點的 ID。

- SecondaryOriginId

類型：字串

描述：(必要) 原點群組中次要原點的 ID。

### 必要的 IAM 許可

此 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`-針對您在`CloudFrontDistributionId`參數中指定的CloudFront發佈啟用來源容錯移轉，並驗證容錯移轉是否已啟用。

## AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

### Description (描述)

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPSRunbook 會啟用您指定的 Amazon CloudFront (CloudFront) 分發的檢視器通訊協定政策。

### [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- `CloudFrontDistributionId`



類型：字串

描述：(必要) 您要啟用檢視器通訊協定原則的CloudFront發行版 ID。

- ViewerProtocolPolicy

類型：字串

有效值：僅限 HTTP , redirect-to-https

說明：(必要) 檢視者可用來存取原始檔案的通訊協定。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

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

### 文件步驟

- aws:executeScript-針對您在CloudFrontDistributionId參數中指定的CloudFront散佈啟用檢視器通訊協定原則，並驗證原則是否已指派。

## CloudTrail

AWS Systems Manager 自動化提供預先定義的 AWS CloudTrail執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

- [AWSConfigRemediation-CreateCloudTrailMultiRegionTrail](#)
- [AWS-EnableCloudTrail](#)
- [AWS-EnableCloudTrailCloudWatchLogs](#)

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

## AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

### Description (描述)

AWSConfigRemediation-CreateCloudTrailMultiRegionTrailrunbook 創建一個AWS CloudTrail ( CloudTrail ) 跟踪，將日誌文件從多個交付AWS 區域到您選擇的亞馬遜簡單存儲服務 ( Amazon S3 ) 存儲桶。

### [運行此自動化 \( 控制台 \)](#)

#### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- BucketName

類型：字串

說明：(必填) 您要將日誌上傳到的 Amazon S3 儲存貯體的名稱。

- **KeyPrefix**

類型：字串

說明：(選用) Amazon S3 金鑰前置詞，位於您指定用於日誌檔交付的儲存貯體名稱之後。

- **TrailName**

類型：字串

描述：(必要) 要建立的CloudTrail軌跡名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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`-接受追蹤名稱和 Amazon S3 儲存貯體名稱作為輸入，並建立CloudTrail追蹤。
- `aws:executeAwsApi`-在建立的追蹤上啟用記錄功能，並開始將日誌傳遞到您指定的 Amazon S3 儲存貯體。
- `aws:assertAwsResourceProperty`-驗證CloudTrail軌跡是否已建立。

## AWS-EnableCloudTrail

### Description (描述)

建立 AWS CloudTrail 追蹤和設定記錄到 S3 儲存貯體。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- S3 BucketName

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 寫入許可。如需相關資訊，請參閱的 [Amazon S3 儲存貯體政策CloudTrail](#)。

- 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 日誌記錄群組。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- CloudWatchLogsLogGroupArn

類型：字串

描述：(必要) 要傳送 CloudWatch 記錄檔之記錄 CloudTrail 檔群組的 ARN。

- CloudWatchLogsRoleArn

類型：字串

說明：(必要) IAM 角色 CloudWatch 日誌記錄的 ARN 假設要寫入指定的記錄群組。

- TrailNames

類型: StringList

描述：(必要) 以逗號分隔的清單，列出您要傳送至 CloudWatch 記錄檔的事件之 CloudTrail 追蹤名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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，將事件傳遞至指定的 CloudWatch 記錄檔記錄群組。

## AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

### Description (描述)

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMSrunbook 會使用您指定的 AWS CloudTrail (CloudTrail) 客戶管理金鑰加密 AWS Key Management Service (AWS KMS) 追蹤。此 runbook 應該只用作基準，以確保您的CloudTrail跟踪根據建議的最低安全性最佳實踐進行加密。我們建議使用不同的 KMS 金鑰加密多個追蹤。CloudTrail摘要檔案未加密。如果您先前已將追蹤的EnableLogFileValidation參數設定true為，請參閱《使用指南》中「[CloudTrail預防性安全性最佳作法](#)」主題的「使用伺服器端加密搭配AWS KMS受管理金鑰」一節，以取得詳細資訊。AWS CloudTrail

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- KeyId

類型：字串

描述：(必要) 您要用來加密您在TrailName參數中指定的追蹤之客戶管理金鑰的 ARN、金鑰 ID 或金鑰別名。

- TrailName

類型：字串

說明：(必要) ARN 或您要更新以加密的軌跡名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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參數中指定的軌跡啟用加密。
- aws:executeAwsApi-針對您在參數中指定的客戶管理金鑰收集 ARN。KMSKeyId
- aws:assertAwsResourceProperty-驗證CloudTrail追蹤上是否已啟用加密。

## AWS-EnableCloudTrailKmsEncryption

### Description

此 runbook 更新一個或多個 AWS CloudTrail 軌跡的配置使用 AWS Key Management Service (AWS KMS) 加密。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- KeyId

類型：字串

說明：(必要) 您要用來加密您在TrailName參數中指定的追蹤之客戶管理金鑰的金鑰識別碼。該值可以是以「alias/」為前綴的別名名稱，別名的完全指定 ARN 或鍵的完全指定 ARN。

- TrailNames

類型: StringList

說明：(必要) 您要更新以加密的追蹤清單 (以逗號分隔)。

必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- cloudtrail:UpdateTrail



- kms:DescribeKey
- kms:ListKeys

## 文件步驟

- aws:executeScript-對您在TrailName參數中指定的追蹤啟用 AWS KMS 加密。

# AWSConfigRemediation-EnableCloudTrailLogFileValidation

## Description

AWSConfigRemediation-EnableCloudTrailLogFileValidationRunbook 會為您的AWS CloudTrail追蹤啟用記錄檔驗證。

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- TrailName

類型：字串

描述：(必填) 您要啟用日誌驗證的追蹤名稱或 Amazon 資源名稱 (ARN)。

## 必要的 IAM 許可

此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-針對您在TrailName參數中指定的AWS CloudTrail追蹤啟用記錄驗證。
- aws:assertAwsResourceProperty-驗證已為您的跟踪啟用日誌驗證。

# AWS-EnableCloudTrailLogFileValidation

## Description

AWS-EnableCloudTrailLogFileValidationrunbook 會為您指定的 AWS CloudTrail 追蹤啟用記錄檔驗證。

## [運行此自動化 \( 控制台 \)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- TrailNames

類型: StringList

描述：(必要) 您要啟用記錄驗證的 CloudTrail 追蹤名稱，以逗號分隔清單。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

### 文件步驟

- aws:executeScript-針對您在TrailNames參數中指定的 AWS CloudTrail 追蹤啟用記錄驗證。

## AWS-QueryCloudTrailLogs

### Description (描述)

該手AWS-QueryCloudTrailLogs冊創建亞馬遜雅典娜表從亞馬遜簡單存儲服務 ( 亞馬遜 S3 ) 存儲桶您選擇包含AWS CloudTrail ( CloudTrail ) 日誌。建立資料表之後，自動化會執行您指定的 SQL 查詢，然後刪除資料表。

### [運行此自動化 \( 控制台 \)](#)

### 文件類型

自動化

擁有者

Amazon

平台

## 資料庫

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- Query

類型：字串

描述：(必要) 您要執行的 SQL 查詢。

- SourceBucketPath

類型：字串

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

- TableName

類型：字串

說明：(選用) 自動化操作所建立的 Athena 表格名稱。

預設值：雲端記錄

### 必要的 IAM 許可

此 AutomationAssumeRole 參數需要執行下列動作，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`-創建一個雅典娜桌子。
- `aws:executeAwsApi`-執行您在參數中指定的查詢字Query串。
- `aws:executeScript`-輪詢並等待查詢完成。
- `aws:executeAwsApi`-取得查詢結果。
- `aws:executeAwsApi`-刪除自動化操作所建立的表格。

## CloudWatch

AWS Systems Manager 自動化為 Amazon CloudWatch 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

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

## AWS-ConfigureCloudWatchOnEC2Instance

### Description (描述)

在受管執行個體上啟用或停用 Amazon CloudWatch 詳細監控。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您要在其上啟用 CloudWatch 監控的 Amazon EC2 執行個體的 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」|「停用」

描述：(選用) 指定要啟用或停用 CloudWatch。

預設：Enabled

### 文件步驟

configureCloudWatch-在具有指定狀態CloudWatch的 Amazon EC2 執行個體上進行設定。

## 輸出

此自動化沒有輸出。

# AWS-EnableCWAlarm

## Description

該 AWS-EnableCWAlarm runbook 創建 Amazon CloudWatch ( CloudWatch ) 的資 AWS 源，在你還沒 AWS 帳戶 有一個警報。 CloudWatch 會針對下列 AWS 資源建立警示：

- 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) 存儲桶
- Amazon Relational Database Service 服務 (Amazon RDS) 叢集

## [運行此自動化 \( 控制台 \)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ComparisonOperator

類型：字串

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

說明：(必要) 比較指定統計資料和臨界值時所使用的算術運算。

- MetricName

類型：字串

描述：(必要) 與警示相關之測量結果的名稱。

- 期間

類型：整數

有效值：10 | 30 | 60 的倍數

描述：(必要) 套用統計值的期間，以秒為單位。

- 資源

類型: StringList

描述：(必要) 用逗號分隔的資源 ARN 清單，用來建立 CloudWatch 警示

- 統計數字

類型：字串

有效值：平均 | 最大值 | 最小值 SampleCount | 總和

說明：(必要) 與警示相關之測量結果的統計資料。

- Threshold

類型：整數

描述：(必要) 要與指定統計資料比較的值。



此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的資源 runbook 參數中指定的值創建 CloudWatch 警報。ResourceARNs

### 輸出

啟用手臂。FailedResources：未針對其建立 CloudWatch 警示的資源 ARN 的對映清單以及失敗原因。

啟用手臂。SuccessfulResources：已成功建立 CloudWatch 警示的資源 ARN 清單。

## Amazon DocumentDB

AWS Systems Manager 自動化為 Amazon DocumentDB (與 MongoDB 兼容性) 提供了預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

### 主題

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

## AWS-EnableDocDbClusterBackupRetentionPeriod

### Description

AWS-EnableDocDbClusterBackupRetentionPeriod執行手冊會為您指定的 Amazon DocumentDB 叢集啟用備份保留期。此功能可設定保留自動備份的總天數。若要修改叢集，叢集必須處於可用狀態且引擎類型為docdb。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DBClusterResourceId

類型：字串

說明：(必填) 您要啟用備份保留期之 Amazon DocumentDB 叢集的資源識別碼。

- BackupRetentionPeriod

類型：整數

說明：(必要) 保留自動備份的天數。必須是 7-35 天之間的值。

- PreferredBackupWindow

類型：字串

說明：(選擇性) 以世界協調時間 (UTC) 為單位的每日時間範圍，格式為 hh24:毫米-h24:mm，例如 07:14-07:44。此值必須至少為 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 文件資料庫叢集識別碼。
- `VerifyDocDbEngine` (`aws:assertAwsResourceProperty`)-驗證 Amazon DocumentDB 引擎類型是 `docdb` 為了防止意外更改其他 Amazon 引擎類型。RDS
- `VerifyDocDbStatus` (`aws:waitAwsResourceProperty`)-驗證 Amazon DocumentDB 叢集狀態為 `available`
- `ModifyDocDbRetentionPeriod` (`aws:executeAwsApi`)-使用為指定的 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，並且已成功設定偏好的備份時段 (如果指定)。

### 輸出

`ModifyDocDbRetentionPeriod`。 `ModifyDbClusterResponse` -來自 `ModifyDBClusterAPI` 操作的響應。

`VerifyDocDbBackupsEnabled`。 `VerifyDbClusterBackupsEnabledResponse` -從確認成功修改 Amazon DocumentDB 叢集的 `VerifyDocDbBackupsEnabled` 步驟輸出。

## CodeBuild

AWS Systems Manager 自動化提供預先定義的 AWS CodeBuild 執行手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

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

## AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

### Description

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMScmkRunbook 會使用 AWS CodeBuild (CodeBuild) 您指定的客戶管理金鑰加密 AWS Key Management Service (AWS KMS) 專案的建置成品。AWS Config 必須在您執行此自動化操作的 AWS 區域 位置啟用。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- KeyId

類型：字串

描述：(必要) 您要用來加密您在ProjectId參數中指定的 CodeBuild 專案之 AWS KMS 客戶受管金鑰的 Amazon 資源名稱 (ARN)。

- ProjectId

類型：字串

描述：(必填) 您要加密其構建成品的 CodeBuild 項目的 ID。

### 必要的 IAM 許可

此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`-對您在 `ProjectId` 參數中指定的 CodeBuild 專案啟用加密。
- `aws:assertAwsResourceProperty`-驗證 CodeBuild 專案是否已啟用加密。

## 輸出

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

# AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

## Description (描述)

`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操作的 AWS 區域位置啟用。

## [運行此自動化 \(控制台\)](#)

## 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- ResourceId

類型：字串

描述：(必要) 您要刪除其存取金鑰環境變數之CodeBuild專案的 ID。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

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

### 文件步驟

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

## AWS CodeDeploy

AWS Systems Manager 自動化提供預先定義的 AWS CodeDeploy執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

- [AWSSupport-TroubleshootCodeDeploy](#)

# AWSsupport-TroubleshootCodeDeploy

## Description (描述)

AWSsupport-TroubleshootCodeDeploy執行手冊可協助診斷 Amazon 彈性運算雲端 (Amazon EC2) 執行個體上AWS CodeDeploy部署失敗的原因。runbook 會輸出步驟來協助您解決問題或進一步疑難排解。也提供的CodeDeploy最佳作法，以協助您避免未來發生類似問題。

此 Runbook 可以幫助您解決以下問題：

- CodeDeploy代理程式未安裝或未在 Amazon EC2 執行個體上執行
- 亞馬遜 EC2 執行個體沒有附加 AWS Identity and Access Management (IAM) 執行個體設定檔
- 連接到 Amazon EC2 執行個體的 IAM 執行個體設定檔沒有必要的 Amazon 簡單儲存服務 (Amazon S3) 許可
- 遺失存放在 Amazon S3 中的修訂版，或使用的 Amazon S3 儲存貯AWS 區域體與 Amazon EC2 執行個體不同
- 應用程式規格 (AppSpec) 檔案問題
- 「文件已存在於位置」錯誤
- CodeDeploy受管理生命週期事件掛接
- 客戶管理生命週期事件掛接
- 部署期間的擴充事件

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux,macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- DeploymentId

類型：字串

描述：(必要) 失敗的部署 ID。

- InstanceId

類型：字串

說明：(必填) 部署失敗之 Amazon EC2 執行個體的 ID。

### 必要的 IAM 許可

此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，並傳回部署失敗原因的分析。

## AWS Config

AWS Systems Manager 自動化提供預先定義的 AWS Config執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。



## 主題

- [AWSSupport-SetupConfig](#)

# AWSSupport-SetupConfig

## Description (描述)

AWSSupport-SetupConfigRunbook 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，以及使用 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體AWS Config傳送組態快照和組態歷史記錄檔案的交付通道。如果您指定AggregatorAccountId和AggregatorAccountRegion參數的值，runbook 也會建立資料彙總的授權，以便從多個和多個AWS 帳戶收集AWS Config組態和符合性資料。AWS 區域若要進一步了解彙總來自多個帳戶和區域的資料，請參閱開發人員指南中的[多帳戶多區域資料彙總](#)。AWS Config

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- AggregatorAccountId

類型：字串

說明：(選擇性) 將將彙總器新增至來自多個帳戶和的彙總AWS Config組態和相容性資料的 ID。AWS 帳戶 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

說明：(選擇性) 將新增彙總器以彙總來自多個帳戶和區域的AWS Config組態和合規資料的區域。

- `IncludeGlobalResourcesRegion`

類型：字串

默認值：美國東部 -1

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

- `分區`

類型：字串

預設：aws

說明：(必要) 您要從中收集AWS Config組態與相容性資料的分割區。

- `S3 BucketName`

類型：字串

預設：aws-config-delivery-channel

說明：(選用) 您要套用至為交付管道建立的 Amazon S3 儲存貯體的名稱。帳號 ID 會附加至名稱的結尾。

### 必要的 IAM 許可

此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`-建立服務連結 IAM 角色 (如AWS Config果尚未存在)。
- `aws:executeScript`-建立組態記錄程式 (如果尚未存在)。
- `aws:executeScript`-建立供交付通道使用的 Amazon S3 儲存貯體 (如果尚未存在)。
- `aws:executeScript`-使用 runbook 創建的資源創建一個交付渠道。
- `aws:executeAwsApi`-啟動配置記錄器。
- `aws:executeScript`-如果您指定AggregatorAccountId和AggregatorAccountRegion參數的值，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 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

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

## **AWSSupport-AssociatePhoneNumbersToConnectContactFlows**

### Description

可 `AWSsupport-AssociatePhoneNumbersToConnectContactFlows` 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。藉由在輸入逗號分隔值 (CSV) 檔案中提供電話號碼和連絡人流程的對應，runbook 會在 14.5 分鐘內將盡可能多的電話號碼與聯絡流程相關聯。runbook 會產生無法在時間限制內關聯的所有電話號碼和聯絡流程配對的 CSV 檔案，以便您可以在下次執行中輸入它們。

它是如何工作的？

Runbook 可 `AWSsupport-AssociatePhoneNumbersToConnectContactFlows` 協助您使用存放在 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體中的映射資料 CSV 檔案，將電話號碼與 Amazon Connect 執行個體中的聯絡流程相關聯。輸入 CSV 檔案應與下列格式對齊，其 `PhoneNumber` 值為 [E.164](#) 格式。

輸入 CSV 文件的例子

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

自動化執行手冊也會在 `DestinationFileBucket` 和 `DestinationFilePath` 中指定的目標位置建立下列檔案。

- **`automation:EXECUTION_ID/ResourceIdList.csv`** : 包含所需的 `PhoneNumberId` 和 `ContactFlowId` 配對的暫存檔案 `AssociatePhoneNumberContactFlowAPI`。
- **`automation:EXECUTION_ID/ErrorResourceList.csv`** : 包含由於錯誤而無法處理的電話號碼和聯絡流程配對 `ResourceNotFoundException` 的檔案，例如 `PhoneNumber,ContactFlowName,ErrorMessage`。
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`** : 包含未處理的電話號碼和聯絡流程配對的檔案。Runbook 嘗試在 14.5 分鐘內處理盡可能多的電話號碼和聯繫流程 (15 分鐘的 AWS Lambda 功能超時-緩衝 30 秒)。如果有一些電話號碼/聯繫流程無法由於時間限制進行處理，runbook 將它們包含在一個 CSV 文件中作為下一個 runbook 執行的輸入使用。

文件類型

自動化

擁有者

## Amazon

### 平台

Linux, macOS, Windows

### 參數

### 必要的IAM權限

此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": "*",
    "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操作：

1. 瀏覽至「文件」下 [AWS Support - Associate Phone Numbers To Connect Contact Flows](#) 的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)

( ) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - ConnectInstanceId (必填)

您的 Amazon Connect 實例的 ID。
  - SourceFileBucket (必填)

儲存包含電話號碼和聯絡流程配對的 CSV 檔案的 Amazon S3 儲存貯體。
  - SourceFilePath (必填)

包含電話號碼和聯絡流程配對的 CSV 檔案的 Amazon S3 物件金鑰。例如：path/to/input.csv。
  - DestinationFileBucket (必填)

自動化將放置中繼檔案和結果報告的 Amazon S3 儲存貯體。
  - DestinationFilePath (選擇性)

應存放中繼檔案和結果報告的 Amazon S3 物件路徑。DestinationFileBucket 例如，如果您指定 path/to/files/，檔案會儲存在下面 s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION\_ID]/。
  - S3 BucketOwnerAccount (選擇性)

擁有您要上傳聯絡流程日誌之 Amazon S3 儲存貯體的 AWS 帳戶號碼。如果您未指定此參數，執行手冊會使用執行自動化的使用者或角色的 AWS 帳戶 ID。
  - S3 BucketOwnerRoleArn (選擇性)

具有取 ARN 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、儲存貯體政策狀態以及將物件上傳到儲存貯體的許可 IAM 角色。ACLs 如果未指定此參數，runbook 會使用 AutomationAssumeRole (如果指定) 或啟動此 runbook 的使用者 (如果 AutomationAssumeRole 未指定)。請參閱 runbook 描述中所需的權限部分。

Input parameters	
<b>AutomationAssumeRole</b> <small>(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.</small>	<b>ConnectInstanceId</b> <small>(Required) The ID of your Amazon Connect instance.</small>
<input type="text" value="test-role"/>	<input type="text" value="01234567-89ab-cdef-0123-456789abcdef"/>
<b>SourceFileBucket</b> <small>(Required) The Amazon S3 bucket name that stores the CSV file which contains the pairs of phone numbers and Contact Flows.</small>	<b>SourceFilePath</b> <small>(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".</small>
<input type="text" value=""/>	<input type="text" value="String"/>
<b>DestinationFileBucket</b> <small>(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.</small>	<b>DestinationFilePath</b> <small>(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://&lt;DestinationFileBucket&gt;/path/to/files/~automation:EXECUTION_ID~".</small>
<input type="text" value=""/>	<input type="text" value="String"/>
<b>S3BucketOwnerAccount</b> <small>(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.</small>	<b>S3BucketOwnerRoleArn</b> <small>(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.</small>
<input type="text" value="String"/>	<input type="text" value=""/>

#### 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 實例是否 ConnectInstanceId 存在。

- 檢查 3 BucketPublicStatus

檢查 Amazon S3 儲存貯體是否在中指

定，SourceFileBucket 並 DestinationFileBucket 允許匿名或公用讀取或寫入存取權限。

- CheckSourceFileExistenceAndSize

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

- GenerateResourceIdMap

下載在中指定的來源 CSV 檔案，SourceFilePathPhoneNumberId 並識別每

個 ContactFlowId 資源的和。完成後，它會將包

含 PhoneNumberPhoneNumberId、ContactFlowName 和的 CSV 檔案上傳 ContactFlowId 到中指定的目的地 Amazon S3 儲存貯體 DestinationFileBucket。如果 PhoneNumberId 無法識別某個數字，則文件中的 CSV 文件將為空。

- AssociatePhoneNumbersToContactFlows

使用 AWS CloudFormation 堆棧在您的帳戶中創建一個 AWS Lambda 函數。

該 AWS Lambda 函數將每個號碼與中指定的源 CSV 文件中列出的聯繫流程相關

聯，SourceFileBucketSourceFilePath 並且 AWS CloudFormation 堆棧調用該函數。

該 AWS Lambda 功能會在超時 ( 15 分鐘 ) 之前將盡可能多的電話號碼映射到聯繫流程。由於

錯誤而無法處理的電話號碼和聯絡流程清單會在中上傳 [automation:EXECUTION\_ID]/

ErrorResourceList.csv。由於單次執行中可以處理的最大電話號碼數量過多而無法處理的電



話號碼將在中上傳[automation:EXECUTION\_ID]/NonProcessedResourceList.csv。如果此步驟失敗，它將進入該DescribeCloudFormationErrorFromStackEvents步驟以顯示為什麼它從 AWS CloudFormation 堆棧事件失敗。

- WaitForPhoneNumberContactFlowAssociationCompletion

等待，直到創建將電話號碼映射到聯繫人流程的 AWS Lambda 函數並完成 AWS CloudFormation 堆棧的調用。

- GenerateReport

產生報告，其中包含對應至聯絡流程的電話號碼數目、由於錯誤而無法處理的電話號碼數目，以及因單次執行中可處理的電話號碼上限而無法處理的報告。此報告也會顯示[automation:EXECUTION\_ID]/ErrorResourceList.csv或[automation:EXECUTION\_ID]/NonProcessedResourceList.csv (如果適用URL) 的位置 (Amazon S3 URI 和 Amazon S3 主控台)。

- DeleteCloudFormationStack

刪除 AWS CloudFormation 堆疊，包括用於對應的 Lambda 函數。

- DescribeCloudFormationErrorFromStackEvent

描述AssociatePhoneNumbersToContactFlows步驟 AWS CloudFormation 堆疊中的錯誤。

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

- GenerateReport.OutputPayload

輸出電話號碼和聯繫流程關聯。此報告包含下列資訊：

- 輸入CSV文件中列出的電話號碼和聯繫流程對的數量
  - 輸入CSV檔案中指定與聯絡流程相關聯的電話號碼數
  - 由於錯誤而無法與聯絡流程相關聯的電話號碼數目
  - 由於時間限制而與聯絡流程無關聯的電話號碼數目
  - CSV檔案的位置 (Amazon S3 URI 和 Amazon S3 主控台URL)，其中包含由於錯誤而無法關聯的電話號碼和聯絡流程配對
  - CSV檔案的位置 (Amazon S3 URI 和 Amazon S3 主控台URL)，其中包含由於時間限制而未關聯的電話號碼和聯絡流程配對
- DescribeCloudFormationErrorFromStackEvents. 活動。

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

## 輸出少量電話號碼和聯繫流程的執行

```

▼ 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
}
}

```

## 由於錯誤或時間限制而未關聯的大量電話號碼和聯繫流程以及電話號碼的執行輸出

```

▼ Outputs

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

GenerateReport.OutputPayload
{"Payload":{
-----
Amazon Connect Phone Number Mapping Result
-----
* Phone number and Contact Flow pairs listed in the provided input: 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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化 workflow 登陸頁](#)

## AWSSupport-CollectAmazonConnectContactFlowLog

### Description

AWSSupport-CollectAmazonConnectContactFlowLog 自動化工作流程手冊用於收集特定聯絡人 ID 的 Amazon Connect 聯絡流程日誌。透過提供您的 Amazon Connect 執行個體 ID 和聯絡人 ID，Runbook 會搜尋聯絡流程日誌以尋找來自 Amazon 日 CloudWatch 誌群組的聯絡人，並將其上

傳到請求參數中指定的 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體。執行手冊會產生輸出，提供 Amazon S3 主控台 URL 和 AWS CLI 命令供您下載日誌。

它是如何工作的？

AWSsupport-CollectAmazonConnectContactFlowLog 自動化執行手冊有助於收集存放在已 CloudWatch 設定日誌群組中的特定聯絡人 ID 的 Amazon Connect 聯絡流程日誌，並將其上傳到指定的 Amazon S3 儲存貯體。為了協助確保從 Amazon Connect 聯絡流程收集的日誌的安全性，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權限 read 還是 write 存取權限，並由 S3BucketOwnerAccountId 參數中指定的 AWS 帳戶擁有。如果您的 Amazon S3 儲存貯體使用具有 AWS Key Management Service 金鑰 (SSE-KMS) 的伺服器端加密，請確定執行此自動化操作的使用者或 AWS Identity and Access Management (IAM) 角色具有金 AWS KMS 鑰的 kms:GenerateDataKey 許可。如需 Amazon Connect 執行個體所產生之日誌的詳細資訊，請參閱 [存放在 Amazon CloudWatch 日誌群組中的流程日誌](#)。

#### Important

CloudWatch 日誌見解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](#)。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

必要的 IAM 權限

此 AutomationAssumeRole 參數需要執行下列動作，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操作：

1. 瀏覽至「文件」下 [AWS Support - Collect Amazon Connect Contact Flow Log](#) 的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - ConnectInstanceId (必填)：

您的 Amazon Connect 實例的 ID。
  - ContactId (必填)：

您要收集聯絡流程記錄的聯絡人識別碼。
  - S3 BucketName (必要)：

您帳戶中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/寫入權限授與不需要存取所收集記錄的對象。
  - S3 ObjectPrefix (選擇性)：

Amazon S3 儲存貯體中用於上傳聯絡流程日誌的 Amazon S3 物件路徑。例如，如果您指定 CollectedLogs，記錄檔將會上傳為 s3://your-s3-bucket/CollectedLogs/ContactFlowLog\_[ContactId][AWSAccountId].gz。如果您未指定此參數，則會使用 Systems Manager 自動化執行 ID，例如：s3://your-s3-bucket/[automation:EXECUTION\_ID]/ContactFlowLog[ContactId]\_[AWSAccountId].gz。注意：如果您指定一個值，S3ObjectPrefix 並使用相同的 [ContactId] 執行此自動化操作，則聯絡流程記錄將會被覆寫。
  - S3 BucketOwnerAccount (選擇性)：

擁有您要上傳聯絡流程日誌之 Amazon S3 儲存貯體的 AWS 帳戶號碼。如果您未指定此參數，runbook 會使用執行自動化操作的使用者或角色的 AWS 帳戶 ID。
  - S3 BucketOwnerRoleArn (選擇性)：

具有取 ARN 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、儲存貯 ACLs 體政策狀態以及將物件上傳到儲存貯體的許可 IAM 角色。如果未指定此參

數，runbook 會使用 AutomationAssumeRole (如果指定) 或啟動此 runbook 的使用者 (如果 AutomationAssumeRole 未指定)。請參閱 runbook 說明中所需的權限部分。

Input parameters	
<p><b>AutomationAssumeRole</b> (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.</p> <input type="text" value="SSMAutomationRole"/>	<p><b>ConnectInstanceId</b> (Required) The ID of your Amazon Connect instance.</p> <input type="text" value="fedcba98-7654-3210-fedc-ba9876543210"/>
<p><b>ContactId</b> (Required) The ID of the contact that you want to collect Contact Flow Log for.</p> <input type="text" value="01234567-89ab-cdef-0123-456789abcdef"/>	<p><b>S3BucketName</b> (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.</p> <input type="text" value="saw-example-bucket"/>
<p><b>S3ObjectPrefix</b> (Optional) The Amazon S3 object path in the Amazon S3 bucket for an uploaded the Contact Flow Log. For example, if you specify 'CollectedLogs', the log will be uploaded as 's3://your-s3-bucket/CollectedLogs/ContactFlowLog_{ContactId}_{AWSAccountId}.gz'. If you do not specify this parameter, the SSM Automation execution ID is used, example: 's3://your-s3-bucket/{AutomationEXECUTION_ID}/ContactFlowLog_{ContactId}_{AWSAccountId}.gz'. Note: If you specify a value for 'S3ObjectPrefix' and you run this automation using the same [ContactId], the Contact Flow Log will be overwritten.</p> <input type="text" value="String"/>	<p><b>S3BucketOwnerAccount</b> (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.</p> <input type="text" value="String"/>
<p><b>S3BucketOwnerRoleArn</b> (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.</p> <input type="text"/>	

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- CheckConnectInstanceExistance

檢查中提供的 Amazon Connect 實例 ConnectInstanceId 是 ACTIVE。

- 檢查 3 BucketPublicStatus

檢查中指定的 Amazon S3 儲存貯體是否 S3BucketName 允許匿名或公用讀取或寫入存取權限。

- GenerateLogSearchTimeRange

根據 StartTime 和 EndTimeLastUpdateTimestamp 傳回的 StartQuery 步驟產生 InitiationTimestamp 和 DescribeContactAPI。StartTime 將是一個小時之前 InitiationTimestamp，EndTime 將是一個小時後 LastUpdateTimestamp。

- StartQuery

針對與 ContactId 中提供的 Amazon Connect 執行個體相關聯的 CloudWatch 日誌記錄群組中提供的，啟動查詢日誌 ConnectInstanceId。查詢在執行時間 60 分鐘後逾時。如果您的查詢逾時，請縮短搜尋的時間範圍。您可以在控制台中查看當前正在進行的查詢以及最近的查詢歷史記錄 CloudWatch 錄。如需詳細資訊，請參閱 [檢視執行中的查詢或查詢記錄](#)

- WaitForQueryCompletion

等待提供的 CloudWatch 記錄檔查詢記錄檔完 ContactId 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，請縮短搜尋的時間範圍。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記錄](#)

- UploadContactFlowLog

取得查詢結果，並將聯絡流程日誌上傳到中指定的 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的範例 AWS CLI 命令。

## 7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

- GenerateReport.OutputPayload

告訴您 runbook 成功擷取指定聯絡人的聯絡流程記錄的輸出。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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化 workflow 登陸頁](#)

## AWS Directory Service

AWS Systems Manager 自動化提供預先定義的 AWS Directory Service 執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉檢視工作手冊內容](#)。

## 主題

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

# AWS-CreateDSManagementInstance

## Description (描述)

該手冊AWS-CreateDSManagementInstance冊創建一個亞馬遜彈性計算雲 ( 亞馬遜 EC2 ) Windows 實例，您可以用它來管理您的AWS Directory Service目錄。管理執行個體無法用來管理 AD 連接器目錄。

## [運行此自動化 \( 控制台 \)](#)

### 文件類型

#### 自動化

### 擁有者

### Amazon

### 平台

### Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 阿米德

類型：字串



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

說明：(必要AMI) 您要用來啟動管理執行處理的 Amazon Machine Image () 識別碼。

- DirectoryId

類型：字串

描述：(必填) 您要管理的AWS Directory Service目錄的 ID。執行個體會連結至您指定的目錄。

- IamInstanceProfileName

類型：字串

說明：(必要) 您指定的名稱會套用至由自動化操作建立並附加至管理執行個體的 IAM 執行個體設定檔。

- InstanceType

類型：字串

預設值：3. 中

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.xlargeManagementInstance

- t3.2xlarge

描述：(必要) 您要啟動的執行個體類型。

- KeyPairName

類型：字串

說明：(選擇性) 建立執行個體時要使用的金鑰配對。如果未指定值，則不會與執行個體相關聯的金鑰配對。

- RemoteAccessCidr

類型：字串

描述：(必要) 您要允許 RDP 流量 (連接埠 3389) 來源的 CIDR 區塊。您指定的 CIDR 區塊會套用至新增至自動化工作所建立之安全性群組的輸入規則。

- SecurityGroupName

類型：字串

描述：(必要) 您指定的名稱會套用至由自動化操作建立並與管理執行處理相關聯的安全性群組。

- Tags (標籤)

類型:MapList

描述：(選用) 您要套用至自動化操作所建立之資源的機碼值配對。

## 必要的 IAM 許可

此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:DescribeInstanceStatus

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

- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

## 文件步驟

- `aws:executeAwsApi`-收集有關您在`DirectoryId`參數中指定目錄的詳細信息。
- `aws:executeAwsApi`-取得啟動目錄之虛擬私有雲 (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`-為新建立的安全性群組建立輸入規則，允許來自您在參數中指定的 CIDR 的 RDP 流量。 `RemoteAccessCidr`
- `aws:executeAwsApi`-使用您在`IamInstanceProfileName`參數中指定的值建立 IAM 角色和執行個體設定檔。
- `aws:executeAwsApi`-根據您在工作流程簿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

R AWSSupport-TroubleshootADConnectorConnectivity unbook 會驗證 AD Connector 的下列必要條件：

- 檢查與 AD Connector 相關聯的安全性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 Systems Manager AWS Security Token Service、和 Amazon CloudWatch 界面VPC端點是否存在於與 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 彈性運算雲端 (AmazonEC2) Linux t2.micro 執行個體。然後會使用netcat和公用nslookup程式執行網路連線測試。

### [運行此自動化 \(控制台\)](#)

**⚠ Important**

使用此 Runbook 可能會 AWS 帳戶 對您的 Amazon EC2 執行個體、Amazon 彈性區塊存放區磁碟區和 Amazon Machine Image (AMI) 在自動化期間建立產生額外費用。如需詳細資訊，請參閱 [Amazon 彈性運算雲端定價](#) 和 [Amazon 彈性區塊存放區定價](#)。

如果aws:deletestack步驟失敗，請移至主 AWS CloudFormation 控制台以手動刪除堆疊。此 Runbook 所建立的堆疊名稱開頭AWSSupport-TroubleshootADConnectorConnectivity為。如需有關刪除 AWS CloudFormation 堆疊的資訊，請參閱《AWS CloudFormation 使用指南》中的 [〈刪除堆疊〉](#)。

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DirectoryId

類型：字串

描述：(必要) 您要疑難排解連線問題之 AD 連接器目錄的識別碼。

- EC2 InstanceProfile

類型：字串

字元數目上限：128

說明：(必要) 您要指派給為執行連線測試而啟動之執行處理的執行處理設定檔名稱。您指定的執行個體設定檔必須附加AmazonSSManagedInstanceCore原則或同等權限。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 相關聯之安全性群組的相關資訊。
- `aws:executeAwsApi`-收集與 AD Connector 子網路相關聯之網路ACL規則的相關資訊。
- `aws:executeScript`-評估 AD Connector 安全性群組規則，以確認允許所需的輸出流量。
- `aws:executeScript`-評估 AD Connector 網路ACL規則，以確認所需的輸出和輸入網路流量是否允許。
- `aws:executeScript`-檢查 AWS Systems Manager, AWS Security Token Service 和 Amazon CloudWatch 界面端點是否存在於與 AD Connector VPC 相同。
- `aws:executeScript`-編譯在先前步驟中執行的檢查的輸出。
- `aws:branch`-根據先前步驟的輸出分支自動化。如果安全群組和網路缺少必要的輸出和輸入規則，自動化會在此停止ACLs。
- `aws:createStack`-建立 AWS CloudFormation 堆疊以啟動 Amazon 執行個體EC2以執行連線測試。
- `aws:executeAwsApi`-收集新推出IDs的 Amazon EC2 執行個體。
- `aws:waitForAwsResourceProperty`-等待第一個新啟動的 Amazon EC2 執行個體報告為受管理的執行個體。 AWS Systems Manager
- `aws:waitForAwsResourceProperty`-等待第二個新啟動的 Amazon EC2 執行個體報告為受 AWS Systems Manager管理。
- `aws:runCommand`-從第一EC2個 Amazon 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EC2個 Amazon 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: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`-如果自動化無法刪除 AWS CloudFormation 堆疊，則輸出如何手動刪除堆疊的指示。

## AWSsupport-TroubleshootDirectoryTrust

### Description (描述)

AWSSupport-TroubleshootDirectoryTrust執行本診斷AWS Managed Microsoft AD和微軟活動目錄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。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- DirectoryId

類型：字串

允許的模式：`^ d-[一個 Z0-9] {10} $`

描述：(必要) 要進行故障診斷的 AWS Managed Microsoft AD ID。

- RemoteDomainCidrs

類型:StringList

允許的模式：`([0-9] | [1-9] [0-9] | 1 [0-9]) [1] [0-9]) [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) AWS Managed Microsoft AD 的預設連接埠需求。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) AWS Managed Microsoft AD 的預設連接埠需求。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

此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`-獲取有關AWS Managed Microsoft AD。
- `aws:branch`-如果為TrustId輸入參數提供了值，則進行分支自動化。
- `aws:executeAwsApi`-取得有關信任關係的資訊。
- `aws:executeAwsApi`-取得的條件式轉寄站 DNS IP 位址。RemoteDomainName
- `aws:executeAwsApi`-取得已新增至的 IP 路由的相關資訊AWS Managed Microsoft AD。
- `aws:executeAwsApi`-取得子網路的 CIDR。AWS Managed Microsoft AD
- `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 ACL 的相關資訊。AWS Managed Microsoft AD
- `aws:executeScript`-確認RemoteDomainCidrs是否有效值。確認AWS Managed Microsoft AD具有的條件式轉寄站RemoteDomainCidrs，並且必要的 IP 路由已新增至非 RFC 1918 IP RemoteDomainCidrs 位址。AWS Managed Microsoft AD
- `aws:executeScript`-評估安全性群組規則。
- `aws:executeScript`-評估網路 ACL。

## 輸出

`evalDirectorySecurityGroup.output`-評估與相關聯的安全群組規則是否AWS Managed Microsoft AD允許建立信任所需流量的結果。

`evalAclEntries.output`-評估與相關聯的網路 ACL 是否AWS Managed Microsoft AD允許建立信任所需流量的結果。

`evaluateRemoteDomainCIDR`. 輸出-評估是否RemoteDomainCidrs為有效值的結果。確認AWS Managed Microsoft AD具有的條件式轉寄站RemoteDomainCidrs，並且必要的 IP 路由已新增至非 RFC 1918 IP RemoteDomainCidrs 位址。AWS Managed Microsoft AD

# AWS AppSync

AWS Systems Manager 自動化提供預先定義的 AWS AppSync 執行手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-EnableAppSyncGraphQLApiLogging](#)

## AWS-EnableAppSyncGraphQLApiLogging

### Description

AWS-EnableAppSyncGraphQLApiLogging 執行手冊會針對您指定的 AWS AppSync GraphQL API 啟用欄位層級記錄和要求層級記錄。即使已啟用記錄，執行手冊也會將變更套用至指定的 GraphQL API。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux, macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- Apild

類型：字串

說明：(必要) 您要啟用記錄功能的 API ID。

- FieldLogLevel

類型：字串

有效值：錯誤 | 全部

描述：(必填) 欄位記錄層級。

- CloudWatchLogsRoleArn

類型：字串

描述：(必要) AWS AppSync 假設發佈到 Amazon CloudWatch 日誌的服務角色的 ARN。

- ExcludeVerboseContent

類型：布林值

預設：False

描述：(選擇性) 設定為True以排除標頭、前後關聯及評估的對映範本等資訊，而不論記錄層次為何。

## 必要的 IAM 許可

此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 -收集與主身份驗證類型相關的身份驗證類型和配置信息。
- aws : 分支-基於認證類型的分支。

- `aws : executeAwsApi` - 根據為工作流程簿的輸入參數指定的值更新 AWS AppSync GraphQL API 的日誌記錄組態。

## 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 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

## AWS-EnableAthenaWorkGroupEncryptionAtRest

### Description

手冊 `AWS-EnableAthenaWorkGroupEncryptionAtRest` 冊為您指定的 Amazon Athena 工作群組啟用靜態加密。

### [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

### 擁有者

## Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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 | 公理

描述：(必要) 指定要使用的加密選項。您可以選擇使用 Amazon S3 受管金鑰 (SSE\_S3) 的伺服器端加密、使用受管金鑰 (SSE\_KMS) 進行伺服器端加密，或使用AWS KMS受管金鑰 (CSE\_KMS) 進行用戶端加密。AWS KMS

- KmsKeyId

類型：字串

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

- EnableMinimumEncryptionConfiguration

類型：布林值

預設：True

說明：(選用) 針對寫入 Amazon S3 的查詢和計算結果，對工作群組強制執行最低層級的加密。啟用後，工作群組使用者只能將加密設定為管理員或更高級別在提交查詢時設定的最低層級。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：(選擇性) 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

此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: 分支-根據參數中指定的加密選項進EncryptionOption行分支。
- aws : executeAwsApi -此步驟使用指定的加密設置更新 Athena 工作組。
- aws : executeAwsApi -使用指定的加密設置更新 Athena 工作組。
- aws : assertAwsResource屬性-驗證工作組的加密是否已啟用。

## DynamoDB

AWS Systems Manager 自動化為 Amazon DynamoDB 提供預先定義的執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 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執行手冊會將一或多個 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。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

#### 自動化

#### 擁有者

#### Amazon

#### 平台

#### 資料庫

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。



- CapacityMode

類型：字串

有效值：已佈建 | 付款請求

描述：(必要) 所需的讀取/寫入容量模式。從隨需 (pay-per-request) 切換至佈建容量時，必須設定初始佈建的容量值。初始佈建的容量值是根據過去 30 分鐘內資料表和全域次要索引耗用的讀取和寫入容量來預估。

- ReadCapacityUnits

類型：整數

預設：0

說明：(選擇性) DynamoDB 傳回節流例外狀況之前，每秒所消耗的強度一致性讀取數目上限。

- TableNames

類型：字串

描述：(必要) 以逗號分隔的 DynamoDB 表格名稱清單，用以變更讀取/寫入容量模式。

- WriteCapacityUnits

類型：整數

預設：0

說明：(選擇性) DynamoDB 傳回節流例外狀況之前，每秒所消耗的寫入次數上限。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- dynamodb:DescribeTable
- dynamodb:UpdateTable

### 文件步驟

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

## 輸出

變更的 BRW CapacityMode。SuccessesTables -已順利變更容量模式的 DynamoDB 表格名稱清單

變更的 BRW CapacityMode。FailedTables -DynamoDB 表格名稱的對映清單，其中變更容量模式失敗以及失敗原因。

## AWS-CreateDynamoDBBackup

### Description (描述)

建立亞馬遜動態資料表的備份。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

#### 資料庫

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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 (描述)

刪除亞馬遜動態資料表的備份。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- BackupArn

類型：字串

描述：(必要) 要刪除的 DynamoDB 資料表之 ARN。

# AWSConfigRemediation-DeleteDynamoDbTable

## Description (描述)

AWSConfigRemediation-DeleteDynamoDbTable執行手冊會刪除您指定的 Amazon 動態資料表。

## [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- TableName

類型：字串

說明：(必要) 您要刪除的 DynamoDB 表格名稱。

### 必要的 IAM 許可

此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-刪除參數中指定的 DynamoDB 表格。TableName
- aws:executeScript-驗證 DynamoDB 資料表已刪除。

## AWS-DeleteDynamoDbTableBackups

### Description (描述)

根據保留天數或計數刪除 DynamoDB 表格備份。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

### 資料庫

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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。RetentionCount或者RetentionDays可以使用，不能同時使用。

- 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。RetentionCount或者RetentionDays可以使用，不能同時使用。

- TableName

類型：字串

描述：(必要) DynamoDB 資料表的名稱。

## AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

### Description

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable執行手冊會使用您為參數指定的 () 客戶受管金鑰來加密 Amazon DynamoDB AWS Key Management Service (DynamoDB AWS KMS) 表格。KMSKeyId

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- KeyId

類型：字串

描述：(必要) 您要用來加密您在參數中指定的 DynamoDB 表格的客戶受管金鑰的 ARN。TableName

- TableName

類型：字串

說明：(必要) 您要加密的 DynamoDB 表格名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

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

### 文件步驟

- aws:executeAwsApi-加密您在參數中指定的 DynamoDB 表格。TableName
- aws:waitForAwsResourceProperty-驗證 DynamoDB 表格的Enabled內容SSESpecification已設定為。true
- aws:assertAwsResourceProperty-驗證 DynamoDB 表是否使用參數中指定的客戶管理金鑰加密。KMSKeyId

# AWSConfigRemediation-EnablePITRForDynamoDbTable

## Description (描述)

AWSConfigRemediation-EnablePITRForDynamoDbTable 執行手冊會在您指定的 Amazon DynamoDB 表格上啟用 point-in-time 復原 (PITR)。

## [運行此自動化 \(控制台\)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- TableName

類型：字串

描述：(必要) 要在其中啟用 point-in-time 復原的 DynamoDB 表格名稱。

### 必要的 IAM 許可

此 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-在您在參數中指定的 DynamoDB 表格上啟用point-in-time復原功能。TableName
- aws:assertAwsResourceProperty-確認已在 DynamoDB 表格上啟用point-in-time復原功能。

## AWS-EnableDynamoDbAutoscaling

### Description

AWS-EnableDynamoDbAutoscaling執行手冊會為您指定的已佈建容量 Amazon DynamoDB 表啟用 Application Auto Scaling。應 Application Auto Scaling 會根據流量模式動態調整佈建的輸送量容量。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](#)。

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- TableName

類型：字串

說明：(必要) 您要啟用應用程式自動調整比例的 DynamoDB 表格名稱。

- MinReadCapacity

類型：整數

說明：(必要) DynamoDB 表格佈建輸送量讀取容量單位的最小數目。

- MaxReadCapacity

類型：整數

描述：(必要) DynamoDB 表格佈建輸送量讀取容量單位的最大數目。

- 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已耗用佈建輸送量的百分比。您可以將 auto 調整的目標使用率值設定在 20% 到 90% 之間。

- ReadScaleOutCooldown

類型：整數

描述：(必要) 等待先前讀取容量向外延展活動生效的時間 (以秒為單位)。

- ReadScaleInCooldown

類型：整數

描述：(必要) 讀取容量縮放活動完成後的時間量 (以秒為單位)，然後再開始另一個縮放活動。

- MinWriteCapacity

類型：整數

描述：(必要) DynamoDB 表格佈建輸送量寫入單位的最小數目。

- MaxWriteCapacity

類型：整數

描述：(必要) DynamoDB 表的佈建輸送量寫入單位數目上限。

- 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已耗用佈建輸送量的百分比。您可以將 auto 調整的目標使用率值設定在 20% 到 90% 之間。

- WriteScaleOutCooldown

類型：整數

描述：(必要) 等待先前寫入容量向外延展活動生效的時間 (以秒為單位)。

- WriteScaleInCooldown

類型：整數

描述：(必要) 寫入容量縮放活動完成後的時間量 (以秒為單位)，再開始另一個縮放活動。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 表上設定 Application Auto Scaling。
- RegisterAppAutoscalingTargetWriteDelay ( aws:sleep ) -睡覺以避免API節流。
- PutScalingPolicyWrite (aws:executeAwsApi)-設定 DynamoDB 表格的目標寫入容量使用率。
- PutScalingPolicyWriteDelay ( aws:sleep ) -睡覺以避免API節流。
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi)-為 DynamoDB 表設定最小和最大讀取容量單位。
- RegisterAppAutoscalingTargetReadDelay ( aws:sleep ) -睡覺以避免API節流。

- PutScalingPolicyRead (aws:executeAwsApi)-設定 DynamoDB 表格的目標讀取容量使用率。
- VerifyDynamoDbAutoscalingEnabled (aws:executeScript)-確認已根據您指定的值為 DynamoDB 表啟用 Application Auto Scaling。

## 輸出

- RegisterAppAutoscalingTargetWrite. 回應。
- PutScalingPolicyWrite. 回應。
- RegisterAppAutoscalingTargetRead. 回應。
- PutScalingPolicyRead. 回應。
- VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse

## AWS-RestoreDynamoDBTable

### Description (描述)

AWS-RestoreDynamoDBTable 執行手冊還原您使用 point-in-time 復原 (PITR) 指定的 Amazon DynamoDB 表格。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

#### 自動化

#### 擁有者

#### Amazon

#### 平台

#### 資料庫

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- EnablePointInTimeRecoverAsNeeded

類型：布林值

預設：true

說明：(選擇性) 決定自動化操作是否視需要開啟point-in-time復原以還原資料表。

- GlobalSecondaryIndexOverride

類型：字串

描述：(選擇性) 用來取代新表格現有次要索引的新全域次要索引。

- LocalSecondaryIndexOverride

類型：字串

描述：(選擇性) 用來取代新表格現有次要索引的新本機次要索引。

- RestoreDateTime

類型：字串

描述：(必要) 過去 35 天內您要將表格還原至的point-in-time復原目標。使用下列格式指定日期和時間：DD/MM/YYYY HH:MM:SS

- SourceTableArn

類型：字串

描述：(必要) 您要還原之表格的 ARN。

- SseSpecificationOverride

類型：字串

描述：(選擇性) 用於新表格的伺服器端加密設定。

- TargetTableName

類型：字串

描述：(必要) 要還原的表格名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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point-in-time用復原還原您在TargetTableName參數中指定的 DynamoDB 表格。

## Amazon EBS

AWS Systems Manager 自動化為 Amazon 彈性區塊存放區提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 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 自動化工冊用於分析 Amazon 彈性塊商店 (Amazon EBS) 上的資源使用情況。它會分析磁碟區使用情況，並識別指定區域中放棄的磁碟 AWS 區、映像和快照。

它是如何工作的？

執行手冊會執行下列四項工作：

1. 驗證亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體是否存在，或建立新的 Amazon S3 儲存貯體。
2. 收集可用狀態下的所有 Amazon EBS 卷。
3. 收集已刪除來源磁碟區的所有 Amazon EBS 快照。
4. 收集所有未被任何未終止的 Amazon 彈性運算雲端 (Amazon AMIs) 執行個體使用的 Amazon 機器映像 (EC2)。

執行手冊會產生 CSV 報告，並將其存放在使用者提供的 Amazon S3 儲存貯體中。提供的存儲桶應按照最後概述的 AWS 安全最佳實踐進行保護。如果使用者提供的 Amazon S3 儲存貯體不存在於帳戶中，則 runbook 會使用名稱格式建立新的 Amazon S3 儲存貯體 <User-provided-name>-awssupport-YYYY-MM-DD，並使用自訂 AWS Key Management Service (AWS KMS) 金鑰加密、啟用物件版本控制、封鎖公共存取，並要求使用 SSL/TLS。

如果您想要指定自己的 Amazon S3 儲存貯體，請確定已按照以下最佳實務進行設定：

- 封鎖值區的公開存取權 (設IsPublic為False)。
- 開啟 Amazon S3 存取記錄功能。
- [只允許向您的值區發出SSL請求](#)。
- 開啟物件版本管理。
- 使用 AWS Key Management Service (AWS KMS) 金鑰來加密儲存貯體。

### Important

使用此執行手冊可能會對您的帳戶產生額外的費用，以建立 Amazon S3 儲存貯體和物件。如需可能產生的費用的詳細資訊，請參閱 [Amazon S3 定價](#)。

## 文件類型

### 自動化

### 擁有者

### Amazon

### 平台

### LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- S3 BucketName

類型：AWS::S3::Bucket::Name

說明：(必填) 您帳戶中要將報告上傳到的 Amazon S3 儲存貯體。確定儲存貯體政策不會將不必要的讀取/寫入權限授與不需要存取所收集記錄的對象。如果帳戶中不存在指定的值區，則



Automation 會在該區域中建立一個新值區，其中以名稱格式啟動自動化<User-provided-name>-awssupport-YYYY-MM-DD，並使用自訂 AWS KMS 金鑰加密。

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

- CustomerManagedKmsKeyArn

類型：字串

說明：(選用) 自訂 AWS KMS 金鑰 Amazon 資源名稱 (ARN)，用於加密新的 Amazon S3 儲存貯體，如果帳戶中沒有指定的儲存貯體，則將建立此儲存貯體。如果在未指定自訂 AWS KMS 金鑰的情況下嘗試建立值區，則自動化會失敗ARN。

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

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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

具有運行此 runbook 所需的最低IAM權限的示例策略：

```
{
  "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操作：

1. 導航到 AWS Systems Manager 控制台中的 [AWSSupport-AnalyzeEBSResource 用法](#)。
2. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- S3 BucketName (必要)：

您帳戶中要將報告上傳到的 Amazon S3 儲存貯體。

- CustomerManagedKmsKeyArn(選擇性)：

用於加密新 Amazon S3 儲存貯體的自訂 AWS KMS 金鑰 Amazon 資源名稱 (ARN)，如果帳戶中指定的儲存貯體不存在，則會建立該儲存貯體。

### Input parameters

<p><b>S3BucketName</b> (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 <code>**&lt;User-provided-name&gt;-awssupport-YYYY-MM-DD**</code>, encrypted with custom Key Management Service (KMS) key</p> <input type="text" value="Enter the name of an existing S3 Bucket"/>	<p><b>CustomerManagedKmsKeyArn</b> (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</p> <input type="text" value="arn:aws:kms:eu-central-1:██████████:key/██████████-4216-a498-460a2132ca4c"/>
<p><b>S3 Bucket</b> <input type="text" value="test-bucket-1"/> Example: s3-bucket-name</p>	<input type="button" value="↻"/>
<p><b>AutomationAssumeRole</b> (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.</p> <input type="text" value="Select an existing IAM Role"/>	<input type="button" value="↻"/>
<p><input type="text" value="admin-my"/> arn:aws:iam:██████████:role/██████████</p>	<input type="button" value="↻"/>

### 3. 選取執行。

### 4. 自動化啟動。

### 5. 自動化工作流程簿執行下列步驟：

- checkConcurrency:

確保在該地區只有一個啟動這個手冊。如果 runbook 發現正在進行的另一個執行，它返回一個錯誤並結束。

- verifyOrCreate桶:

驗證 Amazon S3 儲存桶是否存在。如果沒有，它會在使用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 AMIs (未被任何 Amazon EC2 執行個體使用) 會以名稱格式產生報告 `<region>-images.csv`，並將其上傳到 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`，然後將其上傳到 Amazon S3 儲存貯體。

- gatherSnapshotDetails:

尋找已刪除之 Amazon EBS 磁碟區的 Amazon EBS 快照，使用名稱格式產生報告 `<region>-snapshot.csv`，然後將其上傳到 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	
gatherVolumeDetails.gatherVolumeDetailsOutput No volume found in available state in region eu-central-1	verifyOrCreateS3bucket.createdNewBucket true
gatherAmiDetails.gatherAmiDetailsOutput File eu-central-1-image.csv have been uploaded to bucket aws-support-ssm-[REDACTED]-1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those AMI.	
gatherSnapshotDetails.gatherSnapshotDetailsOutput File eu-central-1-snapshot.csv have been uploaded to bucket aws-support-ssm-[REDACTED]-1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those snapshots.	

## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

## AWS-ArchiveEBSSnapshots

### Description

透過指定套用至快照的標籤，AWS-ArchiveEBSSnapshotsRunbook 可協助您為 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區的快照封存。或者，如果您的快照未標記，您也可以提供磁碟區的 ID。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 描述

類型：字串

說明：(可選) Amazon EBS 快照的說明。

- 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權限，而不實際提出請求，並提供錯誤回應。

- RetentionCount

類型：字串

說明：(選擇性) 您要封存的快照數目。如果您指定的值，請勿為此參數指定值 RetentionDays。

- RetentionDays

類型：字串

說明：(選擇性) 您要封存的前幾天快照數目。如果您指定的值，請勿為此參數指定值 RetentionCount。

- SnapshotWithTag

類型：字串

有效值：是 | 否

描述：(必要) 指定是否標記要封存的快照。

- TagKey

說明：(選擇性) 指派給您要封存之快照的標籤金鑰。

- TagValue

類型：字串

說明：(選擇性) 指派給您要存檔之快照的標記值。

- VolumeId

類型：字串

說明：(選擇性) 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權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

### 文件步驟

aws:executeScript-使用您使用TagKey和參數或TagValue參數指定的標籤來存檔快照。 VolumeId

## AWS-AttachEBSVolume

### Description

將 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區連接到 Amazon 彈性運算雲端 (AmazonEC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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：(必填) Amazon EBS 卷的 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-CalculateEBSPerformanceMetricsRunbook 透過計算效能指標並將 EBS 效能指標發佈到 CloudWatch 儀表板，協助診斷 Amazon 效能問題。儀表板會顯示目標 Amazon 磁 EBS 碟區或連接到目標 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的所有磁碟區的預估平均值 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值 IOPS 和輸送量。runbook 會將連結輸出至新建立的儀表板，該 CloudWatch 儀表板會顯示相關計算 CloudWatch



量度。CloudWatch 儀表板在您的帳戶中創建，名稱為：AWSsupport-<ResourceId>-EBS-Performance-<automation:EXECUTION\_ID>。

它是如何工作的？

執行手冊執行下列步驟：

- 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 作為 ResourceID 時，它會建立一個 CloudWatch 儀表板，其中包含該 Amazon 執行個體的「實際總IOPS/輸送量」，以及連接到 Amazon EC2 執行個體的所有 Amazon EBS 磁碟區的「預估平均IOPS/輸送量」圖表。EC2
- 當您提供 Amazon EBS 磁碟區做為 ResourceID 時，它會建立一個 CloudWatch 儀表板，其中包含該磁碟區的預估平均IOPS/輸送量圖表。
- 產生 CloudWatch 儀表板之後，如果「預估平均輸送量」IOPS 或「預估平均輸送量」分別大於「最大輸送量」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進行微爆發。

#### Note

對於高載磁碟區 (gp2、sc2 和 st1)，在獲得成組分解平衡之前，應考慮最大IOPS/輸送量。完全利用突發平衡後，即它變為零，請考慮基線IOPS/吞吐量指標。

#### Important

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

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

## 平台

Linux 系統 macOS, Windows

## 參數

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

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

### 樣品政策

```
{
  "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操作：

1. 瀏覽至「文件」下 [AWSSupport-CalculateEBSPerformanceMetrics](#) 的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：
 

( ) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - ResourceID (必要)：
 

Amazon EC2 實例或 Amazon EBS 卷的 ID。
  - 開始時間 (必填)：
 

檢視資料的開始時間 CloudWatch。時間必須是格式 yyyy-mm-ddThh:mm:ss 和中 UTC。
  - 結束時間 ( 必填 )：
 

檢視資料的結束時間 CloudWatch。時間必須是格式 yyyy-mm-ddThh:mm:ss 和中 UTC。

Input parameters	
AutomationAssumeRole <small>(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.</small> <input type="text" value="Choose an option"/>	ResourceId <small>(Required) The ID of the EC2 Instance or EBS Volume.</small> <input type="text" value="String"/>
StartTime <small>(Required) The start time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddThh:mm:ss' and is UTC.</small> <input type="text" value="String"/>	EndTime <small>(Required) The end time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddThh:mm:ss' and is UTC.</small> <input type="text" value="String"/>

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，則此執行手冊會建立一個 CloudWatch 儀表板，其中包含 Amazon EBS 磁碟區的估計平均 IOPS 和預估平均輸送量。如果您為參數資源 ID 提供 Amazon EC2 執行個體 ID，則此執行手

冊會建立一個 CloudWatch 儀表板，其中包含 Amazon 執行個體的平均總輸送量 IOPS 和平均總輸送量，以及連接到 Amazon EC2 執行個體的所有 Amazon EBS 磁碟區的預估平均 IOPS 和預估平均輸送量。EC2

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

```
▼ 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.
```

作為 Amazon EC2 執行個體的資源 ID 的範例 CloudWatch 儀表板

### Aggregated Metrics for EC2 Instance i-[redacted]

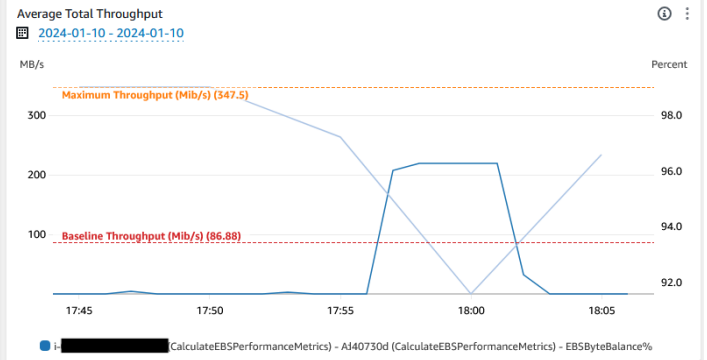
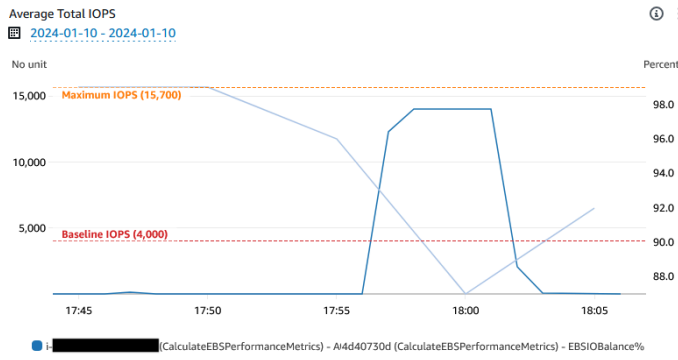
- Instance Type: t3.large
- EBS Optimized: True

[More details on EBS Optimized instances](#) [More details on EBS Volume Types](#)

How do I use CloudWatch to view the aggregate Amazon EBS performance metrics for an EC2 instance?

Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	$SUM(\text{For All Volumes}[(SUM(\text{VolumeReadOps}) + SUM(\text{VolumeWriteOps}))]) / \text{Period}$	IOPS
Average Total Throughput	$SUM(\text{For All Volumes}[(SUM(\text{VolumeReadBytes}) + SUM(\text{VolumeWriteBytes}))]) / \text{Period} / 1024 / 1024$	MiB/s

Note: The maximum performance can only be achieved if `BurstBalance%` for EBS volume or `EBSIOBalance%`, `EBSByteBalance%` for instance is greater than zero.



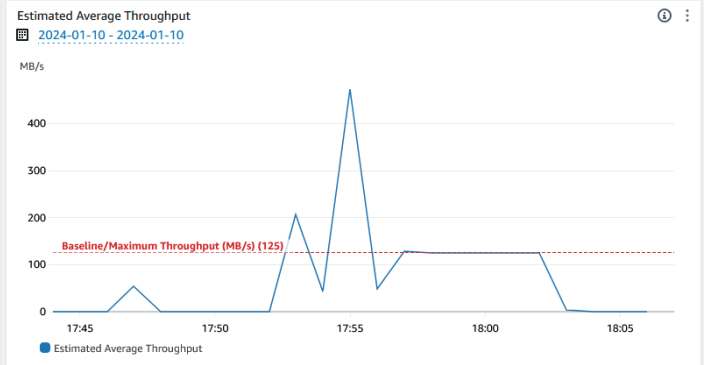
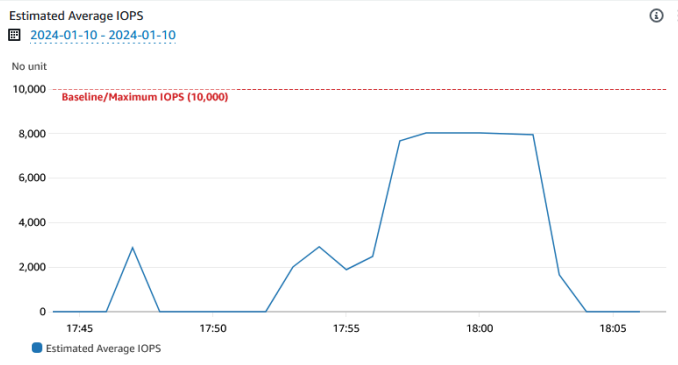
### EBS Volume(s) Metrics

Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	$(SUM(\text{VolumeReadOps}) + SUM(\text{VolumeWriteOps})) / (\text{Period} - SUM(\text{VolumeIdleTime}))$	IOPS
Estimated Average Throughput	$(SUM(\text{VolumeReadBytes}) + SUM(\text{VolumeWriteBytes})) / (\text{Period} - SUM(\text{VolumeIdleTime})) / 1024 / 1024$	MiB/s

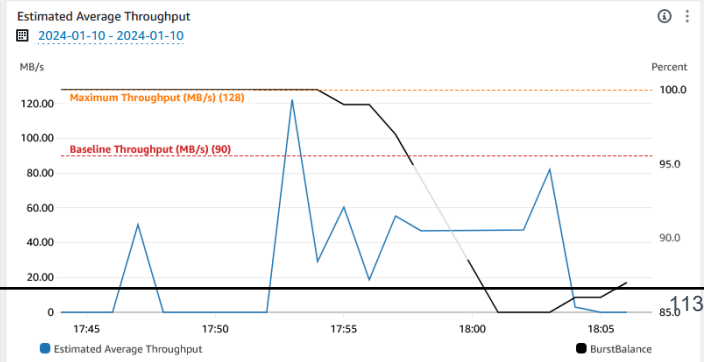
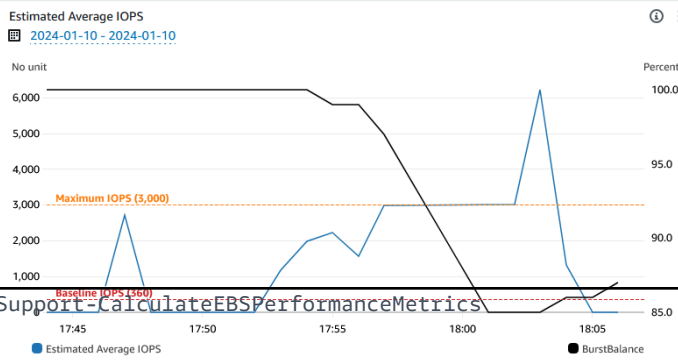
Note: If Estimated Average IOPS / Estimated Average Throughput is more than Maximum IOPS / Maximum Throughput, then microbusting is happening for that particular volume. Realtime analysis for Microbusting may vary, to confirm further you can use OS-level tool that has a finer granularity than CloudWatch. Also, the maximum performance for certain volume types can only be achieved if `BurstBalance%` is greater than zero.

For more information, please review - [How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?](#)

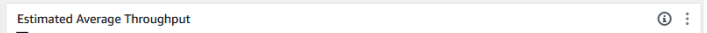
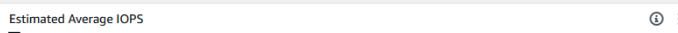
Volume: vol-[redacted] Type: gp3



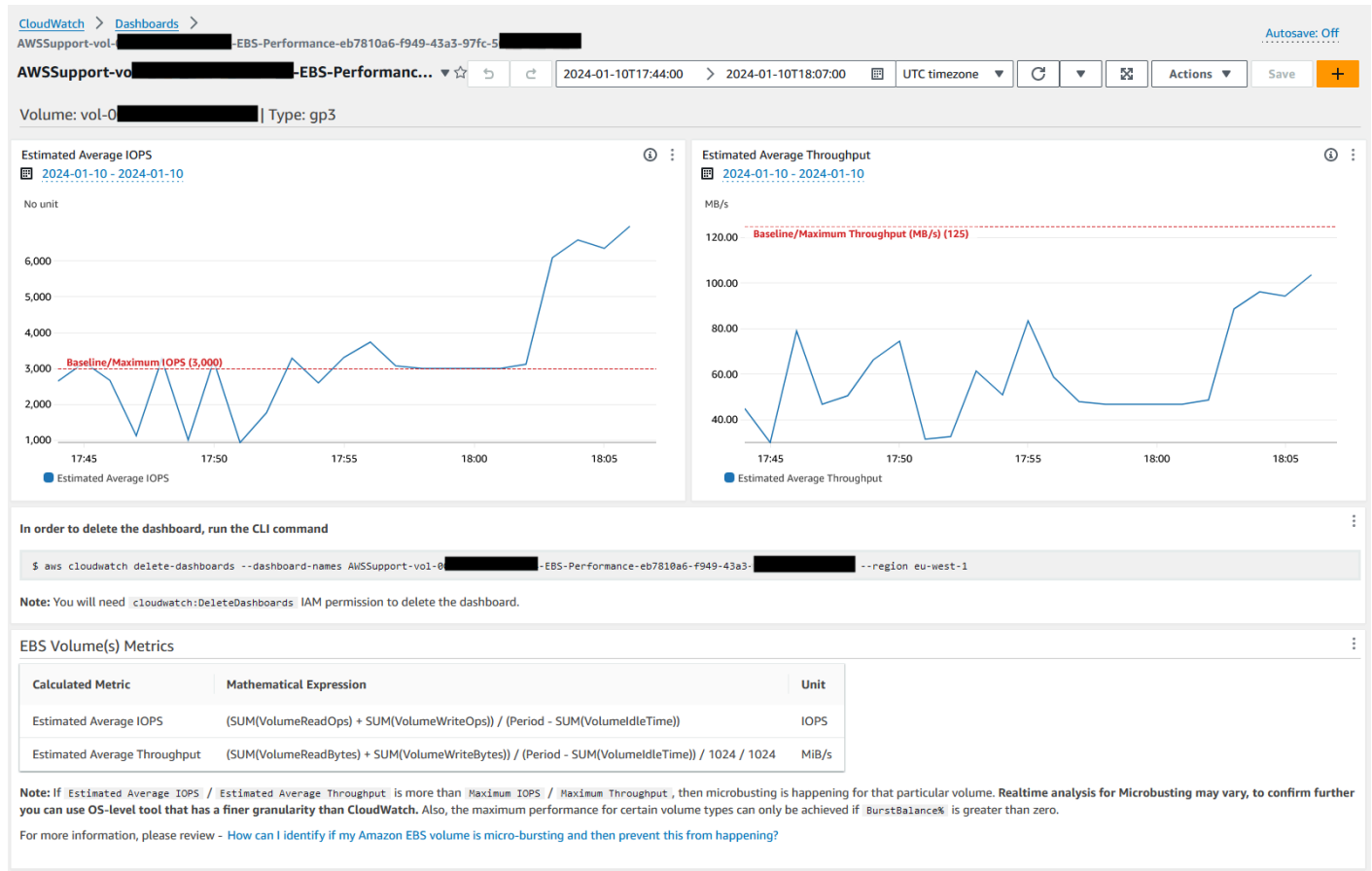
Volume: vol-[redacted] Type: gp2



Volume: vol-[redacted] Type: gp3



## 作為 Amazon EBS 磁碟區識別碼的資源 ID 的範例 CloudWatch 儀表板



### 參考

#### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

#### AWS 服務文件

- [如何確定我的 Amazon EBS 卷是否微爆裂，然後防止這種情況發生？](#)
- [如何使用 CloudWatch 檢視 EC2 執行個體的彙總 Amazon EBS 效能指標？](#)

# AWS-CopySnapshot

## Description

複製 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區的 point-in-time 快照。您可以將相同 AWS 區域區域內的快照複製到另一個區域。加密的 Amazon EBS 快照副本會保持加密狀態。未加密快照的副本仍保持未加密狀態。若要複製從其他帳戶共用的加密快照，您必須擁有用於加密快照之KMS金鑰的權限。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。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 描述

類型：字串

說明：(可選) Amazon EBS 快照的說明。

- SnapshotId

類型：字串

說明：(必填) 要複製的 Amazon EBS 快照的 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 -新快照的識別碼。

## AWS-CreateSnapshot

### Description

建立 Amazon EBS 磁碟區的快照。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。



- 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。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- SnapshotId

類型：字串

說明：(必要) EBS 快照的識別碼。

## AWSConfigRemediation-DeleteUnusedEBSVolume

### Description

該手AWSConfigRemediation-DeleteUnusedEBSVolume冊刪除一個未使用的 Amazon 彈性塊商店 ( AmazonEBS ) 卷。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- CreateSnapshot

類型：布林值

說明：(選擇性) 如果設定為true，自動化會在刪除 Amazon EBS 磁碟區之前建立快照。

- Volumeld

類型：字串

描述：(必填) 您要刪除之 Amazon EBS 磁碟區的 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 磁碟區未使用中，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，則刪除快照。
- aws:executeAwsApi-刪除您在VolumeId參數中指定的 Amazon EBS 磁碟區。
- aws:executeScript-驗證 Amazon EBS 磁碟區已被刪除。

## AWS-DeregisterAMIs

### Description

AWS-DeregisterAMIsrunbook 可以說明您取消註冊 Amazon Machine Images (AMIs) 通過指定你已經應用到你的 AMIs

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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權限，而不實際提出請求，並提供錯誤回應。

- RetainNumber

類型：字串

說明：(選擇性) 您要保留的 AMIs 編號。如果您指定的值，請勿為此參數指定值 Age。

- 年齡

類型：字串

說明：(選擇性) 您要保留的 AMIs 前幾天。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之標籤的金鑰。AMIs

- TagValue

類型：字串

描述：(必要) 指派給您要取消註冊AMI的標籤值。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-使用您AMI使用TagKey和TagValue參數指定的標籤取消註冊。

## AWS-DetachEBSVolume

### Description

從 Amazon 彈性運算雲 ( AmazonEC2 ) 實例分離 Amazon EBS 卷。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LambdaAssumeRole

類型：字串

描述：(選擇性) Lambda 所承擔的角色 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

執行手AWSConfigRemediation-EnableEbsEncryptionByDefault冊會在您執行自動化的所有新 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區上啟用加密功能。AWS 帳戶 AWS 區域 在執行自動化操作之前建立的磁碟區不會加密。

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-驗證預設的 Amazon EBS 加密設定是否已啟用。

## AWS-ExtendEbsVolume

### Description

該手AWS-ExtendEbsVolume冊增加了一個 Amazon EBS 卷的大小，並擴展了文件系統。此自動化支援xfs和ext4檔案系統。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DriveLetter

類型：字串

描述：(選擇性) 您要擴充其檔案系統的磁碟機代號。執行個體需要此參 Windows 數。

- InstanceId

類型：字串

說明：(可選) 您要擴展的 EC2 Amazon EBS 卷附加到的 Amazon 實例的 ID。

- KeepSnapshot

類型：布林值

預設：true

說明：(選擇性) 決定是否在增加 Amazon EBS 磁碟區大小之前保留建立的快照。

- MountPoint

類型：字串

描述：(選擇性) 您要擴充其檔案系統的磁碟機掛載點。Linux 執行個體需要此參數。

- SizeGib

類型：字串

說明：(必填) 您要將 Amazon EBS 磁碟區修改為的 GiB 大小。

- VolumeId

類型：字串

說明：(必要) 您要擴充的 EBS 磁碟區 ID。



## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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，並延伸檔案系統。

# AWSSupport-ModifyEBSSnapshotPermission

## Description

手AWSSupport-ModifyEBSSnapshotPermission冊可幫助您修改多個 Amazon 彈性區塊存放區 (AmazonEBS) 快照的許可。使用此 runbook，您可以製作快照Public或Private與其他 AWS 帳戶人共享它們。使用預設KMS金鑰加密的快照無法與使用此 Runbook 的其他帳戶共用。

## [運行此自動化 \( 控制台 \)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AccountIds

類型: StringList

預設：none

說明：(選擇性) 您要與IDs其共用快照的帳戶。如果您輸入No參數值，則需要此Private參數。

- AccountPermissionOperation

類型：字串

有效值：添加 | 刪除

預設：none

描述：(選擇性) 要執行的作業類型。

- 私有

類型：字串

有效值：是 | 否

說明：(必要) 如果要與特定帳戶共用快照，請輸入No值。

- SnapshotIds

類型: StringList

描述：( 必填 ) 您要修改其許可IDs的 Amazon EBS 快照。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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。驗證之後IDs，指令碼會檢查是否有加密的快照，並輸出清單 (如果找到的話)。
2. `aws:branch`-根據您為Private參數輸入的值分支自動化。
3. `aws:executeScript`-修改指定快照的權限，以便與指定的帳戶共用。
4. `aws:executeScript`-修改快照的權限以將其從變更Public為Private。

## 輸出

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts. 結果。

MakePrivate. 結果。

MakePrivate. 命令

# AWSConfigRemediation-ModifyEBSVolumeType

## Description

手AWSConfigRemediation-ModifyEBSVolumeType冊修改 Amazon 彈性區塊商店 (AmazonEBS) 卷的卷類型。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相關資訊，請參閱 Amazon EC2 使用者指南中的[監控大量修改進度](#)。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- EbsVolumeId

類型：字串

描述：(必填) 您要修改之 Amazon EBS 磁碟區的 ID。

- EbsVolumeType

類型：字串

有效值：標準 | IO1 | IO2 | gp3 |

描述：您想要將 Amazon 磁碟區變更為的 EBS 磁碟區類型。如需 Amazon EBS 磁碟區類型的相關資訊，請參閱 [Amazon EC2 使用者指南中的 Amazon EBS 磁碟區類型](#)。

### 必要的 IAM 權限

此 AutomationAssumeRole 參數需要執行下列動作，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 彈性運算雲端提供預先定義的手冊。Amazon 彈性塊商店的手冊位於手冊參考的[Amazon EBS](#)部分。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatelImage](#)
- [AWS-DeletelImage](#)
- [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-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 (描述)

變更自動擴展群組中 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的待命狀態。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您要變更自動擴展群組中待命狀態之 Amazon EC2 執行個體的 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 (描述)

變更自動擴展群組中 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的待命狀態。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您想要變更自動擴展群組中待命狀態的 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 (描述)

從亞馬遜彈性運算雲端 Amazon Machine Image (Amazon EC2AMI) 執行個體建立新的 ()。



## 運行此自動化 (控制台)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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

此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 (描述)

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

### [運行此自動化 \(控制台\)](#)

#### 文件類型

#### 自動化

#### 擁有者

Amazon

#### 平台

Linux, macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- **ImageId**

類型：字串

描述：(必要) AMI 的 ID。

### 必要的 IAM 許可

此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 (描述)

修補自動擴展群組中的亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

## 擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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期間執行的執行個體 ID。

- LambdaRoleArn

類型：字串

說明：(選用) 允許自動化建立的 Lambda 代表您執行動作的角色 ARN。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

說明：(選擇性) 自動化應進入睡眠狀態以允許執行個體恢復服務的持續時間。

- WaitForReboot

類型：字串

預設：PT5M

說明：(選擇性) 「自動化」應進入睡眠狀態，以允許修補的執行個體重新啟動的持續時間。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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 (描述)

使 EC2 執行個體符合適用的修補程式基準。失敗時復原根磁碟區。

## 運行此自動化 ( 控制台 )

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：( 必填 ) 我們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

說明：(選用) 在處理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	deleteCloudFormation模板	aws:deleteStack

## 輸出

IdentifyRootVolume有效載荷。

PrePatchSnapshot輸出。

SaveComplianceReportTo有效負載

RestoreFromSnapshot有效載荷。

CheckCompliance有效載荷。

## AWS-QuarantineEC2Instance

### Description (描述)

使用 AWS-QuarantineEC2Instance Runbook，您可以將安全群組指派給不允許任何入站或出站流量的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體。

#### Important

RDP 設定的變更應該在執行此 Runbook 之前仔細檢閱。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux 系統macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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

說明：(必要) 您要指派給執行個體以防止輸入或輸出流量的安全性群組名稱。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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-收集有關執行個體的詳細資料。
- aws:executeScript-驗證執行個體不是「自動縮放」群組的一部分。
- aws:executeAwsApi-建立連接至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執行個體。

### 輸出

GetEC2InstanceResources.RevokedSecurityGroupsIds

```
GetEC2InstanceResources.RevokedSecurityGroupsNames
```

```
createSnapshot.SnapId
```

## AWS-ResizeInstance

Description (描述)

變更亞馬遜彈性運算雲端 (Amazon EC2) 執行個體的執行個體類型。

[運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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。

- LambdaAssumeRole

類型：字串

描述：(選用) Lambda 所承擔之角色的 ARN。

## AWS-RestartEC2Instance

Description (描述)

重新啟動一或多個亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。

[運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型:StringList

說明：(必填) 要重新啟動之 Amazon EC2 執行個體的 ID。

# AWS-SetupJupyter

## Description (描述)

AWS-SetupJupyter執行手冊可協助您在亞馬遜彈性運算雲端 (Amazon EC2) 執行個體上設定 Jupyter 筆記本。您可以指定現有執行個體，也可以提供 Amazon Machine Image (AMI) ID 以啟動和設定新執行個體的自動化操作。在開始之前，您必須在「SecureString參數存放區」中建立參數，以用作 Jupyter 筆記本的密碼。參數存放區是的功能AWS Systems Manager。若要取得有關建立參數的資訊，請參閱[AWS Systems Manager使用指南中的〈建立參數〉](#)

## [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

#### Amazon

### 平台

### Linux

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- Amild

類型：字串

說明：(選擇性) 您要用來啟動新執行個體並設定 Jupyter 記事本的識別碼。AMI

- Instanceid

類型：字串

描述：(必要) 您要在其上設定 Jupyter 記事本的執行個體識別碼。

- InstanceType

類型：字串

預設值：3. 中

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

- JupyterPasswordSSMkey

類型：字串

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

- KeyPairName

類型：字串

說明：(選擇性) 您要與新啟動之執行處理產生關聯的金鑰配對。

- RemoteAccessCidr

類型：字串

預設：0.0.0.0/0

說明：(選擇性) 您要允許 SSH 流量的 CIDR 範圍。

- RoleName

類型：字串

預設值：超音波 ManagedInstanceProfileRole

說明：(選擇性) 新啟動之執行處理的執行處理設定檔名稱。

- StackName

類型：字串

預設值：CreateManagedInstanceStack{{自動化：執行 ID}}

說明：(選擇性) 您希望自動化操作使用的AWS CloudFormation堆疊名稱。

- SubnetId

類型：字串

預設：Default

說明：(選擇性) 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

說明：(選用) 您要在其中啟動新執行個體的虛擬私有雲 (VPC) ID。

### 必要的 IAM 許可

此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 (描述)

啟動一或多個亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型:StringList

描述：(必要) 要啟動的 EC2 執行個體。

## AWS-StopEC2Instance

Description (描述)

停止一個或多個亞馬遜彈性運算雲 (Amazon EC2) 執行個體。

[運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux,macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型:StringList



說明：( 必填 ) 要停止的 EC2 執行個體。

## AWS-TerminateEC2Instance

### Description (描述)

終止一個或多個亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceIds

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 發行包和 Amazon 軟件更新 Amazon Machine Image ( AMI ) 。

## [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

預設值：ManagedInstanceProfile

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

- 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

預設值：{「HttpEndpoint」:「已啟用」、HttpTokens「」:「選擇性」}

說明：(選擇性) 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

說明：(必要) 您要套用到至的安全性群組 ID 的逗號分隔清單AMI。

- SourceAmiId

類型：字串

描述：(必要) 來源 Amazon Machine Image ID。

- SubnetId

類型：字串

說明：(選擇性) 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

預設值：UpdateLinuxAmi\_ 從 \_ {{{SourceAmiId}} }\_on\_ {全球：日期時間}}

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 視窗 Amazon Machine Image (AMI)。默認情況下，該手冊安裝所有 Windows 更新，Amazon 軟件和 Amazon 驅動程序。接著會執行 Sysprep 以建立新的 AMI。支援 Windows Server 2008 R2 或更新版本。

#### Important

如果您的執行個體連線到 AWS Systems Manager 使用 VPC 端點，除非在 us-east-1 區域中使用，否則此執行手冊將會失敗。執行個體必須啟用 TLS 1.2 才能使用此工作流程簿。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

## Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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：應用程式，連接器 CriticalUpdates DefinitionUpdates，DeveloperKits，，驅動程序FeaturePacks，指導，Microsoft SecurityUpdates，，ServicePacks，，工具UpdateRollups，更新。有效格式包括單一項目，例如：CriticalUpdates。或者，您可以指定一個逗號分隔的列表：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

預設值：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

預設值：{「HttpEndpoint」:「已啟用」、HttpTokens「」:「選擇性」}

說明：(選擇性) 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

說明：(必要) 您要套用至的安全性群組 ID 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。

- SourceAmiId

類型：字串

描述：(必要) 來源 AMI ID。

- SubnetId

類型：字串

說明：(選擇性) 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

預設值：UpdateWindowsAmi\_ 從 \_{{{SourceAmiId}}}\_on\_{全球：日期時間}}

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 (描述)

執行手冊 `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` 可為您指定的 Amazon EC2 自動擴展 (自動擴展) 群組啟用運作狀態檢查。

## [運行此自動化 \(控制台\)](#)

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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- AutoScalingGroupARN

類型：字串

描述：(必填) 您要啟用運作狀態檢查之自動擴展群組的 Amazon 資源名稱 (ARN)。

- HealthCheckGracePeriod

類型：整數

預設：300

說明：(選用) 自動擴展在檢查已投入服務之 Amazon 彈性運算雲端 (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

此 `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`-啟用您在`AutoScalingGroupARN`參數中指定的「自動調整比例」群組的健康狀態檢查。

## AWSConfigRemediation-EnforceEC2InstanceIMDSv2

### Description

AWSConfigRemediation-EnforceEC2InstanceIMDSv2執行手冊需要您指定使用執行個體中繼資料服務版本 2 (IMDSv2) 的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

Linux macOS, Windows

### 參數

- `InstanceId`

類型：字串

說明：(必填) 您想要使用 IMDSv2 時所需的 Amazon EC2 執行個體識別碼。

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- HttpPutResponseHopLimit

類型：整數

描述：(選擇性) 從 IMDS 服務返回要求者的躍點回應限制。如果 EC2 執行個體託管容器，則設定為 2 或更高版本。設定為 0 則不變更 (預設值)。

允許的模式：`^([1-5]?\d|6[0-4])$`

預設：0

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

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

### 文件步驟

- `aws:executeScript`-在您在InstanceId參數中指HttpTokensrequired定的 Amazon EC2 執行個體上將選項設定為。
- `aws:assertAwsResourceProperty`-驗證亞馬遜 EC2 執行個體上是否需要 IMDSv2。

## AWSEC2-CloneInstanceAndUpgradeSQLServer

### Description

AMI從執行個體建立EC2Windows Server執行 SQL Server 2008 或更新版本的執行個體，然後將伺服器升級AMI至較新版本的SQL伺服器。僅支援英文版的SQL伺服器。

支援下列升級路徑：

- SQL伺服器SQL器 2008 年至伺服器

- SQL伺服器二零一七年、二零一六年或二零一四年SQL伺服器
- SQL伺服器 2012 年至伺服器
- SQL伺服器 2014 年至伺服器
- SQL伺服器 2016 年至SQL伺服器

如果您使用的舊版 Windows 伺服器與SQL伺服器 2019 不相容，則自動化文件必須將您的 Windows 伺服器版本升級到 2016 年。

升級為多步驟程序，可能需要 2 小時才能完成。自動化會AMI從執行個體建立，然後從指定的新AMI執行個體啟動暫存執行個體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，自動化會在暫存執行個體TargetSQLVersion上執行就地升級。升級之後，自動化會AMI從暫存執行個體建立新的執行個體，然後終止暫存執行個體。

您可以透過AMI在VPC. 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EC2執行個體啟動的電腦名稱AMI，請參閱[重新命名裝載獨立SQL伺服器執行個體的電腦](#)。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

先決條件

- TLS版本 1.2。

- 僅支援英文版的SQL伺服器。
- EC2執行個體必須使用 Windows Server 2008 R2 (或更新版本) 和SQL伺服器 2008 (或更新版本) 的 Windows Server版本。
- 確認SSM代理程式已安裝在您的執行個體上。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代理程式](#)。
- 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 [Systems Manager 建立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。
- 對於使用「自攜授權」(BYOL) SQL 伺服器版本的執行個體，則適用下列其他先決條件：
  - 提供包含目標SQL伺服器安裝媒體的EBS快照 ID。若要執行此作業：
    1. 確認執行個體正在EC2執行視窗伺服器 2008 R2 或更新版本。
    2. 在執行個體EBS體的相同可用區域中建立 6 GB 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. 以滑鼠右鍵按一下ISO並將其掛接至執行個體，例如磁碟機 E。
    4. 將驅動器 E : \ ISO 的內容複製到驅動器 D : \
    5. 建立步驟 2 中建立之 6 GB 磁碟區的EBS快照。

## 限制

- 升級只能在使用 Windows 驗證的SQL伺服器上執行。
- 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)。
- SQL不支援 HA 和鏡像模式下的伺服器部署。

## 參數

- IamInstanceProfile

類型：字串

描述：(必要) IAM 執行個體設定檔。

- InstanceId

類型：字串

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

- KeepPreUpgradeImageBackUp

類型：字串

說明：(選用) 如果設為 true，自動化操作不會刪除升級前從執行個體 AMI 建立的項目。如果設定為 true，則您必須刪除 AMI。依預設，AMI 會刪除。

- SubnetId

類型：字串

描述：(必要) 為升級程序提供子網路。確認子網路具有連至 AWS 服務、Amazon S3 和 Microsoft 的輸出連線能力 (以下載修補程式)。

- SQLServerSnapshotId

類型：字串

描述：(條件式) 目標 SQL 伺服器安裝媒體的快照 ID。使用 BYOL SQL 伺服器版本的執行個體需要此參數。對於包含 SQL 伺服器授權的執行個體 (使用 AWS 提供的 Amazon 機器映像啟動的執行個體，適用於 Windows Server 和 Microsoft SQL 伺服器)，此參數是選用的。

- RebootInstanceBeforeTakingImage

類型：字串

說明：(選擇性) 如果設為 true，自動化操作會在建立升級前重新啟動執行個體。AMI 根據預設，自動化操作不會在升級前重新開機。

- TargetSQLVersion

類型：字串

說明：(選擇性) 選取目標 SQL 伺服器版本。

可能的目標：

- SQL 伺服器
- SQL 伺服器
- SQL 伺服器
- SQL 伺服器

預設目標：2016 年 SQL 伺服器

## 輸出

AMIId：從升級至較新版 SQL 伺服器之執行個體所 AMI 建立的識別碼。

## AWSEC2-CloneInstanceAndUpgradeWindows

### Description

從 Windows Server 2008 年 R2、2016 年或 2019 年執行個體建立一個 Amazon Machine Image (AMI)，然後升級 AMI 到 Windows Server 2016 年、2019 年或 2022 年。支援的升級路徑如下。

- Windows Server 二零零八年第二至二零一 Windows Server 六年
- Windows Server 2012 R2 到 Windows Server 2016。
- Windows Server 2012 R2 到 Windows Server 2019。
- Windows Server 二零一二年第二 Windows Server 期至二零二年
- Windows Server 2016 至 Windows Server 2019。
- Windows Server 二零一六至二零二 Windows Server 年
- Windows Server 二零一九 Windows Server 年至二零二

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，然後從您指定的新建立 AMI 啟動暫存執行 SubnetId 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，自動化會在暫存執行個體 TargetWindowsVersion 上執行就地升級。若要將您的 Windows Server 2008 年 R2 執行個體升級至 Windows Server 2016 年、2019 年或 2022 年，系統會執行兩次就地升級，因為不支援將 Windows Server 2008 年 R2 直接升級至 Windows Server 2016 年、2019 年或 2022 年。自動化操作也會更新或安裝暫存執行個體所需的 AWS 驅動程式。升級之後，自動化會從暫存執行個體建立新的 AMI，然後終止暫存執行個體。

您可以透過在 Amazon 虛擬私有雲 (Amazon VPC) 中從升級的 AMI 啟動測試執行個體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 AMI。

### [運行此自動化 \(控制台\)](#)

### 文件類型

## 自動化

### 擁有者

Amazon

### 平台

Windows Server 2008 年 R2、2012 年第二季版或 2019 年標準版和資料中心版

### 先決條件

- TLS 版本 1.2.
- 確認 SSM Agent 安裝於您的執行個體上。如需詳細資訊，請參閱在適用於 [Windows 伺服器的 EC2 執行個體上安裝和設定 SSM 代理程式](#)。
- 視窗 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連線至網際網路的輸出連線，以提供 Amazon S3 AWS 服務等存取權，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 年 R2、2012 年 R2、2016 年和 2019 年執行個體。
- 使用可為 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執行個體。Windows Server 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。
- 如果執行個體不使用 AWS 提供的 Windows 授權，請指定包含 Windows Server 2012 年 R2 安裝媒體的 Amazon EBS 快照識別碼。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

說明：(選擇性) 升級程序期間要使用的替代 key pair 名稱。在指派給原始執行個體的 key pair 無法使用時，這會很有用。如果未為原始例證指定 key pair，您必須指定此參數的值。

- 自攜程式 WindowsMediaSnapshotId

類型：字串

說明：(選擇性) 要複製的 Amazon EBS 快照識別碼，其中包括視窗伺服器 2012R2 安裝媒體。只有在您升級 BYOL 執行個體時需要。

- IamInstanceProfile

類型：字串

說明：(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

說明：(必填) 執行 Windows Server 2008 年第二季、二零一六年或 2019 年執行的 EC2 執行個體。

- KeepPreUpgradeImageBackUp

類型：字串

說明：(選用) 如果設定為 True，則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

說明：( 必填 ) 這是升級程序的子網路以及來源 EC2 執行個體所在的位置。確認子網路具有連至 AWS 服務、Amazon S3 和 Microsoft 的輸出連線能力 (以下載修補程式)。

- TargetWindowsVersion

類型：字串

描述：(必要) 選取目標 Windows 版本。

預設值：

- 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

安全性技術實作指南 (STIGs) 是由美國國防資訊系統機構 (DISA) 建立的組態強化標準，用於保護資訊系統與軟體的安全。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性設定。

Amazon EC2 提供了一個 Systems Manager runbookAWSEC2-ConfigureSTIG，您可以使用它將STIG設置應用於實例。本文件可協助您快速建立符合STIG標準的相容影像。STIG系 Systems Manager 文件會掃描配置錯誤並執行補救指令碼。它也會 InstallRoot 從 Windows AMIs 上的國防部 (DoD) 安裝和更新 DoD 憑證，並移除不必要的憑證以維持STIG合規性。使用「STIGSystems Manager」文件不會收取額外費用。

### Important

除了少數例外之外，Systems Manager 文件下載的STIG強化元件並不會安裝協力廠商套件。如果執行個體上已安裝第三方套件，並且 Amazon EC2 支援STIGs該套件的相關套件，則會套用這STIGs些套件。

本頁列出 Amazon EC2 支援STIG強化元件套用至您的EC2執行個體的所STIGs有功能。

您可以選擇要套用的STIG合規性類別。

## 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)

包括任何可能導致機密性、可用性或完整性喪失，但可以減輕風險的弱點。

- 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](#)
- [視窗STIG設定](#)
- [視窗STIG版本紀錄](#)
- [設STIG定](#)
- [STIG版本歷史記錄](#)

## STIG強化元件下載

Amazon 將STIG強化元件一起分組為每個版本的作業系統相關服務包。套裝軟體是適用於下載和執行所在之目標作業系統的封存檔案。Linux 組件包被存儲為TAR文件 ( .tgz 文件擴展名 )。Windows 元件服務包會儲存為ZIP檔案 (.zip 副檔名)。

Amazon 將組件包存儲在每個 Image Builder S3 存儲STIG桶中 AWS 區域。使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。

元件儲存路徑和束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組件存儲桶。 )

## 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

作業系統套裝軟體的標準名稱前置詞為LinuxAWSConfigureSTIG或AWSConfigureSTIG。為了保持向後兼容性，Windows 的下載不包括平台前綴。

### YYYY

發行版本的四位數年份。

### quarter

指出一年中的季度：1、2、3 或 4。

### release

從 1 開始的增量編號，並為每個新版本遞增 1。該版本不包括在一季中的第一個版本，並且僅在後續發行版本中加入。

### file extension

壓縮檔案格式 tgz (Linux) 或 zip (視窗)。

### 套件檔案名稱範例

- LinuxAWSConfigureSTIG\_2023\_Q1\_2.tgz
- AWSConfigureSTIG\_2022\_Q4.zip

## 視窗STIG設定

Amazon EC2 Windows STIG AMIs 和強化元件專為獨立伺服器所設計，並套用本機群組原則。STIG-相容元件會 InstallRoot 從 Windows 上的國防部 (DoD) 安裝，AMIs以下載、安裝和更新 DoD 憑證。他們也會移除不必要的憑證以維持STIG符合性。目前，Amazon EC2 支援以下版本的視窗伺服器的STIG基準：

本節列出 Amazon 對您的 Windows 基礎STIG設施EC2支持的當前設置，然後是版本歷史記錄日誌。

您可以套用低、中或高STIG設定。

## STIG低視窗 (類別III)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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 的完整清單STIGs，請參閱[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

- 視窗伺服器 2022 年STIG版本 1 版本 1

V-254335, V-254336, V-254337, V-254338, V-254351, 願意, 鼎, 和遷 V-254357 V-254363  
V-254481

- 視窗服務器 2019 STIG 版本 2 發布 5

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

- 視窗伺服器 2016 年STIG版本 2 版本 5

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

- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5

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

- Microsoft。 NET框架 4.0 第二STIG版發行版本 2

沒有STIG設置適用於 Microsoft。 NET類別III漏洞的框架。

- 視窗防火牆STIG版本 2

V-241994, V-241995, V-241996, V-241999, V-242000, 願意, 鼎, 涓涓細節 V-242001 V-242006  
V-242007 V-242008

- 互聯網瀏覽器 11 STIG 版本 2 發布 3

V-46477、V-46629 以及 V-97527

- Microsoft 邊緣STIG版本 1 版本 6 (僅限視窗伺服器 2022)

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

## STIG中型視窗 (類別二)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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 的完整清單STIGs，請參閱[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

### Note

除了 Amazon 針對第 II 類弱點EC2支援的STIG強化設定外，Windows STIG 媒體類別還包含適用於 Windows STIG 低 (類別III) 的所有列出STIG強化設定。

- 視窗伺服器 2022 年STIG版本 1 版本 1

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

V-254247, V, 254269, V-254269, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V 型 254285, V, V-254292, V-254300, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V 17, 伏特, 254319, V 型, 254320, V 型 254321, V-254323, V-254323, V 型, 254325, V 型, 254326, V-254327, V 型 254329, VV-254344, V-254345, V-254346, V-254347, V-254349, V-254350, V-254350, V-254356, V-254358, V-254360, V-254361, V 368, 254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254 型 254383, V 254438, V-254439, V-254442, V-254443, V-254444, V-254449, V-254449, V-254450, V-254452, V-254453, V-254454, V 型 254455, V 型 254456, V 型 254456, V 254464, V-254468, V-254470, V-254471, V-254472,,, 湧, 球, 蘋果, 她, 節制, 節制, 蒸氣, 蒸汽, 向量, 雞翼, 卷, 妻子, 妻子, 妻子, V 型, 254495, V 型 254497, V 型 254499, V 型 254501, V 型 254501, V 型 254502, V 型 254503, V 型 254503, V 型 254504, V 型 254504, V 型 8, V 型, V 型 254510, 電視 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

- 視窗服務器 2019 STIG 版本 2 發布 5

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

V-205625, V-205626, V-205627, V-205629, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V V-205655, V-205656, V-205659, V-205660, V-205662, V-205671,

V-205672, V-205673, V-205676, V-205678, V, V -205687, V-205688, V-205689, V-205690, V-205693, V-205694, V, 電視, 電視, 電視 205717, V., V-205729, V-205730, V-205733, V-205747, V-205752, V-205752, V-205756, V-205756, V. V -205770, V-205771, V-205772, V-205773, V-205774, V-205775, V, 電視 -205777, V, V-205801, V-205808, V-205809, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, VV-205830, V-205832, V-205833, V-205834,, 湧, 球, 蘋果, 四季, 四千三十一, 節制, 蒸汽, 冰, 伏特, 冰壺, 風格, V-205872, V-205873, V 型 205911, V 型 205912, V 型 205915, V 型 205916, V 型 205916, V 型 V 型, 和 V-205835 V-205836 V-205837 V-205838 V-205839 V-205840 V-205841 V-205861 V-205863 V-205865 V-205866 V-205867 V-205868 V-205869

- 視窗伺服器 2016 年 STIG 版本 2 版本 5

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

V-224850, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V 224873, V-224881, V-224882, V-224883, V-224885, V-224886, V-二二四八八八, V-224889, V-224889, V 224896, V-224897, V-224898, V-224999, V-224901, V-224902, V, 電影 -224904, V-224904, V-224905, V-224906, V 24912, V-224913, V-二四四四十四, V 型, V-224927, V-224928, V-224929, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V, V-224948, V-224949, V-224951, V-224953, V-224955, V 型, 電視 -224949, V-224957, V-224959, V-224962, V 16, 影視, 電影, 四十一、二五五十四、七五十四、七五十四、七五十四、七五十五 V-225051, V-225052, V-225055, V-225056,, 保證, 湧, 球, 蘋果, 塔, 妻子, 妻子, 妻子, 妻子, 毫無疑問, 伏特, 冰壺, 妻子, V 型 225082, V 型 225082, V 型 225083, V 型 225084, V 型 225084, V 型 V 型 V-225057 V-225058 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

- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5

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

V-225574, V-225573, V-225572, V-225571, V-225569, V-225568, V 型. 25558, 伏特 -225557, V-225554, 伏特 -225553, 伏特 -225551, 伏特 -225549, 伏特 -225549, 伏特 -225548, V-225545, V, V-225538, V-225535, V-225534, V-225533, 伏特 -225531, 伏特 -225535, 伏特 -225529, V, 二五五十八, V 型, 伏特 -225506, 伏特 -225503, V-225502, V-225501, 伏特 -225500, 伏特 -225494, 伏特, 伏特 25463, V-225461, V-225458, V-225457, V-225456, V-225454, V, 電影 -225453, V-225452, V-225448, V 型 225411, V-225410, V-225409, V-225408, 伏特 -225406, 伏特 -225405, 伏特 -225402, V-225402, V-225393, V, V-225385, V 型, 伏特 -225379, V-225378, V-225377, V-225374, V-225373, V-225372, V, 電影 -225371, V-225370, V-225368, V V-225349, V-225348, V-225347, V-225346, V-225345, V-225341, V-225340, V-225339, V-二 25338, V 314, V-225305, V 型, 二五三

零三, V 型 V-225283, V-225282, V-225281, V-225280,, WING, WING, 蘋果, 早餐, 四面八角, 蒸汽浴缸, 蘋果,, 卷, 風格, V-225264, V-225263, V 型 225260, V 型 225260, V 型 225259, 和 V 型 225239 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

- Microsoft。NET 框架 STIG 4.0 第二版發行版本 2

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

V-225238

- 視窗防火牆 STIG 版本 2

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

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

- 互聯網瀏覽器 11 STIG 版本 2 發布 3

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

V-46473、V-46475、V-46481、V-46483、V-46501、V-46507、V-46509、V-46511、V-46513、V-46515、以及 V-75171

- Microsoft 邊緣 STIG 版本 1 版本 6 (僅限視窗伺服器 2022)

V-235720, V-235721, V-235723, V-235724,, 湧, 球, 蘋果, 四季, 四千〇一年, 妻子, 妻子, 冰壺, 伏特, 冰壺, V-235740, V-235741, 格鬥, V 型 235743, V 型 235745, V 型 235745, V 型 235747, V 型 235747, V 型 235748, V 型 235750, V 型 235750, V 型 235750, V 型 235750, V 型 235750, V 型 235750, V 型電視 235761, 電視 -235763, 電視 -235764, 電視 -235767, 電視 -235768, 電視 -235769, 電視 -235771, 電視 -235772, 電視 -235773, 電視 -235774, 和電視 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-235742

- 後衛 STIG 版本 2 發布 4 ( 僅限視窗服務器 2022 )

V-213427, V-213429, V-213430, V-213431,, 湧, 球, 蘋果, 她, 節制, 節制, 包括, 臘, 基督徒, 毫秒, 伏特, 伏特, 雞翼, V 型 213448, V 型 213449, V 型 213451, V 型 213451, V 型 213455, V 型 213464, V 型 213464, V 型 213465, V 型 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

## STIG高窗 (類別 I)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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 的完整清單STIGs，請參閱[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

### Note

除了 Amazon 針對類別 I 弱點EC2支援的STIG強化設定之外，Windows STIG 高類別還包含適用於 Windows STIG 中和低類別的所有列出STIG強化設定。

- 視窗伺服器 2022 年STIG版本 1 版本 1

V-254293, V-254352, V-254353, V-254354,, 搶, 鼎, 蘋果, 鼎, 電視台,, 杯, 北, 0.00, 和 V-254374  
V-254378 V-254381 V-254446 V-254465 V-254466 V-254467 V-254469 V-254474 V-254475  
V-254500

- 視窗服務器 2019 STIG 版本 2 發布 5

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

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

- 視窗伺服器 2016 年STIG版本 2 版本 5

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

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

- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，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框架 STIG 4.0 第二版發行版本 2



包括 Amazon EC2 支持的 Microsoft 類別 II 和 III (中和低) 漏洞的所有 STIG 強化設置。NET 框架。沒有其他 STIG 設定適用於類別 I 弱點。

- 視窗防火牆 STIG 版本 2

包括 Amazon 針 STIG 對第 II 類和 III (中和低) 弱點 EC2 支援的所有強化設置，以及：

V-241992、V-241997 和 V-242002

- 互聯網瀏覽器 11 STIG 版本 2 發布 3

包括 Amazon 針 STIG 對 IE 瀏覽器 11 的第二類和 III (中和低) 漏洞 EC2 支援的所有強化設置。沒有其他 STIG 設定適用於類別 I 弱點。

- Microsoft 邊緣 STIG 版本 1 版本 6 (僅限視窗伺服器 2022)

包括 Amazon 針 STIG 對第 II 類和 III (中和低) 弱點 EC2 支援的所有強化設置，以及：

V-235758 和 V-235759

- 後衛 STIG 版本 2 發布 4 (僅限視窗伺服器 2022)

包括 Amazon 針 STIG 對第 II 類和 III (中和低) 弱點 EC2 支援的所有強化設置，以及：

V-213426、V-213452 和 V-213453

## 視窗 STIG 版本紀錄

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

2024 年第二季度變更-2024 年 5 月 10 日 (沒有變更)：

對於 2024 年第二季度版本的 Windows 元件 STIGS 沒有任何變更。

2024 年第一季度變更-2024 年 2 月 23 日 (沒有變動)：

對於 2024 年第一季度版本的 Windows 元件 STIGS 沒有任何變更。

2023 年第四季度變更-二零二三年七月十二日 (沒有變更)：

對於 2023 年第四季度發行的視窗元件 STIGS 沒有任何變更。

2023 年第三季變更-2023 年 4 月 10 日 (沒有變動) :

對於 2023 年第三季度版本的視窗元件STIGS沒有任何變更。

2023 年第二季度變動-二零二三年三月五日 (沒有變動) :

對於 2023 年第二季度版本的視窗元件STIGS沒有任何變更。

2023 年第一季度變動-2023 年 3 月 27 日 (沒有變動) :

對於 2023 年第一季度版本的視窗元件STIGS沒有任何變更。

二零二二年第四季變更-二零二三年一月二日 :

更新STIG版本並STIGS適用於 2022 年第四季發行版本，如下所示：

#### STIG-建置視窗低版本

- 視窗伺服器 2022 年STIG版本 1 版本 1
- 視窗服務器 2019 STIG 版本 2 發布 5
- 視窗伺服器 2016 年STIG版本 2 版本 5
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5
- Microsoft。NET框架 4.0 第二STIG版發行版本 2
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 2 發布 3
- Microsoft 邊緣STIG版本 1 版本 6 (僅限視窗伺服器 2022)

#### STIG-建置視窗中型版本

- 視窗伺服器 2022 年STIG版本 1 版本 1
- 視窗服務器 2019 STIG 版本 2 發布 5
- 視窗伺服器 2016 年STIG版本 2 版本 5
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5
- Microsoft。NET框架 4.0 第二STIG版發行版本 2
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 2 發布 3
- Microsoft 邊緣STIG版本 1 版本 6 (僅限視窗伺服器 2022)
- 後衛STIG版本 2 發布 4 ( 僅限視窗服務器 2022 )

## STIG-建置視窗高版

- 視窗伺服器 2022 年STIG版本 1 版本 1
- 視窗服務器 2019 STIG 版本 2 發布 5
- 視窗伺服器 2016 年STIG版本 2 版本 5
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 5
- Microsoft。NET框架 4.0 第二STIG版發行版本 2
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 2 發布 3
- Microsoft 邊緣STIG版本 1 版本 6 (僅限視窗伺服器 2022)
- 後衛STIG版本 2 發布 4 ( 僅限視窗服務器 2022 )

2022 年第三季度變動-二零二二年九月三十日 (不變) :

對於 2022 年第三季度版本的 Windows 元件STIGS沒有任何變更。

二零二二年第二季度變動 :

更新STIG版本並STIGS適用於 2022 年第二季度發行版本。

## STIG-構建窗口低版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 4
- 視窗伺服器 2016 年STIG版本 2 版本 4
- 視窗服務器 2012 R2 MS STIG 版本 3 版本 3
- Microsoft。NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

## STIG-構建窗口中版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 4
- 視窗伺服器 2016 年STIG版本 2 版本 4
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 3
- Microsoft。NET框架 4.0 第二STIG版發行版 1

- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

#### STIG-構建窗口高版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 4
- 視窗伺服器 2016 年STIG版本 2 版本 4
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 3
- Microsoft。NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

2022 年第一季度變動 ( 不變 ) :

對於 2022 年第一季度版本的 Windows 元件STIGS沒有任何變更。

二零二一年第四季度變更 :

更新STIG版本並STIGS適用於 2021 年第四季度發行。

#### STIG-構建窗口低版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 3
- 視窗伺服器 2016 年STIG版本 2 版本 3
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 3
- Microsoft。NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

#### STIG-構建窗口中版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 3
- 視窗伺服器 2016 年STIG版本 2 版本 3
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 3
- Microsoft。NET框架 4.0 第二STIG版發行版 1

- 視窗防火牆STIG版本 2
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

#### STIG-構建窗口高版本 1.5.0

- 視窗服務器 2019 STIG 版本 2 發布 3
- 視窗伺服器 2016 年STIG版本 2 版本 3
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 3
- Microsoft。 NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆 2 STIG 版本 1
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

二零二一年第三季變更-九月三十日：

更新STIG版本並STIGS適用於 2021 年第三季度版本。

#### STIG-構建窗口低版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗伺服器 2016 年STIG版本 2 版本 2
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 2
- Microsoft。 NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 1 發行 7
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

#### STIG-構建窗口中版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗伺服器 2016 年STIG版本 2 版本 2
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 2
- Microsoft。 NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 1 發行 7
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

## STIG-構建窗口高版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗伺服器 2016 年STIG版本 2 版本 2
- 視窗服務器 2012 R2 MS STIG 版本 3 發布 2
- Microsoft。NET框架 4.0 第二STIG版發行版 1
- 視窗防火牆STIG版本 1 發行 7
- 互聯網瀏覽器 11 STIG 版本 1 發布 19

## 設STIG定

本節包含 Amazon EC2 支援的 Linux STIG 強化設定的相關資訊，以及版本歷程記錄日誌。如果 Linux 發行版本沒有自己的STIG強化設置，Amazon 會EC2使用RHEL設置。支援的STIG強化設定適用於 Amazon EC2 Linux AMIs 和以 Linux 發行版為基礎的元件，如下所示：

- 紅帽企業版 (RHEL) 7 個STIG設定
  - RHEL7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- RHEL8 種STIG設定
  - RHEL8
  - CentOS 8
  - Amazon 亞馬遜
- RHEL9 種STIG設定
  - RHEL9
  - CentOS Stream 9

## STIG低 (類別III)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

## RHEL7 第三STIG版發行版本 14

- RHEL7/CentOS 7/AL2

V-204452、V-204576 和 V-204605

## RHEL8 STIG 版本 1 版發行版本 14

- RHEL8/CentOS

V-230241, V-244527, V-230269, V-230270,,, WING, 蘋果, 蘋果, 熱氣囊, 鑼, 北, 13.2, CONTH, CONTROL, 伏擊, 卷, V-230497, V-230498, V-230499, 和 V 型 230281 V-230285 V-230253 V-230346 V-230381 V-230395 V-230468 V-230469 V-230491 V-230485 V-230486 V-230494 V-230495 V-230496

## RHEL9 STIG 版本 1 發行版本 3

- RHEL9/CentOS 第 9 流

V-257782, V-257795, V-257796, V-257824,, 搶, 鼎, 蘋果, 熱潮, 電梯,, 和筆 V-257880 V-257946 V-257947 V-258037 V-258067 V-258069 V-258076 V-258173

## STIG版本二發行版本 14

V-219172, V-219173, V-219174, V-219175,, 搶, 鼎, 蘋果, 熱潮, 電視台,, 北歐, 和基督教 V-219210 V-219164 V-219165 V-219178 V-219180 V-219301 V-219163 V-219332 V-219327 V-219333

## Ubuntu 的 20.04 STIG 版本 1 版本第十二版

V-238202, V-238234, V-238235, V-238237,, 搶, 鼎, 蘋果, 熱潮, 電視台,, 北歐, 和基督教 V-238323 V-238373 V-238221 V-238222 V-238223 V-238224 V-238226 V-238362 V-238357 V-238308

## Ubuntu STIG 版本 1 版本 1 版本 1

V-260472, V-260476, V-260479, V-260480,, 搶, 鼎, 蘋果, 熱潮, 電梯,, 北歐, 和嚴 V-260481 V-260520 V-260521 V-260549 V-260550 V-260551 V-260552 V-260581 V-260596

## Linux STIG 中型 (類別二)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

### Note

除了 Amazon 針對第 II 類弱點EC2支援的STIG強化設定外，Linux STIG 中類別還包含適用於 Linux STIG 低 (類別III) 的所有列出STIG強化設定。

## RHEL7 第三STIG版發行版本 14

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

- RHEL7/CentOS 7/AL2

V-204585, V-204490, V-204491, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V 型 204412, V, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204588, V-204589, V 型, V 型 204590, V, V 型 204600, V-204602, V-204602, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V 型, V 型 204508, V 型 204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V 型, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V., V-204610, V-204611, V-204612, V-204613, V-204614, V-204616, V-204617, V-204617, V., V-204631、V-204633 和 V-256970

## RHEL8 STIG 版本 1 版本發行版本 14

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

- RHEL8/CentOS

伏特 -230257, V-230258, V-230259, 伏特 -230248, 伏特 -230249, 伏特 -230250, V-230245, V-230228, V-230397, V 30233, V-230324, V-230324, 電影 -230378, V-230383, V-230314, V-230314, V-二四五, V-230267, V 30532, V-230535, V-230536, V-230537, V-230539, V-230535, V-230542, V-230542, V-230543, V 型, V 型, V-250317, V-251718, V-230237, V-230356, V-230357, V-230359, V-230359, V-230361, V-230361, V V-244533, V-251713, V-251717, V-251714,



V-251716, 伏特 -230332, 伏特 -230334, V-230335, V -230335, V, V-230343, V-230345, V-230240, V-230282, V 型 398, 伏特 -230402, VV-230405, V-230406, V-230407, V-230408, V-230409, V-230411, V-230412, V-230413, V-230418, V 26, V 型, 230427, V-230429, V-230429, V-230431, V-230432, V-230433, V-230434, V-230435, V, V-230448, V-230449, V-230455, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V V-244542, V 型, V 型V-230296, V-230330, V-230382, V-230526,, 嚮, 綿羊, 蘋果, 早餐,, 蒸汽, 北, 392, 伏地,, 伏特,,, 風格, V-230489, V-230559, V 型 230561, V 型 237640, 和 V 型 256974 V-230527 V-230555 V-230556 V-244526 V-244528 V-237642 V-237643 V-251711 V-230238 V-230239 V-230273 V-230275 V-230478 V-230488

## RHEL9 STIG 版本 1 發行版本 3

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

- RHEL9/CentOS 第 9 流

V -257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257798, V -257799, V -257800, V 7805, V 型, 257806, V-257808, V-257809, 伏特 -257810, 伏特 -257811, V. 7830, 257831, V, 257832, V-257833, V-257834, 伏特 -257836, 伏特 -257838, 伏特 -257839, V.V-257892, V-257893, V-257894, V-257895, V-257896, 伏特 -257897, 伏特 -257898, V-257899, V-257900, V-257902, V-257904, V V-257911, V-257912, V-257913, V-257914, V-257916, V-257916, V-257917, V-257919, V-257920, V-257921, V-257930, V-257931, V-257933, V-257934, V-257935, V-257936, V-257939, V-257942, V-257943, V-257944, V-257949, V -257951, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257970, V-257971, V-257972, V-257973, V-257979, V-257980, V-257982, V-257993, V-257987, V-257988, V-257991, V-257992, V-257993, V-257994, V-257995, V -257996, V, V-258002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258009, V-25809, V-258011, V-258034, V, VV-258054, V-258055, V-258056, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V. V-258104, V-258105, V-258107, V-258109, V-258110, V-258111, V-258112, V-258113, V-258115, V-258116, V, V-258125, V-258126, V-258128, V-258129, V-258133, V-258134, V-258137, V-258140, V-258142, V-258144, V 型 258145, V V -258153, V-258154, V-258156, V-258158, V-258159, 伏特 -258160, V-258161, V-258162, V-258163, V-258165, V V -258175 , 258176 , 258177 , 258178 , V-258179 , V-258180 , V-258181 , V-258182 , V 型 , 258184 , V-258185 , V 型 258186 , V, V-258194, V-258195, V-258196, V-258197,,, 湧, 球, 蘋果, 鼎, 節日, 妻子, 妻子, 雞, 向量, 雞, 伏特, 伏特, 冰河, V 型, 258216, V 型, 258216, V 型

258217, V 型 258218, V 型 258218, V 型 258219, V 型電視 -258225, 電視 -258226, 電視 -258227, 電視 -258228, 電視 -258229, 電視 -258232, 電視 -258234, 電視 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

## STIG版本二發行版本 14

V -219188, V -219190, V -219198, V -219199, 伏特 -219200, V -219201, V -219202, 二 19203, 二 19204, V -219205, V -219206, V -219207, V -219342, V -219189, V -219192, V -219194, 伏特 -219315, 伏特 -219195, 伏特 -219196, V -219197, V., V -219223, V-二一九二二七, V -219228, 伏特 -219229, 伏特 -219230, 伏特 -219231, 二一三三三, 二一三三四, 第二九三三四, V 19244,V-219250, V-219254, V-219257, V-219263,, 湧, 球, 蘋果, 壺, 節制, 節制, 包括, 包括, 領導, 雞翼, 象徵, V-219279, V-219281, V 型, 219287, V 型 219297, V 型, 電視 -233780, 電子 -255906, 電子 -219338, 電子 -219344, 電視 -219184, V 型, 電子 -219156, 電子 -219156, 電子 -219160, 電子 -219306, 電視 19335 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

## Ubuntu 的 20.04 STIG 版本 1 版本第十二版

V-238205, V-238207, V-238329, V-238339, V-238340, V-238344, V-238345, V-238347, V-238347, V-238349, V-238349, V-238350, V V-23825, V-238330, V-238333, V-238369, V-238341, V-238342, V-238343, V-238343, V-238353, V-238228, V-238225, V V-238244, V-238245, V-238246, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V 238255, V 277,V-238278, V-238279, V-238280, V-238281,, 保證, 湧, 球, 杯, 早在, 妻子, 妻子, 妻子, 毫秒, 伏特, 玻璃, 伏特蘭, V 型 238301, V 型 238304, V 型 238309, V 型 238309, V 型 238310, V 型 238315, V 型 238316, V 型 238316, V 型 238319, V 型 238319, V 型 238316, V 型電視 -251505, 電視 -238360, 電視機, 電視 238213, 電視機, 電視 238220, 電視機, 電視 238355, 電視機, 電視 238303, 電視, 電視 238358, 電視 238356, 電視 238359, 電視 238370, 和電視 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

## Ubuntu 版STIG本 1 版本 1 版本

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

伏特 -260473, V-260474, V-260475, 伏特 -260477, 伏特 -260478, 伏特 -260485, V-260491, 伏特 -260491, V 260495, V-260496, V-260498, V-260499, V-260500, 伏特 -260505, V-260506, V-260507, V-260508, V-260509, V 260522, V-260527, V-260528, V-260531, V-260533, V-260533, V-260534, V-260542, V-260543, V 型V-260566, V-260567, V-260568, V-260572, V-260573, V-260576,

V-260582, V-260584, V-260594, V V-260598, V-260599, V-260601, V-260606, V-260606, V-260605, V-260605, V-26066, V-260607, V-260608, V 60614, V 型 260615, V 型 260616, V 型 260618, V 型 260619, 伏特 260619, V 型 260616, V 型 260622, V 型 260623, V 型 630, V-260631, V-260632, V-260633, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642,, 搶, 鼎, 蘋果, 熱量, 電梯, 和 CHIP V-260643 V-260644 V-260645 V-260646 V-260647 V-260648 V-260649

## STIG高分析系統 (類別一)

下列清單包含 Amazon EC2 支援您的基礎STIG設施的設定。如果支援的設定不適用於您的基礎設施，Amazon 會EC2略過該設定，然後繼續進行。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[STIGs文件庫](#)。如需如何檢視完整清單的相關資訊，請參閱[STIG檢視工具](#)。

### Note

除了 Amazon 針對類別 I 弱點EC2支援的STIG強化設定外，Linux STIG 高類別還包含適用於 Linux STIG 中和低類別的所有列出STIG強化設定。

## RHEL7 第三STIG版發行版本 14

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

- RHEL7/CentOS 7/AL2

V-204425, V-204594, V-204455, V-204424,, 搶, 鼎, 蘋果, 熱量, 電梯, 和 CHIP V-204442 V-204443 V-204447 V-204448 V-204502 V-204620 V-204621

## RHEL8 STIG 版本 1 版本發行版本 14

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

- RHEL8/CentOS

V-230265, V-230529, V-230531, V-230264, V-230487, 願意, 鼎, 和遷 V-230492 V-230533 V-230558

## RHEL9 STIG 版本 1 發行版本 3

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

- RHEL9/CentOS 第 9 流

V-257784, V-257785, V-257820, V-257821,, 搶, 鼎, 蘋果, 熱潮, 電視台,, 北歐, 和基督教 V-257826  
V-257835 V-257955 V-257956 V-257984 V-257986 V-258059 V-258078 V-258094 V-258235

STIG版本二發行版本 14

V-219157, V-219158, V-219177, V-219212 V-219308, 愿意, 鼎, 和遷 V-219314 V-219316 V-251507

Ubuntu 的 20.04 STIG 版本 1 版本第十二版

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

Ubuntu 版STIG本 1 版本 1 版本

包括 Amazon 針STIG對第 II 類和 III (中和低) 弱點EC2支援的所有強化設定，以及：

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

## STIG版本歷史記錄

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

二零二四年第二季度變更-二零二四年五月十日：

更新STIG版本並STIGS適用於 2024 年第二季度版本。同時增加了對 RHEL 9、CentOS 流 9 和 Ubuntu 22.04 的支援，如下所示：

STIG-構建-亞歷克斯-低版本 2024.2.x

- RHEL7 第三STIG版發行版本 14
- RHEL8 STIG 版本 1 發行版本 14
- RHEL9 STIG 版本 1 發行版本 3
- STIG版本二發行版本 14
- Ubuntu 的 20.04 STIG 版本 1 版本第十二版

- Ubuntu STIG 版本 1 版本 1 版本 1

#### STIG-構建-亞路線-中型版本 2024.2.x

- RHEL7 第三STIG版發行版本 14
- RHEL8 STIG 版本 1 發行版本 14
- RHEL9 STIG 版本 1 發行版本 3
- STIG版本二發行版本 14
- Ubuntu 的 20.04 STIG 版本 1 版本第十二版
- Ubuntu STIG 版本 1 版本 1 版本 1

#### STIG-構建-亞路線高版本 2024.2.x

- RHEL7 第三STIG版發行版本 14
- RHEL8 STIG 版本 1 發行版本 14
- RHEL9 STIG 版本 1 發行版本 3
- STIG版本二發行版本 14
- Ubuntu 的 20.04 STIG 版本 1 版本第十二版
- Ubuntu STIG 版本 1 版本 1 版本 1

2024 年第一季度變更-二零二四年六月二日：

更新STIG版本並STIGS適用於 2024 年第一季度版本，如下所示：

#### STIG-構建-亞歷克斯-低版本 2024.1.x

- RHEL7 第三STIG版發行版本 14
- RHEL8 STIG 版本一發行版本 13
- STIG版本二版本第十三版
- Ubuntu 的 20.04 STIG 版本 1 版本發布 11

#### STIG-構建-亞路線-中型版本 2024.1.x

- RHEL7 第三STIG版發行版本 14

- RHEL8 STIG 版本一發行版本 13
- STIG版本二版本第十三版
- Ubuntu 的 20.04 STIG 版本 1 版本發布 11

#### STIG-構建-亞路線高版本 2024.1.x

- RHEL7 第三STIG版發行版本 14
- RHEL8 STIG 版本一發行版本 13
- STIG版本二版本第十三版
- Ubuntu 的 20.04 STIG 版本 1 版本發布 11

二零二三年第四季變更-二零二三年七月十二日：

更新STIG版本並STIGS適用於 2023 年第四季度版本，如下所示：

#### STIG-構建-亞歷克斯-低版本 2023.4.x

- RHEL7 第三STIG版發行版本 13
- RHEL8 STIG 版本 1 版本第 12 版
- STIG版本二版本第十二版
- Ubuntu 的 20.04 STIG 版本 1 發布版本 10

#### STIG-構建-亞列克斯中等版本 2023.4.x

- RHEL7 第三STIG版發行版本 13
- RHEL8 STIG 版本 1 版本第 12 版
- STIG版本二版本第十二版
- Ubuntu 的 20.04 STIG 版本 1 發布版本 10

#### STIG-構建-亞路線-高版本 2023.4.x

- RHEL7 第三STIG版發行版本 13
- RHEL8 STIG 版本 1 版本第 12 版
- STIG版本二版本第十二版
- Ubuntu 的 20.04 STIG 版本 1 發布版本 10

二零二三年第三季變更-二零二三年四月十日：

更新STIG版本並STIGS適用於 2023 年第三季發行版本，如下所示：

#### STIG低 (類別III)

- RHEL7 第三STIG版發行版本 12
- RHEL8 STIG 版本 1 版本發行版本 11
- STIG版本二發布版本十一
- Ubuntu 的 20.04 STIG 版本 1 發布版本 9

#### Linux STIG 中型 (類別二)

- RHEL7 第三STIG版發行版本 12
- RHEL8 STIG 版本 1 版本發行版本 11
- STIG版本二發布版本十一
- Ubuntu 的 20.04 STIG 版本 1 發布版本 9

#### STIG高分析系統 (類別一)

- RHEL7 第三STIG版發行版本 12
- RHEL8 STIG 版本 1 版本發行版本 11
- STIG版本二發布版本十一
- Ubuntu 的 20.04 STIG 版本 1 發布版本 9

二零二三年第二季度變動-二零二三年五月三日：

更新STIG版本並STIGS適用於 2023 年第二季度版本，如下所示：

#### STIG低 (類別III)

- RHEL7 STIG 版本 3 版本發行版本 11
- RHEL8 STIG 版本 1 發行版本 10
- STIG版本二發布版本十一
- Ubuntu 20.04 STIG 版本 1 版本 8

## Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 版本發行版本 11
- RHEL8 STIG 版本 1 發行版本 10
- STIG版本二發布版本十一
- Ubuntu 20.04 STIG 版本 1 版本 8

## STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 版本發行版本 11
- RHEL8 STIG 版本 1 發行版本 10
- STIG版本二發布版本十一
- Ubuntu 20.04 STIG 版本 1 版本 8

2023 年第一季度變更-二零二三年三月二十日：

更新STIG版本並STIGS適用於 2023 年第一季度版本，如下所示：

## STIG低 (類別III)

- RHEL7 第三STIG版發行版本 10
- RHEL8 STIG 版本 1 發行版本 9
- STIG版本二發行版本 10
- Ubuntu 20.04 STIG 版本 1 版本 7

## Linux STIG 中型 (類別二)

- RHEL7 第三STIG版發行版本 10
- RHEL8 STIG 版本 1 發行版本 9
- STIG版本二發行版本 10
- Ubuntu 20.04 STIG 版本 1 版本 7

## STIG高分析系統 (類別一)

- RHEL7 第三STIG版發行版本 10



- RHEL8 STIG 版本 1 發行版本 9
- STIG版本二發行版本 10
- Ubuntu 20.04 STIG 版本 1 版本 7

二零二二年第四季變更-二零二三年一月二日：

更新STIG版本並STIGS適用於 2022 年第四季發行版本，如下所示：

#### STIG低 (類別III)

- RHEL7 STIG 版本 3 發行版本 9
- RHEL8 STIG 版本 1 發行版本 8
- Ubuntu 的 18.04 STIG 版本 2 發布版本 9
- Ubuntu 20.04 STIG 版本 1 版本 6

#### Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 發行版本 9
- RHEL8 STIG 版本 1 發行版本 8
- Ubuntu 的 18.04 STIG 版本 2 發布版本 9
- Ubuntu 20.04 STIG 版本 1 版本 6

#### STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 發行版本 9
- RHEL8 STIG 版本 1 發行版本 8
- Ubuntu 的 18.04 STIG 版本 2 發布版本 9
- Ubuntu 20.04 STIG 版本 1 版本 6

2022 年第三季度變動-二零二二年九月三十日 (不變)：

對於 2022 年第三季度版本，Linux 元件STIGS沒有任何變更。

二零二二年第二季度變動：

推出了 Ubuntu 支持，更新STIG版本並STIGS適用於 2022 年第二季度發布，如下所示：

## STIG低 (類別III)

- RHEL7 STIG 版本 3 發行版本 7
- RHEL8 STIG 版本 1 發行版本 6
- Ubuntu 18.04 STIG 版本 2 版本 6 ( 新 )
- Ubuntu 20.04 STIG 版本 1 版本 4 ( 新 )

## Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 發行版本 7
- RHEL8 STIG 版本 1 發行版本 6
- Ubuntu 18.04 STIG 版本 2 版本 6 ( 新 )
- Ubuntu 20.04 STIG 版本 1 版本 4 ( 新 )

## STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 發行版本 7
- RHEL8 STIG 版本 1 發行版本 6
- Ubuntu 18.04 STIG 版本 2 版本 6 ( 新 )
- Ubuntu 20.04 STIG 版本 1 版本 4 ( 新 )

## 二零二二年第一季度變動：

重構以包括對容器的更好支持。將以前的AL2腳本與 RHEL 7 組合。更新STIG版本並STIGS適用於 2022 年第一季度版本，如下所示：

## STIG低 (類別III)

- RHEL7 STIG 版本 3 版本發行版本 6
- RHEL8 STIG 版本 1 發行版本 5

## Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 版本發行版本 6
- RHEL8 STIG 版本 1 發行版本 5

## STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 版本發行版本 6
- RHEL8 STIG 版本 1 發行版本 5

二零二一年第四季度變更：

更新STIG版本，並STIGS適用於 2021 年第四季度版本，如下所示：

## STIG低 (類別III)

- RHEL7 STIG 版本 3 發行版本 5
- RHEL8 STIG 版本 1 發行版本 4

## Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 發行版本 5
- RHEL8 STIG 版本 1 發行版本 4

## STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 發行版本 5
- RHEL8 STIG 版本 1 發行版本 4

二零二一年第三季變更-九月三十日：

更新STIG版本，並STIGS適用於 2021 年第三季度版本，如下所示：

## STIG低 (類別III)

- RHEL7 STIG 版本 3 發行版本 4
- RHEL8 STIG 版本 1 發行版本 3

## Linux STIG 中型 (類別二)

- RHEL7 STIG 版本 3 發行版本 4
- RHEL8 STIG 版本 1 發行版本 3

## STIG高分析系統 (類別一)

- RHEL7 STIG 版本 3 發行版本 4
- RHEL8 STIG 版本 1 發行版本 3

## AWSEC2-PatchLoadBalancerInstance

### Description (描述)

升級和修補連接到任何負載平衡器 (傳統型、ALB 或 NLB) 的亞馬遜 EC2 執行個體 (Windows 或 Linux) 的次要版本。預設連線排除時間會在執行個體進行修補之前套用。您可以透過輸入ConnectionDrainTime參數的自訂排水時間 (分鐘) (1-59) 來覆寫等待時間。

自動化工作流程如下：

1. 系統會判斷執行個體所連接的負載平衡器或目標群組，且執行個體會驗證為健康狀態良好。
2. 執行個體會從負載平衡器或目標群組中移除。
3. 自動化會等待連線排除時間所指定的時間段。
4. 呼叫 [AWS 自RunPatchBaseline](#)動化以修補執行個體。
5. 執行個體會重新連接至負載平衡器或目標群組。

### [運行此自動化 \(控制台\)](#)

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[適用於 Windows 伺服器的 EC2 執行個體上使用 SSM 代理程式](#)。

參數

- InstanceId

類型：字串

說明：(必要) 修正與負載平衡器 (傳統、ALB 或 NLB) 相關聯的執行個體識別碼。

- ConnectionDrainTime

類型：字串

說明：(選擇性) 負載平衡器的連線排空時間，以分鐘為單位 (1-59)。

## AWSEC2-SQLServerDBRestore

### Description (描述)

AWSEC2-SQLServerDBRestore執行手冊將存放在亞馬遜 S3 中的微軟 SQL 伺服器資料庫備份還原到亞馬遜彈性運算雲端 (EC2) Linux 執行個體上執行的 SQL 伺服器 2017 年。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新的 Ubuntu 16.04 EC2 執行個體與 SQL 伺服器 2017 年。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到執行 SQL Server 2017 Linux 的 EC2 執行個體，您可以使用AWS已簽署的PowerShell指令碼[MigrateSQLServerToEC2Linux](#)。

#### Important

此執行手冊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。自動化完成之後，您必須再次設定自己的 SA 使用者密碼，才能連線到 SQL Server 執行個體。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

## Linux

### 先決條件

若要執行此自動化操作，您必須符合下列先決條件：

- 執行此自動化操作的 IAM 使用者或角色必須附加內嵌政策，其中列出了許可[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微軟 SQL 伺服器 2017 年的 Linux 執行個體。
  - 您提供的 EC2 執行個體必須使用附加 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 代理程式必須安裝在 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 代理程式](#)。
  - 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

此自動化操作具有下列參數：

- 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

說明：(可選) 要附加到新 EC2 執行個體的 IAM 執行個體設定檔。IAM 執行個體設定檔必須附加 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。如果沒 InstanceId 有提供，則自動化會使用 ServerEdition 提供的 InstanceType 和 SQL 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。

- Is3PresignedUrl

類型：字串

說明：(選擇性) 如果 S3Input 是預先簽署的 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

- 輸入

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。

- SQL ServerEdition

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 | 網頁 | 快速

- SubnetId

類型：字串

描述：(選用) 要啟動新 EC2 執行個體的子網路。子網路必須擁有到 AWS 服務的對外連線。如果未提供的值，SubnetId則自動化會使用預設子網路。

- 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

此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

若要使用此自動化操作，請依照適用於您執行個體類型的步驟執行：

對於新的 EC2 執行個體：

1. `aws:executeAwsApi`-擷取 SQL 伺服器 2017 年的 AMI 識別碼。
2. `aws:runInstances`-啟動適用於 Linux 的新 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 代理程式。
6. `aws:runCommand`-在中執行 SQL 伺服器還原指令碼 PowerShell。

對於現有的 EC2 執行個體：

1. `aws:waitForAwsResourceProperty`-確認 EC2 執行個體已準備就緒。
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 代理程式。
4. `aws:runCommand`-在中執行 SQL 伺服器還原指令碼 PowerShell。

## 輸出

獲取實例。 InstanceId

restoreToNew執行個體輸出

restoreToExisting執行個體輸出

## AWSSupport-ActivateWindowsWithAmazonLicense

Description (描述)

該手AWSSupport-ActivateWindowsWithAmazonLicense冊Windows Server使用亞馬遜提供的許可證激活亞馬遜彈性計算雲 ( 亞馬遜 EC2 ) 實例。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。這包括前往 Amazon 金鑰管理伺服器的作業系統路由和金鑰管理服務作業系統設定。將 AllowOffline 參數設定為 true 允許自動化成功鎖定不受 AWS Systems Manager管理但需要停止並啟動執行個體的執行個體。

### Note

此 Runbook 無法用於攜帶您自己的授權 (BYOL) 模型執行個體。Windows Server如需使用自有授權的詳細資訊，請參閱[在 AWS 的 Microsoft 授權](#)。

### [運行此自動化 \( 控制台 \)](#)

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：(選擇性) true 如果在線上疑難排解失敗或提供的執行個體不是代管執行個體時允許離線 Windows 啟用補救，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

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- ForceActivation

類型：字串

有效值：true | false

預設：false

描述：(選擇性) true 如果您要繼續，即使 Windows 已經啟動，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

預設值：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SelectedInstanceSubnet用與執行個體使用相同的子網路，或用CreateNewVPC來建立新的 VPC。重要：子網路必須與位於相同的可用區域InstanceId，且必須允許存取 SSM 端點。

## 必要的 IAM 許可

此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 IAM 角色，並附加了ManagedInstanceCore亞馬遜亞馬遜受管政策。您必須至少有 ssm: StartAutomationExecution 和 ssm: SendCommand 才能執行自動化並將命令傳送 SendCommand 至執行個體，再加上 ssm: GetAutomationExecution 才能讀取自動化輸出。如需離線修復，請參閱所需的權限AWSSupport-StartEC2RescueWorkflow。

## 文件步驟

1. aws:assertAwsResourceProperty-檢查提供的執行個體的平台是否為 Windows。
2. aws:assertAwsResourceProperty-確認提供的執行個體是代管執行個體：
  - a. (線上啟動修正) 如果輸入執行個體是代管執行個體，請執行aws:runCommand以執行PowerShell指令碼以嘗試修正 Windows 啟動。
  - 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-驗證AllowOffline旗標是否設定為true。如果是這樣，離線修復程序開始; 否則自動化結束。
    - ii. aws:executeAutomation-AWSSupport-StartEC2RescueWorkflow 使用 Windows 啟用離線修正程式指令碼呼叫。此指令碼會根據作業系統版本使用 EC2Config 或 EC2Launch。
    - iii. aws:executeAwsApi-從中讀取結果AWSSupport-StartEC2RescueWorkflow。

## 輸出

activateWindows.Output

getActivateWindowsOfflineResult輸出。

## AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

### Description

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2執行手冊會分析來自 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 elastic network interface 到 AWS 服務端點的連線。不支援 IPv6。runbook 會使用您為ServiceEndpoint參數指定的值來分析與端點的連接。如果在 VPC 中找不到 AWS PrivateLink 端點，則執行手冊會使用目前服務的公用 IP 位址。AWS 區域此自動化操作使用 Amazon Virtual Private Cloud 的 Reachability Analyzer。如需詳細資訊，請參閱[什麼是 Reachability Analyzer](#)？，在 Reachability Analyzer 中。

此自動化會檢查下列項目：

- 檢查您的虛擬私有雲 (VPC) 是否設定為使用 Amazon 提供的 DNS 伺服器。
- 檢查 VPC 中是否存在您指定 AWS 服務的 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策略。

## 考量

- 您需要針對來源與目標之間執行的分析收費。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。
- 在自動化過程中，會建立網路洞察路徑和網路洞察分析。如果自動化順利完成，runbook 會刪除這些資源。如果清理步驟失敗，網路見解路徑不會被 runbook 刪除，您將需要手動刪除它。如果您沒有手動刪除網路見解路徑，它會繼續計入您的 AWS 帳戶。如需可 Reachability Analyzer 配額的詳細資訊，請參閱可 Reachability Analyzer 中的 [可 Reachability Analyzer 配額](#)。
- 作業系統層級組態 (例如使用 Proxy、本機 DNS 解析程式或主機檔案) 可能會影響連線，即使連線 Reachability Analyzer 傳回也是如此。PASS
- 複查「Reachability Analyzer」所執行之所有檢查的評估。如果有任何檢查傳回的狀態為FAIL，即使整體可達性檢查傳回的狀態也可能會影響連線。PASS

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 來源

類型：字串

說明：(必要) Amazon EC2 執行個體的 ID 或您要從中分析可達性的網路界面。

- ServiceEndpoint

類型：字串

描述：(必要) 您要分析連線能力之服務端點的主機名稱。

- RetainVpcReachabilityAnalysis

類型：字串

預設：false

描述：(選擇性) 決定是否保留網路分析路徑和建立的相關分析。依預設，用於分析可達性的資源會在成功分析後刪除。如果您選擇保留分析，則執行手冊不會刪除分析，您可以在 Amazon VPC 主控台中將其視覺化。自動化輸出中提供主控台連結。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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` : 收集有關 VPC 和子網路的詳細資料。
3. `aws:executeScript` : 評估 VPC 的 DNS 組態。
4. `aws:executeScript` : 評估 VPC 端點檢查。
5. `aws:executeScript` : 找出網際網路閘道以連線到公用服務端點。
6. `aws:executeScript` : 決定用於可達性分析的目標。
7. `aws:executeScript` : 使用可達性分析器分析從來源到端點的可達性，並在分析成功時清除資源。
8. `aws:executeScript` : 產生可達性評估報告。
9. `aws:executeScript` : 以 JSON 格式產生輸出。

## 輸出

- `generateReport.EvalReport`-自動化以文本格式執行的檢查結果。
- `generateJsonOutput.Output`-JSON 格式的結果的最小版本。

## **AWSPremiumSupport-ChangeInstanceTypeIntelToAMD**

### Description (描述)



執行手冊 `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` 可自動從英特爾驅動的亞馬遜彈性運算雲端 (Amazon EC2) 執行個體遷移到同等 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)、高載通用 (T)、運算最佳化 (C) 和記憶體最佳化 (R) 執行個體。此 runbook 可以在不受系統管理員管理的執行個體上使用。

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，以及相同的 AMD 支援執行個體類型是否可在相同的可用區域中使用。根據預設，如果執行個體儲存磁碟區已連接，或執行個體是 AWS CloudFormation 堆疊的一部分，則此 runbook 不會變更執行個體類型。如果您想要變更此行為，請將 `yes` 指定為 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 參數中的任一指定。

#### 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 AWS Support 方案](#)。

## 考量

- 我們建議您在使用此 runbook 之前備份您的執行個體。
- 變更執行個體類型需要 runbook 停止執行個體。當執行個體停止時，儲存在 RAM 或執行個體儲存磁碟區中的任何資料都會遺失，並釋放自動公用 IPv4 位址。如需詳細資訊，請參閱 [停止和啟動執行個體](#)。
- 如果您沒有為 `TargetInstanceType` 參數指定值，runbook 會嘗試以相同執行個體系列中的虛擬 CPU 和記憶體來識別相等的 AMD 執行個體。如果無法識別相等的 AMD 執行個體類型，執行手冊就會結束。
- 透過使用 `DryRun` 此選項，您可以擷取相等的 AMD 執行個體類型，並驗證需求，而無需實際變更執行個體類型。

## [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

### 擁有者

## Amazon

### 平台

Linux 系統 macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 確認

類型：字串

說明：(必要) 輸入yes以確認目標執行個體在執行時將會停止。

- InstanceId

類型：字串

說明：(必填) 您要變更其類型之 Amazon EC2 執行個體的 ID。

- TargetInstanceType

類型：字串

預設值：自動

說明：(選用) 您要將執行個體變更為的 AMD 執行個體類型。預設automatic值使用對等的執行個體類型，就虛擬 CPU 和記憶體而言。例如，m5.large 會變更為 m5a.large。

- AllowInstanceStoreInstances

類型：字串

有效值：否 | 是

預設：否

說明：(選擇性) 如果您指定yes，runbook 會在已連接執行個體儲存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：(選擇性) 如果設定為yes，會在屬於AWS CloudFormation堆疊一部分的執行個體上執行runbook。

- AllowCrossGeneration

類型：字串

有效值：否 | 是

預設：否

說明：(選用) 如果設為yes，runbook 會嘗試在相同的執行個體系列中尋找最新的相等 AMD 執行個體類型。

- DryRun

類型：字串

有效值：否 | 是

預設：否

說明：(選用) 如果設定為yes，runbook 會傳回相等的 AMD 執行個體類型並驗證遷移需求，而不需變更執行個體類型。

- SleepWait

類型：字串

預設值：

描述：(選擇性) runbook 在開始新的自動化操作之前應該等待的時間。您為此參數提供的值必須與ISO 8601 標準相符。如需有關建立 ISO 8601 字串的詳細資訊，請參閱 < [格式化系統管理員的日期和時間字串](#) >。

必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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 執行個體的狀態分支自動化。
  - a. 如果是 `stopped` 或 `stopping`，則自動化會執行，`aws:waitForAwsResourceProperty` 直到 Amazon EC2 執行個體完全停止為止。
  - b. 如果是 `running` 或 `pending`，則自動化會執行，`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 執行個體不屬於自動擴展群組。
5. `aws:executeAwsApi`：收集目前的執行個體類型屬性，以尋找相等的 AMD 執行個體類型。
6. `aws:assertAwsResourceProperty`：確認 AWS Marketplace 產品代碼與 Amazon EC2 執行個體沒有關聯。部分產品並不適用於所有執行個體類型。
7. `aws:branch`：根據您是否希望自動化檢查 Amazon EC2 執行個體是否屬於 AWS CloudFormation 堆疊來分支自動化

- a. 如果將標aws:cloudformation:stack-name籤套用至執行個體，則會執行自動化作業aws:assertAwsResourceProperty以確認執行個體不屬於AWS CloudFormation堆疊。
8. aws:branch：根據執行個體根磁碟區類型是否為 Amazon 彈性區塊存放區 (Amazon EBS) 來分支自動化。
9. aws:assertAwsResourceProperty：確認執行個體關閉行為是stop與否terminate。
- 10aws:executeScript：確認此 runbook 只有一個針對當前實例的自動化操作。如果另一個自動化操作已在針對同一個執行個體進行中，則會傳回錯誤並結束。
- 11aws:executeAwsApi：傳回具有相同記憶體和 vCPU 數量的 AMD 執行個體類型清單。
- 12aws:executeScript：檢查目前的執行個體類型是否受支援，並傳回相等的 AMD 執行個體類型。如果沒有相等的，則自動化結束。
- 13aws:executeScript：確認 AMD 執行個體類型在相同的可用區域中可用，並驗證提供的 IAM 許可。
- 14aws:branch：根據DryRun參數值是否為分支自動化yes。
- 15aws:branch：檢查原始執行個體和目標例證類型是否相同。如果它們是相同的，自動化結束。
- 16aws:executeAwsApi：取得目前執行個體狀態。
- 17aws:changeInstanceState：停止亞馬遜 EC2 實例。
- 18aws:changeInstanceState：如果執行個體停留在停止狀態，則強制停止執行個體。
- 19aws:executeAwsApi：將執行個體類型變更為目標 AMD 執行個體類型。
- 20aws:sleep: 為了達到最終一致性，變更執行個體類型後等待 3 秒。
- 21aws:branch：根據先前的執行個體狀態分支自動化。如果是running，則會啟動執行個體。
  - a. aws:changeInstanceState：如果 Amazon EC2 執行個體在變更執行個體類型之前已執行，請啟動該執行個體。
  - 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，執行個體就會變回其原始執行個體類型。
    - i. aws:changeInstanceState：先停止 Amazon EC2 執行個體，再將其變更為原始執行個體類型。
    - ii. aws:changeInstanceState：強制 Amazon EC2 執行個體停止，然後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：將亞馬遜 EC2 實例更改為其原始類型。
    - iv. aws:sleep: 變更執行個體類型後等待 3 秒，以達到最終一致性。
    - v. aws:changeInstanceState：如果 Amazon EC2 執行個體在變更執行個體類型之前已執行，請啟動該執行個體。

vi. `aws:waitForAwsResourceProperty` : 等待 Amazon EC2 執行個體通過狀態檢查。  
22.`aws:sleep` : 在結束手冊之前等待。

## AWSsupport-CheckXenToNitroMigrationRequirements

### Description (描述)

AWSsupport-CheckXenToNitroMigrationRequirements 執行手冊會驗證 Amazon 彈性運算雲端 (Amazon EC2) 執行個體是否符合預先要求，以便成功將執行個體類型從 Xen 類型執行個體變更為 Nitro-based 執行個體類型。此自動化會檢查下列項目：

- 根裝置是亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區。
- `enaSupport` 屬性已啟用。
- ENA 模組已安裝在執行個體上。
- NVMe 模組已安裝在執行個體上。如果是，則會安裝模組，並且指令碼會驗證該模組是否已載入 `initramfs` 影像中。
- 分析 `/etc/fstab` 並尋找使用裝置名稱掛載的區塊裝置。
- 決定作業系統 (OS) 預設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
- SUSE Linux Enterprise Server

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

## 擁有者

Amazon

平台

Linux

## 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

預設：false

說明：(必填) 您要在遷移到以硝基為基礎的執行個體類型之前檢查先決條件的 Amazon EC2 執行個體 ID。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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:DescribeInstanceTypes`

## 文件步驟

- `aws:executeAwsApi`-收集有關執行個體的詳細資料。
- `aws:executeAwsApi`-收集執行個體虛擬機器管理程序的相關資訊。
- `aws:branch`-根據目標執行個體是否已執行以硝基為基礎的執行個體類型進行分支。
- `aws:branch`-檢查 Nitro-based 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系統管理員管理，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`-根據是否針對執行個體啟用 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檔案中是否有無法辨識的格式。
- `aws:runCommand`-檢查執行個體上是否有可預測的介面名稱組態。
- `aws:executeScript`-根據先前的步驟生成輸出。

## 輸出

最終輸出。輸出-由自動化執行的檢查的結果。

## AWSSupport-ConfigureEC2Metadata

### Description

此執行手冊可協助您設定 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的執行個體中繼資料服務 (IMDS) 選項。使用此 runbook，您可以配置以下內容：



- 針對執行個體中繼資料強制使用 IMDSv2。
- 設定HttpPutResponseHopLimit值。
- 允許或拒絕執行個體元資料存取。

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](#)。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 強制執行 V2

類型：字串

有效值：必要 | 選用

預設值：選擇性

說明：(選擇性) 強制執行 ImDSv2。如果您選擇required，亞馬遜 EC2 執行個體將僅使用 IMDSv2。如果您選擇optional，您可以選擇 IMDSv1 和 IMDSv2 進行中繼資料存取。

**⚠ 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](#)。

- `HttpPutResponseHop` 極限

類型：整數

有效值：0-64

預設：0

說明：(選用) 執行個體中繼資料要求所需的 HTTP PUT 回應躍點限制值 (1-64)。此值控制 PUT 回應可以遍歷的躍點數目。若要防止回應傳送至執行個體之外，請 1 為參數值指定。

- `InstanceId`

類型：字串

說明：(必填) 您要設定其中繼資料設定之 Amazon EC2 執行個體的 ID。

- `MetadataAccess`

類型：字串

有效值：已啟用 | 已停用

預設：啟用

說明：(選用) 允許或拒絕 Amazon EC2 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，而且會拒絕執行個體的中繼資料存取。

### 必要的 IAM 許可

此 `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. 分支 `OnMetadataAccess` -基於`MetadataAccess`參數值的分支自動化。
2. `disableMetadataAccess` -呼叫 `ModifyInstanceMetadataOptions` API 動作以停用中繼資料端點存取。
3. 分支 `OnHttpPutResponseHopLimit` -基於`HttpPutResponseHopLimit`參數值的分支自動化。
4. 維護 `HopLimitAndConfigureImdsVersion` -如果`HttpPutResponseHopLimit`為 0，則維持目前的躍點限制並變更其他中繼資料選項。
5. 等待 `BeforeAsserting Imdsv2` 狀態-在宣告 `ImDSv2` 狀態之前等待 30 秒。
6. `set HopLimitAndConfigureImdsVersion` -如果大`HttpPutResponseHopLimit`於 0，則使用給定的輸入參數配置元數據選項。
7. `wait BeforeAssertingHopLimit` -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. 分支 `VerificationOn IMDSV2Option`-根據參數的值進行分支驗證。 `EnforceIMDSv2`
- 10.判斷提示 `V2 IsOptional` -宣告設定為`HttpTokens`的值。 `optional`
- 11.判斷提示 `V2 IsEnforced` -宣告設定為`HttpTokens`的值。 `required`
- 12.`wait BeforeAssertingMetadataState` -在宣告中繼資料狀態停用之前等待 30 秒。
- 13.斷言 `MetadataIsDisabled` -斷言元數據是。 `disabled`
- 14.`describeMetadataOptions` -套用您指定的變更後，會取得中繼資料選項。

## 輸出

描述`MetadataOptions`。 狀態

描述`MetadataOptions`。 `MetadataAccess`

描述 `MetadataOptions`

描述`MetadataOptions`。 `HttpPutResponseHop`極限

## AWS Support - Copy EC2 Instance

Description (描述)

[AWSSupport-CopyEC2Instancerunbook](#) 針對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](#)？自動化會根據您為Region和SubnetId參數指定的值進行分支。

如果您為參數指定值，但不指定SubnetId參Region數的值，則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中啟動新執行個體。

如果您指定SubnetId參數和參數的值，則自動化會建立目標執行個體AMI的一個，複製AMI到AWS 區域您指定的執行個體，然後從您指定的子網路AMI中啟動新執行個體。Region

如果您為參數指定值，但不指定Region參數的值，則自動化會建立目標執行個體AMI的一個，將該執行個體複製AMI到您指定的區域，然後從目的地區域AMI中虛擬私人雲端 (VPC) 的預設子網路中啟動新執行個體。SubnetId

如果未指定Region或SubnetId參數的值，則自動化會建立目標執行個AMI體，並從 VPC 的預設子網路AMI中啟動新執行個體。

若要將一個複製AMI到不同的「區域」，您必須提供AutomationAssumeRole參數的值。如果waitForAvailableDestinationAmi步驟期間自動化逾時，AMI可能仍在複製。在這種情況下，您可以等待複製完成並手動啟動執行個體。

執行此自動化操作之前，請注意下列事項：

- AMIs 是以亞馬遜彈性區塊存放區 (Amazon EBS) 快照為基礎。對於沒有先前快照的大型檔案系統，AMI建立可能需要數小時的時間。若要縮短建AMI立時間，請先建立 Amazon EBS 快照，然後再建立 AMI
- 建立執行個體AMI並不會為執行個體上的執行個體儲存磁碟區建立快照。如需將執行個體存放磁碟區備份到 Amazon EBS 的相關資訊，請參閱[如何將 Amazon EC2 執行個體上的執行個體存放區磁碟區備份到 Amazon EBS](#)？
- 新的亞馬遜 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 位址來更新舊 IP 位址的所有參照 (例如，在 DNS 項目中)。如果您在來源執行個體上使用彈性 IP 位址，請務必將其附加至新執行個體。
- 當副本啟動並嘗試連絡網域時，可能會發生網域安全性識別碼 (SID) 衝突問題。擷取 AMI 之前，請使用 Sysprep 或從網域移除加入網域的執行個體，以避免發生衝突問題。如需詳細資訊，請參閱[如何使用 Sysprep 建立和安裝自訂可重複使用的 Windows AMI](#)？

[運行此自動化 \(控制台\)](#)

**⚠ Important**

我們不建議使用此 Runbook 複製微軟活動目錄域控制器實例。

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必要) 您要複製之執行個體的 ID。

- KeyPair

類型：字串

說明：(選擇性) 您要與新複製的執行個體建立關聯的金鑰配對。如果您要將執行個體複製到不同的區域，請確定金鑰組存在於指定的 [區域] 中。

- 區域

類型：字串

說明：(選擇性) 您要複製執行個體的目標區域。如果您為此參數指定值，但未指定SubnetId和SecurityGroupIds參數的值，則自動化會嘗試在具有預設安全性群組的預設 VPC 中啟動執行個體。如果目的地區域中已啟用 EC2-Classic，則啟動將失敗。

- SubnetId

類型：字串

說明：(選擇性) 您要將執行個體複製到哪個子網路的 ID。如果在目標區域中啟用 EC2-Classic，您必須提供此參數的值。

- InstanceType

類型：字串

說明：(選擇性) 複製執行處理應啟動為的執行個體類型。如果未指定此參數的值，則會使用來源執行環境型態。如果要複製執行處理的目標區域中不支援來源執行環境型態，則自動化會失敗。

- SecurityGroupIds

類型：字串

說明：(選擇性) 您要與複製執行個體建立關聯的安全性群組 ID 清單 (以逗號分隔)。如果您未指定此參數的值，且未將執行處理複製到其他「區域」，則會使用與來源執行環境相關聯的安全性群組。如果您要將執行個體複製到其他區域，則會使用目標區域中預設 VPC 的預設安全性群組。

- KeepImageSourceRegion

類型：布林值

有效值：true | false

預設：true

說明：(選擇性) 如果您true為此參數指定，則自動化操作不會刪除來源執行環境AMI的。如果您false為此參數指定，則自動化會取消註冊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：(選擇性) 如果您`true`為此參數指定，則自動化操作不會刪除複製到您指定之「區域」的內容。AMI如果您`false`為此參數指定，則自動化會取消註冊AMI並刪除相關聯的快照。

- `NoRebootInstanceBeforeTakingImage`

類型：布林值

有效值：`true` | `false`

預設：`false`

說明：(選擇性) 如果您`true`為此參數指定，則在建立之前，不會重新啟動來源執行處理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

此`AutomationAssumeRole`參數需要執行下列動作，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，您也需要下列權限。

- `ec2:CopyImage`

### 文件步驟

- `describeOriginalInstance` 詳細資訊-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`，如果沒有，則結束自動化操作。
- `evalInputParameters`-評估為輸入參數提供的值。
- `createLocalAmi`-建立AMI來源執行環境。
- `tagLocalAmi`-標記在上一步中AMI創建的。

- `branchAssertRegionIsSame`-根據實例是在相同區域內還是複製到不同區域而定的分支。
- `branchAssertSameRegionWithKeyPair`-根據是否為要在相同區域內複製的例證提供`KeyPair`參數值進行分支。
- `sameRegionLaunchInstanceWithKeyPair`-從相同子網路中的AMI來源執行個體或您使用指定的金鑰組指定的子網路啟動 Amazon EC2 執行個體。
- `sameRegionLaunchInstanceWithoutKeyPair`-從相同子網路中AMI的來源執行個體啟動 Amazon EC2 執行個體，或您指定但不使用金鑰組的子網路。
- `copyAmiToRegion`-複製AMI到目的地區域。
- `waitForAvailableDestinationAmi`-等待複製的AMI狀態變成`available`。
- `destinationRegionLaunch`執行個體-使用複製的執行個體啟動 Amazon EC2 執行個體AMI。
- `branchAssertDestinationAmiToDelete`-根據您為`KeepImageDestinationRegion`參數提供的值進行分支。
- `deregisterDestinationAmiAndDeleteSnapshots`-取消註冊複製的快照AMI並刪除相關聯的快照。
- `branchAssertSourceAmiToDelete`-根據您為`KeepImageSourceRegion`參數提供的值進行分支。
- `deregisterSourceAmiAndDeleteSnapshots`-取消註冊從來源執行個體AMI建立的快照，並刪除相關聯的快照。
- 睡眠-睡眠自動化 2 秒鐘。這是終端機步驟。

## 輸出

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunch`執行個體。 `DestinationInstanceIds`

## **AWSsupport-EnableWindowsEC2SerialConsole**

### Description

手冊可以`AWSsupport-EnableWindowsEC2SerialConsole`幫助您啟用 Amazon EC2 串行控制台，特殊管理控制台 ( SAC ) 和您的 Amazon EC2 Windows 實例上的啟動菜單。使用 Amazon 彈性運算雲端 (AmazonEC2) 序列主控台功能，您可以存取 Amazon EC2 執行個體的序列埠，以對開機、網路組態和其他問題進行疑難排解。`runbook` 會自動執行個體在執行中狀態和管理的執行個體上啟用此功能所需的步驟 AWS Systems Manager，以及處於停止狀態或未受管理的執行個體。AWS Systems Manager



## 它是如何工作的？

AWSSupport-EnableWindowsEC2SerialConsole 自動化手冊有助於啟用 SAC 和啟動菜單上運行 Microsoft Windows 服務器的 Amazon EC2 實例。對於處於執行中狀態且由管理的執行個體 AWS Systems Manager，runbook 會執行「AWS Systems Manager 執行命令」指 PowerShell 令碼來啟用 SAC 和開機功能表。對於 EC2 處於停止狀態或未受管理的執行個體 AWS Systems Manager，runbook 會使用 [AWSSupport-Start EC2RescueWorkflow](#) 建立臨時 Amazon 執行個體，以離線執行所需的變更。

有關詳情，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 SAC 上啟用，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 [用 SAC 來疑難排解 Windows 執行個體](#)。
- 若要設定序列主控台的存取權，您必須在帳戶層級授與序列主控台存取權，然後設定 AWS Identity and Access Management (IAM) 原則以授與使用者存取權。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 Amazon EC2 序列主控台的存取權](#)。
- 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](#)。
- 只有在 [Nitro 系統](#) 上建置的虛擬化執行個體上才支援序列主控台存取。

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

所需 IAM 權限

此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操作：

1. 導覽至主 AWS Systems Manager 控制台 `AWSSupport-EnableWindowsEC2SerialConsole` 中的。
2. 選擇 `Execute automation` (執行自動化)。
3. 對於輸入參數，請輸入以下內容：

- `InstanceId`: (必填)

您要啟用 EC2 Amazon EC2 序列主控台、(SAC) 和開機功能表的 Amazon 執行個體識別碼。

- `AutomationAssumeRole`: (選擇性)

允許 Systems Manager 自動化代表您執行動作的 IAM 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `HelperInstanceType`: (有條件)

runbook 佈建用於為離線 EC2 執行個體設定 Amazon EC2 序列主控台的 Amazon 執行個體類型。

- `HelperInstanceProfileName`: (有條件)

協助程式執行個體 IAM 體現有執行個體設定檔的名稱。如果您要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，則必須執行此動作。如果未指定 IAM 執行個體設定檔，自動化操作會代表您建立一個設定檔。

- `SubnetId`: (有條件)

協助程式執行個體的子網路 ID。依預設，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，則該子網路必須與其位於相同的可用區域中 `InstanceId`，且必須允許存取 Systems Manager 端點。只有在目標執行處於停止狀態或不受管理時，才需要這樣做 AWS Systems Manager。

- `CreateInstanceBackupBeforeScriptExecution`: (選擇性)

指定 `True` 可在啟用 SAC 和啟動功能表之前建立 Amazon EC2 執行個體的 Amazon 機器映像 (AMI) 備份。自動化完成後，AMI 將持續存在。您有責任保護存取 AMI 或刪除它。

- `BackupAmazonMachineImagePrefix`: (有條件)

如果 `CreateInstanceBackupBeforeScriptExecution` 參數設定為 `True`，則會建立 Amazon 機器映像 (AMI) 的前置詞 `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](#)

**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

**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.  
SelectInstanceSubnet

**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

**HelperInstanceType**  
(Conditional) The type of Amazon EC2 instance that the runbook provisions to configure EC2 serial console for an offline instance.  
t3.medium

**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

**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：依預設，無法存取序列主控台。如需詳細資訊，請參閱[設定對 Amazon EC2 序列主控台的存取權限](#)。

- **CheckIfEc2InstancesWindows:**

宣告目標執行個體平台是否為 Windows。

- **GetInstanceType:**

擷取目標執行個體的執行個體類型。

- **CheckIfInstanceTypesNitro:**

檢查執行個體類型虛擬化管理程序是否以硝基為基礎。只有在 Nitro 系統上建置的虛擬化執行個體上才支援序列主控台存取。

- **CheckIfInstancesInAutoScalingGroup:**

透過呼叫來檢查 Amazon EC2 執行個體是否屬於 Amazon EC2 Auto Scaling 群組的一部分 DescribeAutoScalingInstances API。如果執行個體是 Amazon EC2 Auto Scaling 群組的一部分，則可確保移植助理適用於 .NET 執行處理處於待命生命週期狀態。

- **WaitForEc2InstanceStateStablized:**

等待執行處理處於執行中或停止狀態。

- **GetEc2InstanceState:**

取得執行個體的目前狀態。

- **BranchOnEc2InstanceState:**

根據在上一個步驟中擷取的例證狀態進行分支。如果該執行個體狀態正在執行，它會移至CheckIfEc2InstanceIsManagedBySSM步驟，如果沒有，則會移至CheckIfHelperInstanceProfileIsProvided步驟。

- CheckIfEc2 InstanceIsManagedBySSM:

檢查執行個體是否由管理 AWS Systems Manager。如果管理，runbook 啟用SAC和啟動菜單使用 PowerShell 運行命令。

- BranchOnPreEC2RescueBackup:

根據CreateInstanceBackupBeforeScriptExecution輸入參數進行分支。

- CreateAmazonMachineImageBackup:

建立執行個體的AMI備份。

- EnableSACAndBootMenu:

通過運行 PowerShell 行命令腳本啟用SAC和啟動菜單。

- RebootInstance:

重新啟動 Amazon EC2 執行個體以套用組態。如果執行個體在線且由管理，則這是最後一個步驟 AWS Systems Manager。

- CheckIfHelperInstanceProfileIsProvided:

在使用臨時 Amazon EC2 執行個體啟用SAC和離線啟動功能表之前，檢查HelperInstanceProfileName指定項目是否存在。

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

當執行個體處於停止狀態或未受管理時，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映像 ID。

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

- EnableSACAndBootMenu. 輸出:

在步驟中執行命令的輸出EnableSACAndBootMenu出。

- GetExecutionDetails.OfflineScriptOutput:

## 在步驟中執行的離線指令碼

輸入 `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` 出。

- `GetExecutionDetails.BackupBeforeScriptExecution`:

如果 `CreateInstanceBackupBeforeScriptExecution` 輸入參數為 `True`，則採取AMI備份的映像 ID。

## 執行及管理執行個體上的執行輸出 AWS Systems Manager

Outputs	
<pre>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.</pre>	<pre>GetExecutionDetails.OfflineScriptOutput No output available yet because the step is not successfully executed</pre>

## 已停止或未受管理之執行個體的執行輸出 AWS Systems Manager

Outputs	
<pre>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 (18.0.14393.6522) 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</pre>	<pre>GetExecutionDetails.BackupBeforeScriptExecution ami-09c33701932955dde</pre>

## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化工作流登陸頁](#)

## AWSsupport-ExecuteEC2Rescue

### Description (描述)

本手冊使用該EC2Rescue工具對 Linux 或Windows Server指定的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體進行疑難排解，並在可能的情況下修復常見的連線問題。不支援具有加密根磁碟區的執行個體。



## 運行此自動化 ( 控制台 )

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Linux, macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- EC2 RescueInstanceType

類型：字串

有效值：2. 小 | 2. 中等

預設：t2.small

說明：( 必填 ) 執行個體的 EC2 執行個體 EC2Rescue 體類型。建議尺寸:t2.small

- LogDestination

類型：字串

說明：(選用) 您想要上傳疑難排解日誌的帳戶中的 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

預設值：CreateNewVPC

說明：(選擇性) EC2Rescue 執行個體的子網路 ID。根據預設，AWS Systems Manager 自動化會建立新的 VPC。或者，使SelectedInstanceSubnet用與執行個體使用相同的子網路，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，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**

系統管理員自動化會停止此執行個體，並在嘗試任何作業之前建立 AMI。存放在執行個體存放磁碟區的資料會遺失。如果您沒有使用彈性 IP 位址，公用 IP 位址將會變更。

## 必要的 IAM 許可

此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為Windows Server：
  - a. ( `EC2RescueforWindows Server` ) 如果提供的實例是一個Windows Server實例：
    - i. `aws:executeAutomation-AWSSupport-StartEC2RescueWorkflow` 使用 EC2Rescue 進Windows Server行離線指令碼呼叫。
    - 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對於 Linux 而言) 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 離線指令碼的 EC2Rescue 呼叫
  - 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 (描述)

`AWSsupport-ListEC2Resources` 執行手冊會從 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 彈性區塊存放區 (Amazon EBS) 磁碟區、彈性 IP 地址和 Amazon EC2 自動擴展群組。依預設，資訊會從所有區域收集，並顯示在自動化操作的輸出中。或者，您可以指定 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體，以逗號分隔值 (.csv) 檔案形式上傳到的資訊。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux, macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 儲存貯體

類型：字串

說明：(選擇性) 上傳所收集資訊的 S3 儲存貯體名稱。

- DisplayResourceDeletionDocumentation

類型：字串

預設：true

描述：(選擇性) 如果設定為true，自動化操作會在輸出中建立與刪除資源相關的文件連結。

- RegionsToQuery

類型：字串

預設值：全部

說明：(選擇性) 您要從中收集 Amazon EC2 相關資訊的區域。

## 必要的 IAM 許可

此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，若要將收集到的資訊成功上傳到您指定的 S3 儲存貯體，AutomationAssumeRole 需要執行下列動作：

- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

### 文件步驟

- `aws:executeAwsApi`-收集帳戶啟用的區域。
- `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`-如果帳戶沒有啟用區域，則自動化操作結束。
- `aws:executeScript`-列出您指定的帳戶和區域的所有 EC2 執行個體。
- `aws:executeScript`-列出您指定的帳戶和區域的所有 Amazon 機器映像 (AMI)。
- `aws:executeScript`-列出您指定的帳戶和區域的所有 EBS 磁碟區。
- `aws:executeScript`-列出您指定的帳戶和區域的所有彈性 IP 位址。
- `aws:executeScript`-列出您指定的帳戶和區域的所有彈性網路介面。
- `aws:executeScript`-列出您指定的帳戶和區域的所有「自動調整比例」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到指定的 S3 儲存貯體。

## AWSsupport-ManageRDPSettings

### Description (描述)

R AWSsupport-ManageRDPSettings unbook 允許使用者管理常見的遠端桌面通訊協定 (RDP) 設定，例如 RDP 連接埠和網路層驗證 (NLA)。默認情況下，runbook 讀取並輸出設置的值。

#### Important

RDP 設定的變更應該在執行此 Runbook 之前仔細檢閱。

## 運行此自動化 (控制台)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

描述：(必要) 管理 RDP 設定的受管執行個體之 ID。

- NLA SettingAction

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。

- RDP PortAction

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) 要對 FDENYTS 連線設定執行的動作。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

接收命令的 EC2 執行個體必須具有 IAM 角色，並附加了ManagedInstanceCore亞馬遜亞馬遜受管政策。用戶必須至少有 ssm: SendCommand 才能將命令發送到實例，加上 ssm: GetCommandInvocation 才能讀取命令輸出。

### 文件步驟

aws:runCommand-執行指PowerShell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 (描述)

AWSSupport-ManageWindowsServiceRunbook 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。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必要) 要管理其服務的代管執行個體 ID。

- ServiceAction

類型：字串

有效值：檢查 | 重新啟動 | 強制重新啟動 | 開始 | 停止 | 強制停止 | 暫停

預設：Check

說明：(必要) 要套用至 Windows 服務的動作。請注意，Force-Restart 並 Force-Stop 可用於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

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具有 IAM 角色，並附加了ManagedInstanceCore亞馬遜亞馬遜受管政策。用戶必須至少有 ssm: StartAutomationExecution 和 ssm: SendCommand 才能運行自動化並將命令發送到實例，再加上 ssm: GetAutomationExecution 才能讀取自動化輸出。

### 文件步驟

aws:runCommand-執行指PowerShell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輸出。

## AWSSupport-MigrateEC2ClassicToVPC

### Description (描述)

該手AWSSupport-MigrateEC2ClassicToVPC冊將亞馬遜彈性運算雲 ( 亞馬遜 EC2 ) 實例從 EC2-Classic 遷移到虛擬私有雲 ( VPC )。此執行手冊支援使用 Amazon 彈性區塊存放區 (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。

### [運行此自動化 \( 控制台 \)](#)

### 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) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- 審批

類型:StringList

說明：(選用) 可以核准或拒絕動作的 IAM 使用者的 Amazon 資源名稱 (ARN)。僅當您指定參數CutOver值時，此MigrationType參數才適用。

- DestinationSecurityGroupId

類型:StringList

說明：(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識別碼。如果您未指定此參數的值，則自動化會在您的 VPC 中建立安全性群組，並從 EC2-Classical 中的安全性群組複製規則。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

說明：(選用) 您要將 Amazon EC2 執行個體遷移到的子網路識別碼。如果您沒有為此參數指定值，則自動化會從您的 VPC 中隨機選擇子網路。

- InstanceId

類型：字串

說明：(必填) 您要遷移之 Amazon EC2 執行個體的 ID。

- MigrationType

類型：字串

有效值：CutOver| 測試

描述：(必要) 您要執行的移轉類型。

此選CutOver項需要核准才能停止在 EC2-Classic 中執行的 Amazon EC2 執行個體。核准此動作後，Amazon EC2 執行個體會停止，且自動化會建立 Amazon Machine Image (AMI)。當AMI狀態為時available，會從您在 VPC 中指定的AMI中啟動新的 DestinationSubnetId Amazon EC2 執行個體。如果在 EC2-Classic 中執行的 Amazon EC2 執行個體附加了彈性 IP 地址，則該執行個體將移至 VPC 中新建立的 Amazon EC2 執行個體。如果在 VPC 中啟動的 Amazon EC2 執行個體因任何原因無法建立，則會終止該執行個體，並要求核准在 EC2-Classic 中啟動 Amazon EC2 執行個體。

此選Test項會建立一個在 EC2-Classic 中執行AMI的 Amazon EC2 執行個體，而無需重新開機。由於 Amazon EC2 執行個體不會重新啟動，因此我們無法保證所建立映像檔的檔案系統完整性。當AMI狀態為時available，會從您AMI在 VPC 中指定的此執行個體啟動新DestinationSubnetId的 Amazon EC2 執行個體。如果在 EC2-Classic 中執行的 Amazon EC2 執行個體附加了彈性 IP 地址，則自動化會驗證DestinationSubnetId您指定的是公開的。如果在 VPC 中啟動的 Amazon EC2 執行個體因任何原因無法建立，則會終止該執行個體並結束自動化。

- 網絡安全認證 NforApproval

類型：字串

說明：(選用) 您要向其傳送核准請求的亞馬遜簡單通知服務 (Amazon SNS) 主題的 ARN。僅當您指定參數CutOver值時，此MigrationType參數才適用。

- TargetInstanceType

類型：字串

預設值：大

說明：(選用) 您要在 VPC 中啟動的 Amazon EC2 執行個體類型。僅支援以 XENS 為基礎的執行個體類型，例如 T2、M4 或 C4。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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:DescribeInstanceStatus
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroupReferences
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTags
- ec2:DescribeVpcs

- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`

## 文件步驟

- `aws:executeAwsApi`-收集有關您在`InstanceId`參數中指定的 Amazon EC2 執行個體的詳細資訊。
- `aws:assertAwsResourceProperty`-確認您在`TargetInstanceType`參數中指定的例證類型是以 XenM 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`-根據您為參`DestinationSecurityGroupId`數指定的值，視需要建立安全性群組。
- `aws:branch`-根據您在`DestinationSubnetId`參數中指定的值進行分支。
- `aws:executeAwsApi`-識別執行此自動化操作AWS 區域的預設 VPC。
- `aws:executeAwsApi`-隨機選擇位於預設 VPC 中的子網路 ID。
- `aws:createImage`-建立AMI不重新啟動 Amazon EC2 執行個體的情況下。
- `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建立的執行個體啟動新執行個體，而不必在 EC2-Classic 中重新啟動 Amazon EC2 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`-從AMI建立的執行個體啟動新執行個體，而不必在 EC2-Classic 中重新啟動 Amazon EC2 執行個體 (`DestinationSubnetId`如果提供的話)。
- `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 EC2-Classic 中執行的 Amazon EC2 執行個體的停止行為。
- `aws:approve`-等待核准停止 Amazon EC2 執行個體。

- `aws:changeInstanceState`-停止在 EC2-典型中執行的亞馬遜 EC2 執行個體。
- `aws:changeInstanceState`-如果需要，強制停止在 EC2-經典中運行的亞馬遜 EC2 實例。
- `aws:createImage`-在停止後建立一個 AMI Amazon EC2 執行個體。
- `aws:branch`-根據為 `DestinationSubnetId` 參數指定的值進行分支。
- `aws:runInstances`-從 EC2-Classic 中已停止的 Amazon EC2 執行個體所AMI建立的執行個體啟動新執行個體。
- `aws:approve`-如果上一個步驟因任何原因而失敗，則會等待核准終止新啟動的執行個體，並在 EC2-Classic 中啟動 Amazon EC2 執行個體。
- `aws:changeInstanceState`-終止新啟動的 Amazon EC2 執行個體。
- `aws:runInstances`-從參數在 EC2-Classic 中AMI建立的已停止 Amazon EC2 執行個體啟動新執行個體。 `DestinationSubnetId`
- `aws:approve`-如果上一個步驟因任何原因而失敗，則會等待核准終止新啟動的執行個體，並在 EC2-Classic 中啟動 Amazon EC2 執行個體。
- `aws:changeInstanceState`-終止新啟動的 Amazon EC2 執行個體。
- `aws:changeInstanceState`-啟動在 EC2-典型中停止的亞馬遜 EC2 執行個體。
- `aws:branch`-根據 Amazon EC2 執行個體是否具有公有 IP 地址進行分支。
- `aws:executeAwsApi`-驗證公用 IP 位址是否為彈性 IP 位址。
- `aws:branch`-根據您在 `MigrationType` 參數中指定的值進行分支。
- `aws:executeAwsApi`-將彈性 IP 位址移至您的虛擬私人雲端。
- `aws:executeAwsApi`-收集移動到 VPC 的彈性 IP 地址的配置 ID。
- `aws:branch`-根據在 VPC 中執行的 Amazon EC2 執行個體啟動的子網路而定的分支機構。
- `aws:executeAwsApi`-將彈性 IP 地址附加到 VPC 中新啟動的實例。
- `aws:executeScript`-確認在 VPC 中執行的新啟動 Amazon EC2 執行個體是公開的子網路。

## 輸出

`getInstanceProperties.virtualizationType`-在 EC2-典型中執行的亞馬遜 EC2 執行個體的虛擬化類型。

`getInstanceProperties.rootDeviceType`-在 EC2-典型中執行的亞馬遜 EC2 執行個體的根裝置類型。

`createAMIWithoutReboot.ImageId`-所AMI建立的識別碼，無須重新啟動在 EC2-Classic 中執行的 Amazon EC2 執行個體。

`getDefaultVPC.VpcId`-如果未提供`DestinationSubnetId`參數值，則會在其中啟動新 Amazon EC2 執行個體的預設 VPC 識別碼。

`getSubnetIdInDefaultVPC.subnetIdFromDefaultVpc`-預設 VPC 中子網路的識別碼，如果未提供`DestinationSubnetId`參數值，則會在其中啟動新 Amazon EC2 執行個體。

`launchTestInstanceDefaultVPC.InstanceIds-Test` 遷移類型期間，預設 VPC 中新啟動的 Amazon EC2 執行個體識別碼。

`launchTestInstanceProvidedSubnet.InstanceIds`-您在`Test`遷移類型期間指定的新啟動 Amazon EC2 執行個體的 ID。`DestinationSubnetId`

`createAMIAfterStoppingInstance.ImageId`-停止在 EC2-Classic 中執行的 Amazon EC2 執行個體之後AMI建立的識別碼。

`launchCutOverInstanceProvidedSubnet.InstanceIds`-您在`CutOver`遷移類型期間指定的新啟動 Amazon EC2 執行個體的 ID。`DestinationSubnetId`

`launchCutOverInstanceDefaultVPC.InstanceIds-CutOver` 遷移類型期間，預設 VPC 中新啟動的 Amazon EC2 執行個體識別碼。

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`-預設 VPC 中的自動化選擇的子網路是否為公用。

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`-您在中指定的子網路`DestinationSubnetId`是否為公用。

## AWS Support - Migrate Xen To Nitro Linux

Description (描述)

[執行手冊AWS Support - Migrate Xen To Nitro Linux](#)會將亞馬遜彈性運算雲端 (Amazon EC2) Linux Xen 執行個體複製、準備和遷移到執行個體類型。Nitro此 Runbook 為操作類型提供了兩個選項：

- `Clone&Migrate`— 此選項的工作流程包含「初步檢查」、「測試」和「Clone&Migrate階段」。工作流程是使用工作流程執行手冊`AWS Support - Clone Xen EC2 Instance And Migrate To Nitro`。

- 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」的其他步驟。

### Important

使用此執行手冊會對您的帳戶產生 Amazon EC2 執行個體的執行時間、建立 Amazon 彈性區塊存放區 (Amazon EBS) 磁碟區的成本，以及。AMIs如需詳細資訊，請參閱[亞馬遜 EC2 定價](#)和[亞馬遜 EBS 定價](#)。

## 初步檢查

在繼續移轉之前，自動化會執行下列初步檢查。如果有任何檢查失敗，則自動化結束。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經是Nitro執行個體類型。
- 檢查目標執行個體是否已使用 Spot 執行個體購買選項。
- 檢查執行個體儲存磁碟區是否已連接至目標執行個體。
- 驗證目標執行個體作業系統 (OS) 是否為 Linux。
- 檢查目標執行個體是否屬於 Amazon EC2 自動擴展群組的一部分。如果它是 Auto Scaling 群組的一部分，則自動化會驗證執行個體是否處於狀standby態。
- 驗證執行個體是否由AWS Systems Manager管理。

## 測試

自動化會從目標執行個體建立 Amazon Machine Image (AMI)，並從新建立的執行個體啟動測試執行個體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，則自動化會暫停，並透過 Amazon 簡單通知服務 (Amazon SNS) 通知要求指定主體的核准。如果提供核准，則自動化會終止測試執行個體、停止目標執行個體並繼續進行移轉，而新建立AMI的工作流程結束時會取消註冊。Clone&Migrate

### Note

在提供核准之前，建議先確認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

自動化操作會AMI從目標執行個體建立另一個執行個體，然後啟動新執行個體以變更為Nitro執行個體類型。在繼續移轉之前，自動化會完成下列先決條件。如果有任何檢查失敗，則自動化結束。此階段也只是Clone&Migrate工作流程的一部分。

- 開啟增強型網路 (ENA) 屬性。
- 如果尚未安裝 ENA 驅動程式，請安裝最新版本，或將 ENA 驅動程式版本更新為最新版本。若要確保最大的網路效能，如果Nitro執行個體類型是第 6 代，則必須更新為最新的 ENA 驅動程式版本。
- 驗證是否已安裝 NVMe 模組。如果已安裝模組，則自動化會驗證模組是否已載入initramfs。
- 使用區塊裝置名稱 (/dev/sd\*或/dev/xvd\*) 分析/etc/fstab項目，並以各自的 UUID 取代項目。在修改組態之前，自動化會在路徑上建立檔案的備份/etc/fstab\*。
- 關閉可預測的介面命名，方法是將net.ifnames=0選項加入至/etc/default/grub檔案中的GRUB\_CMDLINE\_LINUX行 (如果存在) 或中的核心/boot/grub/menu.lst。
- 移除檔/etc/udev/rules.d/70-persistent-net.rules案 (如果存在)。移除檔案之前，自動化會在路徑上建立檔案的備份/etc/udev/rules.d/。

確認所有需求後，例證類型會變更為您指定的Nitro例證類型。在以執行個體類型啟動之後，自動化會等待新建立的執行個Nitro體通過所有狀態檢查。接著，自動化會等待指定主參與者的核准，以建立已成功啟Nitro動AMI的執行個體。如果核准遭到拒絕，自動化作業會結束，讓新建立的執行個體保持執行中，且目標執行個體會保持停止狀態

## 更換根亞馬遜 EBS 卷

如果您選擇FullMigration為OperationType，自動化會將目標 Amazon EC2 執行個體遷移到您指定的Nitro執行個體類型。自動化請求指定主體的核准，以複製的 Amazon EC2 執行個體的根磁碟區取代目標 Amazon EC2 執行個體的根 Amazon EBS 磁碟區。遷移成功後，複製的 Amazon EC2 執行個體就會終止。如果自動化失敗，原始的 Amazon EBS 根磁碟區會連接到目標 Amazon EC2 執行個體。如果連接到目標 Amazon EC2 執行個體的根 Amazon EBS 磁碟區具有套用aws:前綴的標籤，則不支援該FullMigration操作。

## 開始之前

目標執行個體必須有輸出網際網路存取權。這是為了訪問驅動程序和依賴關係的存儲庫 kernel-devel gcc patch rpm-buildwget，例如dracut，make，linux-headers，，和unzip。如果需要，可以使用包管理器。

需要 Amazon SNS 主題才能傳送核准和更新的通知。如需有關建立 Amazon SNS 主題的詳細資訊，請參閱 [Amazon 簡單通知服務開發人員指南中的建立 Amazon SNS 主題](#)。

此 Runbook 支援下列作業系統：

- RHEL7.
- 亞馬遜 Linux, 亞馬遜 Linux 2
- Debian Server
- Ubuntu 服務器 18.04 LTS , 20.04 LTS 和 20.10 海峽
- SUSE Linux Enterprise Server(SUSE12SP5, SUSE15SP2)

### [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 確認

類型：字串

描述：( 必填 ) 閱讀此自動化 runbook 執行的操作的完整詳細信息，然後輸入 **Yes, I understand and acknowledge** 以繼續使用 runbook。

- 審批

類型：字串

說明：(必要) 可提供自動化核准的 IAM 角色、使用者或使用者名稱的 ARN。您最多可以指定 10 名核准者。

- DeleteResourcesOnFailure

類型：布林值

說明：(選擇性) 決定如果自動化失敗，是否刪除新建立的執行個體和AMI移轉。

有效值：真 | 假

預設：True

- MinimumRequiredApprovals

類型：字串

描述：(選擇性) 要求核准時繼續執行自動化操作所需的最小核准數目。

有效值：1-10

預設：1

- NitroInstanceType

類型：字串

說明：(必要) 您要變更Nitro執行個體的目標執行個體類型。支援的執行個體類型包括 M5、M6、C5、C6、R5、R6 和 T3。

預設值：大

- OperationType

類型：字串

描述：(必要) 您要執行的作業。此選FullMigration項會執行與目標執行個體相同的工作，Clone&Migrate並另外取代目標執行個體的根磁碟區。在遷移程序之後，目標執行個體的根磁碟區會取代為新建立執行個體的根磁碟區。此FullMigration作業不支援邏輯磁碟區管理員 (LVM) 所定義的根磁碟區。

有效值：複製與移轉 | FullMigration

- SNS TopicArn

類型：字串

說明：(必要) 要核准通知之 Amazon SNS 主題的 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

說明：(必填) 要遷移之 Amazon EC2 執行個體的 ID。

## Clone&Migrate 工作流程

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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`-分支至初步檢查工作流程。
- `getTargetInstanceProperties`-從目標執行個體收集詳細資料。
- `checkIfNitroInstanceTypeIsSupportedInAZ`-判斷目標 Amazon EC2 執行個體類型在與目標執行個體相同的可用區域中是否受支援。
- `getXenInstanceTypeInfo`-收集來源執行環境類型的詳細資訊。
- `checkIfInstanceHypervisorIsNitroAlready`-檢查目標執行個體是否已作為執行個體 Nitro 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系統管理員管理。
- `checkIfEphemeralVolumesAreSupported`-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儲存磁碟區。
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`-檢查目標執行個體是否已連接執行個體儲存磁碟區。
- `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「自動縮放」群組的一部分。
- `endOfPreliminaryChecksBranch`-初步檢查分支結束
- `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`-終止測試實例。
- `endOfTestBranch`-測試分支結束。
- `checkIfTestingBranchSucceeded`-檢查測試分支的狀態。
- `approvalToStopTargetInstance`-等待指定主參與者的核准，以停止目標執行處理。
- `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，Force 才會停止目標執行個體。
- `startOfCloneAndMigrateBranch`-分支到Clone&Migrate工作流程。
- `createBackupImage`-建立要做為備份AMI的目標執行個體。
- `launchInstanceInSameSubnet-AMI` 使用與來源執行個體相同的設定，從備份啟動新執行個體。
- `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否由系統管理員管理。
- `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`-檢查裝置名稱是否已在中使用，`/etc/fstab`並視需要將其取代為 UUID。
- `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，Force 才會停止新建立的執行個體。
- `checkENAAttributeForClonedInstance`-檢查是否為新建立的執行個體開啟增強型聯網屬性。
- `setNitroInstanceTypeForClonedInstance`-將新建立例證的執行個體類型變更為您指定的 Nitro 執行個體類型。
- `startClonedInstance`-啟動您已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，則自動化作業會等待所需主體的核准。如果提供了核准，AMI 則會建立一個作為金卡使用 AMI。
- `createImageAfterDriversInstallation`-創建 AMI 一個用作黃金 AMI。

- `endOfCloneAndMigrateBranch-Clone&Migrate` 分支結束
- `cleanupTestImage`-取消註冊為測試而AMI創建的。
- `failureHandling`-檢查是否選擇在失敗時終止資源。
- `onFailureTerminateClonedInstance`-如果自動化失敗，則終止新建立的執行個體。
- `onFailurecleanupTestImage`-取消註冊為測試而AMI創建的。
- `onFailureApprovalToStartTargetInstance`-如果自動化失敗，請等待指定主參與者的核准，以啟動目標執行個體。
- `onFailureStartTargetInstance`-如果自動化失敗，請啟動目標執行個體。

## FullMigration 工作流程

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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工作流程會執行與Clone&Migrate作流程相同的步驟，並另外執行下列步驟：

- `checkConcurrency`-驗證此 Runbook 只有一個針對您指定的 Amazon EC2 執行個體的自動化操作。如果 runbook 發現另一個正在進行中的自動化以相同的執行個體為目標，則自動化結束。
- `getTargetInstanceProperties`-從目標執行個體收集詳細資料。
- `checkRootVolumeTags`-判斷目標 Amazon EC2 執行個體的根磁碟區是否包含任何AWS保留標籤。
- `cloneTargetInstanceAndMigrateToNitro`-使用手AWS-CloneXenInstanceToNitro冊啟動子自動化。
- `branchOnTheOperationType`-針對您為OperationType參數指定的值進行分支。
- `getClonedInstanceId`-從子系自動化擷取新啟動執行個體的 ID。
- `checkIfRootVolumeIsBasedOnLVM`-決定根分割區是否由 LVM 管理。
- `branchOnTheRootVolumeLVMStatus`-如果從主參與者收到所需的最低核准，則自動化會繼續取代根磁碟區。
- `manualInstructionsInCaseOfLVM`-如果根磁碟區由 LVM 管理，則自動化會傳送輸出，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`-基於CloudFormation堆棧狀態的分支。
- `approvalForRootVolumesReplacement(WithCFN)`-如果目標執行個體是由啟動的CloudFormation，則在新啟動的執行個體成功啟動為執行個體類型後，自動化作Nitro業會等待核准。提供核准後，目標執行個體的 Amazon EBS 磁碟區會被新啟動執行個體的根磁碟區取代。
- `approvalForRootVolumesReplacement`-新啟動的執行個體成功啟動為執行個體類型後，等待核准。提供核准後，目標執行個體的 Amazon EBS 磁碟區會被新啟動執行個體的根磁碟區取代。
- `assertIfTargetEC2InstanceIsStillStopped`-在取代根磁碟區之前，驗證目標執行個體是否處於某個stopped狀態。
- `stopTargetInstanceForRootVolumeReplacement`-如果目標執行個體正在執行，自動化會在更換根磁碟區前停止執行個體。
- `forceStopTargetInstanceForRootVolumeReplacement`-如果上一個步驟失敗，Force 會停止目標執行個體。
- `stopClonedInstanceForRootVolumeReplacement`-在更換 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，Force 會停止新建立的執行個體。
- `getBlockDeviceMappings`-擷取目標執行個體和新建立執行個體的區塊裝置對應。
- `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 磁碟區上的標籤。
- `startTargetInstance`-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 執行個體無法以執行個體類型啟動，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以執行個體類型啟動，則將目標 Amazon EC2 執行個體還原為原始 Nitro 執行個體類型。
- `onFailureRollbackRootVolumeReplacement`-如果需要，還原 `replaceRootEbsVolumes` 步驟所做的所有更改。
- `onFailureApprovalToStartTargetInstance`-復原先前的變更後，等待指定主體的核准啟動目標 Amazon EC2 執行個體。
- `onFailureStartTargetInstance`-啟動目標亞馬遜 EC2 實例。
- `terminateClonedEC2Instance`-取代根 Amazon EBS 磁碟區後，終止複製的 Amazon EC2 執行個體。

## AWSsupport-ResetAccess

### Description (描述)

此執行手冊將使用指定 EC2 執行個體上的 EC2Rescue 工具，使用 EC2 主控台 (Windows) 重新啟用密碼解密，或產生並新增安全殼層金鑰對 (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)。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

- `AutomationAssumeRole`

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- EC2 RescueInstanceType

類型：字串

有效值：2. 小 | 2. 中等


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


系統管理員自動化會停止此執行個體，並在嘗試任何作業之前建立 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

預設值：CreateNewVPC

描述：(選用) EC2Rescue 執行個體的子網路 ID。依預設，系統管理員自動化會建立新的 VPC。或者，用於SelectedInstanceSubnet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InstanceId，且必須允許存取 SSM 端點。

## 必要的 IAM 許可

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

您必須至少有 `ssm: StartAutomationExecution`, `ssm: GetParameter` (才能擷取 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 [AWSSupport-StartEC2RescueWorkflow](#)。

## 文件步驟

1. `aws:assertAwsResourceProperty`-如果提供的執行個體為 Windows, 則宣告此項。
  - a. (適用於 Windows 的 EC2Rescue) 如果提供的執行個體為 Windows :
    - i. `aws:executeAutomation-AWSSupport-StartEC2RescueWorkflow` 使用 EC2Rescue 進行視窗離線密碼重設指令碼呼叫
    - ii. `aws:executeAwsApi`-從嵌套自動化中檢索備份 AMI ID
    - iii. `aws:executeAwsApi`-從巢狀自動化擷取啟用密碼的 AMI ID
    - iv. `aws:executeAwsApi`-從嵌套自動化中檢索 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` 使用適用於 Linux 離線安全殼層金鑰插入指令碼的 EC2Rescue 呼叫
    - ii. `aws:executeAwsApi`-從嵌套自動化中檢索備份 AMI ID
    - iii. `aws:executeAwsApi`-擷取插入的 SSH 金鑰的 SSM 參數名稱
    - iv. `aws:executeAwsApi`-從嵌套自動化中檢索 EC2Rescue 摘要

## 輸出

得到 `RescueForWindowsResult` C2. 輸出

`getWindowsBackup`阿美。 `ImageId`

`getWindowsPasswordEnabledAmi`.`ImageId`

得到 `RescueForLinuxResult` C2. 輸出

`getLinuxBackup`阿美。 `ImageId`

獲取. 名稱 `KeyParameter`

## AWSSupport-ResetLinuxUserPassword

### Description

AWSsupport-ResetLinuxUserPasswordrunbook 可協助您重設本機作業系統 (OS) 使用者的密碼。對於需要使用序列主控台存取 Amazon 彈性運算雲端 (AmazonEC2) 執行個體的使用者，此手冊特別有用。runbook 在您的 AWS Identity and Access Management (IAM) 角色中創建一個臨時的 Amazon EC2 實例，AWS 帳戶 並且具有檢索包含密碼的 AWS Secrets Manager 秘密值的權限。

該 runbook 停止你的目標 Amazon EC2 實例，分離根 Amazon 彈性塊存儲 (AmazonEBS) 卷，並將其附加到臨時 Amazon EC2 實例。使用「執行命令」(Run Command) 時，會在暫存執行個體上執行指令碼，以設定您指定之 OS 使用者的密碼。然後，根 Amazon EBS 磁碟區會重新連接到您的目標執行個體。runbook 還提供了一個選項，用於在自動化開始時創建根磁碟區的快照。

## 開始之前

使用您要指派給作業系統使用者的密碼值來建立 Secret Secrets Manager 密碼。該值必須是純文本。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

- 我們建議您在使用此 runbook 之前備份您的執行個體。請考慮將CreateSnapshot參數值設定為**Yes**。
- 變更本機使用者密碼需要 runbook 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儲存磁碟區上的任何資料都會遺失。此外，會釋放任何自動指派的公開IPv4位址。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](#)。
- 如果連接到目標 Amazon EC2 執行個體的 Amazon EBS 磁碟區使用客戶管理 AWS Key Management Service (AWS KMS) 金鑰加密，請確定 AWS KMS 金鑰未加密，deleted否disabled則您的執行個體將無法啟動。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) Amazon EC2 Linux 執行個體的識別碼，該執行個體包含您要重設的作業系統使用者密碼。

- LinuxUserName

類型：字串

默認值：ec2 用戶

說明：(選擇性) 您要重設密碼的作業系統使用者帳戶。

- SecretArn

類型：字串

說明：( 必填 ) 包含新密碼ARN的秘密 Secrets Manager 密碼。

- SecurityGroupId

類型：字串

說明：(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 (AmazonVPC) 安全群組。

- SubnetId

類型：字串

說明：(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，自動化操作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，則該子網路必須與目標執行個體位於相同的可用區域，而且可以存取 Systems Manager 端點。

- CreateSnapshot

類型：字串

有效值：是 | 否

預設值：是

說明：(選擇性) 決定是否在自動化執行之前建立目標 Amazon EC2 執行個體的根磁碟區快照。

- StopConsent

類型：字串

有效值：是 | 否

預設值：否

說明：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。停止 Amazon EC2 執行個體時，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，並釋放自動公用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權限

此AutomationAssumeRole參數需要執行下列動作，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: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`— 根據您是否已提供停止目標 Amazon EC2 執行個體的同意進行分支。
2. `aws:assertAwsResourceProperty`— 確保 Amazon EC2 執行個體狀態處於 `running` 或 `stopped` 態。否則，自動化結束。
3. `aws:executeAwsApi`— 獲取 Amazon EC2 實例屬性。
4. `aws:executeAwsApi`— 取得根磁碟區內容。
5. `aws:branch`— 根據是否提供臨時 Amazon EC2 執行個體的子網路 ID 來分支自動化。
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中。



7. `aws:assertAwsResourceProperty`— 確保目標 Amazon EC2 實例根卷是一個 Amazon EBS 卷。
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 實例關閉行為是 `stop` 而不是 `terminate`。
10. `aws:branch`— 確保 Amazon EC2 執行個體不是競價型執行個體。否則，自動化結束。
11. `aws:executeScript`— 確保 Amazon EC2 執行個體不屬於 `auto` 擴展群組。如果執行個體屬於 `auto` 擴展群組，則自動化會確認 Amazon EC2 執行個體處於 `Standby` 生命週期狀態。
12. `aws:createStack`— 建立暫時的 Amazon EC2 執行個體，用於為您指定的作業系統使用者重設密碼。
13. `aws:waitForAwsResourceProperty`— 等待直到新啟動的臨時 Amazon EC2 實例正在運行。
14. `aws:executeAwsApi`— 獲取臨時 Amazon EC2 實例的 ID。
15. `aws:waitForAwsResourceProperty`— 等待臨時 Amazon EC2 實例報告由系統管理器管理。
16. `aws:changeInstanceState`— 停止目標 Amazon EC2 實例。
17. `aws:changeInstanceState`— 強制目標 Amazon EC2 實例停止以防卡在停止狀態。
18. `aws:branch`— 根據是否要求目標 Amazon EC2 執行個體的根磁碟區快照來分支自動化。
19. `aws:executeAwsApi`— 創建目標 Amazon EC2 實例根 Amazon EBS 卷的快照。
20. `aws:waitForAwsResourceProperty`— 等待快照處於某個狀態 `completed`。
21. `aws:executeAwsApi`— 從目標 Amazon EC2 執行個體分離 Amazon EBS 根磁碟區。
22. `aws:waitForAwsResourceProperty`— 等待 Amazon EBS 根磁碟區與目標 Amazon EC2 執行個體分離。
23. `aws:executeAwsApi`— 將根 Amazon EBS 卷附加到臨時 Amazon EC2 實例。
24. `aws:waitForAwsResourceProperty`— 等待 Amazon EBS 根卷連接到臨時 Amazon EC2 實例。
25. `aws:runCommand`— 使用臨時 Amazon EC2 執行個體上的執行命令執行殼層指令碼，以重設目標使用者密碼。
26. `aws:executeAwsApi`— 從臨時 Amazon EC2 實例中分離 Amazon EBS 根磁碟區。
27. `aws:waitForAwsResourceProperty`— 等待 Amazon EBS 根磁碟區與臨時 Amazon EC2 執行個體分離。
28. `aws:executeAwsApi`— 發生錯誤後，將 Amazon EBS 根磁碟區從暫時的 Amazon EC2 執行個體分離。

- 29aws:waitForAwsResourceProperty— 發生錯誤後，等待 Amazon EBS 根磁碟區與臨時 Amazon EC2 執行個體分離。
- 30aws:branch— 根據是否要求根磁碟區的快照來分支自動化，以便在發生錯誤時判斷復原路徑。
- 31aws:executeAwsApi— 將根 Amazon EBS 卷重新連接到目標 Amazon EC2 實例。
- 32aws:waitForAwsResourceProperty— 等待 Amazon EBS 根卷連接到 Amazon 實例 EC2。
- 33aws:executeAwsApi— 從目標 Amazon 執行個體 EC2 根 EBS 磁碟區快照建立新的 Amazon 磁碟區。
- 34aws:waitForAwsResourceProperty— 等待，直到新的 Amazon EBS 卷處於一個 available 狀態。
- 35aws:executeAwsApi— 將新的 Amazon EBS 磁碟區作為根磁碟區附加至目標執行個體。
- 36aws:waitForAwsResourceProperty— 等待 Amazon 體 EBS 積處於一個 attached 狀態。
- 37aws:executeAwsApi— 描述執行簿無法建立或更新 AWS CloudFormation 堆疊時的 AWS CloudFormation 堆疊事件。
- 38aws:branch— 根據先前的 Amazon EC2 執行個體狀態分支自動化。如果狀態為 running，則會啟動執行個體。如果它處於某個 stopped 狀態，則自動化會繼續進行。
- 39aws:changeInstanceState— 如果需要，啟動 Amazon EC2 實例。
- 40aws:waitForAwsResourceProperty— 等待 AWS CloudFormation 堆疊處於終端機狀態，然後再刪除。
- 41aws:executeAwsApi— 刪除包含臨時 Amazon EC2 執行個體的 AWS CloudFormation 堆疊。

## AWS Premium Support - Resize Nitro Instance

### Description (描述)

該手冊 AWS Premium Support - Resize Nitro Instance 提供了一個自動化的解決方案，用於調整在 Amazon EC2 實例上構建的亞馬遜彈性計算雲 ( Amazon EC2 ) 實例的大小。

為了減少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 自動擴展群組的一部分，且處於 standby 模式下。
- 執行個體狀態和租用。
- 您要變更的執行個體類型支援目前連接至執行個體的網路介面數目。

- 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。
- 如果實例正在運行，則它正在通過所有狀態檢查。
- 您要變更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，則執行手冊會自動回復為先前的執行個體類型。

根據預設，如果執行中且已連接執行個體儲存磁碟區，則此 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，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` 指定為 `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` 參數指定要變更為的執行個體類型。
- 若要大規模執行自動化以變更多個例證的例證類型，請使用 `TargetInstanceTypeFromTagValue` 參數指定例證類型。如需有關大規模執行自動化的資訊，請參閱大規模 [執行自動化](#)。

如果您沒有為任一參數指定值，則自動化會失敗。

#### 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 AWS Support 方案](#)。

## 考量

- 我們建議您在使用此 runbook 之前備份您的執行個體。
- 如需變更執行個體類型相容性的詳細資訊，請參閱 [變更執行個體類型的相容性](#)。
- 如果自動化失敗並回復為原始執行個體類型，請參閱 [疑難排解變更執行個體類型](#)。
- 變更執行個體類型需要 runbook 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儲存磁碟區上的任何資料都會遺失。此外，會釋放任何自動指派的公用 IPv4 位址。如需停止執行個體時會發生什麼情況的詳細資訊，請參閱 [停止並啟動執行個體](#)。

- 透過使用SkipInstancesWithTagKey參數，您可以略過套用特定 Amazon EC2 標籤金鑰的執行個體。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux、Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 確認

類型：字串

描述：(必填) 輸入**yes**以確認您的實例當前正在運行時將停止。

- AllowInstanceStoreInstances

類型：字串

有效值：否 | 是

預設：否

描述：(選擇性) 如果您指定yes，則允許 runbook 在已連接執行個體儲存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：(選擇性) 如果您指定yes，runbook 會在屬於AWS CloudFormation堆疊一部分的執行個體上執行。

- DryRun

類型：字串

有效值：否 | 是

預設：否

描述：(選擇性) 如果您指定yes，runbook 會驗證調整大小的需求，而不變更執行個體類型。

- InstanceId

類型：字串

說明：(必填) 您要變更其類型之 Amazon EC2 執行個體的 ID。

- SkipInstancesWithTagKey

類型：字串

說明：(選擇性) 如果您指定的標記鍵已套用至執行個體，則自動化會略過目標執行個體。

- SleepTime

類型：字串

預設：3

描述：(選擇性) 完成後，此 Runbook 應該睡眠的秒數。

- TagInstance

類型：字串

說明：(選擇性) 使用下列格式，使用您選擇的索引鍵和值來標記執行個體：`# =ChangingType## = True`。此選項可讓您追蹤已由此 Runbook 鎖定目標的執行個體。標籤鍵與值皆區分大小寫。

- `TargetInstanceTypeFromParameter`

類型：字串

說明：(選擇性) 您要將執行個體變更為的執行個體類型。如果您要使用參數中提供的標籤鍵值，請將此`TargetInstanceTypeFromTagValue`參數保留空白。

- `TargetInstanceTypeFromTagValue`

類型：字串

說明：(選擇性) 套用至目標執行個體的標記鍵，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，它會覆寫您為此參數指定的任何值。

### 必要的 IAM 許可

此`AutomationAssumeRole`參數需要執行下列動作，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 執行個體未使用`SkipInstancesWithTagKey`參數中指定的資源標籤金鑰加上標籤。如果找到標籤金鑰套用至執行個體，則步驟會失敗，且自動化結束。

2. `aws:assertAwsResourceProperty` : 確認目標 Amazon EC2 執行個體的狀態為 `running`、`pending`、`stopped`、或 `stopping`。否則，自動化結束。
3. `aws:executeAwsApi` : 從亞馬遜 EC2 執行個體收集屬性。
4. `aws:executeAwsApi` : 收集有關目前 Amazon EC2 執行個體類型的詳細資訊。
5. `aws:branch` : 檢查參數中指定的目前執行個體類型和執行個體類 `TargetInstanceTypeFromParameter` 型是否相同。如果是這樣，自動化結束。
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為亞馬遜彈性區塊存放區 (亞馬遜 EBS) 磁碟區。
8. `aws:assertAwsResourceProperty` : 確認執行個體關閉行為是 `stop` 與否 `terminate`。
9. `aws:branch` : 確保 Amazon EC2 執行個體不是競價型執行個體。
10. `aws:branch` : 確保 Amazon EC2 執行個體租用為預設租用，而非專用主機或專用執行個體。
11. `aws:executeScript` : 確認此 runbook 只有一個針對當前實例 ID 的自動化操作。如果另一個自動化操作已在針對同一個執行個體進行中，則自動化會傳回錯誤並結束。
12. `aws:branch` : 根據 Amazon EC2 執行個體的狀態分支自動化。
  - a. 如果是 `stopped` 或 `stopping`，則自動化會執行，`aws:waitForAwsResourceProperty` 直到 Amazon EC2 執行個體完全停止為止。
  - b. 如果是 `running` 或 `pending`，則自動化會執行，`aws:waitForAwsResourceProperty` 直到 Amazon EC2 執行個體通過狀態檢查為止。
13. `aws:assertAwsResourceProperty` : 透過呼叫 `DescribeAutoScalingInstances` API 操作，確認 Amazon EC2 執行個體不屬於自動擴展群組的一部分。如果執行個體是自動擴展群組的一部分，請確保 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 執行個體是否屬於 AWS CloudFormation 堆疊來分支自動化：
  - a. `aws:executeScript` 透過呼叫 `DescribeStackResources` API 作業，確保 Amazon EC2 執行個體不屬於 AWS CloudFormation 堆疊的一部分。
15. `aws:executeAwsApi` : 傳回具有相同處理器架構類型、虛擬化類型且支援目前連接至目標執行個體之網路介面數目的執行個體類型清單。
16. `aws:executeAwsApi` : 從參數中指定的標籤索引鍵取得目標執行個體類型 `TargetInstanceTypeFromTagValue` 值。
17. `aws:executeScript` : 確認目前執行個體和目標執行個體類型相容。確保目標執行個體類型在相同的子網路中可用。驗證啟動 runbook 的主體具有變更執行個體類型的權限，並在執行個體執行時停止和啟動執行個體。

- 18aws:branch：根據DryRun參數值是否設定為來分支自動化yes。如果yes，自動化結束。
- 19aws:branch：檢查原始執行個體和目標例證類型是否相同。如果它們是相同的，自動化結束。
- 20aws:executeAwsApi：取得目前執行個體狀態。
- 21aws:changeInstanceState：停止亞馬遜 EC2 實例。
- 22aws:changeInstanceState：如果執行個體停留在stopping狀態中，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: 為了達到最終一致性，變更執行個體類型後等待 3 秒。
- 25aws:branch：根據先前的執行個體狀態分支自動化。如果是running，則會啟動執行個體。
- aws:changeInstanceState：如果 Amazon EC2 執行個體在變更執行個體類型之前已執行，請啟動該執行個體。
  - 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，執行個體就會變回其原始執行個體類型。
    - aws:changeInstanceState：先停止 Amazon EC2 執行個體，再將其變更為原始執行個體類型。
    - aws:changeInstanceState：強制 Amazon EC2 執行個體停止，然後再將其變更為原始執行個體類型，以防卡在停止狀態。
    - aws:executeAwsApi：將 Amazon EC2 執行個體變更為其原始類型。
    - aws:sleep: 為了達到最終一致性，變更執行個體類型後等待 3 秒。
    - aws:changeInstanceState：如果 Amazon EC2 執行個體在變更執行個體類型之前已執行，請啟動該執行個體。
    - aws:waitForAwsResourceProperty：等待 Amazon EC2 執行個體通過狀態檢查。
- 26aws:sleep：在結束手冊之前等待。

## AWSSupport-RestoreEC2InstanceFromSnapshot

### Description (描述)

執行手AWSSupport-RestoreEC2InstanceFromSnapshot冊可協助您從根磁碟區的運作中亞馬遜彈性區塊存放區 (Amazon EBS) 快照識別和還原 Amazon 彈性運算雲端 (Amazon EC2) 執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化



## 擁有者

Amazon

平台

Linux, macOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- EndDate

類型：字串

說明：(選擇性) 您希望自動化操作尋找快照的最後日期。

- InplaceSwap

類型：布林值

有效值：true | false

說明：(選擇性) 如果此參數的值設為 true，則從快照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

說明：(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

說明：(選擇性) 如果此參數的值設為true，則自動化會檢查從快照啟動的測試執行處理上是否失敗執行處理狀態檢查。

- SkipSnapshotsBy

類型：字串

說明：(選擇性) 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，而您為此參數指定值為 2，則每三個快照都會複查一次。

預設：0

- SnapshotId

類型：字串

說明：(選擇性) 您要從中還原執行個體的快照識別碼。

- StartDate

類型：字串

說明：(選擇性) 您希望自動化操作尋找快照的第一個日期。

- TotalSnapshotsToLook

類型：字串

說明：(選擇性) 自動化檢閱的快照數目。

## 必要的 IAM 許可

此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`-收集有關目標執行個體的詳細資料。
2. `aws:assertAwsResourceProperty`-驗證目標執行個體是否存在。
3. `aws:assertAwsResourceProperty`-驗證根磁碟區是否為 Amazon EBS 磁碟區。
4. `aws:assertAwsResourceProperty`-驗證目標此執行個體的另一個自動化作業尚未執行。
5. `aws:executeAwsApi`-標記目標實例。
6. `aws:executeAwsApi`-建立執AMI行個體。
7. `aws:executeAwsApi`-收集有關在上一步中AMI創建的詳細信息。
8. `aws:waitForAwsResourceProperty-available` 在繼續之前等待AMI狀態成為。
9. `aws:executeScript`-從新建立的執行個體啟動新執行個體AMI。
10. `aws:assertAwsResourceProperty`-驗證執行個體狀態為available。
11. `aws:executeAwsApi`-收集有關新啟動執行個體的詳細資料。
12. `aws:branch`-根據您是否為SnapshotId參數提供值進行分支。
13. `aws:executeScript`-傳回指定期間內的快照清單。
14. `aws:executeAwsApi`-停止執行個體。

- 15aws:waitForAwsResourceProperty-等待磁碟區狀態為available。
- 16aws: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-附加新的根磁碟區。
- 20aws:waitForAwsResourceProperty-等待要連接的新磁碟區。
- 21aws:executeAwsApi-啟動實例。
- 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，使用自動化識別的快照中新建立的磁碟區或使用您在SnapshotId參數中指定的快照建立的磁碟區來復原執行個體。
- 26aws:executeScript-刪除自動化操作所建立的資源。

## 輸出

launchCloneInstance.InstanceIds

ListSnapshotByDate. 最終快照

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot. 工作快照

InstanceRecovery. 結果。

## AWSSupport-SendLogBundleToS3Bucket

### Description (描述)

AWSSupport-SendLogBundleToS3Bucket執行手冊會將 EC2Rescue 工具產生的記錄服務包從目標執行個體上傳到指定的 S3 儲存貯體。執行手冊會根據目標執行個體的平台安裝 EC2Rescue 的平台特定版本。EC2Rescue 接著會用於收集所有可用的作業系統 (OS) 日誌。

### [運行此自動化 \(控制台\)](#)

## 文件類型

### 自動化

### 擁有者

Amazon

### 平台

Linux 系統 macOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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。

- S3 BucketName

類型：字串

描述：(必要) 供上傳日誌的 S3 儲存貯體。

- S3Path

類型：字串

預設值：AWSsupport-SendLogBundleToS3Bucket/

描述：(選用) 收集日誌的 S3 路徑。

### 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具有 IAM 角色，並附加了 ManagedInstanceCore 亞馬遜亞馬遜受管政策。用戶必須至少有 `ssm: StartAutomationExecution` 和 `ssm: SendCommand` 才能運行自動化並將命令發送到實例，再加上 `ssm: GetAutomationExecution` 才能讀取自動化輸出。

### 文件步驟

1. `aws:runCommand`-通過安裝 EC2 救援。AWS-ConfigureAWSPackage
2. `aws:runCommand`-使用 EC2Rescue 執行 PowerShell 指令碼以收集 Windows 疑難排解記錄檔。
3. `aws:runCommand`-使用 EC2Rescue 執行 bash 指令碼以收集 Linux 疑難排解記錄。

### 輸出

`collectAndUploadWindowsLogBundle` 輸出。

`collectAndUploadLinuxLogBundle` 輸出。

## AWSSupport-StartEC2RescueWorkflow

### Description

運行手 `AWSSupport-StartEC2RescueWorkflow` 冊運行提供的 base64 編碼腳本 ( Bash 或 Powershell ) 上創建的幫助程序實例來營救您的實例。執行個體的根磁碟區會連接並掛接至輔助程式執行個體，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 設置一些環境變量，您可以在你的腳本中使用。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。

### [運行此自動化 \( 控制台 \)](#)

#### Important

此自動化不支援從 Marketplace Amazon 機器映像 (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
\$ 環境:EC2RESCUE_ID ACCOUNT	{{全球:ACCOUNT_ID}}	123456789012
\$ 環境:_ EC2RESCUE DATE	{{全球:DATE}}	2018-09-07
\$ 環境:EC2RESCUE__ DATE TIME	{{全球:DATE_TIME}}	2018-09-07_18.09.59
\$ 環境:EC2RESCUE__ EC2RW DIR	EC2Rescue適用於視窗安裝路 徑	C:\Program 文件\ Amazon\ EC2Rescue
\$ 環境:EC2RESCUE__ EC2RW DIR	EC2Rescue適用於視窗安裝路 徑	C:\Program 文件\ Amazon\ EC2Rescue
\$ 環境:EC2RESCUE_ID EXECUTION	{{自動化:EXECUTION_ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
\$ 環境 : EC2RESCUE__ OFFLINE _ CURRENT _ CONTROL SET	離線 Windows 目前控制集路徑	HKLM:\AWSTempSystem \ControlSet001
\$ 環境:EC2RESCUE__ OFFLINE DRIVE	離線 Windows 磁碟機字母	D:\
\$ 環境 : EC2RESCUE__ OFFLINE _ EBS DEVICE	離線根磁碟區EBS裝置	xvdf
\$ 環境 : EC2RESCUE__ OFFLINE _ KERNEL VER	離線 Windows 核心版本	6.1.7601.24214

變數	描述	範例值
\$ 環境:EC2RESCUE_ 作業系統 _ OFFLINE ARCHITECTURE	離線 Windows 架構	AMD64
\$ 環境:EC2RESCUE_ 作業系統 _ OFFLINE CAPTION	離線 Windows 字幕	Windows Server 2008 R2 Datacenter
\$ 環境:EC2RESCUE_ 作業系統 _ OFFLINE TYPE	離線 Windows 作業系統類型	Server
\$ 環境 : EC2RESCUE_ _ OFFLINE _ PROGRAM _ FILES DIR	離線 Windows 程式檔案目錄路徑	D:\Program Files
\$ 環境:EC2RESCUE_ _ OFFLINE _ X 86 PROGRAM _ FILES DIR	離線 Windows 程式檔案 x86 目錄路徑	D:\Program Files (x86)
\$ 環境 : EC2RESCUE_ _ OFFLINE _ REGISTRY DIR	離線 Windows 登錄檔目錄路徑	D:\Windows\System32\config
\$ 環境 : EC2RESCUE_ _ OFFLINE _ SYSTEM ROOT	離線 Windows 系統根目錄路徑	D:\Windows
\$ 環境:_ EC2RESCUE REGION	{{全球:REGION}}	us-west-1
\$ 環境:EC2RESCUE_S3 _ BUCKET	{{S3BucketName }}	安贊-S3-演示桶
\$ 環境:EC2RESCUE_S3 _ PREFIX	{{ S3Prefix }}	myprefix/
\$ 環境:EC2RESCUE_ _ SOURCE INSTANCE	{{ InstanceId }}	i-abcdefgh123456789



變數	描述	範例值
\$ 腳本 : 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
EC2RESCUEACCOUNT_ 身 份證	{{全球:ACCOUNT_ID}}	123456789012
EC2RESCUE_DATE	{{全球:DATE}}	2018-09-07
EC2RESCUE_DATE_TIME	{{全球:DATE_TIME}}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	EC2Rescue適用於 Linux 安裝 路徑	/usr/local/ec2rl-1.1.3
EC2RESCUEEXECUTION_ 身份證	{{自動化: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	{{全球:REGION}}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3BucketName }}	安贊-S3-演示桶
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/

變數	描述	範例值
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

說明：(選擇性) 備份AMI名稱的前置詞。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- CreatePostEC2RescueBackup

類型：字串

有效值：true | false

預設：false

說明：(選擇性) 將其設定`true`為在執行指令碼AMI之 `InstanceId`後建立的，然後再啟動指令碼。自動化完成後，AMI將持續存在。您有責任安全地存取AMI或刪除它。

- `CreatePreEC2RescueBackup`

類型：字串

有效值：`true` | `false`

預設：`false`

說明：(選擇性) 將其設定`true`為 `InstanceId`在執行指令碼AMI之前建立的。自動化完成後，AMI將持續存在。您有責任安全地存取AMI或刪除它。

- `EC2RescueInstanceType`

類型：字串

有效值：2. 小 | 2. 中等

預設：`t2.small`

說明：(選擇性) EC2 執行處理的執行`EC2Rescue`個體類型。

- `InstanceId`

類型：字串

說明：( 必填 ) EC2執行個體的 ID。IMPORTANT：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。如果您的源代碼實例是 Linux，並且是 Windows，PowerShell 請使用 Bash。

- `S3 BucketName`

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

預設值：SelectedInstanceSubnet

說明：(選擇性) 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。IMPORTANT：如果您提供自訂子網路，則該子網路必須與位於相同的可用區域中 InstanceId，且必須允許存取SSM端點。

- UniqueId

類型：字串

預設值：{{自動化：EXECUTION\_ID}}

描述：(選用) 自動化操作的唯一識別碼。

## 所需IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

建議執行自動化操作的使用者附加 AmazonSSMAutomation Role IAM 受管理的原則。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`-描述提供的實例
2. `aws:executeAwsApi`-描述提供的執行個體的根磁碟區
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 ID
  - a. ( 使用當前實例子網 ) -如果 \* SubnetId = SelectedInstanceSubnet \* 則運行`aws:createStack`以部署EC2Rescue CloudFormation堆棧
  - b. ( 創建新的VPC ) -如果 \* SubnetId = CreateNew VPC \* 則運行`aws:createStack`以部署EC2Rescue CloudFormation堆棧
  - c. (使用自訂子網路) - 所有其他情況 :

`aws:assertAwsResourceProperty`-檢查提供的子網路是否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輔助程式執行個體
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代管執行個體
11. `aws:changeInstanceState`-停止提供的實例
12. `aws:changeInstanceState`-停止提供的實例
13. `aws:changeInstanceState`-強制停止提供的實例
14. `aws:assertAwsResourceProperty`-檢查 `CreatePreEC2RescueBackup` 輸入值
  - a. ( 創建預EC2Rescue備份 ) -如果 `* CreatePre EC2RescueBackup = 真 *`
  - b. `aws:executeAwsApi`-創建提供實例的AMI備份
  - c. `aws:createTags`-標記AMI備份
15. `aws:runCommand`-在EC2Rescue輔助實例EC2Rescue上安裝
16. `aws:executeAwsApi`-將根磁碟區從提供的執行個體分離
17. `aws:assertAwsResourceProperty`-檢查提供的實例平台
  - a. (執行個體為 Windows) :
    - `aws:executeAwsApi`-以 `*xvdf*` 形式將根磁碟區連接至EC2Rescue輔助程式執行個體
    - `aws:sleep`-睡眠 10 秒鐘
    - `aws:runCommand`-在 PowerShell 中運行提供的離線腳本
  - b. (執行個體為 Linux) :
    - `aws:executeAwsApi`-以 `*/dev/sdf*` 形式將根磁碟區連接至EC2Rescue輔助程式執行個體
    - `aws:sleep`-睡眠 10 秒鐘
    - `aws:runCommand`-在 Bash 中運行提供的離線腳本
18. `aws:changeInstanceState`-停止EC2Rescue協助程式執行個體
19. `aws:changeInstanceState`-強制停止EC2Rescue協助程式執行個體
20. `aws:executeAwsApi`-從EC2Rescue輔助程式執行個體中分離根磁碟區
21. `aws:executeAwsApi`-將根磁碟區連接回提供的執行個體

22aws:assertAwsResourceProperty-檢查 CreatePostEC2RescueBackup輸入值

- a. ( 創建後EC2Rescue備份 ) -如果 \* CreatePost EC2RescueBackup = 真 \*
- b. aws:executeAwsApi-創建提供實例的AMI備份
- c. aws:createTags-標記AMI備份

23aws:executeAwsApi-針對所提供執行個體的根磁碟區，還原終止狀態的初始刪除

24aws:changeInstanceState-恢復所提供實例的初始狀態 ( 運行/停止 )

25aws:deleteStack-刪除EC2Rescue CloudFormation 堆疊

輸出

runScriptFor輸出

runScriptFor視窗輸出

preScriptBackup.ImageId

postScriptBackup.ImageId

## AWSPremiumSupport-TroubleshootEC2DiskUsage

Description (描述)

AWSPremiumSupport-TroubleshootEC2DiskUsage執行手冊可協助您調查 Amazon 彈性運算雲端 (Amazon EC2) 執行個體根和非根磁碟用量的問題，並可能修復問題。如果可能的話，runbook 會嘗試藉由延伸磁碟區及其檔案系統來修復問題。若要執行這些工作，此 runbook 會根據受影響執行個體的作業系統，協調數個 Runbook 的執行。

第一個 runbook (AWSPremiumSupport-DiagnoseDiskUsageOnWindows或AWSPremiumSupport-DiagnoseDiskUsageOnLinux) 決定是否可以藉由擴充磁碟區來緩解磁碟問題。

第二個 Runbook，AWSPremiumSupport-ExtendVolumesOnWindows或AWSPremiumSupport-ExtendVolumesOnLinux，使用第一個工作手冊的輸出來執行修改磁碟區的 Python 程式碼。修改磁碟區之後，runbook 會延伸受影響磁碟區的磁碟分割和檔案系統。



**⚠ 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 Support方案](#)。

本文件是與AWS Managed Services ( AMS ) 合作構建的。AMS 可協助您更有效率且安全地管理AWS 基礎架構。AMS 還提供營運彈性、增強的安全性與合規性、容量最佳化，以及節省成本的識別功能。如需詳細資訊，請參閱[AWS Managed Services](#)。

[運行此自動化 \( 控制台 \)](#)

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：^ 我-[一個 Z0-9] {8,17}

說明：( 必填 ) 您的亞馬遜 EC2 執行個體的 ID。

- VolumeExpansionEnabled

類型：布林值

說明:(選擇性) 用來控制文件是否要延伸受影響的磁碟區和分割區的旗標。

預設：true

- VolumeExpansionUsageTrigger

類型：字串

說明：(選擇性) 觸發擴充功能所需的最小分割區空間使用量 (以百分比表示)。

允許的值：^ [0-9] {1,2}

預設值：85

- VolumeExpansionCapSize

類型：字串

說明：(選用) 亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區將增加到的大小上限 (以 GiB 為單位)。

允許的值：^ [0-9] {1,4}

預設值：

- VolumeExpansionGibIncrease

類型：字串

描述：(選擇性) 磁碟區的 GiB 增加。VolumeExpansionGibIncrease和之間的最大淨增幅 VolumeExpansionPercentageIncrease將被使用。

允許的值：^ [0-9] {1,4}

預設：20

- VolumeExpansionPercentageIncrease

類型：字串

說明：(選擇性) 增加磁碟區的百分比。VolumeExpansionGibIncrease和之間的最大淨增幅 VolumeExpansionPercentageIncrease將被使用。

允許的值：^ [0-9] {1,2}

預設：20

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

## 必要的 IAM 許可

此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系統管理員管理
2. aws:executeAwsApi-描述要取得平台的執行個體。
3. aws:branch-基於實例平台的分支自動化。

- a. 如果執行個體是視窗：
  - i. `aws:executeAutomation`-執行 `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` runbook 以診斷執行個體上的磁碟使用問題。
  - ii. `aws:executeAwsApi`-取得先前自動化的輸出。
  - iii. `aws:branch`-根據診斷的輸出進行分支，以及是否有可以擴展以減輕警報的卷。
    - A. 沒有需要擴充的磁碟區：結束自動化。
    - B. 有些磁碟區需要擴充：
      - I. `aws:executeAwsApi`-建立執行個體的 Amazon Machine Image (AMI)。
      - II. `aws:waitForAwsResourceProperty`-等待AMI國家是available。
      - III. `aws:executeAutomation`-運行 `AWSPremiumSupport-ExtendVolumesOnWindows` runbook 以執行卷修改以及操作系統 ( OS ) 中所需的步驟，以使新的空間可用。
- b. ( 平台不是窗口 ) 如果輸入實例不是 Windows：
  - i. `aws:executeAutomation`-執行 `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` runbook 以診斷執行個體上的磁碟使用問題。
  - ii. `aws:executeAwsApi`-取得先前自動化的輸出。
  - iii. `aws:branch`-根據診斷的輸出進行分支，以及是否有可以擴展以減輕警報的卷。
    - A. 沒有需要擴充的磁碟區：結束自動化。
    - B. 有些磁碟區需要擴充：
      - I. `aws:executeAwsApi`-建立執AMI行個體。
      - II. `aws:waitForAwsResourceProperty`-等待AMI狀態是。available
      - III. `aws:executeAutomation`-運行 `AWSPremiumSupport-ExtendVolumesOnLinux` runbook 以執行卷修改以及操作系統中所需的步驟，以使新的空間可用。

## 輸出

`diagnoseDiskUsageAlertOnWindows`輸出。

`extendVolumesOn`視窗輸出

`diagnoseDiskUsageAlertOnLinux`輸出。

`extendVolumesOn`輸出

備份軟件。 `Imageld`

備份程式視窗。Imageld

## AWSsupport-TroubleshootEC2InstanceConnect

### Description

AWSsupport-TroubleshootEC2InstanceConnect 自動化有助於分析和偵測錯誤，防止使用 Amazon 執行個體 [Connect 到 Amazon 彈性運算雲端 \(AmazonEC2\) 執行個體](#) 的連線。它可識別不受支援的 Amazon Machine Image (AMI)、遺失作業系統層級套件安裝或組態、遺失 AWS Identity and Access Management (IAM) 許可或網路組態問題所造成的問題。

它是如何工作的？

執行手冊採用 Amazon EC2 執行個體 ID、使用者名稱、連線模式、來源 IP CIDR、Connect SSH 埠和 Amazon 資源名稱 (ARN)，以供 IAM 角色或使用者使用 Amazon EC2 執行個體連接時遇到問題。然後，它會檢查使用 Amazon 執行個體 Connect 至 Amazon EC2 執行個體的 [先決條件](#)：

- 執行個體正在執行且處於健康狀態良好的狀態。
- 執行個體位於 Amazon 執行個體 Connect 支援的 AWS 區域中。
- AMI 的執行個體是由 Amazon 執行個體 Connect 支援。
- 執行個體可連線至執行個體中繼資料服務 (IMDSv2)。
- Amazon EC2 執行個體 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 ACL、網路和路由表規則) 允許透過 Amazon In EC2 stance Connect 連線至執行個體。
- 用來利用 Amazon EC2 執行個體 Connect 的 IAM 角色或使用者可以存取 Amazon EC2 執行個體的推送金鑰。

### Important

- 若要檢查執行個體 AMI、可 Connect IMDSv2 性和 Amazon EC2 執行個體連接套件安裝，必須 SSM 管理執行個體。否則，它會跳過這些步驟。如需詳細資訊，請參閱 [為什麼我的 Amazon EC2 執行個體不顯示為受管節點](#)。
- 僅當提供為輸入參數時，網路檢查才會偵測安全群組和網路 ACL 規則 SourceIPCIDR 是否封鎖流量。否則，它只會顯示 SSH 相關規則。
- 使用 [Amazon EC2 執行個體連線端點的連線](#) 不會在此執行手冊中進行驗證。

- 對於私人連線，自動化操作不會檢查SSH用戶端是否已安裝在來源機器上，以及是否可以連線到執行個體的私有 IP 位址。

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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操作：

1. 導覽至主 AWS Systems Manager 控制台 [AWSSupport-TroubleshootEC2InstanceConnect](#) 中的。

2. 選擇 Execute automation (執行自動化)。

3. 對於輸入參數，請輸入以下內容：

- InstanceId (必填)：

您無法使用 Amazon EC2 執行個體 Connect 到的目標 Amazon EC2 執行個體識別碼。

- AutomationAssumeRole (選擇性)：

可讓 Systems Manager 自動化代表您執行動作的IAM角色。ARN如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 使用者名稱 (必填)：

用於使用 Amazon 執行個體 Connect 到 Amazon EC2 執行個體的使用者名稱。EC2它是用來評估，如果IAM訪問被授予這個特定的用戶。

- EC2InstanceConnectRoleOrUser (必填)：

利用 Amazon EC2 執行個體 Connect 將金鑰推送至執行個體ARN的IAM角色或使用者。

- SSHPort(選擇性)：

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兩者之間1-65535。

- SourceNetworkType (選擇性)：

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。
  - 公用：您可以透過網際網路 (例如，您的本機電腦) 連線至公用子網路中的執行個體。
  - 私人：您可以透過執行個體的私有 IP 位址進行連線。
- SourceIpCIDR(選擇性)：

包CIDR含您將使用 Amazon EC2 執行個體 Connect 登入的裝置 (例如您的本機電腦) IP 位址的來源。範例：二零一七年三十一月三十八日 如果沒有提供公有或私有存取模式的值，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。它將顯示SSH相關的規則。

**Input parameters**

**InstanceId**  
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.

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.

**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.

**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.

**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.

**SSHPort**  
(Optional) The SSH port configured on the EC2 instance. Default value is '22'. The port number must be between '1-65535'.

**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.

#### 4. 選取執行。

#### 5. 自動化啟動。

#### 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，自動化結束。

- GetInstanceProperties:

取得目前 Amazon EC2 執行個體屬性 (PlatformDetails PublicIpAddress Vpclid、SubnetId 和 MetadataHttpEndpoint)。

- GatherInstanceInformationFromSSM:

如果執行個體SSM受管 Systems Manager，則會取得系統管理員執行個體的 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 執行個體 Connect 的 AWS 區域中。

- BranchOnIfAWSRegionSupported:

如果 Amazon 執行EC2個體 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 執行個體 Connect 是否支援與執行EC2個體AMI相關聯的項目。

- BranchOnIfInstanceAMIsSupported:



如果執行個AMI體受支援，它會執行作業系統層級檢查，例如中繼資料可達性和 Amazon EC2 執行個體 Connect 套件安裝和設定。否則，它會檢查HTTP中繼資料是否使用啟用 AWS API，然後進入網路檢查步驟。

- C heckIMDSReachabilityFromOs:

在目標 Amazon EC2 Linux 實例上運行一個 Bash 腳本，以檢查它是否能夠到達IMDSv2.

- C heckEICPackage 安裝方式：

在目標 Amazon EC2 Linux 執行個體上執行 Bash 指令碼，以檢查 Amazon EC2 執行個體 Connect 套件是否已正確安裝和設定。

- C heckSSHConfigFromOs:

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。

- C heckEICNetwork 存取權限：

檢查網路組態 (安全群組ACL、網路和路由表規則) 是否允許透過 Amazon In EC2 stance Connect 連線至執行個體。

- C heckIAMRoleOrUserPermissions:

檢查用於利用 Amazon EC2 執行個體 Connect 的IAM角色或使用者是否可以使用提供的使用者名稱將金鑰推送至 Amazon EC2 執行個體。

- MakeFinalOutput:

合併所有先前步驟的輸出。

## 7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

目標執行處理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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

## AWS 服務文件

- [如何解決使用 Amazon 執行個體 Connect 到 Amazon EC2 執行EC2個體的問題？](#)

## AWSsupport - TroubleshootLinuxMGNDRAgentLogs

## Description

AWSSupport-TroubleshootLinuxMGNDRAgentLogs 自動化 runbook 用於在 Linux 服務器中安裝 AWS Application Migration Service ( AWS MGN ) 和 AWS Elastic Disaster Recovery ( AWS DRS ) 複製代理以將源服務器遷移到 AWS 雲時檢測常見錯誤。

它是如何工作的？

該 runbook AWSSupport-TroubleshootLinuxMGNDRAgentLogs 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` 作為參數上傳。然後，它會執行下列工作：

- 驗證：檢查提供的記錄檔是否有效，以及是否包含至少一個代理程式安裝。
- 剖析：徹底剖析記錄檔中最新的代理程式安裝是否有已知 AWS MGN 或 AWS DRS 錯誤。
- 錯誤偵測和解決方法：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。對於每個偵測到的錯誤，runbook 會提供詳細的步驟，以協助解決或緩解問題。

## [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Linux

參數

必要的 IAM 權限

此 `AutomationAssumeRole` 參數需要執行下列動作，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操作：

1. 瀏覽至「文件」下 [AWSsupport-TroubleshootLinuxMGNDRSAGENTLOGS](#) 的「Systems Manager」。

2. 選擇 Execute automation (執行自動化)。

3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- BucketName (必填)：

存放複寫代理程式日誌之 Amazon S3 儲存貯體的名稱。

- S3ObjectKey (必要)：

存放複寫代理程式安裝程式日誌檔的 Amazon S3 物件金鑰。範例：如果URI是 Amazon S3s3://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 (必填)：

安裝複寫代理程式的服務名稱。允許的值：AWS MGN 或 AWS DRS

Input parameters	
<p><b>AutomationAssumeRole</b> (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.</p> <input type="text"/>	<p><b>BucketName</b> (Required) The name of the Amazon S3 bucket where the replication agent log is stored.</p> <input type="text" value="s3bucket-name"/>
<p><b>S3ObjectKey</b> (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is `s3://bucket_name/path/to/file/aws_replication_agent_installer.log` then you should provide `path/to/file/aws_replication_agent_installer.log` as input.</p> <input type="text" value="aws_replication_agent_installer.log"/>	<p><b>ServiceName</b> (Required) The name of the service for which the Replication agent is done: <b>**AWS MGN**</b>: AWS Application Migration Service. <b>**AWS DRS**</b>: AWS Elastic Disaster Recovery.</p> <input type="text" value="AWS MGN"/>

4. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- ValidateInput**

確保複寫代理程式日誌檔有效且可使用提供的 Amazon S3 儲存貯體名稱和物件的路徑存取，然後傳回最新代理程式安裝的位元組編號。

- **CheckReplicationAgentLogErrors**

從最新的安裝位元組開始讀取複寫代理程式記錄檔，並搜尋已知 AWS MGN 或 AWS DRS 錯誤。

- **MakeFinalOutput**

建立先前檢查的輸出，包括找到的錯誤的相關資訊和疑難排解建議。

## 7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

### ▼ 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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

## AWSsupport-TroubleshootRDP

### Description (描述)

R AWSSupport-TroubleshootRDP unbook 可讓使用者檢查或修改目標執行個體上的一般設定，這些設定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。默認情況下，runbook 讀取並輸出設置的值。

### Important

對 RDP 設置，RDP 服務和 Windows 防火牆配置文件的更改應仔細檢查使用此手冊之前。

## [運行此自動化 \(控制台\)](#)

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 | 自訂

預設：Custom

描述：(選用) [自訂] 使用防火牆、RDP、RDP ServiceStartupType、RDP ServiceAction、NLA 中的值PortAction，SettingAction並管理設RemoteConnections定。[CheckAll] 讀取設置的值而不更改它們。[FixAll] 恢復 RDP 默認設置，並禁用視窗防火牆。

- 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

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- 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。

- NLA SettingAction

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)。

- RDP PortAction

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。

- RDP ServiceAction

類型：字串

有效值：檢查 | 開始 | 重新啟動 | 強制重新啟動

預設：Check

說明：(選擇性) 檢查、啟動、重新啟動或強制重新啟動 RDP 服務 ()。TermService

- RDP ServiceStartupType

類型：字串

有效值：檢查 | 自動

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：核取 | 啟用

預設：Check

描述：(選用) 在 fDenyTSConnections 設定上執行的動作：Check，Enable。

- S3 BucketName

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



預設值：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 自動化會建立新的 VPC。重要：子網路必須與位於相同的可用區域中 InstanceId，且必須允許存取 SSM 端點。

## 必要的 IAM 許可

此 AutomationAssumeRole 參數需要執行下列動作，才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具有 IAM 角色，並附加了 ManagedInstanceCore 亞馬遜亞馬遜受管政策。對於線上修復，使用者必須具有至少 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution 和 ssm: SendCommand，才能執行自動化並將命令傳送 SendCommand 至執行個體，再加上 ssm: GetAutomationExecution 才能讀取自動化輸出。對於離線補救，使用者必須具有至少 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution、ec2: DescribeInstances，GetAutomationExecution 才能讀取自動化輸出。AWSSupport-TroubleshootRDP 執行 AWSSupport-ExecuteEC2Rescue 行離線修復的呼叫-請檢閱的權限，以確保 AWSSupport-ExecuteEC2Rescue 保您可以成功執行自動化操作。

## 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代管執行個體
3. (線上疑難排解) 若執行個體為受管執行個體，則：
  - a. aws:assertAwsResourceProperty-檢查提供的操作值
  - b. (線上檢查) 如果「作業」= CheckAll，則：

aws:runPowerShellScript-執行 PowerShell 指令碼以取得 Windows 防火牆資料檔狀態。

aws:executeAutomation-獲取 AWSSupport-ManageWindowsService 取 RDP 服務狀態的呼叫。

aws:executeAutomation-呼叫 AWSSupport-ManageRDPSettings 以獲取 RDP 設置。

- c. (線上修正) 如果動作 = 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-通話AWSSupport-ManageRDPSettings`以啟用遠程連接並禁用 NLA。

d. (線上管理) 若 Action = Custom ，則：

`aws:runPowerShellScript`-執行指PowerShell令碼以管理 Windows 防火牆設定檔。

`aws:executeAutomation-呼叫AWSSupport-ManageWindowsService`以管理 RDP 服務。

`aws:executeAutomation-AWSSupport-ManageRDPSettings` 用於管理 RDP 設置的呼叫。

4. (離線修復) 如果執行個體不是受管執行個體，則：

a. `aws:assertAwsResourceProperty`-斷言 AllowOffline= 真

b. `aws:assertAwsResourceProperty`-斷言動作 = FixAll

c. `aws:assertAwsResourceProperty`-斷言的值 SubnetId

(使用提供的執行個體的子網路) 如果SubnetId已選取 \_INSTANCE\_子網路

`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的子網路執行。

d. (使用提供的自訂子網路) 如果未選取 \_INST SubnetId ANCE\_子網路

`aws:executeAutomation-AWSSupport-ExecuteEC2Rescue` 使用提供的SubnetId值運行。

## 輸出

`manageFirewallProfiles`輸出。

管理員. 輸ServiceSettings出

`manageRDPSettings.Output`

`checkFirewallProfiles`輸出。

檢查 RDP. 輸ServiceSettings出

`checkRDPSettings.Output`

`disableFirewallProfiles`輸出。

## 還原預設輸出 ServiceSettings

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

疑難排解輸出 OfflineWithSubnetId

## AWSSupport-TroubleshootSSH

### Description (描述)

AWSSupport-TroubleshootSSH執行手冊會安裝適用於 Linux 的亞馬遜 EC2Rescue 工具，然後使用 EC2Rescue 工具檢查或嘗試修正阻止透過 SSH 遠端連線至 Linux 機器的常見問題。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。依預設，Runbook 會以唯讀模式運作。

### [運行此自動化 \(控制台\)](#)

如需使用 AWSSupport-TroubleshootSSH runbook 的相關資訊，請參閱進AWS階支援中的這個[AWSSupport-TroubleshootSSH疑難排解主題](#)。

### 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

預設值：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

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

描述：(必要) Linux 之 EC2 執行個體的 ID。

- S3 BucketName

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

預設值：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 自動化會建立新的 VPC。

**⚠ Important**

子網路必須與位於相同的可用區域InstanceId，而且必須允許 SSM 端點的存取。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

建議接收命令的 EC2 執行個體具有 IAM 角色，並附加了ManagedInstanceCore亞馬遜亞馬遜受管政策。對於線上修復，使用者必須具有至少 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution 和 ssm: SendCommand，才能執行自動化並將命令傳送SendCommand至執行個體，再加上 ssm: GetAutomationExecution才能讀取自動化輸出。對於離線補救，使用者必須具有至少 ssm: DescribeInstanceInformation、ssm: StartAutomationExecution、ec2: DescribeInstances，GetAutomationExecution才能讀取自動化輸出。AWSSupport-TroubleshootSSH執AWSSupport-ExecuteEC2Rescue行離線修復的呼叫-請檢閱的權限，以確保AWSSupport-ExecuteEC2Rescue保您可以成功執行自動化操作。

## 文件步驟

1. aws:assertAwsResourceProperty-檢查執行個體是否為代管執行個體
  - a. (線上修復) 如果執行個體是受管執行個體，則：
    - i. aws:configurePackage-通過安裝 EC2 救援 AWS-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-斷言 AllowOffline= 真
    - ii. aws:assertAwsResourceProperty-斷言動作 = FixAll
    - iii. aws:assertAwsResourceProperty-斷言的值 SubnetId
    - iv. ( 使用提供的實例的子網 ) 如果SubnetId是SelectedInstanceSubnet我們使aws:executeAutomation用提供AWSSupport-ExecuteEC2Rescue的實例的子網運行。
    - v. ( 使用提供的自定義子網 ) 如果SubnetId不SelectedInstanceSubnet使aws:executeAutomation用提供AWSSupport-ExecuteEC2Rescue的SubnetId值運行。

## 輸出

troubleshootSSH.Output

troubleshootSSHOffline.Output

疑難排解。輸出 OfflineWithSubnetId

## AWSSupport-TroubleshootSUSERegistration

### Description (描述)

執行手AWSSupport-TroubleshootSUSERegistration冊可協助您識別向 SUSE 更新基礎設施註冊 Amazon 彈性運算雲端 (Amazon SUSE Linux Enterprise Server EC2) 執行個體失敗的原因。自動化輸出提供解決或協助您疑難排解問題的步驟。如果執行個體在自動化期間通過所有檢查，則執行個體會向 SUSE 更新基礎結構註冊。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux

#### 參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許系統管理員自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，系統管理員自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您要疑難排解之 Amazon EC2 執行個體的 ID。

### 必要的 IAM 許可

此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`-檢查亞馬遜 EC2 實例平台是否為SLES。
- `aws:runCommand`-檢查套件cloud-regionsrv-client版本是否大於或等於所需版本 9.0.10。
- `aws:runCommand`-檢查基礎產品的符號鏈接是否損壞，並修復其損壞的鏈接。
- `aws:runCommand`-檢查 hosts 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curl命令是否已安裝。
- `aws:runCommand`-檢查亞馬遜 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 連線至少 1 個區域伺服器。
- `aws:runCommand`-檢查 Amazon EC2 執行個體是否可以透過 HTTP 連線到訂閱管理工具 (SMT) 伺服器。
- `aws:runCommand`-檢查 Amazon EC2 執行個體是否可以透過 HTTPS 連線到達訂閱管理工具 (SMT) 伺服器。

- `aws:runCommand`-檢查亞馬遜 EC2 實例是否可以通過 HTTPS 訪問該 `smt-ec2.susecloud.net` 地址。
- `aws:runCommand`-使用 SUSE 更新基礎設施註冊 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

執行手冊 `AWSSupport-TroubleshootWindowsPerformance` 可協助疑難排解 Amazon 彈性運算雲端 (Amazon EC2) Windows 執行個體上持續的效能問題。runbook 會擷取目標執行個體的記錄檔，並分析 CPU、記憶體、磁碟和網路效能指標。或者，自動化可以擷取處理作業傾印，以協助您判斷效能降低的潛在原因。自動化還捕獲事件和系統日誌通過使用最新的 [EC2Rescue](#) 工具，如果你允許這個 runbook 安裝它。

它是如何工作的？

執行手冊執行下列步驟：

- 檢查 Amazon EC2 執行個體是否有先決條件。
- 在 Amazon EC2 Windows 執行個體的根磁碟中產生效能日誌
- 將擷取的記錄儲存在資料 C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance
- 如果提供 Amazon Simple Storage Service (Amazon S3) 儲存貯體，且自動化假設角色具有所需的許可，則擷取的日誌會上傳到 Amazon S3 儲存貯體。
- 如果您選擇安裝 Amazon EC2 Windows 執行個體，請將最新 EC2Rescue 工具安裝到 Amazon Windows 執行個體以擷取事件和系統日誌，但不會分析所擷取的程序傾印和日誌 EC2Rescue。

### Important

- 若要執行此執行手冊，Amazon EC2 視窗執行個體必須由 AWS Systems Manager 管理。如需詳細資訊，請參閱 [為什麼我的 Amazon EC2 執行個體不顯示為受管節點](#)。
- 要執行此手冊，Amazon EC2 視窗實例必須在版本上運行視窗 8.1 / 視窗服務器 2012 R2 ( 6.3 ) 或更高版本 PowerShell 4.0 或更高版本。如需詳細資訊，請參閱 [Windows 作業系統版本](#)。



- 若要產生效能記錄，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處理程序，則可用空間必須大於 10 GB，再加上處理程序消耗超過 10 GB 記憶體時，處理序使用的總記憶體大小。
- 系統不會自動刪除根裝置上產生的記錄。
- 工作流程簿不會解除安裝該EC2Rescue工具。如需詳細資訊，請參閱[用EC2Rescue於Windows 伺服器](#)。
- 最佳做法是在效能影響期間執行此自動化。您也可以使用 AWS Systems Manager 狀態管理員關聯或排程 AWS Systems Manager 維護視窗來定期執行它。

## [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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

(選擇性) 附加在執行個體設定檔或執行個體上設定的IAM使用者上的IAM角色需要執行下列動作，才能將日誌上傳到為參數指定的 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操作：

1. 瀏覽至「文件」下 [AWSSupport-TroubleshootWindowsPerformance](#) 的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - InstanceId ( 必填 )：

您要在其中執行自動化的目標 Amazon EC2 Windows 執行個體的識別碼。執行個體必須由系統管理員管理，才能執行自動化。
  - CaptureProcessDump (選擇性)：

要擷取的處理作業傾印類型。自動化可以為處理序擷取一個處理序傾印，這些處理程序可能會在自動化開始時造成效能影響。執行個體根磁碟區至少需要 10 GB 的可用空間 (當根磁碟區大小超

過 100 GB 時，超過磁碟大小的 10%，10 GB 加上處理程序消耗超過 10 GB 記憶體時所耗用的總記憶體大小)。

- **LogCaptureDuration** (選擇性) :

此自動化操作會在問題出現時擷取記錄檔的分鐘數 (介於1和15之間)。預設值為 5。

- **LogUploadBucketName** (選擇性) :

您帳戶中要上傳日誌的 Amazon S3 儲存貯體。值區必須設定伺服器端 encryption (SSE)，且儲存貯體政策不得將不必要的讀取/寫入權限授與不需要存取擷取記錄的對象。Amazon 視 EC2 窗執行個體必須能夠存取 Amazon S3 儲存貯體。

- **安裝EC2RescueTool** (可選) :

設定為 Yes 允許執行手冊安裝最新版本的 EC2Rescue 工具，以擷取 Windows 事件和系統記錄檔。預設值為 No。

- **確認 (必填):**

閱讀此自動化 runbook 執行的操作的完整詳細信息，如果您同意，請鍵入 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.

**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).

**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.

**LogUploadBucketName**  
(Optional) The Amazon S3 bucket in your account to upload the logs to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

**InstallEC2RescueTool**  
(Optional) Set it to 'True' if you allow the runbook to install the latest version of the 'EC2Rescue' tool to capture the Windows Events and System logs. Default value 'No'.

**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:**

確保只有一個執行此 runbook 針對實例。如果 runbook 找到另一個針對相同執行個體的執行，它會傳回錯誤並結束。

- **AssertInstanceIsWindows:**

斷言 Amazon EC2 實例在 Windows 操作系統上運行。否則，自動化結束。

- **AssertInstanceIsManagedInstance:**

聲明 Amazon EC2 執行個體由 AWS Systems Manager 管理。否則，自動化結束。

- **VerifyPrerequisites:**

驗證執行個體作業系統上的 PowerShell 版本，並確保執行個體可透過 Systems Manager 連線以執行 PowerShell 指令。這種自動化支持 PowerShell 4.0 及以上版本上運行視窗 8.1 / 服務器 2012 R2 ( 6.3 ) 或更高版本。如果版本較舊，則自動化會失敗。當您選擇將日誌上傳到 Amazon S3 儲存貯體時，此自動化會檢查 PowerShell 模組的 AWS 工具是否可用。如果沒有，自動化結束。

- **BranchOnProcessDump:**

根據您是否將其設置為捕獲影響性能的進程的轉儲進程的分支。

- **CaptureProcessDump:**

檢查執行個體是否有足夠的空間來執行此自動化操作 (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 效能錄製程式記錄。指令碼會在定義 LogCaptureDuration 的符合後停止。

- **SummarizePerformanceLogs:**

摘要列出上一個步驟產生的 XML 報告 CapturePerformanceLogs，以找出在自動化上顯示為輸出顯示最多 WorkingSet 64 (記憶體) 和 % 處理器時間 (CPU) 的負責處理程序。它生成類似的信息 LogicalDisk，網絡接口，內存，TCPv4，IPv4，UDPv4 並將其保存到輸出文件夾 analysis\_output.log 中。

- **BranchOnInstallEC2Rescue:**

如果您將其設置為在 Amazon EC2 實例中安裝最新 EC2Rescue 工具，則分支機構。

- **InstallEC2RescueTool:**

在執行個體作業系統中安裝 EC2Rescue 工具，以使用擷取 EC2Rescue 記錄檔 AWS-ConfigureAWSPackage。

- **RunEC2RescueTool:**

在執行個體作業系統中執行EC2Rescue工具，以擷取所需的所有記錄檔。EC2Rescue僅擷取必要的記錄檔以節省空間。

- **BranchOnIfS3BucketProvided:**

根據的使用者輸入進行分支，LogUploadBucketName以查看是否有值區名稱可用於上傳記錄檔。

- **GetS3BucketPublicStatus:**

判斷是否提供 Amazon S3 儲存貯體，如果是，請確認 Amazon S3 儲存貯體不是公開且已使用設定SSE。

- **UploadLogResult:**

將日誌上傳到提供的 Amazon S3 儲存貯體。如果 PowerShell 版本為 5.0 或更高版本，它會將日誌壓縮到ZIP存檔並上傳它們。它刪除上傳完成後的ZIP文件。如果 PowerShell 版本低於 5.0，它會將文件直接上傳到文件夾。

- **CleanUpLogsOnFailure:**

當步驟失敗時，會清除CapturePerformanceLogs步驟產生的所有記錄檔。如果SSM代理程式無法正常運作，或 Windows 系統沒有回應，此CleanUpLogsOnFailure步驟可能會失敗或逾時。

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

目標執行處理具有所有必要先決條件的執行。

**▼ Outputs**

CaptureProcessDump.Output  
No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output  
The instance has enough space to capture performance logs.  
WPR capture process is in 'Stopped' state.  
Data Collector Set TroubleshootWindowsPerformance [redacted] was not found.  
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance [redacted] .....  
Data Collector Set TroubleshootWindowsPerformance [redacted] created successfully.  
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance [redacted] .....  
Data Collector Set TroubleshootWindowsPerformance [redacted] started successfully.  
Current CPU usage is '54.73%' and Memory usage is '17.15%'  
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.  
Starting Windows Performance Recording (WPR) capture process.  
Stopping WPR capture process.  
WPR capture process is in 'Stopped' state.  
The Data Collector Set TroubleshootWindowsPerformance [redacted] is currently generating logs.  
The Data Collector Set TroubleshootWindowsPerformance [redacted] has finished generating logs and is currently in 'Stopped' state.  
Attempting to delete Data Collector Set TroubleshootWindowsPerformance [redacted] .....  
Data Collector Set TroubleshootWindowsPerformance [redacted] deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\ [redacted]  
The captured log files will not be deleted by this automation, please manually delete it after analysis.

RunEC2RescueTool.Output  
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\ [redacted]\_EC2Rescue\_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output  
Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.

Process	Counter	Min %	Max %	Avg %
sppsv	Processor	0.00	106.00	9.00
WmiPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenVclObj	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

CleanUpLogsOnFailure.Output  
No output available yet because the step is not successfully executed

CaptureProcessDump.Output  
No output available yet because the step is not successfully executed

RunEC2RescueTool.Output  
No output available yet because the step is not successfully executed

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

目標執行個體在 Linux 平台上且執行失敗的執行。您可以選取步驟 ID 以查看失敗詳細資訊。

**▼ Outputs**

CapturePerformanceLogs.Output  
No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output  
No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output  
No output available yet because the step is not successfully executed

VerifyPrerequisites.Output  
No output available yet because the step is not successfully executed

CaptureProcessDump.Output  
No output available yet because the step is not successfully executed

RunEC2RescueTool.Output  
No output available yet because the step is not successfully executed

UploadLogResult.Output  
No output available yet because the step is not successfully executed

**Execution status**

Overall status	All executed steps	# Succeeded
Failed	2	1
# Failed	# Cancelled	# TimedOut
1	0	0


**Executed steps (2)**

Find Steps

Step ID	Step #	Step name	Action	Status	Start time	End time
[redacted]	1	CheckConcurrency	aws:executeScript	Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
[redacted]0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

步驟的失敗詳細資訊AssertInstanceIsWindows。

**Failure details**

 **Failure message**  
Step fails when it is Execute/Canceling 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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

## AWSsupport-TroubleshootWindowsUpdate

### Description

AWSsupport-TroubleshootWindowsUpdate執行手冊是用來識別可能失敗的問題，Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體的 Windows 更新。

它是如何工作的？

執行手冊執行下列步驟：

- 檢查目標 Amazon EC2 執行個體是否由管理 AWS Systems Manager。
- 檢查系統管理員修補作業是否支援代理程式 (SSM 代理程式) 和 Windows 伺服器版本。AWS Systems Manager
- 檢查建議用於 Windows 更新的可用磁碟空間，以及重新開機是否處於擱置狀態。擱置中的重新啟動通常表示更新正在擱置中，並且在執行其他更新之前需要重新啟動。
- 在作業系統層級設定 Proxy 設定，這有助於疑難排解連線問題。
- 執行 Amazon Simple Storage Service (Amazon S3) 端點連線測試，並呼叫 [GetDeployablePatchSnapshotForInstance](#) API 操作以擷取受管節點使用之修補基準的目前快照。
- 如果連線失敗，提供執行手冊 [AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2](#) 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 伺服器更新服務 (WSUS) (如果適用)。

#### Important

- 不支援使用中目錄網域控制站。
- 不支援視窗伺服器 2008 R2 版或以前的版本。
- 不支援 SSM 代理程式 1.2.371 或之前的版本。
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2runbook 用來分析[VPC Reachability Analyzer](#)來源和服務端點之間的網路連線。您需要針對來源與目標之間執行的分析收費。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。
- 並非所有支援「Systems Manager」的地區都可使用 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

Windows

參數


必要的 IAM 許可

此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 `RunbookAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`，請新增[此文件](#)中列出的權限。

## 指示

請依照下列步驟設定自動化操作：

1. 瀏覽至「文件」下[AWSSupport-TroubleshootWindowsUpdate](#)的「Systems Manager」。

2. 選擇 `Execute automation` (執行自動化)。

3. 對於輸入參數，請輸入以下內容：

- `AutomationAssumeRole` (可選)：

(IAM) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARN)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `InstanceId` (必填)：

輸入視窗更新失敗的 Amazon EC2 執行個體識別碼。

- `RunVpcReachabilityAnalyzer` (可選)：

如果網路問題是由延伸檢查判斷，或指定 `true` 的執行個體 ID 不是代管執行個體，請指定執行 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 自動化操作。如需有關此子自動化的詳細資訊，請參閱[文件](#)。預設值為 `false`。

- `RetainVpcReachabilityAnalysis` (可選)：

只有相關 `RunVpcReachabilityAnalyzer`，如果是 `true`。指定 `true` 保留由建立的網路分析路徑和相關分析 `Reachability Analyzer`。依預設，這些資源會在成功分析後刪除。如果您選擇保留分析，子工作流程簿不會刪除分析，您可以在 Amazon VPC 主控台中將其視覺化。控制台鏈接將在子自動化輸出中可用。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的，AWS Systems Manager 並取得 SSM 代理程式版本和 Windows 版本的詳細資料。

- **assertIfInstanceIsSsmManaged:**

確保 Amazon EC2 實例由 AWS Systems Manager (SSM) 管理，否則自動化結束。

- **CheckProxy:**

檢查 Windows 執行個體的所有代理伺服器類型。

- **CheckPrerequisites:**

取得 SSM 代理程式版本和 Windows 版本，並判斷它是否為使用中目錄網域控制站 (DC)。如果執行個體是 DC 或 SSM 代理程式或 Windows 版本不受支援，執行手冊就會停止。

- **CheckDiskSpace:**

取得並驗證 Windows 執行個體上的可用磁碟空間 (如果它足以執行 Windows 更新)。

- **CheckPendingReboot:**

檢查 Windows 執行個體上是否有擱置中的重新開機。

- **CheckS3Connectivity:**

檢查執行個體是否可以連接的 Amazon S3 端點Patchbaseline。

- **branchOnRunVpcReachabilityAnalyzer:**

如果RunVpcReachabilityAnalyzer是 true，則它會分支自動化以執行更深入的分析，以偵錯 Amazon S3 連線。

- **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 runbook，以檢查所選執行處理至所需端點的連線能力AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2。

- **CheckWindowsUpdateServices:**

檢查 Windows 更新服務狀態和啟動類型。

- **CheckWindowsUpdateSettings:**

檢查透過 Windows 執行個體設定的 Windows 更新原則。

- **CheckWSUSSettings:**

檢查 Windows 更新是否設定 WSUS 或 Microsoft 更新目錄，並驗證連線能力。

- **CheckWUGlobalSettings:**

檢查透過 Windows 執行個體設定的 Windows 更新全域設定。

- **GenerateLogs:**

將 Windows 更新記錄檔和 CBS 記錄檔下載至執行個體桌面，並檢查 Windows 事件記錄檔是否有失敗。

- **FinalReport:**

產生所有步驟的完整報告。

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

```

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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)

- [設定自動化操作](#)
- [Support 自動化 workflow 登陸頁](#)

與 AWS 服務相關的文件

- 如需詳細資訊，請參閱 [Troubleshoot Windows 更新](#) 文章。

## AWSsupport-UpgradeWindowsAWSdrivers

### Description

AWSsupport-UpgradeWindowsAWSdriversrunbook 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 會嘗試透過呼叫 SSM 代理程式，在線上安裝最新版本的 AWS 驅動程式。如果 SSM 代理程式無法連絡，runbook 可以在明確要求時執行 AWS 驅動程式的離線安裝。

#### Note

線上和離線升級都會在嘗試任何作業之前建立 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

如果您的執行個體連線到 AWS Systems Manager 使用 VPC 端點，除非在 us-east-1 區域中使用，否則此 Runbook 將失敗。此 Runbook 也會在網域控制站上失敗。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 \(AWS PV 升級\)](#)。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

## 平台

Linux, macOS, 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

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

預設值：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 自動化將建立新的 VPC。

 Important

子網路必須與位於相同的可用區域 InstanceId，且必須允許存取 SSM 端點。

## 必要的 IAM 許可

此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SendCommand至少必須具有包含 ssm: StartAutomationExecution 和 ssm: 許可的 IAM 角色，才能執行自動化並將命令傳送到執行個體，再加上 ssm: GetAutomationExecution 才能讀取自動化輸出。您可以將 AmazonSSManagedInstanceCore 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-驗證輸入實例是否為 Windows。
2. aws:assertAwsResourceProperty-驗證輸入執行個體是否為受控執行個體。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-通過安裝AWS光伏驅動器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`-驗證 `AllowOffline` 旗標是否設定為 `true`。如果是這樣，離線升級會開始，否則自動化會結束。
- ii. `aws:changeInstanceState`-停止來源執行環境。
- iii. `aws:changeInstanceState`-強制停止來源執行環境。
- 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`-斷言 `ForceUpgrade` 旗
- viii. 強制離線升級 ) 如果 `ForceUpgrade = true`，則運行 `aws:executeAutomation` 以 `AWSSupport-StartEC2RescueWorkflow` 使用驅動程序強制升級腳本調用。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` 則運行 `aws:executeAutomation` 以 `AWSSupport-StartEC2RescueWorkflow` 使用驅動程序升級腳本調用。

## 輸出

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup. ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline` 輸出。

`forceUpgradeDrivers` 離線輸出

## Amazon ECS

AWS Systems Manager 自動化為 Amazon 彈性容器服務提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題



- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRUNTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

## AWSSupport-CollectECSInstanceLogs

### Description

AWSSupport-CollectECSInstanceLogsRunbook 會從 Amazon 彈性運算雲端 (Amazon ECS) 執行個體收集作業系統和 Amazon 彈性容器服務 (Amazon EC2) 相關的日誌檔，以協助您疑難排解常見的 Amazon ECS 問題。自動化收集關聯的記錄檔時，會對檔案系統進行變更。這些變更包括建立暫存目錄和記錄目錄、將記錄檔複製到這些目錄，以及將記錄檔壓縮到歸檔中。

如果您為LogDestination參數指定值，則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。為了確保從 Amazon EC2 執行個體收集的日誌的安全性，如果政策狀態設isPublic為true，或者如果存取控制清單 (ACL) 授READ|WRITE予 All Users Amazon S3 預先定義群組的許可，則不會上傳日誌。此外，如果您的帳戶中沒有提供的存儲桶，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 S3 簡單儲存服務使用者指南中的預先定義群組](#)。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ECSInstanceid

類型：字串

說明：(必填) 您要從中收集記錄檔的執行個體 ID。您指定的執行個體必須由「系統管理員」管理。

- LogDestination

類型：字串

說明：(選用) 您要將存檔日誌上傳 AWS 帳戶 到的 Amazon S3 儲存貯體。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 執行個體具有附加 AmazonSSMManagedInstanceCore Amazon 受管政策的IAM角色。若要將日誌存檔上傳到您在LogDestination參數中指定的 Amazon S3 儲存貯體，您必須新增以下許可：

- s3:PutObject
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl

### 文件步驟

- `assertInstanceIsManaged`-驗證您在`ECSInstanceId`參數中指定的例證是否由系統管理員管理。
- `getInstancePlatform`-取得`ECSInstanceId`參數中指定之執行個體之作業系統 (OS) 平台的相關資訊。
- `verifyInstancePlatform`-分支基於操作系統平台的自動化。
- `runLogCollectionScriptOnLinux`-在 Linux 執行個體上收集作業系統和 Amazon ECS 相關的日誌檔案，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 相關的日誌檔案，並在`C:\ProgramData\collectECSlogs`目錄中建立封存檔案。
- `verifyIfS3BucketProvided`-驗證是否為參數指定了`LogDestination`值。
- `runUploadScript`-根據操作系統平台分支自動化步驟。
- `runUploadScriptOnLinux`-將日誌存檔上傳到`LogDestination`參數中指定的 Amazon S3 儲存貯體，並從 OS 刪除存檔的日誌檔。
- `runUploadScriptOnWindows`-將日誌存檔上傳到`LogDestination`參數中指定的 Amazon S3 儲存貯體，並從 OS 刪除存檔的日誌檔。

## AWS-InstallAmazonECSAgent

### Description

`AWS-InstallAmazonECSAgentRunbook` 在您指定的 Amazon 彈性計算雲 ( AmazonECS ) 實例上安裝 Amazon 彈性容器服務 ( AmazonEC2 ) 代理。此手冊僅支持 Amazon Linux 和 Amazon Linux 2 實例。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceIds

類型: StringList

說明：(必填) 您要在 IDs 其上安裝 EC2 Amazon ECS 代理程式的 Amazon 執行個體。

### 必要的IAM權限

此 AutomationAssumeRole 參數需要執行下列動作，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-在您在 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。 SuccessfullInstances -成功安裝 Amazon ECS 代理程式的執行個體識別碼。

InstallAmazonECSAgent。 FailedInstances -安裝 Amazon ECS 代理程式失敗的執行個體識別碼。

InstallAmazonECSAgent。 InProgressInstances -正在安裝 Amazon ECS 代理程式的執行個體識別碼。

# AWS-ECSRunTask

## Description

AWS-ECSRunTask執行手冊執行您指定的 Amazon 彈性容器服務 (AmazonECS) 任務。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- capacityProviderStrategy

類型：字串

描述：(選擇性) 用於工作的容量提供者策略。

- 叢集

類型：字串

說明：(選擇性) 要在其上執行工作ARN的叢集的簡短名稱。如果未指定叢集，則會使用預設叢集。

- count

類型：字串

描述：(選擇性) 要放置在叢集上之指定工作的建立數目。您最多可以為每個請求指定 10 個任務。

- enableECSManaged标签

類型：布林值

說明：(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 彈性容器服務開發人員指南中的標記 Amazon ECS 資源](#)。

- enableExecuteCommand

類型：布林值

描述：(選擇性) 決定是否啟動此工作中容器的執行命令功能。如果為 true，則會在工作中的所有容器上啟動執行命令功能。

- 群組

類型：字串

描述：(選擇性) 要與任務相關聯的任務群組名稱。預設值是工作定義的系列名稱。例如：family:my-family-name。

- launchType

類型：字串

有效值：EC2| FARGATE | EXTERNAL

描述：(選擇性) 執行獨立工作的基礎結構。

- networkConfiguration

類型：字串

描述：(選擇性) 工作的網路組態。若工作定義使用awsvpc網路模式接收自己的 elastic network interface，則需要此參數，而其他網路模式則不支援此參數。

- 覆蓋

類型：字串

描述：(選擇性) 容器覆寫的JSON格式清單，用來指定指定工作定義中容器的名稱，以及該容器應接收的覆寫。您可以覆寫在工作定義或 Docker 映像檔中指定的容器的預設命令，並使用命令覆寫。您

也可以覆寫在工作定義或容器上 Docker 映像檔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：(選擇性) 要用於工作的位置限制物件陣列。您最多可以為每個任務指定 10 個條件約束，包括任務定義中的條件約束和在執行時間指定的條件約束。

- placementStrategy

類型：字串

描述：(選擇性) 用於任務的放置策略物件。您最多可以為每個任務指定 5 個策略規則。

- platformVersion

類型：字串

說明：(選擇性) 工作使用的平台版本。平台版本僅針對在 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：(選擇性) 決定標籤是否從作業定義傳播至作業。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：(選擇性) 用於工作的參照 ID。參照識別碼的長度上限為 1024 個字元。

- startedBy

類型：字串

說明：(選擇性) 在工作啟動時指定的選用標籤。這可協助您識別哪些工作屬於特定工作，方法是篩選 ListTasksAPI 作業的結果。允許最多 36 個字母 (大寫和小寫)，數字，連字符 (-) 和底線 (\_)。

- 標籤

類型：字串

描述：(選用) 您要套用至工作的中繼資料，以協助您分類和組織工作。每個標籤都包含使用者定義的索引鍵和值。

- taskDefinition

類型：字串

描述：(選擇性) 要執行ARN的工作定義family與 revision (family:revision) 或完整。如果未指定修訂，則會使用最新的ACTIVE修訂版本。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ecs:RunTask

### 文件步驟

aws:executeScript-根據您為執行簿輸入參數指定的值執行 Amazon ECS 任務。

## AWSsupport-TroubleshootECSContainerInstance

### Description

AWSsupport-TroubleshootECSContainerInstance執行手冊可協助您對無法在 Amazon ECS 叢集註冊的 Amazon 彈性運算雲端 (AmazonEC2) 執行個體進行疑難排解。此自動化操作會檢查執行個體的使用者資料是否包含正確的叢集資訊、執行個體設定檔是否包含必要的權限，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，且 Amazon ECS 叢集狀態必須為ACTIVE。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

說明：(必填) 執行個體註冊失敗的 Amazon ECS 叢集名稱。

- InstanceId

類型：字串

說明：(必填) 您要疑難排解之 Amazon EC2 執行個體的 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 執行個體是否符合在 Amazon ECS 叢集註冊所需的先決條件。

# AWSSupport-TroubleshootECSTaskFailedToStart

## Description

該手 `AWSSupport-TroubleshootECSTaskFailedToStart` 冊可以幫助您解決 Amazon ECS 集群中的 Amazon 彈性容器服務 ( AmazonECS ) 任務無法啟動的原因。您必須在相同 AWS 區域 的任務，無法啟動運行此 runbook。runbook 會分析下列常見問題，這些問題可能會導致工作無法啟動：

- 與已設定容器登錄的網路連線
- 缺少任務執行角色所需的IAM權限
- VPC端點連線
- 安全性群組規則組態
- AWS Secrets Manager 秘密參考
- 記錄設定

### Note

如果分析確定需要測試網路連線，則會在您的帳戶中建立 Lambda 函數和必要IAM角色。這些資源可用來模擬失敗工作的網路連線。自動化會在不再需要這些資源時刪除這些資源。但是，如果自動化操作無法刪除資源，您必須手動執行此操作。

## 運行此自動化 (控制台)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

描述：(必填) 任務無法啟動的 Amazon ECS 叢集名稱。

- CloudwatchRetentionPeriod

類型：整數

說明：(選用) Lambda 函數日誌存放在 Amazon CloudWatch 日誌中的保留期 (以天為單位)。只有在分析確定需要測試網路連線時，才需要這樣做。

有效值：1 | 3 | 7

預設：30

- TaskId

類型：字串

描述：(必要) 失敗工作的 ID。使用最近失敗的工作。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-驗證啟動自動化操作的使用者或角色是否具有必要的IAM權限。如果您沒有足夠的權限來使用此 runbook，缺少必要的權限會包含在自動化的輸出中。
- aws:branch-根據您是否擁有對 runbook 的所有必需操作的權限分支。
- aws:executeScript-VPC 如果分析確定網路連線需要測試，請在您的中建立 Lambda 函數。
- aws:branch-根據上一步的結果進行分支。
- aws:executeScript-分析無法啟動任務的可能原因。
- aws:executeScript-刪除此自動化操作所建立的資源。
- aws:executeScript-格式化自動化輸出，以將分析結果傳回主控台。您可以在此步驟之後檢閱分析，然後再完成自動化操作。
- aws:branch-根據是否建立 Lambda 函數和相關資源並需要刪除分支。
- aws:sleep-休眠 30 分鐘，因此可以刪除 Lambda 函數的 elastic network interface。
- aws:executeScript-刪除 Lambda 函數網路介面。

- `aws:executeScript`-格式化 Lambda 函數網路介面刪除步驟的輸出。

## AWS-UpdateAmazonECSAgent

### Description

AWS-UpdateAmazonECSAgentRunbook 更新您指定的 Amazon 彈性運算雲 ( AmazonECS ) 實例上的 Amazon 彈性容器服務 ( AmazonEC2 ) 代理。此手冊僅支持 Amazon Linux 和 Amazon Linux 2 實例。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 叢集 ARN

類型: StringList

說明：(必填) 您的容器執行個體註冊的 Amazon ECS 叢集的 Amazon 資源名稱 (ARN)。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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識別碼。

UpdateAmazonECSAgent。 FailedContainers -Amazon ECS 代理程式更新失敗的執行個體識別碼。

UpdateAmazonECSAgent。 InProgressContainers -正在進行 Amazon ECS 代理程式更新的執行個體 ID。

## Amazon EFS

AWS Systems Manager 自動化為 Amazon Elastic File System 提供預先定義的執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

## 主題

- [AWSSupport-CheckAndMountEFS](#)

# AWSSupport-CheckAndMountEFS

## Description

AWSSupport-CheckAndMountEFS執行手冊會驗證裝載 Amazon 彈性檔案系統 (AmazonEFS) 檔案系統並將檔案系統掛接到您指定的 Amazon 彈性運算雲端 (AmazonEC2) 執行個體的先決條件。此執行手冊支援使用DNS名稱或使用掛載目標的 IP 位址掛載您的 Amazon EFS 檔案系統。

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 動作

類型：字串

有效值：檢查 | CheckAndMount

描述：(必要) 決定 Runbook 是否驗證必要條件，還是驗證必要條件並裝載檔案系統。



- EfsId

類型：字串

描述：(必要) 您要掛載之檔案系統的 ID。

- InstanceId

類型：字串

說明：(必填) 您要掛載檔案系統之 Amazon EC2 執行個體的 ID。

- MountOptions

類型：字串

說明：(選擇性) 您要在EFS掛載檔案系統時使用的 Amazon 掛載協助程式支援的選項。如果您指定選tls項，請確認目標執行個體上的 stunnel 已升級。

- MountPoint

類型：字串

描述：(選擇性) 您要掛載檔案系統的目錄。如果您指定Action參數的Check值，則不應指定此參數。

- MountTargetIP

類型：字串

描述：(選擇性) 掛載目標的 IP 位址。依 IP 位址裝載可在停用的環境中DNS運作，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 (路線 53) 以外的DNS供應商，則可以使用此選項。

- 區域

類型：字串

說明：(必填) Amazon EC2 執行個體和檔案系統所 AWS 區域 在的位置。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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`-收集有關您在`InstanceId`參數中指定的 Amazon EC2 執行個體的詳細資訊。
- `aws:executeScript`-收集有關您在`EfsId`參數中指定之檔案系統的詳細資訊。
- `aws:executeScript`-驗證與檔案系統關聯的安全群組允許連接埠 2049 從您在參數中指定的 Amazon EC2 執行個體傳輸。 `InstanceId`
- `aws:assertAwsResourceProperty`-驗證您在`InstanceId`參數中指定的 Amazon EC2 執行個體是由系統管理員管理，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`參數中指定的檔案系統的先決條件。

- `aws:runCommand`-驗證掛接您在`EfsId`參數中指定的檔案系統的先決條件，並將檔案系統掛接到您在`InstanceId`參數中指定的 Amazon EC2 執行個體上。

## Amazon EKS

AWS Systems Manager 自動化為 Amazon Elastic Kubernetes Service 提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [AWSSupport-CollectEKSIInstanceLogs](#)
- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)

## AWSSupport-CollectEKSIInstanceLogs

### Description

執行手冊`AWSSupport-CollectEKSIInstanceLogs`會從 Amazon 彈性運算雲端 (Amazon) 執行個體收集作業系統和 Amazon 彈性 Kubernetes 服務 (AmazonEKS) 相關的日誌檔，以協助您疑難排解常見問題。EC2自動化收集關聯的記錄檔時，會對檔案系統結構進行變更，包括建立暫存目錄、將記錄檔複製到暫存目錄，以及將記錄檔壓縮到歸檔中。此活動可能會導致執行個體CPUUtilization上的增加。如需詳細資訊CPUUtilization，請參閱 Amazon CloudWatch 使用者指南中的執行個體[指標](#)。

如果您為`LogDestination`參數指定值，則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。為了協助確保從EC2執行個體收集的日誌的安全性，如果政策狀

態設isPublic為true，或者如果存取控制清單 (ACL) 授READ|WRITE予 All Users Amazon S3 預先定義群組的許可，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 S3 簡單儲存服務使用者指南中的預先定義群組](#)。

### Note

此自動化需要連接至EC2執行個體的根 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區上至少有 10% 的可用磁碟空間。如果根磁碟區上沒有足夠的可用磁碟空間，自動化會停止。

## [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EKSInstanceid

類型：字串

說明：(必填) 您要從中收集日誌的 Amazon EKS EC2 執行個體 ID。

- LogDestination

類型：字串

說明：(選用) 您帳戶中要將存檔日誌上傳到的 S3 儲存貯體。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`

我們建議接收命令的EC2執行個體具有附加 `mazonSSMManaged InstanceCore Amazon` 受管政策的IAM角色。若要將日誌存檔上傳到您在LogDestination參數中指定的 S3 儲存貯體，您必須新增`s3:PutObject`權限。

### 文件步驟

- `aws:assertAwsResourceProperty`-確認作業系統EKSIInstanceId參數中指定的值為 Linux。
- `aws:runCommand`-收集作業系統和 Amazon EKS 相關的日誌檔，並將其壓縮到目錄中的存檔中/`var/log`。
- `aws:branch`-確認是否為LogDestination參數指定值。
- `aws:runCommand`-將日誌存檔上傳到您在LogDestination參數中指定的 S3 儲存貯體。

## AWS-CreateEKSClusterWithFargateProfile

### Description

手AWS-CreateEKSClusterWithFargateProfile冊創建一個 Amazon Elastic Kubernetes Service (AmazonEKS) 集群使用. AWS Fargate

[運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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) 提供 Kubernetes 控制平面權限ARN的IAM角色，以代表您呼叫 AWS API 作業。

- 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 網繭執行IAM角色ARN的說明。

- FargateProfileSelectors

類型：字串

描述：(必要) 用來比對網繭與 Fargate 設定檔的選取器。

- SubnetIds

類型: StringList

描述：(必填) 您要用於 Amazon EKS 叢集IDs的子網路。Amazon EKS 會在這些子網路中建立彈性網路界面，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IDs。

- EKSEndpointPrivateAccess

類型：布林值

預設：True

描述：(選擇性) 將此值設為True允許叢集的 Kubernetes API 伺服器端點進行私人存取。如果啟用私有存取，則叢集內的 Kubernetes API 要求會VPC使用私有端點。VPC如果停用私人存取，且叢集中有節點或 AWS Fargate 網繭，請確定publicAccessCidrs包含與節點或 Fargate 網繭通訊的必要CIDR區塊。

- EKSEndpointPublicAccess

類型：布林值

預設：False

描述：(選擇性) 將此值設為以停用False對叢集 Kubernetes API 伺服器端點的公開存取權。如果停用公用存取權，叢集的 Kubernetes API 伺服器只能從啟動該伺服器的位VPC置接收要求。

- PublicAccessCIDRs

類型: StringList

說明：(選擇性) 允許存取叢集公用 Kubernetes API 伺服器端點的CIDR區塊。拒絕從您指定之CIDR 區塊外的位址與端點的通訊。如果您已停用私人端點存取，且叢集中有節點或 Fargate 網繭，請確定您已指定必要的CIDR區塊。

- SecurityGroupIds

類型: StringList

說明：(選擇性) 指定一或多個安全群組，以與 Amazon 在您帳戶中建立的彈性網路界面建立關聯 EKS。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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` ( `AWSexecuteAwsApi`):-創建一個 Amazon EKS 集群。
- `VerifyEKSClusterIsActive` ( `aws waitforAwsResourceProperty`):-驗證叢集狀態為ACTIVE。
- `CreateFargateProfile` ( `aws:executeAwsApi` ) -為集群創建一個 Fargate。
- `VerifyFargateProfileIsActive` ( `aws: waitforAwsResourceProperty` ) -驗證 Fargate 配置文件狀態是。ACTIVE

## 輸出

`CreateEKSCluster.CreateClusterResponse`

描述：收到來自CreateClusterAPI電話的回應。

`CreateFargateProfile.CreateFargateProfileResponse`

描述：收到來自CreateFargateProfileAPI電話的回應。

## AWS-CreateEKSClusterWithNodegroup

### Description



AWS-CreateEKSClusterWithNodegroup執行手冊會使用節點群組來建立 Amazon Elastic Kubernetes Service (AmazonEKS) 叢集以取得容量。

## [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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) 提供 Kubernetes 控制平面權限ARN的IAM角色，以代表您呼叫 AWS API作業。

- 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) 與節點群組產生關聯ARN的IAM角色。Amazon EKS 工作者節點 kubelet 精靈會代表您撥打 AWS APIs電話。節點會透過IAM執行個體設定檔和相關政策接收這些API呼叫的權限。在啟動節點並將其註冊到叢集之前，您必須先建立這些節點在啟動時使用的IAM角色。

- SubnetIds

類型: StringList

描述：(必填) 您要用於 Amazon EKS 叢集IDs的子網路。Amazon EKS 會在這些子網路中建立彈性網路界面，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IDs。

- EKSEndpointPrivateAccess

類型：布林值

預設：True

描述：(選擇性) 將此值設為True允許叢集的 Kubernetes API 伺服器端點進行私人存取。如果啟用私有存取，則叢集內的 Kubernetes API 要求會VPC使用私有端點。VPC如果停用私人存取，且叢集中有節點或 AWS Fargate 網繭，請確定publicAccessCidrs包含與節點或 Fargate 網繭通訊的必要CIDR區塊。

- EKSEndpointPublicAccess

類型：布林值

預設：False

描述：(選擇性) 將此值設為以停用False對叢集 Kubernetes API 伺服器端點的公開存取權。如果停用公用存取權，叢集的 Kubernetes API 伺服器只能從啟動該伺服器的位VPC置接收要求。

- PublicAccessCIDRs

類型: StringList

說明：(選擇性) 允許存取叢集公用 Kubernetes API 伺服器端點的CIDR區塊。拒絕從您指定之CIDR 區塊外的位址與端點的通訊。如果您已停用私人端點存取，且叢集中有節點或 Fargate 網繭，請確定您已指定必要的CIDR區塊。

- SecurityGroupIds

類型: StringList

說明：(選擇性) 指定一或多個安全群組，以與 Amazon 在您帳戶中建立的彈性網路界面建立關聯 EKS。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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` ( `AWSexecuteAwsApi`):-創建一個 Amazon EKS 集群。
- `VerifyEKSClusterIsActive` ( `aws waitForAwsResourceProperty`):-驗證叢集狀態為ACTIVE。
- `CreateNodegroup` ( `aws:executeAwsApi` ) -為集群創建一個節點組。
- `VerifyNodegroupsActive` ( `aws waitForAwsResourceProperty`):-驗證節點組狀態是否為ACTIVE。

## 輸出

- `CreateEKSCluster.CreateClusterResponse` : 從CreateClusterAPI呼叫收到的響應。
- `CreateNodegroup.CreateNodegroupResponse` : 從CreateNodegroupAPI呼叫收到的響應。

# AWS-DeleteEKSCluster

## Description

此執行手冊會刪除與 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的節點、用於建立節點的堆 AWS CloudFormation 疊，以及叢集的 VPC CloudFormation 堆疊。如需有關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

如果叢集中有與負載平衡器關聯的作用中服務，則必須先刪除這些服務，然後再刪除叢集。如果不這樣做，系統將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。

## 尋找並刪除叢集中的服務

1. 安裝 Kubernetes 命令行公用程式。kubect1 如需詳細資訊，請參閱 Amazon EKS 使用者指南中的[安裝 kubect1](#)。
2. 執行下列命令以列出叢集中執行的所有服務。

```
kubect1 get svc --all-namespaces
```

3. 執行下列命令，以刪除任何具有關聯 EXTERNAL-IP 值的服務。這些服務由負載平衡器前置，您必須在 Kubernetes 中刪除它們，才能正確釋放負載平衡器和關聯的資源。

```
kubect1 delete svc  
service-name
```

您現在可以執行 `AWS-DeleteEKSCluster Runbook`。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EKSClusterName

類型：字串

描述：(必填) 要刪除的 Amazon EKS 叢集名稱。

- VPCCloudFormationStack

類型：字串

描述：(選擇性) 要刪除之 EKS 叢集 VPC 的 AWS CloudFormation 堆疊名稱。這將刪除 AWS CloudFormation 堆棧以 VPC 及由堆棧創建的任何資源。

- VPCCloudFormationStackRole

類型：字串

描述：(選擇 ARN 性) AWS CloudFormation 假設要刪除 VPC CloudFormation 堆疊的 IAM 角色。AWS CloudFormation 使用角色的認證代表您撥打電話。

- SelfManagedNodeStacks

類型：字串

說明：(可選) 以逗號分隔的自我管理節點的 AWS CloudFormation 堆棧名稱列表，這將刪除自我管理節點的 AWS CloudFormation 堆棧。

- SelfManagedNodeStacksRole

類型：字串

描述：(選用) AWS CloudFormation 假設要刪除自我管理節點堆疊ARN的IAM角色。AWS CloudFormation 使用角色的認證代表您撥打電話。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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：尋找並刪除EKS叢集中的所有節點群組。
- aws:executeScript- DeleteFargateProfiles：查找並刪除EKS群集中的所有 Fargate 配置文件。
- aws:executeScript- DeleteSelfManagedNodes：刪除所有自我管理節點以及用於建立節點的 CloudFormation 堆疊。
- aws:executeScript-DeleteEKSCluster：刪除EKS叢集。
- aws:executeScript-DeleteVPCCloudFormationStack：刪除VPC CloudFormation 堆棧。

## AWS-MigrateToNewEKSSelfManagedNodeGroup

### Description

AWS-MigrateToNewEKSSelfManagedNodeGroup執行手冊可協助您建立新的 Amazon Elastic Kubernetes Service (AmazonEKS) Linux 節點群組，以將您現有的應用程式遷移到。如需詳細資訊，請參閱 Amazon EKS 使用者指南中的[移轉至新節點群組](#)。

## [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- OldStackName

類型：字串

說明：(必填) 現有堆疊的名稱或 AWS CloudFormation 堆疊 ID。

- NewStackName

類型：字串

描述：(選擇性) 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，則會使用以下格式建立堆疊名稱：`NewNodeGroup-ClusterName-AutomationExecutionID`。

- ClusterControlPlaneSecurityGroup

類型：字串

說明：(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 堆疊中指定的安全性群組。

- NodeInstanceType

類型：字串

說明：(選擇性) 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：(選擇性) 新節點群組的名稱。如果您沒有為此參數指定值，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：(選擇性) 建立新堆疊時所要擴充的節點數目。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：(選擇性) 節點群組可向外延展至的節點數目上限。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：(選擇性) 節點群組可擴充至的節點數目下限。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：(選擇性) 您要節點群組使用的 Amazon Machine Image (AMI) 識別碼。

- NodeImageIdSSMParam

類型：字串

描述：(選擇性) 您要節點群組使用的公用 Systems Manager 參數。AMI



- NodeVolumeSize

類型：字串

說明：(選擇性) 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

說明：(選擇性) 您要用於節點根EBS磁碟區的 Amazon 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：(選擇性) 您要指派給節點的 key pair。如果您沒有為此參數指定值，則會使用現有 AWS CloudFormation 堆疊中指定的 key pair。

- 子網

類型: StringList

描述：(選擇性) 要用於新節點群組IDs的子網路清單 (逗號分隔)。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。

- DisableIMDSv

類型：布林值

說明：(選擇性) 指定停用「執行處理中繼資料服務版本 1」(IMDSv1)。預設情況下，節點支援 IMDSv1和IMDSv2。

- BootstrapArguments

類型：字串

說明：(選用) 您要傳遞至節點啟動程序指令碼的其他引數。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

AWS-MigrateToNewEKSSelfManagedNodeGroup

- `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:DescribeInstanceStatus`
- `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`)-收集要用於新節點群組的參數值。
- `CreateStack` (`aws:createStack`)-為新節點組創建 AWS CloudFormation 堆棧。
- `GetNewStackNodeInstanceRole` (`aws:executeAwsApi`) -獲取節點實例角色。
- `GetNewStackSecurityGroup` (`aws:executeAwsApi`) -該步驟獲取節點安全組。
- `AddIngressRulesToNewNodeSecurityGroup` (`aws:executeAwsApi`) -將輸入規則添加到新創建的安全組，以便它可以接受來自分配給先前節點組的流量。
- `AddIngressRulesToOldNodeSecurityGroup` (`aws:executeAwsApi`) -將輸入規則添加到先前的安全組，以便它可以接受來自分配給新創建節點組的流量。
- `VerifyStackComplete` (`aws:assertAwsResource` 屬性) -驗證新的堆棧狀態是 `CREATE_COMPLETE`。

## 輸出

DetermineParameterValuesForNewNodeGroup。 NewStackParameters -用於創建新堆棧的參數。

GetNewStackNodeInstanceRole。 NewNodeInstanceRole -新節點群組的節點執行個體角色。

GetNewStackSecurityGroup。 NewNodeSecurityGroup -新節點群組的安全性群組識別碼。

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執行手冊可診斷 Amazon 彈性 Kubernetes 服務 (AmazonEKS) 叢集、基礎基礎設施的常見問題，並提供建議的修復步驟。

#### Important

存取 AWSPremiumSupport-\* Runbook 需要企業或商業 Support 訂閱。如需詳細資訊，請參閱 [比較 S AWS support 方案](#)。

如果您為 S3BucketName 參數指定值，則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。為了協助確保從 EC2 執行個體收集的日誌的安全性，如果政策狀態設 isPublic 為 true，或者如果存取控制清單 (ACL) 授 READ|WRITE 予 All Users Amazon S3 預先定義群組的許可，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 S3 簡單儲存服務使用者指南中的預先定義群組](#)。

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

說明：(必填) 您要疑難排解的 Amazon EKS 叢集名稱。

- S3 BucketName

類型：字串

說明：(選用) 應在其中上傳工作流程簿產生的報告的私有 Amazon S3 儲存貯體的名稱。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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，連接到啟動自動化的使用者或角色的 AWS Identity and Access Management (IAM) 政策必須允許對下列公用 AWS Systems Manager 參數進 `ssm:GetParameter` 行操作，才能取得背景工作節點的最新建議 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`

若要將執行手冊產生的報告上傳到 Amazon S3 儲存貯體，您指定的指定 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 叢集的詳細資料。

- `aws:executeScript`-收集 Amazon 彈性運算雲端 (AmazonEC2) 執行個體、Auto AMI Scaling 群組和 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 (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) 的詳細資料。
- `aws:executeScript`-收集連接的IAM執行個體設定檔和角色原則的詳細資料。
- `aws:executeScript`-收集您在S3BucketName參數中指定的 Amazon S3 儲存貯體的詳細資訊。
- `aws:executeScript`-將 Amazon VPC 子網分類為公共或私有。
- `aws:executeScript`-檢查 Amazon VPC 子網路是否有 Amazon EKS 叢集中所需的標籤。
- `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`-檢查工作節點 Amazon EC2 執行個體是否使用最新的 Amazon 最EKS佳AMI 化
- `aws:executeScript`-檢查是否連接到工作節點的 Amazon VPC 安全群組是否有必要的標籤。
- `aws:executeScript`-檢查 Amazon EKS 叢集和工作者節點 Amazon VPC 安全群組規則是否有建議的 Amazon EKS 叢集輸入規則。
- `aws:executeScript`-檢查 Amazon EKS 叢集和工作者節點 Amazon VPC 安全群組規則是否有建議的 Amazon EKS 叢集輸出規則。
- `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調度資源的必要標記。
- `aws:executeScript`-檢查工作節點 Amazon EC2 執行個體是否已連接到網際網路。
- `aws:executeScript`-根據先前步驟的輸出產生報告。如果為S3BucketName參數指定了值，則產生的報告會上傳到 Amazon S3 儲存貯體。

## AWSsupport-TroubleshootEKSSWorkerNode

### Description

AWSsupport-TroubleshootEKSSWorkerNode執行手冊會分析 Amazon 彈性運算雲端 (AmazonEC2) 工作者節點和 Amazon Elastic Kubernetes Service (AmazonEKS) 叢集，以協助您識別和疑難排解阻止工作者節點加入叢集的常見原因。runbook 輸出指導，以幫助您解決所識別的任何問題。

**⚠ Important**

若要成功執行此自動化，Amazon EC2 工作者節點的狀態必須是running，且 Amazon EKS 叢集狀態必須為ACTIVE。

## 運行此自動化 (控制台)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

描述：(必填) Amazon EKS 叢集的名稱。

- 工作者識別碼

類型：字串

描述：(必要) 無法加入叢集之 Amazon EC2 工作者節點的 ID。

必要的IAM權限



此AutomationAssumeRole參數需要執行下列動作，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 工作節點存在且running處於狀態。
- aws:executeScript-執行 Python 指令碼，以協助識別 Worker 節點無法加入叢集的可能原因。

# AWS-UpdateEKSCluster

## Description

AWS-UpdateEKSCluster 執行手冊可協助您將 Amazon Elastic Kubernetes Service (AmazonEKS) 叢集更新為您想要使用的 Kubernetes 版本。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

描述：(必填) 您的 Amazon EKS 叢集的名稱。

- 版本

類型：字串

描述：(必要) 您要將叢集更新至的目標 Kubernetes 版本。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- eks:DescribeUpdate
- eks:UpdateClusterVersion

#### 文件步驟

- aws:executeAwsApi-更新 Amazon 叢集所使用的 Kubernetes 版本。EKS
- aws:waitForAwsResourceProperty-等待更新狀態為Successful。

## AWS-UpdateEKSMangedNodeGroup

### Description

AWS-UpdateEKSMangedNodeGroup執行手冊可協助您更新 Amazon Elastic Kubernetes Service (AmazonEKS) 受管節點群組。您可以選擇Version或Configuration更新。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

預設值：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

說明：(可選) 您要使用的 Amazon EKS 優化AMI版本。根據預設會使用最新版本。

- ForceUpgrade

類型：布林值

說明：(選擇性) 如果為 true，則更新不會因為網繭中斷預算違規而失敗。

- KubernetesVersion

類型：字串

描述：(選擇性) 要將節點群組更新至的 Kubernetes 版本。

- LaunchTemplateId

類型：字串

描述：(選擇性) 啟動範本的 ID。

- **LaunchTemplateName**

類型：字串

描述：(選擇性) 啟動範本的名稱。

- **LaunchTemplateVersion**

類型：字串

說明：(可選) Amazon 彈性計算雲 (AmazonEC2) 啟動模板版本。只有在從啟動範本建立節點群組時，此參數才有效。

下列參數僅適用於Configuration更新類型：

- **AddOrUpdateNodeGroupLabels**

類型: StringMap

說明：(選用) 您要新增或更新的 Kubernetes 標籤。

- **AddOrUpdateKubernetesTaintsEffect**

類型: StringList

描述：(選擇性) 您要新增或更新的 Kubernetes 污染。

- **MaxUnavailableNodeGroups**

類型：整數

預設：0

說明：(選擇性) 在版本更新期間無法使用的節點數目上限。

- **MaxUnavailablePercentageNodeGroup**

類型：整數

預設：0

說明：(選擇性) 在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：(選擇性) 受管理節點群組應維護的節點數目。

- NodeGroupMaxSize

類型：整數

預設：0

描述：(選擇性) 受管理節點群組可向外延展至的節點數目上限。

- NodeGroupMinSize

類型：整數

預設：0

描述：(選擇性) 受管理節點群組可擴充至的節點數目下限。

- RemoveKubernetesTaintsEffect

類型: StringList

描述：(選擇性) 您要移除的 Kubernetes 污染。

- RemoveNodeGroupLabels

類型: StringList

說明：(選擇性) 您要移除的標籤清單，以逗號分隔。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

## 文件步驟

- `aws:executeScript`-根據您為執行簿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 執行手冊會使用堆疊來更新 Amazon Elastic Kubernetes Service (AmazonEKS) 叢集中的自我管理節點群組。AWS CloudFormation

如果您的叢集使用 auto 擴展，我們建議您在使用此 runbook 之前將部署擴展到兩個複本。

將部署調整為兩個複本的步驟

1. 安裝 Kubernetes 命令行公用程式。kubectl 如需詳細資訊，請參閱 [Amazon EKS 使用者指南](#) kubectl 中的安裝。
2. 執行下列命令。

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. 運 AWS-UpdateEKSSelfManagedLinuxNodeGroups 行手冊。
4. 執行下列命令，將部署調整回所需的複本數目。

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterName

類型：字串

描述：(必填) Amazon EKS 叢集的名稱。

- NodeGroupName

類型：字串

描述：(必要) 受管理節點群組的名稱。

- ClusterControlPlaneSecurityGroup

類型：字串

描述：(必要) 控制平面安全性群組的識別碼。

- DisableIMDSv

類型：布林值

說明：(選擇性) 決定您是否要允許執行個體中繼資料服務版本 1 (IMDSv1) 和 IMDSv2。

- KeyName

類型：字串

說明：(選擇性) 執行處理的金鑰名稱。

- NodeAutoScalingGroupDesiredCapacity

類型：字串

描述：(選擇性) 節點群組應維護的節點數目。

- NodeAutoScalingGroupMaxSize



類型：字串

描述：(選擇性) 節點群組可向外延展至的節點數目上限。

- NodeAutoScalingGroupMinSize

類型：字串

描述：(選擇性) 節點群組可擴充至的節點數目下限。

- NodeInstanceType

類型：字串

預設值：

說明：(選擇性) 要用於節點群組的執行個體類型。

- NodeImageId

類型：字串

描述：(選擇性) 您要節點群組使用的 Amazon Machine Image (AMI) 識別碼。

- NodeImageIdSSMParam

類型：字串

默認值：/AWS /服務/ek/ 優化阿米/1.21 亞馬遜亞馬遜 2 /推薦/圖像ID

描述：(選擇性) 您要節點群組使用的公用 Systems Manager 參數。AMI

- StackName

類型：字串

描述：(必要) 用來更新節點群組的 AWS CloudFormation 堆疊名稱。

- 子網

類型：字串

描述：(必要) 您要叢集使IDs用之子網路的逗號分隔清單。

- 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權限

此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-根據您為執行簿輸入參數指定的值更新 Amazon EKS 叢集節點群組。
- aws:waitForAwsResourceProperty-等待傳回 AWS CloudFormation 堆疊更新狀態。

## Elastic Beanstalk

AWS Systems Manager 自動化提供預先定義的 AWS Elastic Beanstalk 執行手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [AWSSupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)

- [AWSSupport-TroubleshootElasticBeanstalk](#)

## AWSSupport-CollectElasticBeanstalkLogs

### Description

AWSSupport-CollectElasticBeanstalkLogs執行手冊會從彈性 Elastic Beanstalk 啟動的 Amazon 彈性運算雲端 (AmazonEC2) Windows Server 執行個體收集 AWS Elastic Beanstalk 相關的日誌檔，以協助您疑難排解常見問題。自動化收集關聯的記錄檔時，會對檔案系統結構進行變更，包括建立暫存目錄、將記錄檔複製到暫存目錄，以及將記錄檔壓縮到歸檔中。此活動可能會導致 Amazon EC2 執行個體CPUUtilization上的增加。如需詳細資訊CPUUtilization，請參閱 Amazon CloudWatch 使用者指南中的執行個體指**標**。

如果您為S3BucketName參數指定值，則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。為了確保從 Amazon EC2 執行個體收集的日誌的安全性，如果政策狀態設isPublic為true，或者如果存取控制清單 (ACL) 授READ|WRITE予 All Users Amazon S3 預先定義群組的許可，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 S3 簡單儲存服務使用者指南中的預先定義群組](#)。

如果您沒有為S3BucketName參數指定值，則自動化會將日誌服務包上傳到您執行自動化所在的預設 Elastic Beanstalk Amazon S3 儲存貯體。AWS 區域 該目錄根據以下結構命名 elasticbeanstalk- *region* - *accountID* 。所以此 *region* 以及 *accountID* 值會根據「區域」而有所不同，而且 AWS 帳戶 您在中執行自動化。記錄服務包將儲存到目 resources/environments/logs/bundle/ *environmentID* / *instanceID* 錄中。所以此 *environmentID* 以及 *instanceID* 值會根據您的 Elastic Beanstalk 環境和收集日誌的 Amazon EC2 執行個體而有所不同。

根據預設，連接到 Elastic Beanstalk 環境 Amazon EC2 執行個體的 AWS Identity and Access Management (IAM) 執行個體設定檔具有將服務包上傳到您環境的預設 Elastic Beanstalk Amazon S3 儲存貯體所需的許可。如果為S3BucketName參數指定值，則連接到 Amazon 執行個體的執EC2行個體設定檔必須允許指定的 Amazon S3 儲存貯體和路徑執行s3:GetBucketPolicyStatus、和s3:PutObject動作。s3:GetBucketAcl s3:GetBucketPolicy

#### Note

此自動化需要連接到 Amazon EC2 執行個體的根 Amazon 彈性區塊存放區 (AmazonEBS) 磁碟區上至少有 500 MB 的可用磁碟空間。如果根磁碟區上沒有足夠的可用磁碟空間，自動化會停止。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EnvironmentId

類型：字串

描述：(必要) 您要從中收集記錄服務包的 Elastic Beanstalk 環境識別碼。

- InstanceId

類型：字串

(必要) 您要從中收集日誌服務包的 Elastic Beanstalk 環境中的 Amazon EC2 執行個體識別碼。

- S3 BucketName

類型：字串

(選擇性) 您要將存檔日誌上傳到的 Amazon S3 儲存貯體。

- S3 BucketPath

類型：字串

(選擇性) 您要將日誌服務包上傳到的 Amazon S3 儲存貯體路徑。如果您未指定參數值，則會忽略此 `S3BucketName` 參數。

### 必要的IAM權限

此 `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 執行個體是由管理的 AWS Systems Manager。
- `aws:assertAwsResourceProperty`-確認您在 `InstanceId` 參數中指定的 Amazon EC2 執行個體為 Windows Server 執行個體。
- `aws:runCommand`-檢查執行個體是否屬於 Elastic Beanstalk 環境的一部分、是否有足夠的磁碟空間來捆綁日誌，以及將日誌上傳到的 Amazon S3 儲存貯體是否為公開狀態。
- `aws:runCommand`-收集日誌檔並將存檔上傳到 `S3BucketName` 參數中指定的 Amazon S3 儲存貯體，或者如果未指定值，則將存檔上傳到 Elastic Beanstalk 環境的預設儲存貯體。

## AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

### Description

`AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` 執行手冊會在您指定的 AWS Elastic Beanstalk (Elastic Beanstalk) 環境上啟用記錄。

[運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- EnvironmentId

類型：字串

描述：(必要) 您要啟用登入之 Elastic Beanstalk 環境的識別碼。

### 必要的IAM權限

此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-在您在參數中指定的 Elastic Beanstalk 環境上啟用記錄功能。EnvironmentId
- aws:waitForAwsResourceProperty-等待環境狀態變更為Ready。

- `aws:executeScript`-驗證已在 Elastic Beanstalk 環境中啟用記錄。

## AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

### Description

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications 執行手冊會針對您指定的 AWS Elastic Beanstalk (Elastic Beanstalk) 環境啟用通知。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- EnvironmentId

類型：字串

描述：(必要) 您要啟用通知的 Elastic Beanstalk 環境識別碼。

- TopicArn

類型：字串

說明：(必填) 您要傳送通知ARN的 Amazon 簡易通知服務 (AmazonSNS) 主題。

## 必要的IAM權限

此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`-啟用您在參數中指定的 Elastic Beanstalk 環境的EnvironmentId通知。
- `aws:waitForAwsResourceProperty`-等待環境狀態變更為Ready。
- `aws:executeScript`-驗證 Elastic Beanstalk 環境的通知已啟用。

# AWSSupport-TroubleshootElasticBeanstalk

## Description

AWSSupport-TroubleshootElasticBeanstalkrunbook 可協助您疑難排解 AWS Elastic Beanstalk 環境處於Degraded或Severe狀態的潛在原因。此自動化會檢查下列與您 Elastic Beanstalk 環境相關聯的 AWS 資源：

- 負載平衡器、AWS CloudFormation 堆疊、Amazon EC2 Auto Scaling 群組、Amazon 彈性運算雲端 (AmazonEC2) 執行個體和虛擬私有雲 (VPC) 的組態詳細資料。
- 與子網路相關聯的安全性群組規則、路由表以及網路存取控制清單 (ACLs) 的網路組態問題。
- 驗證與 Elastic Beanstalk 端點的連線能力和公用網際網路存取。
- 驗證負載平衡器的狀態。
- 驗證 Amazon EC2 執行個體的狀態。
- 從 Elastic Beanstalk 環境擷取記錄檔服務包，並選擇性地將檔案上傳到。AWS Support

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ApplicationName

類型：字串

說明：(必填) Elastic Beanstalk 應用程式的名稱。

- EnvironmentName

類型：字串

描述：(必填) Elastic Beanstalk 環境的名稱。

- AWSS3UploaderLink

類型：字串

描述：(選擇性) URL 提供給您的 A，可將記錄服務包從您的 Elastic Beanstalk 環境上傳 AWS Support 至。此選項僅適用於已購買 AWS Support 方案且已開立 Support 案例的客戶。

### 必要的IAM權限

此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) 主參與者具有執行 runbook 中定義之所有動作的必要權限。
- `aws:branch`-根據上一步的結果分支工作流程。
- `aws:executeScript`-收集有關 Elastic Beanstalk 環境的資訊，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`-檢查路由表的網路連線問題，以及ACLs與VPC
- `aws:executeScript`-檢查與 Amazon EC2 執行個體相關聯的安全群組規則的網路連線問題。

- `aws:executeScript`-驗證 Amazon EC2 執行個體的狀態檢查。
- `aws:executeScript`-生成 Elastic Beanstalk 環境的日誌包的鏈接。
- `aws:executeScript`-將日誌包上傳到 AWS Support。
- `aws:executeScript`-輸出行動項目的報告，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。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 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-DropInvalidHeadersForALBrunbook 可讓您指定的應用程式負載平衡器移除含有無效HTTP標頭的標頭。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- LoadBalancerArn

類型：字串

描述：(必填) 您要刪除無效標頭之負載平衡器的 Amazon 資源名稱 (ARN)。

### 必要的IAM權限

此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-為您在參數中指定的負載平衡器啟用刪除無效標頭設定LoadBalancerArn。
- aws:executeScript-驗證已在您在LoadBalancerArn參數中指定的負載平衡器上啟用刪除無效標頭設定。

# AWS-EnableCLBAccessLogs

## Description

AWS-EnableCLBAccessLogsrunbook 會啟用 Classic Load Balancer 的存取記錄。

[運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EmitInterval

類型：整數

有效值：5

預設：60

說明：(選擇性) 發佈存取記錄的間隔 (以分鐘為單位)。

- LoadBalancerNames

類型：字串

說明：(必要) 您要啟用存取記錄的傳統負載平衡器清單 (以逗號分隔)。

- S3 BucketName

類型：字串

說明：(必填) 存放存取日誌的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的名稱。

- S3 BucketPrefix

類型：字串

說明：(選用) 例如，您為 Amazon S3 儲存貯體建立的邏輯階層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權限

此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參數中指定的傳統負載平衡器啟用存取記錄。

### 輸出

電子nableCLBAccess日誌。 SuccessesLoadBalancers -成功啟用存取記錄的負載平衡器名稱清單。

電子nableCLBAccess日誌。 FailedLoadBalancers -啟用存取記錄失敗 MapList 的負載平衡器名稱以及失敗原因。

## AWS-EnableCLBConnectionDraining

### Description

AWS-EnableCLBConnectionDrainingrunbook 可將 Classic Load Balancer (CLB) 上的連線排除至指定的逾時值。連線耗盡可能完成對已取消註冊或狀態不良的執行個體所發出的執行中要求，而指定的逾時是在將執行個體報告為已取消註冊之前保持連線作用中的時間。如需有關排除連線的詳細資訊 CLBs，請參閱 [Classic Load Balancer 使用者指南中的設定傳統負載平衡器的連線排空](#)。

[運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LoadBalancerName

類型：字串

描述：(必要) 您要啟用排除連線的負載平衡器名稱。

- ConnectionTimeout

類型：整數

有效值：

預設：300

描述：(必要) 負載平衡器的連線逾時值。逾時值可設定在 1 到 3600 秒之間。

### 必要的IAM權限

此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`) : 啟用連線排空，並為您指定的負載平衡器設定指定的逾時值。
- `VerifyLoadBalancerConnectionDrainingEnabled` (`aws:assertAwsResource` 屬性) : 驗證負載平衡器是否啟用了連接排除。
- `VerifyLoadBalancerConnectionDrainingTimeout` (`aws:assertAwsResourceProperty`) : 驗證負載平衡器的連接超時值是否與您指定的值匹配。

## 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。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN



- LoadBalancerName

類型：字串

摘要：(必要) 您要啟用跨區域負載平衡的名稱。CLB

#### 必要的IAM權限

此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-啟用CLB您在LoadBalancerName參數中指定的跨區域負載平衡。
- aws:assertAwsResourceProperty-驗證已在上啟用跨區域負載平衡。CLB

## AWSConfigRemediation-EnableELBDeletionProtection

### Description

AWSConfigRemediation-EnableELBDeletionProtectionrunbook 會為您指定的彈性負載平衡器 (ELB) 啟用刪除保護。

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- LoadBalancerArn

類型：字串

描述：(必填) 您要在其上啟用刪除保護的 Amazon 資源名稱 (ARN)。ELB

### 必要的IAM權限

此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-啟用ELB您在LoadBalancerArn參數中指定的刪除保護。

## AWSConfigRemediation-EnableLoggingForALBAndCLB

### Description

AWSConfigRemediation-EnableLoggingForALBAndCLB runbook 會啟 AWS 用指定應用程式負載平衡器或 Classic Load Balancer (CLB) 的記錄功能。

[運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- LoadBalancerId

類型：字串

描述：(必要) 「Classic Load Balancer」名稱或「Application Load Balancer」ARN。

- S3 BucketName

類型：字串

說明：(必填) Amazon S3 存儲桶名稱。

- S3 BucketPrefix

類型：字串

說明：(選用) 例如，您為 Amazon Simple Storage Service (Amazon S3) 貯體建立的邏輯階層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權限

此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-啟用和驗證 Classic Load Balancer 或應用程式負載平衡器的記錄。

# AWSSupport-TroubleshootCLBConnectivity

## Description

AWSSupport-TroubleshootCLBConnectivity執行手冊可協助您疑難排解 Classic Load Balancer (CLB) 和 Amazon 彈性運算雲端 (AmazonEC2) 執行個體之間的連線問題。此外，用戶端與用戶端之間的連線問題也CLB會進行檢閱。此 runbook 也會檢閱的健康狀態檢查CLB、驗證是否遵循最佳作法，並為您建立疑難排解儀表板。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，這個 runbook 不支援將輸出上傳到可公開存取的 S3 儲存貯體。我們建議您為此自動化建立暫時的 S3 儲存貯體。

### Important

使用此 runbook 可能會產生所建立的儀表板的費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#)

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InvestigationType

類型：字串

有效值：最佳做法 | 連線問題 | 疑難排解儀表板

描述：(必要) 您希望 Runbook 執行的作業。

- LoadBalancerName

類型：字串

描述：(必要) 的名稱 CLB。

- S3Location

類型：字串

說明：(選擇性) 您要傳送自動化結果的 S3 儲存貯體名稱。不支援可公開存取的值區。如果您的 S3 儲存貯體使用伺服器端加密，則執行此自動化操作的使用者或角色必須具有 AWS KMS 金鑰的 kms:GenerateDataKey 許可。

- S3 LocationPrefix

類型：字串

說明：(選用) 您要將自動化輸出上傳到的 Amazon S3 key prefix (子資料夾)。輸出格式存儲在以下格式：`amzn-S3-演示桶/S3LocationPrefix/{{InvestigationType}}_{{自動化}}:EXECUTION_ID.txt`。

### 必要的IAM權限

此 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CLB您在`LoadBalancerName`參數中指定的是否存在。

- `aws:branch`-根據為InvestigationType參數指定的值進行分支。
- `aws:executeScript`-執行連線檢查CLB。
- `aws:executeScript`-驗證CLB組態是否遵循 Elastic Load Balancing 最佳作法。
- `aws:executeScript`-為您創建一個 Amazon CloudWatch 儀表板CLB。
- `aws:executeScript`-建立包含自動化結果的文字檔案，並將其上傳到您在S3Location參數中指定的 Amazon S3 儲存貯體。

## 輸出

RunBestPractices. 摘要

RunConnectivityChecks. 摘要

CreateTroubleshootingDashboard輸出。

UploadOutputTo輸出

# AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

## Description

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancingrunbook 會為您指定的網路負載平衡器 (NLB) 啟用跨區域負載平衡。

## [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- LoadBalancerArn

類型：字串

描述：(必填) 您要在其上啟用跨區域負載平衡的 Amazon 資源名稱 (ARN)。NLB

### 必要的IAM權限

此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-啟用您在LoadBalancerArn參數中指NLB定的跨區域負載平衡。
- aws:executeScript-驗證已在上啟用跨區域負載平衡。NLB

## AWS-UpdateALBDesyncMitigationMode

### Description

AWS-UpdateALBDesyncMitigationModerunbook 會將 Application Load Balancer (ALB) 上的不同步緩和模式更新為指定的緩和模式。dessync 緩和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性風險的要求。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LoadBalancerArn

類型：字串

描述：(必填) 您要修改的不同步緩和模式的 Amazon 資源名稱 (ARN)。ALB

- DesyncMitigationMode

類型：字串

有效值：監控 | 防守 | 最嚴格

描述：(必要) 您要使用的 ALB 緩和模式。如需有關不同步緩和模式的資訊，請參閱《應用程式負載平衡器使用者指南》中的「[不同步緩和模式](#)」。

## 必要的IAM權限

此 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: assertAwsResource Property)-在繼續執行下一個步驟之前，先驗證為 `LoadBalancerArn` 輸入參數指定的值是否適用於應用程式負載平衡器。
- `ModifyLoadBalancerDesyncMode` ( `aws:executeAwsApi`)-更新 ALB 以使用指定的 `DesyncMitigationMode`。
- `VerifyLoadBalancerDesyncMitigationMode` ( `aws:executeScript` ) -驗證目標的不同步緩解模式是否已更新。ALB

## 輸出

`VerifyLoadBalancerDesyncMitigationMode`。 `ModificationResult` -腳本的消息有效負載驗證您的 ALB。

# AWS-UpdateCLBDesyncMitigationMode

## Description

`AWS-UpdateCLBDesyncMitigationMode` 會將 Classic Load Balancer (CLB) 上的不同步緩和模式更新為指定的緩和模式。`desync` 緩和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性風險的要求。

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LoadBalancerName

類型：字串

描述：(必要) 您要修改 CLB 的不同步緩和模式的名稱。

- DesyncMitigationMode

類型：字串

有效值：監控 | 防守 | 最嚴格

描述：(必要) 您要使用的 CLB 緩和模式。如需有關不同步緩和模式的資訊，請參閱《應用程式負載平衡器使用者指南》中的「[不同步緩和模式](#)」。

### 必要的IAM權限

此 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` ) - 驗證目標的不同步緩解模式是否已更新。CLB

### 輸出

VerifyLoadBalancerDesyncMitigationMode。ModificationResult - 腳本的消息有效負載驗證您的 CLB。

# Amazon EMR

AWS Systems Manager 自動化為 Amazon EMR 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 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 會分析檔案系統上已定義的記錄清單，並尋找預先定義的關鍵字清單。這些日誌項目用於建立 Amazon E CloudWatch vents 事件，因此您可以根據事件採取任何必要的動作。或者，執行手冊會將日誌項目發佈到您選擇的 Amazon CloudWatch 日誌日誌群組。此 runbook 目前會在記錄檔中尋找下列錯誤和模式：

- 內存YARN容器-容器內存不足，運行作業可能會失敗。
- yarn\_nodemanager 健康：CORE或TASK節點的磁碟空間不足，將無法執行工作。
- 節點無法存取：CORE或TASK節點無法存取。MASTER
- 步驟失敗：EMR步驟失敗。
- no\_core\_nodes\_run: 目前沒有節點在執行中，CORE叢集狀況不佳。
- 缺失的區塊：有可能導致資料遺失的HDFS區塊。
- hdfs\_high\_util：HDFS使用率很高，可能會影響工作和叢集健康狀況。
- 重新啟動：執行個體控制器處理程序已重新啟動。此程序對於叢集健全狀況至關重要。
- 執行個體控制器處理程序已重新啟動。此程序對於叢集健全狀況至關重要。
- high\_load：偵測到高負載平均值，可能會影響節點健全狀況報告，或導致逾時或變慢。
- yarn\_node\_列入黑名單：CORE或TASK節點已透過執行的工作列入黑名單。YARN
- yarn\_node\_lost：CORE或TASK節點已標記為LOST可能的連線問題。YARN

與您指定之相關聯ClusterID的執行個體必須由管理 AWS Systems Manager。您可以執行此自動化操作一次、將自動化排程在特定時間間隔執行，或移除先前由自動化操作建立的排程。這本手冊支持 Amazon EMR 發布版本 5.20 到 6.30。

## 運行此自動化 (控制台)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterID (ClusterID)

類型：字串

描述：(必要) 您要分析其節點記錄之叢集 ID。

- 作業

類型：字串

有效值：「運行一次」|「計劃」|「刪除計劃」

描述：(必要) 要在叢集上執行的作業。

- IntervalTime

類型：字串

有效值：5 分鐘 | 10 分鐘 | 15 分鐘

說明：(選擇性) 執行自動化操作之間的持續時間。僅當您為參數指定 Schedule 時，此 Operation 參數才適用。

- `LogToCloudWatchLogs`

類型：字串

有效值：是 | 否

描述：(選擇性) 如果您指定`yes`此參數的值，自動化作業會以參數中指定的名稱建立「CloudWatch 記錄」記錄群組，以儲存任何符合的記錄項目。`CloudWatchLogGroup`

- `CloudWatchLogGroup`

類型：字串

說明：(選擇性) 您要儲存任何符合 CloudWatch 記錄項目的記錄檔日誌群組名稱。僅當您為參數指定`yes`時，此`LogToCloudWatchLogs`參數才適用。

- `CreateLogInsightsDashboard`

類型：字串

有效值：是 | 否

描述：(選擇性) 如果您指定`yes`，如果 CloudWatch 儀表板尚未存在，則會建立儀表板。僅當您為參數指定`yes`時，此`LogToCloudWatchLogs`參數才適用。

- `CreateMetricFilters`

類型：字串

有效值：是 | 否

說明：(選擇性) 指定是`yes`否要為「CloudWatch 記錄」日誌群組建立測量結果篩選器。僅當您為參數指定`yes`時，此`LogToCloudWatchLogs`參數才適用。

## 必要的IAM權限

此`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`-基於輸入的分支。

- 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IDs的所有執行個體。
  - `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`-根據您指定執行一次或依排程執行自動化作業而定的分支。
    - 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`-檢查具有在參數中指定名稱的 CloudWatch 記錄記錄群組是否CloudWatchLogGroup已存在。如果不是，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`-每個公制過濾器運行 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`-使用在CloudWatchLogGroup參數中指定的相同名稱建立 CloudWatch儀表板 (如果尚未存在)。
                - 如果`CreateLogInsightsDashboard`值為no：
                  - `aws:runCommand`-執行 shell 指令碼以尋找叢集中每個執行個體的記錄檔模式。
            - 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`-使用在CloudWatchLogGroup參數中指定的相同名稱建立 CloudWatch儀表板 (如果尚未存在)。
                - 如果`CreateLogInsightsDashboard`值為no：
                  - `aws:runCommand`-執行 shell 指令碼以尋找叢集中每個執行個體的記錄檔模式。
        - 如果`LogToCloudWatchLogs`值為no：
          - `aws:executeAwsApi`-執行 shell 指令碼以尋找叢集中每個執行個體的記錄檔模式。



- 如果提供的操作是Schedule：
  - `aws:createStack`-創建一個以此手冊為目標的 Amazon EventBridge 事件。
- 如果提供的操作是Remove Schedule：
  - `aws:executeAwsApi`-驗證叢集的排程是否存在。
  - `aws:deleteStack`-刪除排程。

## 輸出

`GetClusterInformation.ClusterName`

`GetClusterInformation.ClusterState`

`ListingClusterInstances. InstanceIDs`

`CreatingScheduleCloudFormationStack.StackStatus`

`RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus`

`CheckIfLogGroupExists. 輸出。`

`FindLogPatternOnEMRNode.CommandId`

## AWS Support - Diagnose EMR Logs With Athena

### Description

使用 `AWS Support - Diagnose EMR Logs With Athena` Amazon Athena 與 AWS Glue 資料目錄整合，協助診斷亞馬遜EMR日誌。Amazon Athena 可用來查詢容器、節點日誌或兩者的 Amazon 日誌檔，並提供特定日期範圍或關鍵字搜尋的選用參數。

執行手冊可以自動擷取現有叢集的 Amazon EMR 日誌位置，或者您也可以指定 Amazon S3 日誌位置。為了分析日誌，手冊：

- 在 Amazon Amazon S3 日誌位置建立資料 AWS Glue 庫並執行 EMR Amazon Athena 資料定義語言 (DDL) 查詢，以建立叢集日誌的表格和已知問題清單。
- 執行資料操作語言 (DML) 查詢以搜尋 Amazon EMR 日誌中已知的問題模式。查詢會依 Amazon S3 檔案路徑傳回偵測到的問題清單、發生次數，以及符合的關鍵字數目。
- 結果會上傳到您在前置詞下指定的 Amazon S3 儲存貯體 `saw_diagnose_EMR_known_issues`。
- Runbook 會傳回 Amazon Athena 查詢結果，反白顯示發現結果、建議和參考資料，以及來自預先定義子集的 Amazon 知識中心 (KC) 文章。

- 完成或失敗時，會刪除上傳到 Amazon S3 儲存貯體的 AWS Glue 資料庫和已知問題檔案。

它是如何工作的？

使用 Amazon Athena `AWSSupport-DiagnoseEMRLogsWithAthena` 執行 Amazon EMR 日誌的分析，以偵測錯誤並突出顯示發現結果、建議和相關知識中心文章。

執行手冊執行下列步驟：

- 使用 EMR 叢集 ID 取得 Amazon 叢集日誌位置，或輸入 Amazon S3 位置以擷取日誌位置和大小。
- 根據記錄位置大小提供 Athena 成本估算。
- 在執行 Athena 查詢之前，請先要求指定 IAM 主體的核准，然後繼續執行後續步驟，以取得核准。
- 將已知問題上傳到指定的 Amazon S3 儲存貯體，並建立 AWS Glue 資料庫和資料表。
- 在 Amazon EMR 日誌資料上執行 Athena 查詢。查詢可以按日期範圍，關鍵字，兩個條件進行搜索，也可以根據提供的輸入不進行過濾器運行。
- 分析結果以突出顯示發現結果，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理環境。

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：

- 雅典娜：GetQueryExecution
- 雅典娜：StartQueryExecution
- 雅典娜：GetPreparedStatement
- 雅典娜：CreatePreparedStatement
- 膠水:GetDatabase

- 膠水:CreateDatabase
- 膠水>DeleteDatabase
- 膠水:CreateTable
- 膠水:GetTable
- 膠水>DeleteTable
- 彈性構圖 : DescribeCluster
- S3 : ListBucket
- S3 : GetBucketVersioning
- S3 : ListBucketVersions
- S3 : GetBucketPublicAccessBlock
- S3 : GetBucketPolicyStatus
- S3 : GetObject
- S3 : GetBucketLocation
- 定價 : GetProducts
- 定價 : GetAttributeValues
- 定價 : DescribeServices
- 定價 : ListPriceLists

**⚠ Important**

若要限制只存取此自動化所需的資源，請將下列原則附加至信任SSM服務的IAM角色。將「分割區」、「區域」和「帳戶」取代為執行報表簿所在的分割區、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操作：

1. 導航 [AWSSupport-D iagnoseEMRLogs WithAthena](#) 在 AWS Systems Manager 下文檔。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM) ，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ClusterID (必要) :

Amazon EMR 群集 ID。

- S3 LogLocation (選擇性) :

Amazon S3 Amazon EMR 日誌位置。輸入路徑樣式的 URL Amazon S3 位置，例如：`s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/`。如果 Amazon EMR 叢集終止超過30天，請提供此參數。

- S3 BucketName (必要) :

用於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。儲存貯體應啟用「[區塊公共存取](#)」，並且位於與 Amazon EMR 叢集相同的 AWS 區域和帳戶。

- 核准人 (必要):

能夠核准或拒絕動作的 AWS 已驗證主參與者清單。您可以使用下列任一格式來指定主參與者：使用者名稱、使用者ARN、IAM角色或IAM假定角色ARN。核准者的數量上限為 10。

- FetchNodeLogsOnly (選擇性) :

如果設為true，則自動化會診斷 Amazon EMR 應用程式容器日誌。預設值為 false。

- FetchContainersLogsOnly(選擇性) :

如果設定為true，則自動化會診斷 Amazon EMR 容器日誌。預設值為 false。

- EndSearchDate (選擇性) :

記錄搜尋的結束日期。如果提供，自動化操作將專門搜尋截至指定日期之前產生的記錄，格式為 YYYY-MM-DD (例如：)。2024-12-30

- DaysToCheck (選擇性) :

如果EndSearchDate提供此參數，就必須使用此參數來決定從指定的回溯搜尋記錄的天數。EndSearchDate最大值為30天。預設值為 1。

- SearchKeywords (選擇性) :

要在記錄檔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

**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-1K48XXXXXXHCB/`.

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

**FetchContainersLogsOnly**  
(Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster.

false

**DaysToCheck**  
(Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days.

1

**ClusterID**  
(Required) The Amazon EMR cluster ID.

j-1K48XXXXXXHCB

**S3BucketName**  
(Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have [Block Public Access Enabled](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) and be in the same AWS region as the Amazon EMR cluster provided.

[redacted]

**FetchNodeLogsOnly**  
(Optional) If set to "true", the automation diagnoses the Amazon EMR node logs.

false

**EndSearchDate**  
(Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30").

String

**SearchKeywords**  
(Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes.

StringList

#### 4. 選取執行。

#### 5. 自動化啟動。

#### 6. 文件會執行下列步驟：

- `getLogLocation`:

透過查詢指定的 Amazon EMR 叢集 ID 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，則執行手冊會使用 `S3LogLocation` 輸入參數。

- `branchOnValid` 日誌：

驗證 Amazon EMR 日誌的位置。如果該位置有效，請在 Amazon EMR 日誌上執行查詢時，繼續估算 Amazon Athena 潛在成本。

- `estimateAthenaCosts`:

判斷 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 分區），此步驟只提供日誌大小而不估計成本。您可以使用指定區域中的 Athena 定價文件計算成本。

- `approveAutomation`:

等待指定的 IAM 主參與者核准，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 掃描的估計成本，以及自動化佈建資源的詳細資訊。

- `uploadKnownIssuesExecuteAthenaQueries`:

將預先定義的已知問題上傳到 `S3BucketName` 參數中指定的 Amazon S3 儲存貯體。創建 AWS Glue 數據庫和表。根據輸入參數在 AWS Glue 資料庫中執行 Amazon Athena 查詢。

- `getQueryExecution` 狀態：

等待 Amazon Athena 查詢執行SUCCEEDED狀態為止。Amazon Athena DML 查詢會在 Amazon EMR 叢集日誌中搜尋錯誤和例外狀況。

- analyzeAthenaResults:

分析 Amazon Athena 結果，以提供來自一組預先定義對應的調查結果、建議和知識中心 (KC) 文章。

- getAnalyzeResults查詢 1 : ExecutionStatus

等待直到查詢執行SUCCEEDED處於狀態。Amazon Athena DML 查詢會分析先前DML查詢的結果。此分析查詢將返回匹配的異常與分辨率和 KC 文章

- getAnalyzeResults查詢二 : ExecutionStatus

等待直到查詢執行SUCCEEDED處於狀態。Amazon Athena DML 查詢會分析先前DML查詢的結果。此分析查詢將傳回在每個 Amazon S3 日誌路徑中偵測到的例外/錯誤清單。

- printAthenaQueries訊息:

列印 Amazon Athena DML 查詢結果的連結。

- cleanupResources:

刪除建立的資 AWS Glue 料庫以清理資源，並刪除 Amazon EMR Logs 儲存貯體中建立的已知問題檔案。

## 7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

輸出提供三個 Athena 查詢結果連結：

- 列出 Amazon EMR 叢集日誌中發現的所有錯誤和經常發生的例外狀況，以及對應的日誌位置 (Amazon S3 前綴)。
- Amazon EMR 日誌中符合的唯一已知例外摘要，以及建議的解決方案和 KC 文章，以協助進行疑難排解。
- 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.QueriesLinksMessage
log 0:04 Query Link: This link provides a comprehensive view of all the exceptions encountered within your EMR logs.
https://

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://

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://
  
```

## 參考



## Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

### AWS 服務文件

- 如需詳細資訊，請參閱[疑難排解 Amazon EMR 叢集](#)

## Amazon OpenSearch 服務

AWS Systems Manager 自動化為 Amazon OpenSearch 服務提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

## AWSConfigRemediation-DeleteOpenSearchDomain

### Description

該手AWSConfigRemediation-DeleteOpenSearchDomain冊刪除使用給定的 Amazon OpenSearch 服務域. [DeleteDomainAPI](#)

### [運行此自動化 \(控制台\)](#)

### 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 至 Z] {1} [a-z0-9-] {2,28}`

描述：(必填) 您要刪除的 Amazon OpenSearch 服務網域名稱。

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

## 必要的IAM權限

此 `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 服務網域名稱作為輸入、刪除並驗證刪除。

# **AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain**

## Description

該手冊AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain冊啟用EnforceHTTPS在給定的 Amazon OpenSearch 服務域使用 [UpdateDomainConfig](#) API。

## [運行此自動化 \(控制台\)](#)

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 至 Z] {1} [a-z0-9-] {2,28}

描述：(必填) 您要用來強制執行的 Amazon OpenSearch 服務網域名稱HTTPS。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

必要的IAM權限

此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`-在您在`DomainName`參數中指定的 Amazon OpenSearch 服務網域上啟用`EnforceHTTPS`端點選項。

# AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

## Description

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups執行手冊會使用更新指定 Amazon OpenSearch 服務網域上的安全群組組態。[UpdateDomainConfigAPI](#)

### Note

AWS 安全群組只能套用至針對 Amazon 虛擬私有雲端 (VPC) 存取設定的 Amazon OpenSearch 服務網域，而不能套用至針對公用存取設定的 Amazon OpenSearch 服務網域。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

### 參數

- `DomainName`

類型：字串

描述：(必填) 您要用來更新安全群組的 Amazon OpenSearch 服務網域名稱。

- SecurityGroupList

類型: StringList

描述 : (必要) 您要指派給 Amazon OpenSearch 服務網域的安全群組IDs。

- AutomationAssumeRole

類型 : 字串

描述 : (必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

### 必要的IAM權限

此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 服務網域上的安全群組組態。

## AWSSupport-TroubleshootOpenSearchRedYellowCluster

### Description

AWSSupport-TroubleshootOpenSearchRedYellowCluster 自動化 runbook 用於識別[紅色或黃色叢集健康狀態](#)的原因，並引導您將叢集變更回綠色。

它是如何工作的？

runbook 可AWSSupport-TroubleshootOpenSearchRedYellowCluster協助您疑難排解紅色或黃色叢集的原因，並提供透過分析叢集配置和資源使用率來解決此問題的後續步驟。

執行手冊執行下列步驟：

- 呼叫 [DescribeDomain](#) API 針對目標網域以取得叢集配置。
- 檢查 OpenSearch 服務網域是以網際網路為基礎 (公用) 還是以 [Amazon Virtual Private Cloud \(VPC\) 為基礎](#)。
- 根據叢集組態建立公用或 [Amazon VPC 型](#) AWS Lambda 函數。備註：Lambda 函數包含 APIs 針對叢集執行 OpenSearch 服務的疑難排解程式碼，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 權限

此 `AutomationAssumeRole` 參數需要執行下列動作，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`

此 `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` 政策概述：

以下是 Lambda 函數的執行角色 (AWS Identity and Access Management (IAM) 角色) 範例，該角色授與函數存取此 Runbook 所需 AWS 服務和資源的權限。如需更多詳細資訊，請參閱 [Lambda 執行角色](#)。

#### Note

只 `ec2>DeleteNetworkInterface` 有當您的 `ec2:DescribeNetworkInterfaces` OpenSearch 服務叢集是 [VPC 以 Amazon 為基礎](#) `ec2:CreateNetworkInterface`，以允許 Lambda 函數建立和管理 Amazon VPC 網路界面時，才需要、和。如需詳細資訊，請參閱將 [輸出網路連線至 Amazon VPC 和 Lambda 執行角色中的資源](#)。

```
{
```

```

    "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操作：



1. 導覽至主 AWS Systems Manager 控制台 TroubleshootOpenSearchRedYellowCluster 中的 [AWSSupport-](#)

2. 選擇 Execute automation (執行自動化)。

3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LambdaExecutionRole (必填)：

Lambda 將用來向您ARN的 Amazon OpenSearch 服務叢集簽署請求的IAM角色。

- DomainName (必填)：

具有紅色或黃色叢集健全狀況狀態的 OpenSearch 服務網域名稱。

- UtilizationThreshold (選擇性)：

用來比較CPUUtilization和JVMMemoryPressure測量結果的使用率臨界值百分比。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'.

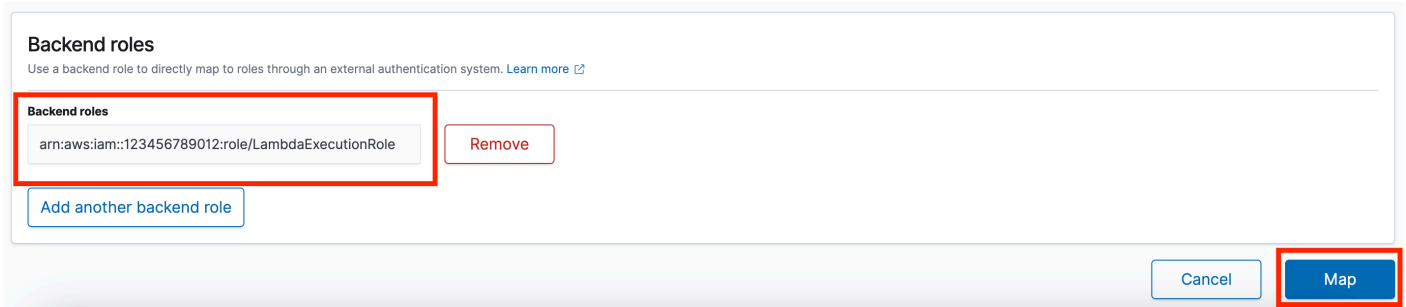
80

4. 如果您已在 OpenSearch Service 叢集上啟用[精細的存取控制](#)，請確定LambdaExecutionRole角色 arn 已對應至少cluster\_monitor具有權限的角色。

**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



5. 選取執行。

6. 自動化啟動。

7. 自動化工作流程簿執行下列步驟：

- GetClusterConfiguration:

擷取 OpenSearch 服務叢集配置。

- CreateAWSLambdaFunctionStack:

使用建立帳戶中的臨時 Lambda 函數 AWS CloudFormation。Lambda 函數用於執行 OpenSearch 服務APIs。

- WaitForAWSLambdaFunctionStack:

等待 CloudFormation 堆棧完成。

- GetClusterMetricsFromCloudWatch:

取得 Amazon CloudWatch ClusterStatus CPUUtilization、和JVMMemoryPressure OpenSearch 服務叢集相關指標及其建立日期。

- RunOpenSearchAPIs:

使用 Lambda 函數呼叫 OpenSearch 服務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:

刪除帳戶中此自動化操作所建立的 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:

提供叢集健全狀況為紅色或黃色狀態的已識別原因的概觀。

- IssueDescription:

提供叢集為何處於紅色或黃色狀態的詳細資訊，以及將叢集恢復為綠色狀態的可能步驟。

## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化 workflow 登陸頁](#)

### AWS 服務文件

- 如需詳細資訊，請參閱[疑難排解 Amazon OpenSearch 服務](#)

## AWSSupport-TroubleshootOpenSearchHighCPU

### Description

AWSSupport-TroubleshootOpenSearchHighCPURunbook 提供自動化的解決方案，可從 Amazon OpenSearch 服務網域收集診斷資料，以便對[高CPU](#)問題進行疑難排解。

它是如何工作的？

AWSSupport-TroubleshootOpenSearchHighCPU執行手冊有助於疑難排解 Amazon OpenSearch 服務網域中的高CPU使用率。

執行手冊執行下列步驟：

- [DescribeDomain](#) API針對提供的 Amazon OpenSearch 服務網域執行，以取得叢集中繼資料。
- 檢查 Amazon OpenSearch 服務域是公共或VPC基於 Amazon 的，並在的幫助下 AWS CloudFormation，創建一個[VPC基於公共或 Amazon](#)的 AWS Lambda 功能。
- Lambda 函數會從 Amazon OpenSearch 服務網域擷取診斷資料。
- 使用 AWS Step Functions 狀態機器協調多個 Lambda 函數執行，以收集更全面的資料。
- 依預設，將收集的資料存放在 Amazon CloudWatch 日誌群組中 24 小時。
- 刪除建立的資源 ( CloudWatch 記錄群組除外)。

## 文件類型

自動化

擁有者

Amazon

平台

Linux, macOS, Windows

參數

必要的IAM權限

此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

此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 執行角色授予函數存取此手冊所需 AWS 服務和資源的權限。如需更多詳細資訊，請參閱 [Lambda 執行角色](#)。

**Note**

只 `ec2:DeleteNetworkInterface` 有當您的 `ec2:DescribeNetworkInterfaces`。OpenSearch 服務叢集是 [VPC 以 Amazon 為基礎 `ec2:CreateNetworkInterface`](#)，以允許 Lambda 函數建立和管理 Amazon VPC 網路界面時，才需要、和。如需詳細資訊，請參閱將 [輸出網路連線至 Amazon VPC 和 Lambda 執行角色中的資源](#)。

**指示**

請依照下列步驟設定自動化操作：

1. 導覽至主 AWS Systems Manager 控制台 TroubleshootOpenSearchHighCPU 中的 [AWSSupport-](#)。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DomainName (必填)：

您要針對高CPU問題進行疑難排解的 Amazon OpenSearch 服務網域名稱。

- LambdaExecutionRoleForOpenSearch (必填)：

要附加至 Lambda 函數ARN的IAM角色。Lambda 函數使用此角色的登入資料，將請求簽署到 Amazon OpenSearch 服務網域。如果在 Amazon OpenSearch 服務網域上啟用了精細的存取控制，則必須將此角色對應至少具有「cluster\_monitor」權限的 OpenSearch 服務儀表板後端角色。

- DataRetentionDays (選擇性)：

保留從 Amazon OpenSearch 服務網域收集的診斷資料的天數。依預設，資料會保留 24 小時 (一天)。您可以選擇保留資料最多 30 天。

- NumberOfDataSamples (選擇性)：

要從 Amazon OpenSearch 服務網域收集的資料樣本數量。依預設，會收集 5 個資料樣本。您最多可以收集 10 個樣本，並針對每個樣本集合叫用 Lambda 函數。

**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.

**LambdaExecutionRoleForOpenSearch**  
(Required) The ARN of the IAM role to attach to the Lambda function. The Lambda function uses the credentials from this role sign requests to your AOS domain. If Fine-grained access control (FGAC) is enabled on your AOS domain, you must map this role to an OpenSearch dashboards backend role with minimum of "cluster\_monitor" permission.

**NumberOfDataSamples**  
(Optional) The number of data samples to collect from the AOS domain. By default, 5 data sample are collected by the automation. You can collect up to 10 samples and the Lambda function will be invoked for each sample collection.

**DomainName**  
(Required) The name of the Amazon OpenSearch domain that you want to troubleshoot for high CPU issues.

**DataRetentionDays**  
(Optional) The number of days to retain the diagnostic data collected from the AOS domain. By default, the data retained for 24 hours (1 day). You can choose to retain the data for maximum of 7 days period.

4. 如果您已在 OpenSearch Service 叢集上啟用精細的存取控制，請確定LambdaExecutionRole角色 arn 已對應至少cluster\_monitor具有權限的角色。

**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::[redacted]:role/LambdaExecutionRole Remove

Add another backend role

Cancel Map

5. 選取執行。
6. 自動化啟動。
7. 自動化工作流程簿執行下列步驟：

- checkConcurrency:

確保只有一個執行此手冊針對指定的 Amazon OpenSearch 服務域。如果 runbook 找到另一個針對相同網域名稱的執行，則會傳回錯誤並結束。

- getDomainConfig:

取得目標 OpenSearch 服務網域的組態詳細資訊。

- provisionResources:

規定使用的資源收集數據 AWS CloudFormation。

- waitForStack創作：

等待 AWS CloudFormation 堆棧完成。

- describeStackResources:

描述 AWS CloudFormation 堆疊並取得ARN狀態機器。

- runStateMachine:

透過執行 Step Functions 函數狀態機器叫用資料收集器 Lambda 函數一或多次。

- describeErrorsFromStackEvents:

描述錯誤 AWS CloudFormation 堆疊中的錯誤。

- unstageOpenSearchHighCPUAutomation:

刪除AWSSupport-TroubleshootOpenSearchHighCPU AWS CloudFormation 堆疊。

- describeErrorsFromStackDeletion:

說明刪除 AWS CloudFormation 堆疊時遇到的錯誤。

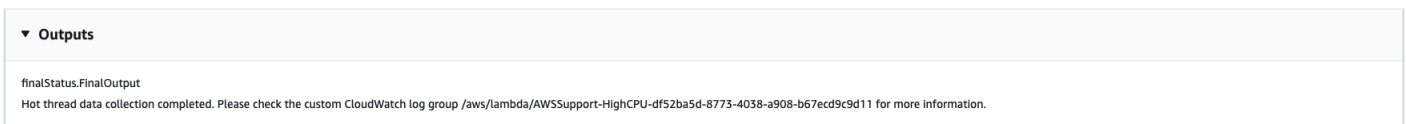
- finalStatus:

返回工作AWSSupport-TroubleshootOpenSearchHighCPU簿的最終輸出。

8. 完成後，請檢閱「輸出」區段以取得執行的詳細結果。

- finalStatus.FinalOutput:

提供儲存診斷資料的 CloudWatch 記錄群組。



## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化 workflow 登陸頁](#)

### AWS 服務文件



- 如需詳細資訊，請參閱[疑難排解 Amazon OpenSearch 服務](#)

## EventBridge

AWS Systems Manager 自動化為 Amazon EventBridge 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

## AWS-AddOpsItemDedupStringToEventBridgeRule

### Description

AWS-AddOpsItemDedupStringToEventBridgeRuleRunbook 為所有與 Amazon EventBridge 規則 AWS Systems Manager OpsItems 相關聯的重複資料刪除新增字串。runbook 不會將重複資料刪除字串新增至規則 (如果已套用)。若要瞭解更多重複資料刪除字串 OpsItems，請參閱AWS Systems Manager 使用指南 OpsItems中的〈[減少重複項目](#)〉。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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權限

此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

手AWS-DisableEventBridgeRule冊禁用您指定的 Amazon 規 EventBridge 則。要了解有關 EventBridge 規則的更多信息，請參閱 [Amazon 用戶指南中的 Amazon EventBridge 規則](#)。

### [運行此自動化 \(控制台\)](#)

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EventBusName

類型：字串

預設值：預設

描述：(選擇性) 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權限

此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。

# Amazon FSx

AWS Systems Manager 自動化為 Amazon FSx 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWSSupport-ValidateFSxWindowsADConfig](#)

## AWSSupport-ValidateFSxWindowsADConfig

### Description

該手冊AWSSupport-ValidateFSxWindowsADConfig用於驗證自我管理的活動目錄 ( AD ) 配置的 Amazon 的 Windows 文件FSx服務器

它是如何工作的？

該手冊AWSSupport-ValidateFSxWindowsADConfig執行 Amazon FSx 驗證腳本上的臨時 Amazon 彈性計算雲 ( AmazonEC2 ) Windows 實例由流行簿在 Amazon FSx 子網上啟動。指令碼會執行多項檢查，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。該手冊可以驗證失敗或錯誤配置的 Amazon FSx Windows 文件服務器或創建一個新的 Amazon FSx 的 Windows 文件服務器與自我管理 AD。

根據預設，執行手冊會在 Amazon FSx 子網路 AWS CloudFormation 上建立 Amazon EC2 Windows 執行個體、AWS Systems Manager AWS Identity and Access Management (SSMIAM) 存取的安全群組、() 角色和政策。如果要在現有 Amazon 執行個體上執行指令碼，請在參數中提供 ID InstanceId。在成功執行時，它會刪除 CloudFormation 資源。但是，若要保留資源，請將RetainCloudFormationStack參數設定為true。

CloudFormation 範本會代表您建立具有必要許可的IAM角色，以便連接到 Amazon EC2 執行個體以執行 Amazon FSx 驗證指令碼。若要指定暫存IAM例證的既有例證紀要，請使用InstanceProfileName參數。相關聯的IAM角色必須包含下列權限：

- `ec2:DescribeSubnets`和`ec2:DescribeVpcs`許可和 Amazon 託管政策AmazonSSMManagedInstanceCore。

- 通過調用從 Systems Manager 獲取 Amazon FSx 服務帳戶用戶用戶名和密碼的許可 GetSecretValueAPI。
- 將物件放入 Amazon Simple Storage Service (Amazon S3) 貯體中以進行指令碼輸出的許可。

## 先決條件

建立臨時 Amazon EC2 執行個體的子網路 (或 InstanceId 參數中提供的現有執行個體) 必須允許存取 AWS Systems Manager AWS Secrets Manager、和 Amazon S3 端點，才能使用執行命令 SSM 執行指令 AmazonFSxADValidation 碼。

## AWS Secrets Manager 設置

驗證指令碼會透過執行時間呼叫 Secrets Manager 擷取 Amazon FSx 服務帳戶使用者名稱和密碼來連線至 Microsoft AD 網域。依照 [建立密 AWS Secrets Manager 碼](#) 中的步驟來建立新的 Secrets Manager 密碼。確保使用格式的鍵/值對存儲用戶名和密碼。{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"} 如需有關保護密碼 [存取的 AWS Secrets Manager 資訊](#)，請參閱 [驗證和存取控制](#)。

如需有關此工具的詳細資訊，請參閱 [AmazonFSx ADValidation](#) 檔案中的 TROUBLESHOOTING.md 和 README.md 檔案。

## 手冊執行

使用 Amazon FSx ID 或 AD 參數執行手冊。以下是手冊工作流程：

- 從 Amazon FSx ID 取得參數，或使用輸入 AD 參數。
- 在 Amazon FSx 子網路上建立臨時驗證 Amazon EC2 Windows 執行個體、使用的 SSM 存取安全群組、IAM 角色和政策 (條件式) CloudFormation。如果指定了 InstanceId 參數，則會使用該參數。
- 在 Amazon FSx 主要子網路中的目標 Amazon 執行 EC2 個體上下載並執行驗證指令碼。
- 在自動化輸出中提供 AD 驗證結果代碼。此外，完整的指令碼輸出也會上傳到 Amazon S3 儲存貯體。

## [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

### 擁有者

## Amazon

### 平台

### Windows

### 參數

#### 必要的IAM權限

此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

## 自動化假設角色的範例IAM原則

```
{
  "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操作：

1. 瀏覽至「文件」下 [AWSSupport-ValidateFSxWindowsADConfig](#) 的「Systems Manager」。
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 驗證自我管理 ADFSx，請輸入下列參數：

- AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- FSxId (有條件)：

Amazon FSx 視窗檔案伺服器識別碼。這是驗證現有失敗或配置錯誤的 Amazon FSx 所必需的。

- SecretArn (必填)：

您的 ARN 的 Secrets Manager 秘密包含 Amazon FSx 服務帳戶用戶名和密碼。確保使用格式的鍵/值對存儲用戶名和密碼。{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"} CloudFormation 堆棧創建具有執行 GetSecretValue 此操作的權限的驗證實例 ARN。

- FSxSecurityGroupId ( 必填 ) :

適用於 Windows 檔案伺服器的 Amazon FSx 安全群組識別碼。

- BucketName ( 必填 ) :

用於將驗證結果上傳到的 Amazon S3 儲存貯體。請確定值區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/寫入權限授與不需要存取記錄的對象。此外, 還要確保 Amazon EC2 Windows 實例具有對 Amazon S3 存儲桶的必要訪問權限。

**Input parameters**

**InstanceId**  
 (Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. **\*\*Caution\*\*:** The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, **\*\*do not use a production instance\*\***. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

Show interactive instance picker

**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.

**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"}.

**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.

**FSxSecurityGroupId**  
 (Required) The security group ID of the Amazon FSx for Windows File Server.

**RetainCloudFormationStack**  
 (Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

**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.

#### 4. 若要驗證新 FSx 建 Amazon 的自我管理 AD 組態, 請輸入下列參數 :

- AutomationAssumeRole ( 選擇性 ) :

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM) , 可讓 Systems Manager 自動化代表您執行動作。如果未指定角色, Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- SecretArn ( 必填 ) :

您ARN的 Secrets Manager 秘密包含 Amazon FSx 服務帳戶用戶名和密碼。確保使用格式的鍵/值對存儲用戶名和密碼。{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"} CloudFormation 堆棧創建具有執行GetSecretValue此操作的權限的驗證實例ARN。

- FSxSecurityGroupId ( 必填 ) :

適用於 Windows 檔案伺服器的 Amazon FSx 安全群組識別碼。

- BucketName ( 必填 ) :

用於將驗證結果上傳到的 Amazon S3 儲存貯體。請確定值區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/寫入權限授與不需要存取記錄的對象。此外, 還要確保 Amazon EC2 Windows 實例具有對 Amazon S3 存儲桶的必要訪問權限。

- FSxPreferredSubnetId ( 有條件 ) :

Amazon FSx 視窗檔案伺服器偏好的子網路。

- DomainName ( 有條件 ) :

您自我管理的 Microsoft AD 網域的完整網域名稱。

- DnsIpAddresses ( 有條件 ) :

自我管理 AD 網域中最多兩個DNS伺服器或網域控制站 IP 位址的清單。對於最多兩個IPs, 輸入它們以逗號分隔。

- FSxAdminsGroup ( 有條件 ) :

Amazon FSx 視窗檔案伺服器委派的檔案系統管理員群組。根據預設, 此為 Domain Admins。

- FSxOrganizationalUnit ( 有條件 ) :

您要在其中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

**DnsIpsAddresses**

(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與其物件的讀取和/或寫入公開存取權。

- **BranchOnInputParameters** ( aws : 分支機構 ) :

在提供的輸入參數 ( 如 Amazon FSx ID 或 Amazon FSx 參數 ) 上的分支機構。

- **AssertFileSystemTypesWindows** ( AWS : assertAwsResource屬性 ) :

如果提供 Amazon FSx ID , 則驗證 Windows 文件服務器的文件系統類型是 Amazon FSx。

- **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 : 分支機構 ) :

在所提供的輸入分支InstanceId。如果InstanceId有提供 , 驗證指令碼會透過自動化在目標 Amazon EC2 執行個體上執行step:RunValidationScript。

- **創建EC2InstanceStack** ( AWS : createStack ) :

使用將執行AmazonFSxADValidation工具的位 AWS CloudFormation 置，在偏好的子網路中建立 Amazon 執行EC2個體

- DescribeStackResources ( AWS : executeAwsApi ) :

描述取得暫存 Amazon EC2 執行個體 ID 的 CloudFormation 堆疊。

- WaitForEC2InstanceToBeManaged ( AWS : waitForAwsResourceProperty ) :

等待 Amazon EC2 執行個體由系統管理員管理，才能使用執行命令SSM執行驗證指令碼。

- GetAmazonFSxADValidationAttachment ( AWS : executeAwsApi ) :

URL從AmazonFSxADValidation工作流程簿附件中取得工具。

- RunValidationScript ( AWS : runCommand ) :

在臨時 Amazon 執行個體上EC2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 ) :

描述工作流程簿無法建立 CloudFormation 堆疊時的堆疊事件。

- BranchOnRetainCloudFormationStack ( aws : 分支機構 ) :

RetainCloudFormationStack和InstanceId參數上的分支，以確定是否應刪除 CloudFormation 堆疊。

- DeleteCloudFormationStack ( AWS : deleteStack ) :

刪除 AWS CloudFormation 堆疊。

8. 完成後，請檢閱「輸出」區段以瞭解執行結果：



```
▼ Outputs

DescribeInstanceAndSubnet.InstanceId
i-06: ██████████

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:██████████: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.msf.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-0██████████
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.
```

執行手冊會將驗證指令碼執行的結果上傳到 Amazon S3 儲存貯體。

## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

### AWS 服務文件

- [什麼是 Amazon FSx 的視窗文件服務器？](#)
- [驗證適用於 Windows 檔案伺服器的 Amazon FSx 自我管理 AD 組態](#)

## GuardDuty

AWS Systems Manager 自動化為 Amazon GuardDuty 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

## 主題

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

# AWSConfigRemediation-CreateGuardDutyDetector

## Description

該手AWSConfigRemediation-CreateGuardDutyDetector冊創建一個 Amazon GuardDuty ( GuardDuty ) 檢測器在 AWS 區域 那裡你運行自動化。

## [運行此自動化 \( 控制台 \)](#)

## 文件類型

自動化

## 擁有者

Amazon

## 平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

## 必要的IAM權限

此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`-創建一個 GuardDuty 檢測器。
- `aws:assertAwsResourceProperty`-驗證檢測器Status的是ENABLED。

## IAM

AWS Systems Manager 自動化提供預先定義的 AWS Identity and Access Management 執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [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](#)

## AWS-AttachIAMToInstance

### Description

將 AWS Identity and Access Management (IAM) 角色附加至代管執行個體。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- ForceReplace

類型：布林值

說明：(選擇性) 指定是否要取代現有 IAM 設定檔的旗標。

預設：true

- InstanceId

類型：字串

說明：(必要) 您要指派 IAM 角色的執行個體 ID。

- RoleName

類型：字串

說明：(必要) 要新增至代管執行個體的 IAM 角色名稱。

### 文件步驟

1. `aws:executeAwsApi- DescribeInstanceProfile` - 查找附加到IAM實例的實EC2例配置文件。
2. `aws:branch- CheckInstanceProfileAssociations` - 檢查附加到IAM實例的實EC2例配置文件。
  - a. 如果已貼附IAM執行個體設定ForceReplace檔並設定為true：
    - i. `aws:executeAwsApi- DisassociateIAMInstanceProfile` - 取消IAM實例配置文件與實EC2例的關聯。
    - b. `aws:executeAwsApi- ListInstanceProfilesForRole` - 列出所提供IAM角色的執行個體設定檔。
    - c. `aws:branch- CheckInstanceProfileCreated` - 檢查提供的IAM角色是否具有相關聯的執行個體設定檔。
      - i. 如果IAM角色具有相關聯的執行個體設定檔：
        - A. `aws:executeAwsApi- AttachIAMProfile ToInstance` - 將執行個IAM體設定檔角色附加至EC2執行個體。
      - i. 如果IAM角色沒有關聯的執行個體設定檔：
        - A. `aws:executeAwsApi- CreateInstanceProfileForRole` - 為指定角色建立執行個體設定檔IAM角色。
        - B. `aws:executeAwsApi- AddRoleToInstanceProfile` - 將執行個體設定檔角色附加至指定的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- AttachIAMProfile ToInstanceWithRetry` - 將執行個IAM體設定檔角色附加至EC2執行個體。

## 輸出

`AttachIAMProfileToInstanceWithRetry. AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`AttachIAMProfileToInstance. AssociationId`

`ListInstanceProfilesForRole.InstanceProfileName`

`ListInstanceProfilesForRole.InstanceProfileArn`

## AWS-DeleteIAMInlinePolicy

### Description

AWS-DeleteIAMInlinePolicyrunbook 會刪除所有 AWS Identity and Access Management (IAM) 內嵌原則附加至您指定的IAM識別。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- IamArns

類型：字串

說明：(必要) 您要刪除內嵌原則之IAM身分的ARNs逗號分隔清單。此清單可包括IAM使用者、群組或角色。

必要的IAM權限

此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-刪除附加至目標IAM身分的IAM內嵌原則。

## AWSConfigRemediation-DeleteIAMRole

### Description

R AWSConfigRemediation-DeleteIAMRole unbook 會刪除您指定的 AWS Identity and Access Management (IAM) 角色。此自動化操IAM作不會刪除與角色或服務連結角色相關聯的執行個體設定檔。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMRoleID

類型：字串

描述：( 必填 ) 您要刪除的IAM角色 ID。

### 必要的IAM權限

此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設定檔。
- `aws:executeScript`-刪除附加的策略。
- `aws:executeScript`-刪除IAM角色並驗證角色已刪除。

## AWSConfigRemediation-DeleteIAMUser

### Description

R AWSConfigRemediation-DeleteIAMUser unbook 會刪除您指定的 AWS Identity and Access Management (IAM) 使用者。此自動化操作會刪除或分離下列與IAM使用者相關聯的資源：

- 存取金鑰



- 附加的管理策略
- Git 認證
- 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公開金鑰

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMUserId

類型：字串

描述：(必要) 您要刪除的IAM使用者 ID。

必要的IAM權限

此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>ListGroupsForUser
- 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使用者的使用者名稱。
- aws:executeScript-收集與IAM使用者關聯的存取金鑰、憑證、憑證、MFA裝置和SSH金鑰。

- `aws:executeScript`-收集使IAM用者的群組成員資格和政策。
- `aws:executeScript`-刪除與IAM使用者關聯的存取SSH金鑰、憑證、認證、MFA裝置和金鑰。
- `aws:executeScript`-刪除IAM使用者的群組成員資格和原則。
- `aws:executeScript`-刪除使IAM用者並確認使用者已刪除。

## AWSConfigRemediation-DeleteUnusedIAMGroup

### Description

R AWSConfigRemediation-DeleteUnusedIAMGroup unbook 會刪除不包含任何使用者的IAM群組。

R AWSConfigRemediation-DeleteUnusedIAMGroup unbook 會刪除不包含任何使用者的IAM群組。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

#### 自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- GroupName

類型：字串

描述：(必要) 您要刪除的IAM群組名稱。

### 必要的IAM權限

此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`-移除附加至目標IAM群組的受管理和內嵌IAM政策，然後刪除IAM群組。

## AWSConfigRemediation-DeleteUnusedIAMPolicy

### Description

AWSConfigRemediation-DeleteUnusedIAMPolicyrunbook 會刪除未附加至任何使用者、群組或角色的 AWS Identity and Access Management (IAM) 原則。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMResourceId

類型：字串

描述：(必要) 您要刪除之IAM策略的資源識別碼。

### 必要的IAM權限

此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參數中指定的策略，並驗證策略已刪除。

## AWSConfigRemediation-DetachIAMPolicy

### Description

AWSConfigRemediation-DetachIAMPolicy執行本會分離您指定的 AWS Identity and Access Management (IAM) 原則。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMResourceId

類型：字串

描述：(必要) 您要卸離的IAM原則識別碼。

### 必要的IAM權限

此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`-從所有資源中分離IAM策略。

# AWSConfigRemediation-EnableAccountAccessAnalyzer

## Description

該 `AWSConfigRemediation-EnableAccountAccessAnalyzer` runbook 創建一個 AWS Identity and Access Management ( IAM ) 訪問分析器在您的 AWS 帳戶. 如需有關存取分析器的資訊, 請參閱 [使用IAM者指南中的使用 AWS IAM存取分析器](#)。

## [運行此自動化 \( 控制台 \)](#)

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, 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) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

## 必要的IAM權限

此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-為您的帳戶創建訪問分析器。
- 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 會將指定的權限授予IAM群組 (新的或現有的)，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](#)。若要啟用的帳單存取權IAM，請記得同時啟[IAM用使用者和同盟使用者存取 \[Billing and Cost Management\] 頁面](#)。

### Important

如果您提供現有IAM群組，群組中的所有目前IAM使用者都會收到新的權限。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台



## LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- IAMGroupName

類型：字串

預設值：ExampleSupportAndBillingGroup

描述：(必要) 可以是新的或現有的群組。必須符合[IAM 實體名稱限制](#)。

- IAMUserName

類型：字串

預設值：ExampleUser

描述：(必要) 必須是現有的使用者。

- LambdaAssumeRole

類型：字串

描述：(選擇ARN性) lambda 所承擔的角色。

- 許可

類型：字串

有效值：SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

預設值：SupportAndBillingFullAccess

說明：(必要) 選擇下列其中一項：SupportFullAccess 授予 Support 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 Support 中心和帳單控制面板的完整存取權。您可以在文件詳細資訊下的政策找到更多資訊。

## 必要的IAM權限

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

所需的權限取決於執AWSSupport-GrantPermissionsToIAMUser行方式。

以目前登入的使用者或角色身分執行

我們建議您附加 AmazonSSMAutomationRole Amazon 受管政策，以及下列其他許可，以便能夠建立 Lambda 函數和要傳遞給 Lambda 的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` 權限，以及 `iam: PassRole` 以和傳遞的 IAM 角色。AutomationAssumeRoleLambdaAssumeRole 以下是每個 IAM 角色所需的權限：

### AutomationAssumeRole

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda>DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
"arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
            "Effect": "Allow"
        }
    ]
}

```

```
}
```

### LambdaAssumeRole

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
            "arn:aws:iam::aws:policy/job-function/Billing",
            "arn:aws:iam::aws:policy/AWSSupportAccess"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
      ],
    }
  ]
}
```

```
        "Resource" : "*"
      }
    ]
  }
```

### 文件步驟

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權限。
3. `aws:deleteStack`-刪除 CloudFormation 模板。

### 輸出

配置IAM. 有效載荷

## AWSConfigRemediation-RemoveUserPolicies

### Description

AWSConfigRemediation-RemoveUserPoliciesrunbook 會刪除 AWS Identity and Access Management (IAM) 內嵌原則，並卸離任何附加至您指定之使用者的受管理策略。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMUserID

類型：字串

描述：(必要) 您要從中移除策略的使用者 ID。

- PolicyType

類型：字串

有效值：全部 | 內嵌 | 管理

預設值：全部

描述：(必要) 您要從使用者移除的IAM策略類型。

### 必要的IAM權限

此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-從您在IAMUserID參數中指定的使用者刪除和解除連結IAM策略。

## AWSConfigRemediation-ReplaceIAMInlinePolicy

### Description

AWSConfigRemediation-ReplaceIAMInlinePolicyrunbook 會以複寫的受管理原則取代內嵌 AWS Identity and Access Management (IAM) IAM 原則。針對連結至使用者、群組或角色的內嵌原則，內嵌原則權限會複製到受管理的IAM原則中。受管理的IAM策略會新增至資源，並移除內嵌政策。AWS Config 必須在您執行此自動化操作的 AWS 區域 位置啟用。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。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) 您要取代其內嵌原則之IAM使用者、群組或角色的 ID。

### 必要的IAM權限

此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原則取代為您指定之資源上的 AWS 複寫原則。

## AWSConfigRemediation-RevokeUnusedIAMUserCredentials

### Description

AWSConfigRemediation-RevokeUnusedIAMUserCredentialsrunbook 撤銷未使用的 AWS Identity and Access Management ( IAM ) 密碼和活動訪問密鑰。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操作的 AWS 區域 位置啟用。

### [運行此自動化 \( 控制台 \)](#)

### 文件類型

#### 自動化



## 擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- IAMResourceId

類型：字串

描述：(必要) 您要撤銷未使用認證的IAM資源 ID。

- MaxCredentialUsageAge

類型：字串

預設：90

說明：(必要) 必須使用認證的天數。

## 必要的IAM權限

此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參數中指定之使用者的IAM認證。過期的存取金鑰會停用，並刪除過期的登入設定檔。

#### Note

請務必將此修正動作的MaxCredentialUsageAge參數設定為符合您用來觸發此動作的 AWS Config 規則maxAccessKeyAge參數：[access-keys-rotated](#)。

## AWSConfigRemediation-SetIAMPASSWORDPolicy

### Description

AWSConfigRemediation-SetIAMPASSWORDPolicyrunbook 會設定您 AWS 帳戶的 AWS Identity and Access Management (IAM) 使用者密碼原則。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- AllowUsersToChangePassword

類型：布林值

預設：false

描述：(選用) 如果設定為true，則您中的所有使用IAM者都 AWS 帳戶 可以使用 AWS Management Console 來變更其密碼。

- HardExpiry

類型：布林值

預設：false

說明：(選擇性) 如果設定為true，IAM使用者將無法在密碼到期後重設密碼。

- MaxPasswordAge

類型：整數

預設：0

說明：(選擇性) IAM 使用者密碼有效的天數。

- MinimumPasswordLength

類型：整數

預設：6

說明：(選擇性) 使IAM用者密碼可包含的字元數目下限。

- PasswordReusePrevention

類型：整數

預設：0

說明：(選擇性) 使用IAM者無法重複使用的先前密碼數目。

- `RequireLowercaseCharacters`

類型：布林值

預設：false

描述：(選擇性) 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) 的小寫字元。

- `RequireNumbers`

類型：布林值

預設：false

描述：(選擇性) 如果設定為true，則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：(選擇性) 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：(選擇性) 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) 的大寫字元。

## 必要的IAM權限

此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`-根據您為您的 `runbook` 參數指定的值設定IAM使用者密碼原則。AWS 帳戶

# Amazon Kinesis Data Streams

AWS Systems Manager 自動化為 Amazon Kinesis Data Streams 提供預先定義的執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 `runbook` 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-EnableKinesisStreamEncryption](#)

## AWS-EnableKinesisStreamEncryption

### Description

`AWS-EnableKinesisStreamEncryption`執行手冊可在 Amazon Kinesis 資料串流 (Kinesis 資料串流) 上啟用加密功能。如果生產者應用程式無法存取 AWS Key Management Service (AWS KMS) 金鑰，寫入加密串流時會遇到錯誤。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- KinesisStreamName

類型：字串

說明：(必要) 您要啟用加密的串流名稱。

- KeyId

類型：字串

預設值：別名/AWS/ 運動

說明：(必要) 您要用於加密的客戶管理 AWS KMS 金鑰。這個值可以是一個全局唯一的標識符，一個別名或一個鍵，或者一個別名名稱前綴ARN為「alias/」。您也可以使用參數的預設值來使用 AWS 受管理的金鑰。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 的加密功能。
- VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty)-等待 Kinesis Data Streams 狀態返回。ACTIVE

- `VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty)`-確認 Kinesis Data Streams 已啟用加密功能。

## AWS KMS

AWS Systems Manager 自動化提供預先定義的 AWS Key Management Service 執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

### 主題

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

## AWSConfigRemediation-CancelKeyDeletion

### Description

AWSConfigRemediation-CancelKeyDeletionrunbook 會取消刪除您指定的 AWS Key Management Service (AWS KMS) 客戶管理的金鑰。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- KeyId

類型：字串

描述：(必要) 您要取消刪除之客戶管理金鑰的 ID。

### 必要的IAM權限

此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參數中指定的客戶管理金鑰。
- aws:assertAwsResourceProperty-確認已停用客戶管理金鑰上的金鑰刪除功能。

## AWSConfigRemediation-EnableKeyRotation

### Description

AWSConfigRemediation-EnableKeyRotationrunbook 可為對稱 AWS Key Management Service (AWS KMS) 客戶管理的金鑰啟用自動金鑰輪換。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon



## 平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- KeyId

類型：字串

說明：(必要) 您要啟用自動金鑰輪換的客戶管理金鑰 ID。

## 必要的IAM權限

此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參數中指定的客戶管理金鑰啟用自動金鑰輪換。
- aws:assertAwsResourceProperty-確認您的客戶管理金鑰上已啟用自動金鑰輪換功能。

## Lambda

AWS Systems Manager 自動化提供預先定義的 AWS Lambda執行手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

## AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

### Description

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracingrunbook 可在您在參數中指定的 AWS Lambda 函FunctionName數上啟用 AWS X-Ray 即時追蹤。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- FunctionName

類型：字串

描述：(必要) 啟用追蹤ARN的 Lambda 函數的名稱或名稱。

### 必要的IAM權限

此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`-對您在參數中指定的 Lambda 函數FunctionName數啟用 X-Ray 追蹤。
- `aws:assertAwsResourceProperty`-驗證 Lambda 函數上是否已啟用 X-Ray 追蹤。

### 輸出

UpdateLambdaConfig。 UpdateFunctionConfigurationResponse -來自UpdateFunctionConfigurationAPI電話的回應

## AWSConfigRemediation-DeleteLambdaFunction

### Description

R AWSConfigRemediation-DeleteLambdaFunction unbook 會刪除您指定的 AWS Lambda 函數。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- LambdaFunctionName

類型：字串

說明：(必要) 您要刪除的 Lambda 函數名稱。

### 必要的IAM權限

此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-刪除參數中指定的 Lambda 函LambdaFunctionName數。
- aws:executeScript-驗證 Lambda 函數已刪除。

## AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

### Description

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMKrunbook 會在靜態時加密您使用 () 客戶受管金鑰指定之 AWS Lambda (Lambda) 函數的 AWS Key Management Service 環境變數。AWS KMS此 runbook 應該只用作基準，以確保您的 Lambda 函數的環境變數會根據建議的最低安全性最佳實務進行加密。我們建議使用不同的客戶管理金鑰加密多個功能。

## 運行此自動化 (控制台)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- FunctionName

類型：字串

說明：(必要) 您要加密其環境變數ARN之 Lambda 函數的名稱或名稱。

- KMSKeyArn

類型：字串

說明：(必要) 您要用來加密 Lambda 函數環境變數ARN的 AWS KMS 客戶受管金鑰。

### 必要的IAM權限

此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`-等待該LastUpdateStatus物業是Successful。
- `aws:executeAwsApi`-使用您在參數中指定的 AWS KMS 客戶管理金鑰，為您 在FunctionName參數中指定的 Lambda 函數加密環境變數KMSKeyArn數。
- `aws:assertAwsResourceProperty`-確認已在 Lambda 函數的環境變數上啟用加密。

## AWSConfigRemediation-MoveLambdaToVPC

### Description

手AWSConfigRemediation-MoveLambdaToVPC冊將 AWS Lambda ( Lambda ) 函數移動到 Amazon Virtual Private Cloud ( AmazonVPC ) 。

### [運行此自動化 \( 控制台 \)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- FunctionName

類型：字串

說明：( 必填 ) Lambda 函數移動到 Amazon 的名稱VPC。

- SecurityGroupIds

類型：字串

描述：(必要) IDs 您要指派給與 Lambda 函數相關聯之彈性網路介面 (ENIs) 的安全性群組。

- SubnetIds

類型：字串

描述：(必要) IDs 您要建立與 Lambda 函數相關聯之彈性網路介面 (ENIs) 的子網路。

### 必要的IAM權限

此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-更新您在參數中指定的 Lambda 函FunctionName數的 Amazon VPC 組態。
- aws:waitForAwsResourceProperty-等待 Lambda 函數LastUpdateStatus為successful。
- aws:executeScript-驗證 Lambda 函數 Amazon VPC 組態已成功更新。

## AWSSupport-RemediateLambdaS3Event

### Description

AWSSupport-TroubleshootLambdaS3EventRunbook 為知 AWS 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 事件通知沒有觸發我的 Lambda 函數？](#) 以及[為什麼在建立 Amazon S3 事件通知以觸發 Lambda 函數時，出現「無法驗證下列目的地組態」的錯誤訊息？](#) 此 Runbook 可協助您識別並修復 Amazon Simple Storage Service (Amazon S3) 事件通知無法觸發您指

定 AWS Lambda 功能的原因。[如果 runbook 輸出建議驗證和設定 Lambda 函數並行，請參閱非同步叫用和函數擴展。AWS Lambda](#)

#### Note

由於 Amazon 簡單通知服務 (Amazon) 和亞馬遜簡單佇列服務 (Amazon SNS/SQS) Amazon S3 事件組態不正確，也可能發生「無法驗證下列目的地組態」錯誤。此執行手冊只會檢查 Lambda 函數組態。如果在使用 runbook 之後，您仍然收到「無法驗證以下目的地組態」錯誤訊息，請檢閱任何現有的 Amazon SNS 和 Amazon SQS Amazon S3 事件組態。

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LambdaFunctionArn

類型：字串

說明：(必要) Lambda 函數 ARN 的。

- S3 BucketName



類型：字串

說明：(必要) 事件通知會觸發 Lambda 函數的 Amazon S3 儲存貯體的名稱。

- 動作

類型：字串

有效值：疑難排解 | 修復

描述：(必要) 您希望 Runbook 執行的動作。此選Troubleshoot項有助於識別任何問題，但不會執行任何變更動作來解決問題。此選Remediate項有助於識別並嘗試為您解決問題。

### 必要的IAM權限

此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-運AWSsupport-TroubleshootLambdaS3Event行手冊。
- aws:executeAwsApi-檢查在上一個步驟中執行的 AWSsupport-TroubleshootLambdaS3Event Runbook 的輸出。

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 事件通知無法觸發我的 Lambda 函數？](#) 以及 [為什麼在建立 Amazon S3 事件通知以觸發 Lambda 函數時，出現「無法驗證下列目的地組態」的錯誤訊息？](#) 知識中心文章。

輸出

結帳輸出

修復問題 3 事件輸出

## AWSsupport-TroubleshootLambdaInternetAccess

Description

AWSsupport-TroubleshootLambdaInternetAccessRunbook 可協助您針對啟動到 Amazon 虛擬私有雲 (AmazonVPC) 的 AWS Lambda 功能進行疑難排解網際網路存取問題。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，以確認允許輸出網際網路存取。

[運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- FunctionName

類型：字串

說明：(必要) 您要疑難排解網際網路存取問題的 Lambda 函數名稱。

- destinationIp

類型：字串

描述：(必要) 您要建立輸出連線的目的地 IP 位址。

- destinationPort

類型：字串

預設：443

說明：(選擇性) 您要在其上建立輸出連線的目的地連接埠。

### 必要的IAM權限

此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 函數所在VPC位置的各種資源的組態。
- aws:branch-根據指定的 Lambda 函數是否在 a 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，並驗證存在至網路位址轉譯 (NAT) 閘道和網際網路閘道的路由。確認 Lambda 函數不在公有子網路中。
- aws:executeScript-驗證與 Lambda 函數關聯的安全群組，允許根據為destinationIp和destinationPort參數指定的值對外網際網路存取。
- aws:executeScript-驗證與 Lambda 函數子網路相關聯的ACL規則，NAT閘道允許輸出網際網路存取，根據為destinationIp和destinationPort參數指定的值。

## 輸出

checkVpc.vpc-啟動 Lambda 函數所在VPC位置的識別碼。

checkVpc子網路-啟IDs動 Lambda 函數的子網路。

checkVpc。 securityGroups -與 Lambda 函數相關聯的安全性群組。

檢查NACL。 NACL-帶有資源名稱的分析消息。 LambdaIp指的是 Lambda 函數 elastic network interface 的私有 IP 位址。只有具有NAT通往閘道之路由的子網路才會產生LambdaIpRules物件。下面的內容是輸出的一個例子。

```
{
  "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 函數相關聯的安全性群組。下面的內容是輸出的一個例子。

```
{
  "sg-123456789":{
```

```
    "Status": "Allowed",
    "Analysis": "This security group has allowed destination IP and port in its
outbound rule."
  }
}
```

checkSubnet.subnets-分析您與 Lambda 函數 VPC 相關聯的子網路。下面的內容是輸出的一個例子。

```
{
  "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"
  }
}
```

## AWS Support - Troubleshoot Lambda S3 Event

### Description

AWS Support - Troubleshoot Lambda S3 Event Runbook 為知 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 事件通知沒有觸發我的 Lambda 函數？](#) 以及 [為什麼在建立 Amazon S3 事件通知以觸發 Lambda 函數時，出現「無法驗證下列目的地組態」的錯誤訊息？](#) 此 Runbook 可協助您識別 Amazon Simple Storage Service (Amazon S3) 事件通知無法觸發您指定的 AWS Lambda 功能的原因。[如果 runbook 輸出建議驗證和設定 Lambda 函數並行，請參閱非同步叫用和函數擴展。AWS Lambda](#)

[運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LambdaFunctionArn

類型：字串

說明：(必要) Amazon S3 事件通知觸發 ARN 的 Lambda 函數。

- S3 BucketName

類型：字串

說明：(必要) 事件通知會觸發 Lambda 函數的 Amazon S3 儲存貯體的名稱。

## 必要的IAM權限

此 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 函數的以資源為基礎的 IAM 政策，並產生 AWS Command Line Interface (AWS CLI) 命令以新增所需的權限 (如果原則遺失所需的權限)。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，並在缺少所需權限時產生 AWS CLI 命令作為輸出。

## 輸出

## 羊巴達 3 事件輸出

# Amazon Managed Workflows for Apache Airflow

AWS Systems Manager 自動化為 Apache 氣流提供預先定義的 Amazon 受管工作流程手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)

## AWSSupport-TroubleshootMWAAEnvironmentCreation

### Description

AWSSupport-TroubleshootMWAAEnvironmentCreationRunbook 提供針對 Apache Airflow (AmazonMWAA) 環境建立問題的 Amazon 受管工作流程進行偵錯的資訊，並以最大的方式執行檢查以及記錄的原因，以協助識別失敗。

### 它是如何工作的？

執行手冊執行下列步驟：

- 檢索 Amazon MWAA 環境的詳細信息。
- 驗證執行角色權限。
- 檢查環境是否具有使用提供的 AWS KMS 金鑰進行記錄的權限，以及所需的記 CloudWatch 錄群組是否存在。
- 剖析提供的記錄群組中的記錄檔，以找出任何錯誤。
- 檢查網路組態以確認 Amazon MWAA 環境是否可存取所需端點。
- 產生包含發現項目的報告。

### [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

## 擁有者

Amazon

平台

/

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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操作：

1. 瀏覽至「文件」下 [AWSSupport-TroubleshootMWAAEnvironmentCreation](#) 的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：
 

( ) 角色的 Amazon 資源名稱 AWS AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - EnvironmentName (必填)：
 

您要評估的 Amazon MWAA 環境的名稱。

The screenshot shows the 'Input parameters' section of a console interface. It contains two input fields:

- AutomationAssumeRole**: Labeled as '(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.' It features a dropdown menu and a clear button.
- EnvironmentName**: Labeled as '(Required) Name of the MWAA environment you wish to evaluate.' It is a text input field with a 'String' type indicator.

4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

- **GetMWAAEnvironmentDetails:**

檢索 Amazon MWAA 環境的詳細信息。如果此步驟失敗，自動化過程將停止並顯示為 Failed。

- **CheckIAMPermissionsOnExecutionRole:**

驗證執行角色是否具有 Amazon MWAA、Amazon S3、CloudWatch 日誌和 Amazon SQS 資源所需的許可。CloudWatch 如果偵測到客戶 managed AWS Key Management Service (AWS KMS) 金鑰，則自動化會驗證金鑰的必要權限。此步驟會使用 `iam:SimulateCustomPolicyAPI` 來確定自動化執行角色是否符合所有必要的權限。

- **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 日誌。如果 AWS KMS 金鑰是 AWS 受管理的，則自動化會略過此檢查。

- **CheckIfRequiredLogGroupsExists:**

檢查 Amazon MWAA 環境所需的 CloudWatch 日誌群組是否存在。如果沒有，自動化會檢查 CloudTrail 查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 日誌群組存在進行分支。如果至少有一個記錄群組存在，自動化會剖析該群組以尋找錯誤。如果沒有記錄群組存在，自動化操作會略過下一個步驟。

- **CheckForErrorsInLogGroups:**

剖析 CloudWatch 記錄群組以尋找錯誤。

- **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AWSSupport-ConnectivityTroubleshooter子自動化以驗證 Amazon 與所需端點 MWAA 的連接。

- **CheckS3BlockPublicAccess:**

檢查 Amazon MWAA 環境的 Amazon S3 儲存貯體是否已Block Public Access啟用，並檢閱帳戶的整體 Amazon S3 區塊公開存取設定。

- **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，請查看「輸出」部分以獲取執行的詳細結果：

- 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 日誌和 Amazon SQS 資源的必要許可。CloudWatch 如果偵測到客戶管理 AWS KMS 金鑰，則自動化會驗證金鑰的必要權限。

- 檢查 Amazon MWAA 環境 AWS KMS 密鑰政策：

驗證執行角色是否擁有 Amazon MWAA、Amazon S3、CloudWatch 日誌和 Amazon SQS 資源的必要許可。CloudWatch 此外，如果偵測到客戶管理 AWS KMS 金鑰，系統會自動檢查金鑰的必要權限。

- 檢查 Amazon MWAA 環境 CloudWatch 日誌組：

檢查 Amazon MWAA 環境所需的 CloudWatch 日誌群組是否存在。如果他們不這樣做，自動化然後檢 CloudTrail 查定位 CreateLogGroup 和 DeleteLogGroup 事件。

- 檢查 Amazon MWAA 環境路由表：

檢查 Amazon MWAA 環境中的 Amazon VPC 路由表是否正確配置。

- 檢查 Amazon MWAA 環境安全組：

檢查 Amazon MWAA 環境 Amazon VPC 安全組是否配置正確。

- 檢查 Amazon MWAA 環境網絡 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：

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能力：

驗證 Amazon MWAA 環境是否可以存取所需的端點。為此，自動化會叫用自動 AWS Support-Connectivity Troubleshooter 化。

- 檢查 Amazon MWAA 環境 Amazon S3 桶：

檢查亞馬遜 MWAA 環境的 Amazon S3 儲存貯體是否已 Block Public Access 啟用，並檢閱帳戶的 Amazon S3 區塊公開存取設定。

- 檢查 Amazon MWAA 環境 CloudWatch 日誌組錯誤：

剖析 Amazon MWAA 環境的現有 CloudWatch 日誌群組以找出錯誤。

## ▼ Outputs

## GenerateReportAutomationReport

Troubleshooting report for MIAA environment

👉 The automation found no issues with the MIAA environment configuration ✓

🔍 Checking the MIAA environment execution role permissions

All the required permissions for the MIAA environment execution role are in place ✓

🔍 Checking the MIAA environment KMS key policy

KMS key is an AWS managed key ✓

🔍 Checking the MIAA environment CloudWatch logs groups

The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MIAA environment [REDACTED] is 5. This suggests that all log groups were created successfully ✓

🔍 Checking the MIAA 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 MIAA environment Security Groups

Security group [REDACTED] has self-referencing rules for all traffic. ✓

🔍 Checking the MIAA environment Network ACLs

NACL: [REDACTED] allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔍 Checking the MIAA environment Subnets

Subnet: subnet: [REDACTED] is private ✓

Subnet: subnet: [REDACTED] is private ✓

🔍 Checking the MIAA 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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](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 MIAA 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](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1)

🔍 Checking the MIAA environment S3 bucket

Environment's S3 bucket and/or account block public access ✓

🔍 Checking the MIAA 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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

# Neptune

AWS Systems Manager 自動化為 Amazon Neptune 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

## AWS - EnableNeptuneDbAuditLogsToCloudWatch

### Description

AWS-EnableNeptuneDbAuditLogsToCloudWatch 執行手冊可協助您將 Amazon Neptune 資料庫叢集的稽核日誌傳送至 Amazon CloudWatch 日誌。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `DbClusterResourceId`

類型：字串

描述：(必要) 您要啟用稽核記錄之 Neptune 資料庫叢集的資源識別碼。

#### 必要的IAM權限

此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 資料庫叢集的識別碼。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`)-驗證 Neptune DB 引擎類型為 `neptune`。
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`)-啟用要傳送記錄的 Neptune DB 叢集的稽核 CloudWatch 記錄。
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`)-驗證 Neptune 資料庫叢集狀態為 `available`。
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`)-驗證稽核記錄是否已成功設定為傳送至 CloudWatch 防護記錄。

## AWS-EnableNeptuneDbBackupRetentionPeriod

### Description

AWS-EnableNeptuneDbBackupRetentionPeriod執行手冊可協助您啟用 Amazon Neptune 資料庫叢集的備份保留期為 7 到 35 天之間的自動備份。

## 運行此自動化 ( 控制台 )

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DbClusterResourceid

類型：字串

描述：(必要) 您要啟用備份之 Neptune 資料庫叢集的資源識別碼。

- BackupRetentionPeriod

類型：整數

有效值：7-35

說明：(必要) 備份的保留天數。

- PreferredBackupWindow

類型：字串

說明：(選擇性) 進行備份時，每日至少 30 分鐘的時間範圍。該值必須使用世界協調時 (UTC)，並使用以下格式：hh24:mm-hh24:mm。備份保留期間不能與偏好的維護時段衝突。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 資料庫叢集的識別碼。
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`)-驗證 Neptune DB 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執行手冊可為您指定的 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DbClusterResourceid

類型：字串

描述：(必要) 您要在其上啟用刪除保護的 Neptune 叢集識別碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 資料庫叢集的識別碼。
- VerifyNeptuneDbEngine ( aws:assertAwsResourceProperty ) -驗證指定的數據庫集群的引擎類型。neptune
- VerifyNeptuneStatus (aws:waitForAwsResourceProperty)-驗證叢集的狀態是否為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 提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 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-CreateEncryptedRdsSnapshotRunbook 從未加密的 Amazon 關聯式資料庫服務 (AmazonRDS) 執行個體建立加密的快照。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DBInstanceIdentifier

類型：字串

說明：(必填) 您要建立快照的 Amazon RDS 執行個體 ID。

- DBSnapshotIdentifier

類型：字串

說明：(可選) Amazon RDS 快照的名稱模板。預設名稱範本為 *DBInstanceIdentifier-yyyymmddhhmmss*。

- EncryptedDBSnapshot 識別碼

類型：字串

說明：(選擇性) 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

說明：(選用) 要新增至資料庫執行個體的標籤。(例如：鍵 = tagKey 1，值 = tagValue 1；鍵 = tagKey 2，值 = 2) 'tagValue

- KmsKeyId

類型：字串

預設：alias/aws/rds

說明：(選用) 您要用來加密快照之客戶管理金鑰的金鑰、金鑰 ID 或金鑰別名。ARN

- SnapshotTags

類型：字串

說明：(選擇性) 要新增至快照的標籤。(例如：鍵 = tagKey 1，值 = tagValue 1；鍵 = tagKey 2，值 = 2) 'tagValue

## 必要的IAM權限

此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`-驗證在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 執行個體建立 Amazon Relational Database Service 服務 (RDSAmazonRDS) 快照。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DBInstanceIdentifier

類型：字串

說明：(必要) 要從中建立快照的 RDS 執行處理 DBInstanceID ID。

- DBSnapshotIdentifier

類型：字串

說明：(選擇性) 要建立之 RDS 快照的 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 — 檢查在上一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執行手冊會刪除您指定的 Amazon Relational Database Service (AmazonRDS) 叢集。AWS Config 必須在您執行此自動化操作的 AWS 區域 位置啟用。

## [運行此自動化 \( 控制台 \)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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碼。

必要的IAM權限

此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

該手AWSConfigRemediation-DeleteRDSClusterSnapshot冊刪除給定的 Amazon Relational Database Service ( AmazonRDS ) 集群快照。

### [運行此自動化 \( 控制台 \)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `DBClusterSnapshotId`

類型：字串

說明：(必填) 要刪除的 Amazon RDS 叢集快照識別碼。



## 必要的IAM權限

此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available處於狀態。如果不可用，則流程結束。
- `aws:executeAwsApi`-使用資料庫 (DB) RDS 叢集快照識別碼刪除指定的 Amazon 叢集快照。
- `aws:executeScript`-驗證指定的 Amazon RDS 叢集快照是否已刪除。

# AWSConfigRemediation-DeleteRDSInstance

## Description

AWSConfigRemediation-DeleteRDSInstance執行手冊會刪除您指定的 Amazon Relational Database Service (AmazonRDS) 執行個體。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，且無法復原。不會刪除手動資料庫快照。如果要刪除的資料庫執行個體處於failedincompatible-network、或incompatible-restore狀態，則必須將SkipFinalSnapshot參數設定為true。

### Note

如果您要刪除的資料庫執行個體位於 Amazon Aurora 資料庫叢集中，則執行本是僅供讀取複本且資料庫叢集中唯一的執行個體時，不會刪除該資料庫執行個體。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DbiResourceId

類型：字串

說明：(必要) 您要刪除的資料庫執行個體的資源識別碼。

- SkipFinalSnapshot

類型：布林值

預設：false

說明：(選擇性) 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權限

此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執行手冊會刪除您指定的 Amazon Relational Database Service (AmazonRDS) 執行個體快照。只會刪除狀`available`態中的快照。此執行手冊不支援從 Amazon Aurora 資料庫執行個體刪除快照。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `DbSnapshotId`

類型：字串

說明：(必要) 您要刪除之快照的 ID。

## 必要的IAM權限

此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`-驗證快照已刪除。

# AWSConfigRemediation-DisablePublicAccessToRDSInstance

## Description

AWSConfigRemediation-DisablePublicAccessToRDSInstanceRunbook 會停用您指定之 Amazon Relational Database Service (AmazonRDS) 資料庫 (DB) 執行個體的公有可存取性。

## [運行此自動化 \( 控制台 \)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `DbiResourceId`

類型：字串

說明：(必要) 您要停用其公開存取性之資料庫執行個體的資源識別碼。

### 必要的IAM權限

此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碼收集資料庫執行個體識別碼。
- `aws:assertAwsResourceProperty`-驗證資料庫執行個體處於某個AVAILABLE狀態。
- `aws:executeAwsApi`-停用資料庫執行個體的公用存取權。
- `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`-確認資料庫執行個體已停用公用存取功能。

## AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

### Description

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster執行手冊會在您指定的 Amazon Relational Database Service (AmazonRDS) 叢集上啟用CopyTagsToSnapshot設定。啟用

此設定會將資料庫叢集中的所有標記複製到資料庫叢集的快照。預設為不複製它們。AWS Config 必須在您的執行此自動化操作的 AWS 區域 位置啟用。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- `ApplyImmediately`

類型：布林值

預設：false

描述：(選擇性) 如果您true為此參數指定，則無論資料庫叢集的設定為何，都會儘快以非同步方式套用此要求中的修改和任何擱PreferredMaintenanceWindow置的修改。

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `DbClusterResourceid`

類型：字串

描述：(必要) 您要在其上啟用CopyTagsToSnapshot設定的資料庫叢集的資源識別碼。

必要的IAM權限

此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碼收集資料庫叢集識別碼。
- `aws:assertAwsResourceProperty`-確認資料庫叢集處於某個AVAILABLE狀態。
- `aws:executeAwsApi`-啟用資料庫叢集上的CopyTagsToSnapshot設定。
- `aws:assertAwsResourceProperty`-確認資料庫叢集上已啟用CopyTagsToSnapshot設定。

# AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

## Description

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance執行手冊會在您指定的 Amazon Relational Database Service (AmazonRDS) 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操作的 AWS 區域 位置啟用。

## [運行此自動化 \( 控制台 \)](#)

### 文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- ApplyImmediately

類型：布林值

預設：false

說明：(選擇性) 如果您true為此參數指定，則無論資料庫執行個體的設定為何，都會儘快以非同步方式套用此要求中的修改和任何擱PreferredMaintenanceWindow置的修改。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DbResourceId

類型：字串

說明：(必要) 要在其上啟用CopyTagsToSnapshot設定的資料庫執行個體的資源識別碼。

## 必要的IAM權限

此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碼收集資料庫執行個體識別碼。
- aws:assertAwsResourceProperty-確認資料庫執行個體處於某個AVAILABLE狀態。
- aws:executeAwsApi-啟用資料庫執行個體上的CopyTagsToSnapshot設定。
- aws:assertAwsResourceProperty-確認資料庫執行個體上已啟用CopyTagsToSnapshot設定。



# AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

## Description

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstanceRunbook 在您指定的 Amazon RDS 資料庫執行個體上啟用增強型監控功能。如需增強型監控的相關資訊，請參閱 Amazon RDS 使用者指南中的 [增強型監控](#)。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- MonitoringInterval

類型：整數

有效值：1

說明：(必要) 從資料庫執行個體收集「增強型監控」測量結果的間隔 (秒)。

- MonitoringRoleArn

類型：字串

描述：( 必填 ) 允許 Amazon 將增強型監控指標傳送RDS到 Amazon CloudWatch 日誌的IAM角色的 Amazon 資源名稱 ( ARN )。

- ResourceId

類型：字串

說明：(必要) 您要啟用增強型監控之資料庫執行個體的資源識別碼。

### 必要的IAM權限

此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碼收集資料庫執行個體識別碼。
- aws:assertAwsResourceProperty-確認資料庫執行個體處於某個AVAILABLE狀態。
- aws:executeAwsApi-啟用資料庫執行個體的增強型監控功能。
- aws:executeScript-確認資料庫執行個體已啟用增強型監控功能。

## AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

### Description

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS執行手冊會在您指定的 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自動套用至資料庫執行個體。

[運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DbiResourceId

類型：字串

說明：(必要) 您要對其進行AutoMinorVersionUpgrade設定的資料庫執行個體的資源識別碼。

### 必要的IAM權限

此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碼收集資料庫執行個體識別碼。
- aws:assertAwsResourceProperty-確認資料庫執行個體處於某個AVAILABLE狀態。
- aws:executeAwsApi-啟用資料庫執行個體上的AutoMinorVersionUpgrade設定。
- aws:executeScript-確認資料庫執行個體上已啟用此AutoMinorVersionUpgrade設定。

# AWSConfigRemediation-EnableMultiAZOnRDSInstance

## Description

AWSConfigRemediation-EnableMultiAZOnRDSInstanceRunbook 會將您的 Amazon Relational Database Service (AmazonRDS) 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`。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- ApplyImmediately

類型：布林值

預設：false

說明：(選擇性) 如果您 `true` 為此參數指定，則無論資料庫執行個體的設定為何，都會儘快以非同步方式套用此要求中的修改和任何擱 PreferredMaintenanceWindow 置的修改。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DbResourceId

類型：字串

說明：(必要) 資料庫執行個體的 AWS 區域唯一、不可變的識別碼，以啟用此設定MultiAZ。

### 必要的IAM權限

此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-使用參數中提供的值擷取資料庫執行個體名DBInstanceId稱。
- aws:executeAwsApi-驗證DBInstanceStatus是available。
- aws:branch-檢查您在DbiResourceId參數中指定的資料庫執行個體true上MultiAZ是否已設定為。
- aws:executeAwsApi-將您在DbiResourceId參數中指MultiAZ定true的資料庫執行個體上的設定變更為。
- aws:assertAwsResourceProperty-驗證您在DbiResourceId參數中指定的true資料庫執行個體上將設定為。MultiAZ

## AWSConfigRemediation- EnablePerformanceInsightsOnRDSInstance

### Description

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance執行手冊可在您指定的 Amazon RDS 資料庫執行個體上啟用 Performance Insights。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DbiResourceId

類型：字串

說明：(必要) 您要啟用 Performance Insights 之資料庫執行個體的資源識別碼。

- PerformanceInsightsKMSKeyId

類型：字串

預設：alias/aws/rds

說明：(選用) Amazon 資源名稱 (ARN)、金鑰 ID 或 AWS Key Management Service (AWS KMS) 客戶受管金鑰的金鑰別名，您希望 Performance Insights 用來加密所有潛在敏感資料。如果您輸入此參數的關鍵別名，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

說明：(選用) 您要保留「Performance Insights」資料的天數。

必要的IAM權限

此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碼收集資料庫執行個體識別碼。
- `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ARN的 AWS KMS 客戶管理金鑰。
- `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`-針對您在`DbiResourceId`參數中指定的資料庫執行個體啟用 Performance Insights 見。
- `aws:assertAwsResourceProperty`-確認為`PerformanceInsightsKMSKeyId`參數指定的值是用來啟用資料庫執行個體的 Performance Insights 的加密功能。
- `aws:assertAwsResourceProperty`-確認資料庫執行個體已啟用 Performance Insights。

## AWSConfigRemediation-EnableRDSClusterDeletionProtection

### Description

`AWSConfigRemediation-EnableRDSClusterDeletionProtection` 執行手冊會在您指定的 Amazon Relational Database Service (AmazonRDS) 叢集上啟用刪除保護。AWS Config 必須在您執行此自動化操作的 AWS 區域 位置啟用。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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碼。

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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碼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-EnableRDSInstanceBackupRunbook 會為您指定的 Amazon Relational Database Service (AmazonRDS) 資料庫執行個體啟用備份。此執行手冊不支援啟用 Amazon Aurora 資料庫執行個體的備份功能。

## [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- ApplyImmediately

類型：布林值

預設：false

說明：(選擇性) 如果您true為此參數指定，則無論資料庫執行個體的設定為何，都會儘快以非同步方式套用此要求中的修改和任何擱PreferredMaintenanceWindow置的修改。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BackupRetentionPeriod

類型：整數

有效值：1-35

說明：(必要) 保留備份的天數。

- DbResourceId

類型：字串

說明：(必要) 您要啟用備份的資料庫執行個體的資源識別碼。

- PreferredBackupWindow

類型：字串

說明：(選擇性) 建立備份的每日時間範圍 (inUTC)。

約束：

- 必須為格式 hh24:mi-hh24:mi
- 必須在協調世界時 () UTC
- 不得和慣用的維護時段衝突
- 必須至少 30 分鐘

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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碼收集資料庫執行個體識別碼。啟用資料庫執行個體的備份。確認資料庫執行個體上已啟用備份。

## AWSConfigRemediation-EnableRDSInstanceDeletionProtection

### Description

AWSConfigRemediation-EnableRDSInstanceDeletionProtection執行手冊可在您指定的 Amazon RDS 資料庫執行個體上啟用刪除保護。

[運行此自動化 \(控制台\)](#)

## 文件類型

自動化

擁有者

Amazon

平台

資料庫

參數

- `ApplyImmediately`

類型：布林值

預設：false

說明：(選擇性) 如果您true為此參數指定，則無論資料庫執行個體的設定為何，都會儘快以非同步方式套用此要求中的修改和任何擱置的修改。

- `AutomationAssumeRole`

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `DbInstanceResourceId`

類型：字串

說明：(必要) 要在其上啟用刪除保護的資料庫執行個體的資源識別碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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碼收集資料庫執行個體識別碼。
- `aws:executeAwsApi`-在資料庫執行個體上啟用刪除保護。
- `aws:assertAwsResourceProperty`-確認資料庫執行個體已啟用刪除保護。

# AWSConfigRemediation-ModifyRDSInstancePortNumber

## Description

AWSConfigRemediation-ModifyRDSInstancePortNumber執行手冊會修改 Amazon 關聯式資料庫服務 (AmazonRDS) 執行個體接受連線的連接埠號碼。執行此自動化操作將重新啟動資料庫。

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `PortNumber`

類型：字串

說明：(選擇性) 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

說明：(必要) 您要修改其輸入連接埠號碼之資料庫執行個體的資源識別碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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碼收集資料庫執行個體識別碼。
- `aws:assertAwsResourceProperty`-確認資料庫執行個體處於某個AVAILABLE狀態。
- `aws:executeAwsApi`-修改資料庫執行個體接受連線的輸入連接埠號碼。
- `aws:waitForAwsResourceProperty`-等待資料庫執行個體處於某個MODIFYING狀態。
- `aws:waitForAwsResourceProperty`-等待資料庫執行個體處於某個AVAILABLE狀態。

## AWSsupport-ModifyRDSSnapshotPermission

### Description

AWSsupport-ModifyRDSSnapshotPermissionRunbook 可協助您修改多個 Amazon Relational Database Service (AmazonRDS) 快照的許可。使用此 runbook，您可以製作快照Public或Private與其他 AWS 帳戶人共享它們。使用預設KMS金鑰加密的快照無法與使用此 Runbook 的其他帳戶共用。

### [運行此自動化 \(控制台\)](#)

### 文件類型

## 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AccountIds

類型: StringList

預設：none

說明：(選擇性) 您要與IDs其共用快照的帳戶。如果您輸入No參數值，則需要此Private參數。

- AccountPermissionOperation

類型：字串

有效值：添加 | 刪除

預設：none

描述：(選擇性) 要執行的作業類型。

- 私有

類型：字串

有效值：是 | 否

說明：(必要) 如果要與特定帳戶共用快照，請輸入No值。

- SnapshotIdentifiers

類型: StringList

描述 : (必填) 您要修改其權限的 Amazon RDS 快照名稱。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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IDs數中提供的快照。驗證之後IDs，指令碼會檢查是否有加密的快照，並輸出清單 (如果找到的話)。
2. aws:branch-根據您為Private參數輸入的值分支自動化。
3. aws:executeScript-修改指定快照的權限，以便與指定的帳戶共用。
4. aws:executeScript-修改快照的權限以將其從變更Public為Private。

#### 輸出

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts. 結果。

MakePrivate. 結果。

MakePrivate. 命令

## AWSPremiumSupport-PostgreSQLWorkloadReview

### Description

該手冊 `AWSPremiumSupport-PostgreSQLWorkloadReview` 冊捕獲您的 Amazon 關係數據庫服務 (亞馬遜 RDS) PostgreSQL 數據庫使用情況統計的多個快照。AWS Support [主動式服務](#) 專家需要擷取的統計資料，才能執行作業複查。使用一組自訂 SQL 和殼層指令碼收集統計資料。這些指令碼會下載到暫時的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體，AWS 帳戶該執行個體是由此執行手冊建立的。runbook 要求您使用包含用戶名和密碼鍵值對的 AWS Secrets Manager 秘密提供憑據。用戶名必須具有查詢標準 PostgreSQL 統計視圖和功能的權限。

這個 runbook 會自動在您的 AWS 帳戶使用 AWS CloudFormation 堆棧中創建以下 AWS 資源。您可以使用 AWS CloudFormation 主控台監視堆疊建立。

- 在私 VPC 有子網路中啟動的虛擬私有雲端 (VPC) 和 Amazon EC2 執行個體，可選擇使用 NAT 閘道連線至網際網路。
- 附加至臨時 Amazon EC2 執行個體的 AWS Identity and Access Management (IAM) 角色，具有擷取機 Secrets Manager 碼值的權限。該角色還提供將檔案上傳到您選擇的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的許可，以及選擇性地將檔案上傳到 AWS Support 案例。
- 一種 VPC 對等連接，可讓您的資料庫執行個體與臨時 Amazon EC2 執行個體之間進行連線。
- Systems Manager 員、Secrets Manager 和 Amazon S3 VPC 端點連接到暫存端點 VPC。
- 包含已註冊任務的維護時段，可定期啟動和停止臨時 Amazon EC2 執行個體、執行資料收集指令碼，以及將檔案上傳到 Amazon S3 儲存貯體。也會為維護時段建立 IAM 角色，提供執行已註冊工作的權限。

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，並選擇性地將 AWS Support 案例上傳。

#### Note

依預設，暫時 Amazon EC2 執行個體的根 Amazon EBS 磁碟區會保留。您可以將 `EbsVolumeDeleteOnTermination` 參數設定為來取代此選項 `true`。

#### 先決條件

- 企業 Support 訂閱此 Runbook 和主動式服務工作負載診斷和檢閱需要企業 Support 訂閱。在使用本 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 [AWS Support 主動式服務](#)。
- 帳戶和 AWS 區域 配額請確保您沒有達到 Amazon EC2 實例的最大數量，或者您的 VPCs 可以在您使用此 runbook 的帳戶和區域中創建。如果您需要申請提高限制，請參閱 [提高服務限制表單](#)。



## • 資料庫組態

1. 您在DatabaseName參數中指定的資料庫應該已設定pg\_stat\_statements副檔名。如果尚未pg\_stat\_statements在中配置shared\_preload\_libraries，則必須編輯「資料庫參數群組」中的值並套用變更。變更參數時，您shared\_preload\_libraries必須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](#)。添加pg\_stat\_statements到shared\_preload\_libraries將增加一些性能開銷。不過，這對於追蹤個別陳述式的效能很有用。如需有關pg\_stat\_statements擴充功能的詳細資訊，請參閱[Postgre SQL 文件](#)。如果您未設定pg\_stat\_statements擴充功能，或是擴充功能不存在於用於統計資料收集的資料庫中，則作業檢閱中將不會顯示陳述式層級分析。
2. 確保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，將無法使用有意義的統計資料。變更這些參數時，您必須重新啟動資料庫執行個體。如需詳細資訊，請參閱[在您的 Amazon RDS 上使用 Postgre 資SQL料庫執行個體](#)的參數。
3. 如果關閉track\_io\_timing參數，I/O 層級統計資料將不會包含在作業檢閱中。變更時，您track\_io\_timing必須重新啟動資料庫執行個體，並根據資料庫執行個體工作負載產生額外的效能額外負荷。儘管關鍵工作負載會產生效能額外負荷，但此參數仍提供與每個查詢 I/O 時間相關的有用資訊。

帳單和費用您 AWS 帳戶 需支付與臨時 Amazon EC2 執行個體、關聯的 Amazon EBS 磁碟區、NAT 閘道以及執行此自動化時傳輸的資料相關費用。默認情況下，這個手冊創建一個 t3.micro Amazon Linux 2 實例來收集統計信息。runbook 會啟動和停止執行個體之間的步驟，以降低成本。

資料安全性和治理這本 Runbook 透過查詢 [Postgre 統計資料檢視和功能來收集SQL統計](#)資料。請確定SecretId參數中提供的認證只允許統計資料檢視和函數的唯讀權限。作為自動化的一部分，收集指令碼會上傳到您的 Amazon S3 儲存貯體，並且可以位於中s3://*amzn-s3-demo-bucket/automation execution id/queries/*。

這些指令碼會收集「AWS 專家」用來複查物件層級的關鍵績效指標的資料。指令碼會收集資訊，例如資料表名稱、結構描述名稱和索引名稱。如果任何這些資訊包含敏感資訊，例如收益指標、使用者名稱、電子郵件地址或任何其他個人識別資訊，我們建議您停止進行此工作負載檢查。請與您 AWS TAM 聯絡，討論工作負載檢閱的替代方法。

確保您獲得必要的批准和許可，以便與此自動化操作共享所收集的統計信息和元數據 AWS。

安全考量如果將UpdateRdsSecurityGroup參數設定為yes，runbook 會更新與資料庫執行個體關聯的安全群組，以允許來自臨時 Amazon EC2 執行個體私有 IP 地址的輸入流量。

如果將UpdateRdsRouteTable參數設定為yes，runbook 會更新與執行資料庫執行個體所在子網路相關聯的路由表，以允許透過對VPC等連線傳輸臨時 Amazon EC2 執行個體的流量。

建立使用者若要允許收集指令碼連線到 Amazon RDS 資料庫，您必須設定具有權限的使用者才能讀取統計資料檢視。然後，您必須將認證存儲在 Secrets Manager 中。我們建議您為此自動化操作建立新的專屬使用者。建立個別使用者可讓您稽核和追蹤此自動化操作所執行的活動。

### 1. 建立新使用者。

```
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建立唯讀連線。

```
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;"
```

### 4. 將pg\_monitor權限授予新使用者，以便它可以存取資料庫統計資料。(pg\_monitor角色是pg\_read\_all\_settingspg\_read\_all\_stats、和的成員pg\_stat\_scan\_table。)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

透過此 Systems Manager 自動化新增至臨時 Amazon EC2 執行個體設定檔的許可將以下許可新增至與臨時 Amazon EC2 執行個體相關聯的IAM角色。受AmazonSSMManagedInstanceCore管政策也與IAM角色相關聯，以允許系統管理員管理 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"
  }
]
}

```

由此 Systems Manager 自動化新增至暫時維護時段的權限下列權限會自動新增至與維護 Windows 工作相關聯的 IAM 角色。維護視窗工作會啟動、停止，並將命令傳送到暫時的 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"
    }
  ]
}

```

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DBInstanceIdentifier

類型：字串

說明：(必要) 資料庫執行個體的 ID。

- DatabaseName

類型：字串

說明：(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組ARN的 Secret Secrets Manager 密碼。AWS CloudFormation 堆疊會建立具有此GetSecretValue作業權限的IAM原則ARN。證明資料是用來允許暫時執行處理收集資料庫統計資料。請聯絡您STAM的TAM或討論所需的最低權限。

- 確認

類型：字串

描述：(必要) **yes** 如果您確認此 runbook 將在您的帳戶中建立暫時資源，以便從資料庫執行個體收集統計資料，請輸入。我們建議STAM在執行此自動化操作之前聯絡您的TAM或。

- SupportCase

類型：字串

說明：(選擇性) 您TAM或提供的 AWS Support 案例編號STAM。如果提供，runbook 會更新案例並附加收集的資料。此選項需要臨時 Amazon EC2 執行個體具有網際網路連線才能存取 AWS Support API端點。您必須將AllowVpcInternetAccess參數設定為true。案例主題必須包含短語AWSPremiumSupport-PostgreSQLWorkloadReview。

- S3 BucketName

類型：字串

說明：(必填) 您帳戶中要上傳自動化收集之資料的 Amazon S3 儲存貯體名稱。確認值區政策不會將任何不必要的讀取或寫入權限授與不需要存取值區內容的主體。我們建議為此自動化目的建立新的暫時 Amazon S3 儲存貯體。執行手冊為連接到臨時 Amazon EC2 執行個體的IAM角色提供s3:PutObjectAPI操作的許可。上傳的文件將位於s3://*bucket name/automation execution id/*。

- InstanceType

類型：字串

說明：(選用) 將執行自訂SQL和殼層指令碼之臨時 Amazon EC2 執行個體的類型。

有效值:微 | t2. 小 | t2. 中 | t2. 大 | 微型 | 三. 小 | t3. 中

預設值：微

- VpcCidr

類型：字串

描述：(選擇性) 新的 CIDR IP 位址範圍 VPC (例如，172.31.0.0/16)。請確定您選取的資料庫執行CIDR個體不會重疊或符合任何現VPC有連線能力的資料庫執行個體。VPC您可以建立的最小值使用 /28 子網路遮罩，而最大的遮罩則VPC使用 /16 子網路遮罩。

預設值：

- StackResourcesNamePrefix

類型：字串

描述：(可選) AWS CloudFormation 堆棧資源名稱前綴和標籤。runbook 使用此前綴作為應用於資源的名稱和標籤的一部分創建 AWS CloudFormation 堆棧資源。標籤鍵值配對的結構為。*StackResourcesNamePrefix*:{{automation:EXECUTION\_ID}}

預設值：AWSPostgreSQLWorkloadReview

- 排程

類型：字串

摘要：(選擇性) 維護時段排程。指定維護時段執行工作的頻率。預設值為「間隔」1 hour。

有效值：15 分鐘 | 30 分鐘 | 1 小時 | 2 小時 | 4 小時 | 6 小時 | 6 小時 | 12 小時 | 1 天 | 2 天 | 4 天

預設值：1 小時

- 持續時間

類型：整數

說明：(選擇性) 您要允許自動化執行的持續時間上限 (以分鐘為單位)。支持的最長持續時間為 8,640 分鐘 (6 天)。預設值為 4,320 分鐘 (3 天)。

有效值：

預設值：

- UpdateRdsRouteTable

類型：字串

說明：(選擇性) 如果設定為true，runbook 會更新與資料庫執行個體執行個體所在子網路相關聯的路由表。會新增IPv4路由，透過新建立的VPC對等連線將流量路由到臨時 Amazon EC2 執行個體私有IPV4地址。

有效值：true | false

預設：false

- AllowVpcInternetAccess

類型：字串

說明：(選用) 如果設定為`true`，執行手冊會建立NAT閘道，以提供網際網路連線到臨時 Amazon EC2 執行個體，以便與 AWS Support API端點通訊。您可以保留此參數，`false`就好像您只希望 runbook 將輸出上傳到 Amazon S3 儲存貯體一樣。

有效值：true | false

預設：false

- UpdateRdsSecurityGroup

類型：字串

說明：(選擇性) 如果設為`true`，runbook 會更新與資料庫執行個體關聯的安全群組，以允許來自臨時執行個體私有 IP 位址的流量。

有效值：假 | 真

預設：false

- EbsVolumeDeleteOnTermination

類型：字串

說明：(選擇性) 如果設定為`true`，則會在EC2執行簿完成後刪除暫存 Amazon 執行個體的根磁碟區並刪除 AWS CloudFormation 堆疊。

有效值：假 | 真

預設：false

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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`-收集有關資料庫執行個體的詳細資訊。
3. `aws:executeScript`-檢查在中指定的 Amazon S3 儲存貯體是否S3BucketName允許匿名或公開讀取或寫入存取權限。
4. `aws:executeScript`-從自動化 runbook 附件中獲取 AWS CloudFormation 模板內容，該附件用於在中創建臨時 AWS 資源。AWS 帳戶
5. `aws:createStack`-建立 AWS CloudFormation 堆疊資源。
6. `aws:waitForAwsResourceProperty`-等待 AWS CloudFormation 範本建立的 Amazon EC2 執行個體執行為止。
7. `aws:executeAwsApi`-取得由 AWS CloudFormation建立IDs的臨時 Amazon EC2 執行個體和VPC對等連線。
8. `aws:executeAwsApi`-取得臨時 Amazon EC2 執行個體的 IP 位址，以設定與資料庫執行個體的連線。
9. `aws:executeAwsApi`-標記附加到臨時 Amazon EC2 實例的 Amazon EBS 卷。
10. `aws:waitForAwsResourceProperty`-等待直到臨時 Amazon EC2 執行個體通過狀態檢查為止。

- 11 `aws:waitForAwsResourceProperty`-等待直到臨時 Amazon EC2 執行個體由系統管理員管理為止。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，請重新啟動臨時 Amazon EC2 執行個體。
  - b. `aws:waitForAwsResourceProperty`-等待直到臨時 Amazon EC2 執行個體在重新開機後由系統管理員管理。
- 12 `aws:runCommand`-在臨時 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限。
- 14 `aws:executeAwsApi`-建立維護視窗，以使用執行命令定期執行中繼資料收集器應用程式。維護時段會啟動和停止指令之間的執行個體。
- 15 `aws:waitForAwsResourceProperty`-等待 AWS CloudFormation 範本建立的維護視窗準備就緒為止。
- 16 `aws:executeAwsApi`-獲取 IDs 維護窗口並更改由創建的日曆 AWS CloudFormation。
- 17 `aws:sleep`-等待到維護時段的結束日期。
- 18 `aws:executeAwsApi`-關閉維護視窗。
- 19 `aws:executeScript`-取得維護時段期間執行的工作結果。
- 20 `aws:waitForAwsResourceProperty`-等待維護時段完成最後一項工作，然後再繼續。
- 21 `aws:branch`-根據您是否提供 `SupportCase` 參數值來分支工作流程。
- a. `aws:changeInstanceState`-啟動臨時 Amazon EC2 執行個體，並等待狀態檢查通過，然後再上傳報告。
  - b. `aws:waitForAwsResourceProperty`-等待直到臨時 Amazon EC2 執行個體由系統管理員管理為止。如果此步驟逾時或失敗，則執行本會重新啟動執行個體。
    - i. `aws:executeAwsApi`-如果上一個步驟失敗或逾時，請重新啟動臨時 Amazon EC2 執行個體。
    - ii. `aws:waitForAwsResourceProperty`-等待直到臨時 Amazon EC2 執行個體在重新開機後由系統管理員管理。
  - c. `aws:runCommand`-如果您為 `SupportCase` 參數提供了值，AWS Support 則將中繼資料報表附加至大小寫。指令碼會將報表壓縮並分割成 5 MB 的檔案。腳本附加到案 AWS Support 例的最大文件數為 12。
- 22 `aws:changeInstanceState`-停止暫存 Amazon EC2 執行個體，以防 AWS CloudFormation 堆疊無法刪除。
- 23 `aws:executeAwsApi`-描述執行簿無法建立或更新 AWS CloudFormation 堆疊時的 AWS CloudFormation 堆疊事件。

24.`aws:waitForAwsResourceProperty`-等待 AWS CloudFormation 堆疊處於終端機狀態後再刪除。

25.`aws:executeAwsApi`-刪除維護時段以外的 AWS CloudFormation 堆疊。如果 `EbsVolumeDeleteOnTermination` 參數值設定為 `true`，則會保留與臨時 Amazon EC2 執行個體關聯的根 Amazon EBS 磁碟區 `false`。

## AWS-RebootRdsInstance

### Description

如果 Amazon 關聯式資料庫服務 (AmazonRDS) 資料庫 `AWS-RebootRdsInstance` 執行個體尚未重新啟動，則執行手冊會重新啟動該執行個體。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您要重新開機之 Amazon RDS 資料庫執行個體的 ID。

## 文件步驟

RebootInstance -重新啟動資料庫執行個體 (如果尚未重新啟動)。

WaitForAvailableState -等待資料庫執行個體完成重新開機程序。

## 輸出

此自動化沒有輸出。

# AWSSupport-ShareRDSSnapshot

## Description

AWSSupport-ShareRDSSnapshotRunbook 針對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) 快照已使用預設值加密 AWS 受管金鑰，則無法共用快照。在此情況下，您必須使用客戶管理的金鑰複製快照，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，或針對所選 Amazon RDS 資料庫執行個體或叢集找到的最新快照來執行這些步驟。

### Note

如果您未指定KMSKey參數值，自動化作業會在您的帳 AWS KMS 戶中建立新的客戶管理金鑰，用於加密快照集。

## [運行此自動化 \(控制台\)](#)

### 文件類型

### 自動化

### 擁有者

### Amazon

### 平台

### 資料庫

### 參數

- AccountIds

類型: StringList

說明 : (必填) 要與之共用快照的帳號 ID 清單 (以逗號分隔)。

- AutomationAssumeRole

類型 : 字串

說明 : (選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色, Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 資料庫

類型 : 字串

說明 : (必填) 您要共用其快照之 Amazon RDS 資料庫執行個體或叢集的名稱。如果您為參數指定值, 則此SnapshotName參數為可選。

- 科姆斯基

類型 : 字串

說明 : (選用) 用於加密快照之 AWS KMS 客戶受管金鑰的完整 Amazon 資源名稱 (ARN)。

- SnapshotName

類型 : 字串

說明 : (選擇性) 您要使用的資料庫叢集或執行個體快照的 ID。

### 必要的 IAM 許可

此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

用於執行自動化的 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。如需將金鑰使用者新增至 KMS 金鑰的詳細資訊，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參數值，則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，並在找不到任何值時建立 AWS KMS 客戶管理的金鑰。
2. aws:branch-檢查是否為SnapshotName參數提供了值，並相應地進行分支。
3. aws:executeAwsApi-檢查提供的快照是否來自資料庫執行個體。
4. aws:executeScript-格式化用連字符替換冒號的SnapshotName參數。
5. aws:executeAwsApi-使用指定的複製快照KMSKey。
6. aws:waitForAwsResourceProperty-等待複製快照作業完成。
7. aws:executeAwsApi-與AccountIds指定的快照共用新快照。
8. aws:executeAwsApi-檢查提供的快照是否來自資料庫叢集。
9. aws:executeScript-格式化用連字符替換冒號的SnapshotName參數。
10. aws:executeAwsApi-使用指定的複製快照KMSKey。
11. aws:waitForAwsResourceProperty-等待複製快照作業完成。

- 12aws:executeAwsApi-與AccountIds指定的快照共用新快照。
- 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-從上一個步驟中組裝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-等待複製快照作業完成。
- 19aws:executeAwsApi-與AccountIds指定的快照共用新快照。
- 20aws:executeAwsApi-擷取指定的快照清單Database。
- 21aws:executeScript-從上一個步驟中組裝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-等待複製快照作業完成。
- 24aws:executeAwsApi-與AccountIds指定的快照共用新快照。
- 25aws:executeScript-如果您未指定KMSKey參數值且自動化失敗，則刪除由自動化建立的 AWS KMS 客戶管理金鑰。

## AWS-StartRdsInstance

### Description

啟動 Amazon Relational Database Service 服務 (AmazonRDS) 執行個體。

[運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：( 必填 ) 要啟動的 Amazon RDS 執行個體 ID。

## AWS-StartStopAuroraCluster

### Description

此手冊啟動或停止 Amazon Aurora 集群。

#### 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叢集是 Aurora 無伺服器叢集、Aurora 多主機叢集、Aurora 全域資料庫的一部分，或使用 Aurora parallel 查詢的叢集。

### [運行此自動化 \( 控制台 \)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

預設值：開始

描述：(必要) 您要停止或啟動的 Aurora 叢集名稱。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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訊息-自動化的詳細資訊

## AWS-StopRdsInstance

### Description

停止 Amazon Relational Database Service 服務 (AmazonRDS) 執行個體。

[運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：( 必填 ) 要停止的 Amazon RDS 執行個體 ID。

## AWSsupport-TroubleshootConnectivityToRDS

### Description

AWSSupport-TroubleshootConnectivityToRDSRunbook 診斷執行個體和 Amazon Relational Database Service EC2 執行個體之間的連線問題。自動化可確保資料庫執行個體可用，然後檢查相關聯的安全群組規則、網路存取控制清單 (網路ACLs) 和路由表是否有潛在的連線問題。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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：`^i-[a-z0-9]{8,17}$`

說明：(必要) 測試連線的 EC2 執行個體 ID。

必要的 IAM 權限

此AutomationAssumeRole參數需要執行下列動作，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的相關資訊ACLs。
- 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執行個體網路的相關資訊ACLs。
- 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執行個體之 Amazon VPC 相關聯之主路由表的相關資訊。
- 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-取得資料庫執行個體與 Amazon 相關聯之主路由表VPC的相關資訊。
- aws:executeScript-評估安全性群組規則。
- aws:executeScript-評估網絡ACLs。
- aws:executeScript-評估路由表。
- aws:sleep-結束自動化

### 輸出

getRDSInstance屬性。 DBInstanceIdentifier-自動化中使用的資料庫執行個體。

getRDSInstance屬性。 DBInstanceStatus-的目前狀態DBInstance。

evalSecurityGroup規則。 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。

evalNetworkAcl規則。 NetworkAclEvaluation -比較SourceInstance網ACLs路與資料庫執行個體網路的結果ACLs。

evalRouteTable項目。 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有助於針對 Postgre 的 Amazon，我的 AmazonRDS，MariaDB 的 AmazonSQL，亞馬遜 RDS Aurora Postgre 和 Amazon Aurora 我SQL的實RDS例進行故障排除 AWS Identity and Access Management ( IAM ) 身份驗證。SQL SQL使用此執行手冊來驗證使用 Amazon RDS 執行個體或 Aurora 叢集進行IAM身份驗證所需的組態。同時也提供修正 Amazon RDS 執行個體或 Aurora 叢集之連線問題的步驟。

#### Important

這本手冊不支持 Amazon RDS 的甲骨文或 Amazon Microsoft RDS 服SQL務器。

#### Important

如果提供來源 Amazon EC2 執行個體，且目標資料庫為 AmazonRDS，則會叫用子自動化以AWSsupport-TroubleshootConnectivityToRDS對TCP連線進行疑難排解。輸出還提供您可以在 Amazon EC2 執行個體或來源機器上執行的命令，以使用IAM身份驗證連接到 Amazon RDS 執行個體。

它是如何工作的？

此手冊由六個步驟組成：

- 第 1 步validateInputs：驗證輸入到自動化。
- 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 3validateRDSConnectivity：驗證來源 Amazon EC2 執行個體的 Amazon RDS 連線 (若有提供)。



- 步驟 4 `validateRDSIAMAuthentication` : 驗證 IAM 證功能是否已啟用。
- 步驟 5 `validateIAMPolicies` : 驗證所提供的 IAM 用戶/角色中是否存在所需的 IAM 權限。
- 第 6 步 `generateReport` : 生成先前執行的步驟的結果的報告。

## [運行此自動化 \( 控制台 \)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色, Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `RDSType`

類型 : 字串

描述 : (必要) : 選取您嘗試連線並進行認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

說明 : (必填) 目標 Amazon RDS 資料庫執行個體或 Aurora 資料庫叢集的識別碼。

允許的模式 : `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

最多字元數目:63

- SourceEc2 InstanceIdentifier

類型 : AWS::EC2::Instance::Id

說明 : (選擇性) 如果您要從相同帳戶和區域中EC2執行的 Amazon 執行個體連線至 Amazon RDS 資料庫EC2執行個體，則為 Amazon 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 : (選擇性) 用IAM於驗證的IAM角色名稱。僅在未提供參數DBIAMUserName時提供，否則請將其保留空白。DBIAMRoleName或DBIAMUserName必須提供。

允許的模式 : `^[a-zA-Z0-9+,.@_-]{1,64}$|^$`

最多字元數目:64

預設 : ""

- DBIAMUserName

類型 : 字串

說明 : (選擇性) 用IAM於基礎驗證的使用IAM者名稱。僅在未提供DBIAMRoleName參數時提供，否則請將其保留空白。DBIAMRoleName或DBIAMUserName必須提供。

允許的模式 : `^[a-zA-Z0-9+,.@_-]{1,64}$|^$`

最多字元數目:64

預設 : ""

- DBUserName

類型 : 字串

描述 : (選擇性) 對應至資料庫中IAM以進行認證之IAM角色/使用者的資料庫使用者名稱。預設選項\*會評估資料庫中是否允許所有使用者使用`rds-db:connect`權限。

允許的模式：`^[a-zA-Z0-9+,.@*_-]{1,64}$`

最多字元數目:64

預設：`*`

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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. 導覽至主 AWS Systems Manager 控制台 `troubleshootRDSIAMAuthentication` 中的 [AWSSupport-T](#)。
2. 選擇執行自動化

### 3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole(選擇性)：

() 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- RDSType ( 必填 )：

選擇您嘗試連接和進行身份驗證的 Amazon RDS 類型。從兩個允許的值中選擇：Amazon RDS 或 Amazon Aurora Cluster。

- DBInstanceIdentifier ( 必填 )：

輸入您嘗試連接的目標 Amazon RDS 資料庫執行個體或 Aurora 叢集的識別碼，並使用 IAM 登入資料進行身份驗證。

- SourceEc2 InstanceIdentifier (選擇性)：

如果您要從相同帳戶和區域中的 Amazon EC2 執行個體連接到 Amazon RDS 資料庫 EC2 執行個體，請提供 Amazon 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(選擇性)：

輸入用於「IAM 基礎」驗證的「IAM 角色」名稱。僅在未提供 DBIAMUserName 時提供；否則，請留空。DBIAMRoleName 或 DBIAMUserName 必須提供。

- DBIAMUserName(選擇性)：

輸入用於「IAM 基於」驗證的「使用 IAM 者」。僅在未提供 DBIAMRoleName 時提供，否則保留空白。DBIAMRoleName 或 DBIAMUserName 必須提供。

- DBUserName(選擇性)：

輸入對應至資料庫中「IAM 基於」驗證之 IAM 角色/使用者的資料庫使用者。預設選項用 \* 於評估；此欄位中未提供任何內容。

### 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

< 1 ... >

| Name   | Instance ID | State | Availability zone | Platform |
|--|-------------|-------|-------------------|----------|
| There are no managed Instances in this account.<br>We recommend using <a href="#">Quick Setup</a> to configure your Instances for Systems Manager.<br>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.

**RDSInstanceIdentifier**  
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

**DBIAMRoleName**  
(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter `DBIAMRoleName` is not provided, otherwise leave it empty. Either `DBIAMRoleName` or `DBIAMUserName` must be provided.

**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：
  - 步驟一-validateInputs:

驗證輸入到自動化-SourceEC2InstanceIdentifier ( 可選 )，DBInstanceIdentifier或ClusterID，和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，它還會執行其他驗證，例如提到的資料庫是否處於 [可用] 狀態。

- 步驟二 branchOnSourceEC2Provided:

驗證 Amazon 來源EC2是否在輸入參數提供和數據庫是 Amazon RDS。如果是，則會繼續執行步驟 3。如果沒有，它會跳過步驟 3，這是 EC2 Amazon RDS 連接驗證，並繼續步驟 4。

- 步驟三validateRDSConnectivity:

如果在輸入參數中EC2提供了源 Amazon，並且數據庫是 AmazonRDS，則步驟 2 啟動步驟 3。在此步驟中，會叫用子自動化AWSSupport-TroubleshootConnectivityToRDS來驗證來源 Amazon 的 Amazon RDS 連線能力EC2。子自動化執行手冊AWSSupport-TroubleshootConnectivityToRDS會驗證所需的網路組態 (Amazon Virtual Private Cloud

[AmazonVPC]、安全群組、網路存取控制清單 [NACL]、Amazon 可RDS用性) 是否已到位，以便您可以從 Amazon 執行個體連接到 Amazon EC2 執行個體。RDS

- 步驟四validateRDSIAMAuthentication:

驗證IAM證是否在 Amazon RDS 執行個體或 Aurora 叢集上啟用了身份驗證功能。

- 步驟五validateIAMPolicies:

驗證傳遞的使用IAM者/角色中是否存在所需的IAM許可，以便讓IAM登入資料為指定的資料庫使用者 (如果有) 向 Amazon RDS 執行個體進行驗證。

- 步驟六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 執行RDS個體的參考和執行步驟。

## 7. 自動化操作完成後，請查看「輸出」部分以獲取詳細結果：

- 檢查用IAM戶/角色權限以連接到數據庫：

驗證傳遞的使用IAM者/角色中是否存在所需的IAM許可，以便讓IAM登入資料為指定的資料庫使用者 (如果有) 向 Amazon RDS 執行個體進行驗證。

- 檢查資料庫的IAM基礎驗證屬性：

驗證是否為指定的 Amazon RDS 資料庫/Aurora 叢集啟用IAM身份驗證功能。

- 檢查 Amazon 執行個體與 Amazon EC2 執行個體的連線能力：RDS

驗證是否已設置所需的網路組態 (Amazon VPC、安全群組NACL、Amazon 可RDS用性)，以便您可以從 Amazon 執行個體連接到 Amazon EC2 執行RDS個體。

- 後續步驟:

列出使用IAM登入資料連接 Amazon 執行RDS個體時所要參考和執行的命令和步驟。

**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**

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化工作流登陸頁](#)

**AWSSupport-ValidateRdsNetworkConfiguration****Description**

AWSSupport-ValidateRdsNetworkConfiguration在執行或操作之前，自動化有助於避免現有的 Amazon Relational Database Service (AmazonRDS)/Amazon Aurora/Amazon DocumentDB 執行個體出現不相容的網路狀態。ModifyDBInstance StartDBInstance如果執行個體已經處於不相容的網路狀態，則 Runbook 會提供原因。

**它是如何工作的？**

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，或是否有，請判斷其處於不相容網路狀態的原因。

執行手冊會針對您的 Amazon RDS 資料庫執行個體執行下列檢查：

- Amazon 彈性網路界面 (ENI) 每個區域的配額。
- 資料庫子網路群組中的所有子網路都存在。
- 有足夠的可用 IP 位址供子網路使用。
- (適用於可公開存取的 Amazon RDS 執行個體) VPC 屬性設定 (enableDnsSupport和enableDnsHostnames)。

#### Important

對 Amazon Aurora/Amazon DocumentDB 叢集使用此文件時，請確保您使用的DBInstanceIdentifier是。ClusterIdentifier否則，文檔將在第一個步驟中失敗。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

資料庫

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- rds:DescribeDBInstances
- servicequotas:GetServiceQuota
- ec2:DescribeNetworkInterfaces
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets

樣本政策：



```

{
  "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. 導航到 AWS Systems Manager 控制台 ValidateRdsNetworkConfiguration 中的 [AWSSupport-](#)
2. 選擇執行自動化
3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole(選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DBInstanceIdentifier ( 必填 )：

輸入 Amazon Relational Database Service 執行個體識別碼。

The screenshot shows the 'Input parameters' section of the AWS Systems Manager console. It contains two input fields:

- AutomationAssumeRole**: A dropdown menu with the text 'Select an existing IAM Role'. The selected option is 'AutomationAssumeRoleSSM'.
- DBInstanceIdentifier**: A text input field with 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：

- 步驟一 `assertRdsState`:

檢查提供的執行個體識別碼是否存在，且具有下列任何狀態：`availablestopped`、`incompatible-network`。

- 步驟二 `gatherRdsInformation`:

收集 Amazon RDS 執行個體的必要資訊，以便稍後在自動化中使用。

- 步驟三 `checkEniQuota`:

檢查該區域的 Amazon ENI 目前可用配額。

- 步驟四 `validateVpcAttributes`:

驗證 Amazon 的 DNS 參數 (`enableDnsSupport` 和 `enableDnsHostnames`) 是否設 VPC 置為 `true` ( 或者，如果 Amazon 實 RDS 例是否 `PubliclyAccessible` )。

- 步驟五 `validateSubnetAttributes`:

驗證中是否存在子網路，`DBSubnetGroup` 並檢查每個子網路是否可 IP 用。

- 步驟六 `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 執行 RDS 個體的參考和執行步驟。

## 7. 自動化操作完成後，請查看「輸出」部分以獲取詳細結果：

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.
```

具有錯誤網路組態的 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-vcattr (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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

### AWS 服務文件

- [如何解決處於不兼容網絡狀態的 Amazon RDS 數據庫的問題？](#)
- [如何解決處於不相容網路狀態的 Amazon DocumentDB 執行個體的問題？](#)

## Amazon Redshift

AWS Systems Manager 自動化為 Amazon Redshift 提供了預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

## 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 執行手冊會刪除您指定的 Amazon Redshift 叢集。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- **ClusterIdentifier**

類型：字串

說明：(必填) 您要刪除的 Amazon Redshift 叢集識別碼。

- **SkipFinalClusterSnapshot**

類型：布林值

預設：false

說明：(選擇性) 如果設定為false，則自動化會在刪除 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權限

此AutomationAssumeRole參數需要執行下列動作，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-確認已刪除 Amazon Redshift 叢集。

## **AWSConfigRemediation-DisablePublicAccessToRedshiftCluster**

### Description

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster執行手冊會停用您指定之 Amazon Redshift 叢集的公用可存取性。

[運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- ClusterIdentifier

類型：字串

描述：(必要) 您要停用公用存取性之叢集的唯一識別碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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用可存取性。
- aws:waitForAwsResourceProperty-等待叢集狀態變更為available。
- aws:assertAwsResourceProperty-確認叢集上的公用可存取性設定已停用。

# AWSConfigRemediation-EnableRedshiftClusterAuditLogging

## Description

AWSConfigRemediation-EnableRedshiftClusterAuditLogging 執行手冊會為您指定的 Amazon Redshift 叢集啟用稽核記錄。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BucketName

類型：字串

說明：(必填) 您要將日誌上傳到的 Amazon Simple Storage Service (Amazon S3) 儲存貯體的名稱。

- 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碼。

- S3 KeyPrefix

類型：字串



說明：(選用) 您要將日誌上傳到的 Amazon S3 key prefix (子資料夾)。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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`-驗證已在叢集上啟用稽核記錄。

## AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

### Description

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot執行手冊會為您指定的 Amazon Redshift 叢集啟用自動化快照。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- AutomatedSnapshotRetentionPeriod

類型：整數

有效值：1-35

說明：(必要) 自動化快照的保留天數。

- ClusterIdentifier

類型：字串

說明：(必要) 您要啟用自動快照之叢集的唯一識別碼。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-等待叢集狀態變更為available。
- aws:executeScript-確認已在叢集上啟用自動快照。

# AWSConfigRemediation-EnableRedshiftClusterEncryption

## Description

AWSConfigRemediation-EnableRedshiftClusterEncryption 執行手冊會在您使用 AWS Key Management Service (AWS KMS) 客戶受管金鑰指定的 Amazon Redshift 叢集上啟用加密。此執行手冊只應用作基準，以確保您的 Amazon Redshift 叢集根據建議的最低安全性最佳實務進行加密。我們建議使用不同的客戶託管金鑰加密多個叢集。此 runbook 無法變更已加密叢集上使用的 AWS KMS 客戶管理金鑰。若要變更用於加密叢集的 AWS KMS 客戶管理金鑰，您必須先停用叢集上的加密。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- ClusterIdentifier

類型：字串

說明：(必要) 您要啟用加密之叢集的唯一識別碼。

- KMSKeyARN

類型：字串

描述：(必填) 您要用來加密叢集資料的 AWS KMS 客戶受管金鑰的 Amazon 資源名稱 (ARN)。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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執行手冊可為您指定的 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](#)。

## [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-確認已在叢集上啟用增強型VPC路由。

## AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

### Description

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster執行手冊需要傳入連線才能用SSL於您指定的 Amazon Redshift 叢集。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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碼。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-在參數中指定的叢集上啟用require\_ssl設ClusterIdentifier定。
- aws:assertAwsResourceProperty-確認已在叢集上啟用require\_ssl設定。

- `aws:executeScript`-驗證叢集的`require_ssl`設定。

## AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

### Description

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings執行手冊會修改您指定的 Amazon Redshift 叢集的維護設定。

### [運行此自動化 \(控制台\)](#)

#### 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`，則在維護時段期間將主要版本升級自動套用至叢集。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- AutomatedSnapshotRetentionPeriod

類型：整數

有效值：1-35

說明：(必要) 自動化快照的保留天數。

- 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碼。

- PreferredMaintenanceWindow

類型：字串

描述：(必要) 可以進行系統維護的每週時間範圍 (inUTC)。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

### 文件步驟

- aws:executeAwsApi-修改參數中指定之叢集的維護設ClusterIdentifier定。
- aws:assertAwsResourceProperty-確認已為叢集配置修改的維護設定。

## AWSConfigRemediation-ModifyRedshiftClusterNodeType

### Description

AWSConfigRemediation-ModifyRedshiftClusterNodeType執行手冊會修改您指定的 Amazon Redshift 叢集的節點類型和節點數目。

[運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 傳統

類型：布林值

描述：(選擇性) 如果設定為true，調整大小作業會使用傳統的調整大小程序。

- 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碼。

- ClusterType

類型：字串

有效值：單節點 | 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：大尺寸 | 大尺寸 | DC1.8 倍大 | 直流 1.8 倍大 | 直流 2-大 | 大型 | 拉 3.4 倍大 | 拉 16 倍大

描述：(必要) 您要指派給叢集的節點類型。

- NumberOfNodes

類型：整數

有效值：

描述：(選擇性) 您要指派給叢集的節點數目。如果您的叢集是single-node類型，請勿指定此參數的值。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ResizeCluster

#### 文件步驟

- aws:executeScript-修改參數中指定之叢集的節點類型和節點ClusterIdentifier數目。

## Amazon S3

AWS Systems Manager 自動化為 Amazon 簡單儲存服務提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

#### 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](#)

## AWS-ArchiveS3BucketToIntelligentTiering

### Description

AWS-ArchiveS3BucketToIntelligentTieringRunbook 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。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- BucketName

類型：字串

說明：(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。這可以是新的組態識別碼，也可以是現有組態的識別碼。

- NumberOfDaysToArchive

類型：字串

有效值：

說明：(必要) 值區中的物件可轉換至封存存取層之後的連續天數。

- NumberOfDaysToDeepArchive

類型：字串

有效值：

說明：(必要) 值區中的物件可轉換至深層封存存取層之後的連續天數。

- S3Prefix

類型：字串

說明：(選擇性) 您要套用組態之物件的索引鍵名稱前置碼。

- 標籤

類型: MapList

說明：(選擇性) 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權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetIntelligentTieringConfiguration
- s3:PutIntelligentTieringConfiguration

## 文件步驟

- `PutBucketIntelligentTieringConfiguration` (`aws:executeScript`)-為指定儲存貯體建立或更新 Amazon S3 智慧型分層組態。
- `VerifyBucketIntelligentTieringConfiguration` (`aws : assertAwsResource`屬性) -驗證 S3 存儲桶智能配置已應用於指定的存儲桶。

## AWS-ConfigureS3BucketLogging

### Description

在亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體上啟用日誌記錄。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

### 參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `BucketName`

類型：字串

說明：(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 | 組

描述：(必要) 被授予者的類型。

- **GranteeUri**

類型：字串

描述：(選擇性) URI 受權者群組。

- **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。在這種情況下，您應該 TargetPrefix 為每個來源值區選擇不同的值區，以便透過金鑰區分傳送的記錄檔。

- **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

為亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體設定版本控制。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- BucketName

類型：字串

說明：(必填) 您要為其設定版本控制的 Amazon S3 儲存貯體的名稱。

- VersioningState

類型：字串

有效值：已啟用 | 已暫停

預設：Enabled

說明：(選擇性) 已套用至 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。設定為時Suspended，此程序會停用值區中物件的版本控制。所有新增至值區的物件都會收到版本 ID null。

## AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

### Description

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock執行手冊會根據您在執行手冊參數中指定的值，為 Amazon S3 儲存貯體設定 Amazon S3 儲存貯體的 Amazon 簡單儲存服務 (Amazon S3) 公有存取區塊設定。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BlockPublicAcls

類型：布林值

預設：true



說明：(選用) 如果設為true，Amazon S3 會封鎖 S3 儲存貯體的公用存取控制清單 (ACLs)，以及存放在您在BucketName參數中指定之 S3 儲存貯體中的物件。

- BlockPublicPolicy

類型：布林值

預設：true

說明：(選用) 如果設為true，Amazon S3 會針對您在BucketName參數中指定的 S3 儲存貯體封鎖公用儲存貯體政策。

- BucketName

類型：字串

說明：(必要) 您要設定的 S3 儲存貯體名稱。

- IgnorePublicAcls

類型：布林值

預設：true

說明：(選擇性) 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ACLs用。

- RestrictPublicBuckets

類型：布林值

預設：true

說明：(選用) 如果設為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權限

此AutomationAssumeRole參數需要執行下列動作，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-為BucketName參數中指定的 S3 儲存貯體建立或修改PublicAccessBlock組態。
- aws:executeScript-傳回參數中指定之 S3 儲存貯體的PublicAccessBlock組態，並根據runbook BucketName 參數中指定的值驗證變更成功。

## AWSConfigRemediation-ConfigureS3PublicAccessBlock

### Description

AWSConfigRemediation-ConfigureS3PublicAccessBlock執行手冊會根據您在工作 AWS 帳戶流程冊參數中指定的值來設定 Amazon 簡單儲存服務 (Amazon S3) 公用存取區塊設定。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AccountId

類型：字串

說明：(必要) 擁有您正在 AWS 帳戶 設定之 S3 儲存貯體的 ID。

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BlockPublicAcls

類型：布林值

預設：true

說明：(選用) 如果設為true，Amazon S3 會針對 AWS 帳戶 您在AccountId參數中指定的所擁有的 S3 儲存貯體封鎖公用存取控制清單 (ACLs)。

- BlockPublicPolicy

類型：布林值

預設：true

說明：(選用) 如果設為true，Amazon S3 會封鎖 AWS 帳戶 您在AccountId參數中指定之 S3 儲存貯體所擁有的公有儲存貯體政策。

- IgnorePublicAcls

類型：布林值

預設：true

說明：(選擇性) 如果設為true，Amazon S3 會忽略 AWS 帳戶 您在AccountId參數中指定的 S3 儲存貯體所擁有的所有公ACLs用。

- RestrictPublicBuckets

類型：布林值

預設：true

說明：(選用) 如果設為true，Amazon S3 會限制 AWS 帳戶 您在AccountId參數中指定的 S3 儲存貯體所擁有的公有儲存貯體政策。

此AutomationAssumeRole參數需要執行下列動作，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 AWS 帳戶 指定的PublicAccessBlock組態。
- aws:executeScript-傳回參數中 AWS 帳戶 指定的PublicAccessBlock組態，並根據 runbook AccountId 參數中指定的值驗證變更是否成功完成。

## AWS-CreateS3PolicyToExpireMultipartUploads

### Description

AWS-CreateS3PolicyToExpireMultipartUploadsrunbook 會為指定值區建立生命週期政策，該儲存貯體會在定義的天數後過期不完整的多部分上傳作業。此 runbook 會將新的生命週期原則與任何現有的生命週期儲存貯體政策合併。

### [運行此自動化 \( 控制台 \)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- BucketName

類型：字串

說明：(必要) 您要設定的 S3 儲存貯體名稱。

- DaysUntilExpire

類型：整數

說明：(必填) 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

摘要：(必要) 用來識別生命週期時段規則的識別碼。這必須是唯一的值。

- S3Prefix

類型：字串

說明：(選擇性) 您要套用組態之物件的索引鍵名稱前置碼。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration

## 文件步驟

- ConfigureExpireMultipartUploads (aws:executeScript)-設定值區的生命週期政策。

- `VerifyExpireMultipartUploads (aws:executeScript)`-驗證儲存貯體已設定生命週期政策。

## 輸出

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

## AWS-DisableS3BucketPublicReadWrite

### Description

使用 Amazon Simple Storage Service (Amazon S3) 停用 `Block Public Access` 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 簡單儲存服務使用者指南中的使用 Amazon S3 區塊公開存取](#)。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- `S3 BucketName`

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) 貯體的預設加密。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

預設值：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-EnableS3BucketKeysRunbook 在您指定的亞馬遜簡單存儲服務 ( Amazon S3 ) 存儲桶上啟用存儲桶密鑰。此儲存貯體層級金鑰會在新物件的生命週期中建立資料金鑰。如果您未指定KmsKeyId參數值，則使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密將用於預設加密組態。

#### 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。

### [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。



- BucketName

類型：字串

說明：(必要) 您要啟用儲存貯體金鑰的 S3 儲存貯體名稱。

- KMSKeyId

類型：字串

說明：(選用) 您要用於伺服器端加密之 (ARN) 客戶受管金鑰的 Amazon 資源名稱 AWS Key Management Service (AWS KMS)、金鑰 ID 或金鑰別名。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetEncryptionConfiguration
- s3:PutEncryptionConfiguration

### 文件步驟

- ChooseEncryptionType (aws: 分支)-評估為KmsKeyId參數提供的值，以確定是否要使用 SSE-S3 (AES256) 或 SSE-KMS。
- PutBucketKeysKMS(aws:executeAwsApi)-使用指定的指定 S3 儲存貯體將BucketKeyEnabled屬性設定true為KmsKeyId。
- PutBucketKeysAES256 ( aws:executeAwsApi ) -使用AES256加密將指定 S3 存儲桶的BucketKeyEnabled屬性設置true為。
- 驗證 3BucketKeysEnabled ( aws : assertAwsResource屬性 ) -驗證目標 S3 儲存貯體上已啟用儲存貯體金鑰。

## AWSConfigRemediation- RemovePrincipalStarFromS3BucketPolicy

### Description

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicyrunbook 會從您的 Amazon 簡單儲存服務 (Amazon S3Principal: "AWS": \*) 儲存貯體政策中移除具有萬用字元 (Principal: \*或) Allow 動作的主要政策陳述式。包含條件的政策聲明也會被移除。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BucketName

類型：字串

說明：(必填) 您要修改其政策的 Amazon S3 儲存貯體名稱。

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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，並使用萬用字元驗證主體政策陳述式已從您在參數中指定的 Amazon S3 儲存貯體中BucketName移除。

# AWSConfigRemediation-RestrictBucketSSLRequestsOnly

## Description

AWSConfigRemediation-RestrictBucketSSLRequestsOnlyRunbook 會建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策聲明，明確拒絕對您指定的 Amazon S3 儲存貯體的HTTP請求。

## [運行此自動化 \(控制台\)](#)

## 文件類型

自動化

## 擁有者

Amazon

## 平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- BucketName

類型：字串

說明：(必要) 您要拒絕HTTP請求的 S3 儲存貯體名稱。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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BucketName參數中指定的 S3 儲存貯體建立儲存貯體政策，以明確拒絕 HTTP 請求。

# AWSSupport-TroubleshootS3PublicRead

## Description

AWSSupport-TroubleshootS3PublicReadRunbook 診斷從您在參數中指定的公用 Amazon Simple Storage Service (Amazon S3) 儲存貯體讀取物件的S3BucketName問題。系統也會針對 S3 儲存貯體中的物件分析設定子集。

## [運行此自動化 \( 控制台 \)](#)

## 限制

- 此自動化操作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金鑰。
- 如果您使用的是 AWS Organizations，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

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- CloudWatchLogGroupName

類型：字串

說明：(選用) 您要傳送自動化輸出的 Amazon CloudWatch 日誌日誌群組。如果找不到符合您指定值的記錄群組，自動化操作會使用此參數值建立記錄群組。此自動化操作所建立之記錄群組的保留期為 14 天。

- CloudWatchLogStreamName

類型：字串

說明：(選擇性) 您要傳送自動化輸出的 CloudWatch 記錄資料流。如果找不到符合您指定值的記錄資料流，則自動化操作將使用此參數值建立記錄資料流。如果您未指定此參數的值，則自動化操作將使用 ExecutionId 為記錄資料流的名稱。

- HttpGet

類型：布林值

有效值：true | false

預設：true

描述：(選擇性) 如果此參數設定為 true，則自動化會對 S3BucketName 您指定的物件發出部分 HTTP 要求。只有物件的第一個位元組會使用 Range 標 HTTP 頭傳回。

- IgnoreBlockPublicAccess

類型：布林值

有效值：true | false

預設：false

說明：(選擇性) 如果此參數設定為true，則自動化會忽略您在S3BucketName參數中指定之 S3 儲存貯體的公用存取區塊設定。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

說明：(選擇性) 您在參數中指定的 S3 儲存貯體中要分析的物件S3BucketName數目。

- S3 BucketName

類型：字串

說明：(必要) 要疑難排解的 S3 儲存貯體名稱。

- S3 PrefixName

類型：字串

說明：(選擇性) 您要在 S3 儲存貯體中分析之物件的金鑰名稱前置詞。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的[物件金鑰](#)。

- StartAfter

類型：字串

說明：(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

說明：(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：(選擇性) 若要在自動化期間傳回更詳細的資訊，請將此參數設定為true。如果參數設定為，則只會傳回警告和錯誤訊息false。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

只有當logs:CreateLogGroup您希望自動化操作將記錄資料傳送至 CloudWatch 記錄檔時，才需要logs:CreateLogStream、和logs:PutLogEvents權限。

```
{
  "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 儲存貯體位置和規範使用者 ID。
- `aws:executeScript`-傳回帳戶和 S3 儲存貯體的公用存取區塊設定。
- `aws:assertAwsResourceProperty`-確認 S3 儲存貯體付款人已設定為BucketOwner。如果Requester Pays在 S3 儲存貯體上啟用，則自動化結束。
- `aws:executeScript`-傳回 S3 儲存貯體政策狀態，並判斷其是否被視為公開。如需有關公用 S3 儲存貯體的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中 [「public」的意義](#)。
- `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金鑰。
- `aws:assertAwsResourceProperty`-確認該GetObjectAPI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，則會建立 CloudWatch Logs 記錄群組和記錄串流。
- `aws:executeScript`-根據您在 runbook 輸入參數中指定的值，評估自動化期間收集的任何 S3 儲存貯體設定是否阻止公眾存取物件。此指令碼執行下列功能：



- 評估公用存取區塊設定
- 根據您在MaxObjects、S3PrefixName和StartAfter參數中指定的值，從 S3 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，則對傳回的物件執行部分HTTP要求true。只有物件的第一個位元組會使用 Range 標HTTP頭傳回。
- 檢查傳回物件的索引鍵名稱，以確認是否以一個或兩個句點結束。無法從 Amazon S3 主控台下載以期間結束的物件金鑰名稱。
- 檢查傳回物件的擁有者是否符合 S3 儲存貯體的擁有者。
- 檢查物件是否ACL授與READ或FULL\_CONTROL權限給匿名使用者。
- 傳回與物件相關聯的標籤。
- 使用模擬IAM政策來確認該GetObjectAPI動作的 S3 儲存貯體政策中是否有此物件的明確拒絕。
- 傳回物件的中繼資料，以確認是否支援儲存類別。
- 檢查物件的伺服器端加密設定，以確認物件是否使用 AWS Key Management Service (AWS KMS) 客戶管理的金鑰加密。

## 輸出

AnalyzeObjects. 桶

AnalyzeObjects. 物件。

## SageMaker

AWS Systems Manager 自動化為 Amazon SageMaker 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWS-DisableSageMakerNotebookRootAccess](#)

## AWS-DisableSageMakerNotebookRootAccess

### Description

`AWS-DisableSageMakerNotebookRootAccess` 執行本會停用 Amazon SageMaker 筆記本執行個體上的根存取權。在自動化期間，筆記本執行個體會停止以進行必要的變更。SageMaker 不支援 Studio 筆記本執行個體。

## [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- NotebookInstanceName

類型：字串

描述：(必要) 要停用 root 存取權的 SageMaker 筆記本執行個體名稱。

- StartInstanceAfterUpdate

類型：布林值

預設：true

描述：(選擇性) 決定是否在停用 root 存取權後啟動筆記本執行個體。此參數的預設設定為 true。如果設定為 true，則會在停用 root 存取權限之後啟動執行個體。如果設定為 false，則在停用 root 存取權限之後，執行個體會保留在 stopped 狀態。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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` ) : 檢查筆記本實例的當前狀態。
- `StopOrUpdateNotebookInstance` ( `aws` : 分支 ) : 根據筆記本實例的狀態進行分支。
- `StopNotebookInstance` ( `aws:executeAwsApi` ) : 如果狀態為 `Running`，則啟動實例 `stopped`。
- `WaitForInstanceToStop` ( `aws:waitAwsResourceProperty` ) : 驗證實例是 `stopped` 否正確。
- `UpdateNotebookInstance` ( `aws:executeAwsApi` ) : 禁用筆記本實例上的根訪問權限。
- `WaitForNotebookUpdate` ( `aws:waitAwsResourceProperty` ) : 驗證 `root` 訪問權限已被禁用，並且實例具有 `stopped` 狀態。
- `ChooseInstanceStart` ( `aws` : 分支 ) : 根據是否應該啟動實例的分支。
- `StartNotebookInstance` ( `aws:executeAwsApi` ) : 啟動筆記本實例。
- `VerifyNotebookInstanceStatus` ( `aws:waitAwsResourceProperty` ) : `available` 在禁用 `root` 訪問權限之前驗證實例是否處於狀態。
- `VerifyNotebookInstanceRootAccess` ( `aws` : `assertAwsResource` 屬性 ) : 驗證筆記本實例根訪問設置是否成功禁用。

## Secrets Manager

AWS Systems Manager 自動化提供預先定義的 AWS Secrets Manager 手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

## AWSConfigRemediation-DeleteSecret

### Description

AWSConfigRemediation-DeleteSecretrunbook 會刪除一個秘密和儲存在中 AWS Secrets Manager的所有版本。您可以選擇性地指定復原視窗，在此期間您可以還原密碼。如果未指定RecoveryWindowInDays參數值，則作業預設為 30 天。

### [運行此自動化 \( 控制台 \)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- RecoveryWindowInDays

類型：整數

有效值：7-30

預設：30

說明：(選擇性) 您可以還原密碼的天數。

- SecretId

類型：字串

描述：(必填) 您要刪除的密碼的 Amazon 資源名稱 (ARN)。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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參數中指定的密碼。
- aws:executeScript-驗證密碼已排定要刪除。

## AWSConfigRemediation-RotateSecret

### Description

工作AWSConfigRemediation-RotateSecret流程簿會旋轉儲存在中 AWS Secrets Manager的秘  
密。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- RotationInterval

類型：間隔

有效值：1

描述：(必要) 密碼輪換之間的天數。

- RotationLambdaArn

類型：字串

描述：(必填) 可以旋轉秘密的 AWS Lambda 功能的 Amazon 資源名稱 (ARN)。

- SecretId

類型：字串

描述：(必填) 您要旋轉的密碼的 Amazon 資源名稱 (ARN)。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:InvokeFunction
- secretsmanager:DescribeSecret
- secretsmanager:RotateSecret

## 文件步驟

- aws:executeAwsApi-旋轉您在SecretId參數中指定的密碼。

- `aws:executeScript`-驗證秘密已啟用旋轉。

## 安全中樞

AWS Systems Manager 自動化提供預先定義的 AWS Security Hub 手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

### 主題

- [AWSConfigRemediation-EnableSecurityHub](#)

## AWSConfigRemediation-EnableSecurityHub

### Description

AWSConfigRemediation-EnableSecurityHubRunbook 會啟用 AWS Security Hub (Security Hub)，以 AWS 帳戶及您執行自動化的 AWS 區域位置。如需 Security Hub 的相關資訊，請參閱[什麼是 AWS Security Hub?](#) 在《AWS Security Hub 使用者指南》中。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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 指定的預設安全性標準。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- securityhub:DescribeHub
- securityhub:EnableSecurityHub
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

#### 文件步驟

- aws:executeAwsApi-在當前帳戶和區域中啟用安全中心。
- aws:executeAwsApi-驗證 Security Hub 已啟用。

## AWS Shield

AWS Systems Manager 自動化提供預先定義的 AWS Shield手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

#### 主題

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

## AWSPremiumSupport-DDoSResiliencyAssessment

#### Description

該AWSPremiumSupport-DDoSResiliencyAssessment, AWS Systems Manager 自動化 runbook 可以幫助您檢查DDoS漏洞和資源的配置，按照 AWS Shield Advanced 保護您 AWS 帳戶的。它會針對容易受到分散式拒絕服務 (DDoS) 攻擊的資源提供組態設定報告。它可用來收集、分析和評估下列資



源：Amazon Route 53、Amazon 負載平衡器、Amazon CloudFront 分發 AWS Global Accelerator 和 AWS 彈性，根據建議IPs的 AWS Shield Advanced 保護最佳實務來針對其組態設定進行。最終組態報告可在您選擇的 Amazon S3 儲存貯體中以HTML檔案形式提供。

它是如何工作的？

此 Runbook 包含一系列檢查各種類型的已啟用公用存取的資源，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。手冊執行以下操作：

- 檢查是否已啟用 AWS Shield Advanced 的訂閱。
- 如果啟用，它會發現是否有任何神 Shield 進階受保護的資源。
- 它會尋找中的所有全球和區域資源，AWS 帳戶 並檢查這些資源是否受到 Shield 保護。
- 它需要用於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)。
- 它會以存放在 Amazon S3 儲存貯體提供的HTML報告形式傳回發現項目。

輸入參數AssessmentType決定是否對所有資源的檢查將被執行。依預設，runbook 會檢查所有類型的資源。如果只選取GlobalResources或RegionalResources參數，runbook 只會對選取的資源類型執行檢查。

#### Important

- 存取 AWSPremiumSupport-\* Runbook 需要企業或商業 Support 訂閱。如需詳細資訊，請參閱[比較 AWS Support 方案](#)。
- 此手冊需要ACTIVE[AWS Shield Advanced 訂閱](#)。

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

## • AssessmentType

類型：字串

描述：(選擇性) 決定要評估 DDoS 復原能力評估的資源類型。默認情況下，runbook 將評估全球和區域資源。對於區域資源，runbook 描述了所有的應用程式 (ALB) 和網路 (NLB) 負載平衡器，以及您的 / 區域中的所有 Auto Scaling 群組。AWS 帳戶

有效值：['Global Resources', 'Regional Resources', 'Global and Regional Resources']

預設值：全域和區域資源

## • S3 BucketName

類型：AWS::S3::Bucket::Name

說明：(必填) 將上傳報告的 Amazon S3 儲存貯體名稱。

允許的模式：`^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

## • S3 BucketOwnerAccount

類型：字串

說明：(選用) 擁 AWS 帳戶 有 Amazon S3 儲存貯體的儲存貯體。如果 Amazon S3 儲存貯體屬於其他儲存貯體，請指定此參數 AWS 帳戶，否則您可以將此參數保留空白。

允許的模式：`^$|^[0-9]{12,13}$`

## • S3 BucketOwnerRoleArn

類型：AWS::IAM::Role::Arn

說明：(選用) 具有權限的ARNIAM角色，用於描述 Amazon S3 儲存貯體，並在儲存貯體位於不同的情況下 AWS 帳戶 封鎖公用存取組態 AWS 帳戶。如果未指定此參數，runbook 會使用AutomationAssumeRole或啟動此 runbook 的使用IAM者 (如果AutomationAssumeRole未指定)。請參閱 runbook 描述中所需的權限部分。

允許的模式：`^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

類型：字串

說明：(選用) Amazon S3 中用於存放結果的路徑前置詞。

允許的模式：`^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$|^$`

### 必要的IAM權限

此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`

### 自動化假設角色的範例IAM原則

```
{
  "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. 導航到 AWS Systems Manager 控制台 DDoSResiliencyAssessment 中的 [AWSPremiumSupport-](#)。
2. 選擇執行自動化
3. 對於輸入參數，請輸入以下內容：

- AutomationAssumeRole(選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AssessmentType(選擇性)：

決定要評估 DDoS 復原能力評估的資源類型。默認情況下，runbook 評估全球和區域資源。

- S3 BucketName (必要)：

用於以 HTML 格式儲存評估報告的 Amazon S3 儲存貯體名稱。

- S3 BucketOwner (選擇性)：

用於擁有權驗 AWS 帳戶 證的 Amazon S3 儲存貯體識別碼。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相同，則需 AWS 帳戶 要此 ID。

- S3 BucketPrefix (選擇性)：

用於存放結果的 Amazon S3 中路徑的任何前置詞。

**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

**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

**S3BucketName**  
(Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.

Select an existing S3 Bucket

[redacted]
✕

**S3BucketOwner**  
(Required) The Account ID of the Amazon S3 bucket for ownership verification.

[redacted]

**S3BucketPrefix**  
(Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix>

String

#### 4. 選取執行。

#### 5. 自動化啟動。

#### 6. 文件會執行下列步驟：

- CheckShieldAdvancedState:

檢查「S3BucketName」中指定的 Amazon S3 儲存貯體是否允許匿名或公開讀取或寫入存取權限、儲存貯體是否啟用靜態加密，以及「S3BucketOwner」中提供的 AWS 帳戶 ID 是否為 Amazon S3 儲存貯體的擁有者。

- 中三BucketSecurityChecks：

檢查「S3BucketName」中指定的 Amazon S3 儲存貯體是否允許匿名或公開讀取或寫入存取權限、儲存貯體是否啟用靜態加密，以及「S3BucketOwner」中提供的 AWS 帳戶 ID 是否為 Amazon S3 儲存貯體的擁有者。

- BranchOnShieldAdvancedStatus:

分支機會根據 AWS Shield Advanced 訂閱狀態和/或 Amazon S3 儲存貯體擁有權狀態記錄步驟。

- ShieldAdvancedConfigurationReview:

檢閱 Shield 進階組態，以確保最低需要的詳細資料存在。例如：IAM 存取 AWS Shield 回應小組 (SRT) 小組、聯絡人清單詳細資料和 SRT 主動參與狀態。

- ListShieldAdvancedProtections:

列出受保 Shield 的資源，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 受保護的全域資源數量來分支文件步驟。

- ReviewGlobalResources:

查看 Shield 進階受保護的全球資源，例如 Route 53 託管區域、CloudFront 分佈和全球加速器。

- BranchOnResourceType:

根據 [資源] 類型選項 (如果是 [全域]、[區域] 或兩者) 來分支文件步驟。

- ReviewRegionalResources:

檢閱 Shield 進階受保護的區域資源，例如應用程式負載平衡器、網路負載平衡器、傳統負載平衡器、Amazon 彈性運算雲端 (AmazonEC2) 執行個體 (彈性)。IPs

- SendReportTo中三：

將DDoS評估報告詳細資訊上傳到 Amazon S3 儲存貯體。

7. 完成後，Amazon S3 儲存貯體會提供評估報告HTML檔案：URI

S3 控制台鏈接和 Amazon S3，URI用於成功執行手冊的報告

▼ 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-a505-7faefb373ce-2023-06-24\\_04.08.37.html](https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faefb373ce-2023-06-24_04.08.37.html)

SendReportToS3.AssessmentReportS3Uri  
[S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faefb373ce-2023-06-24\\_04.08.37.html](S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faefb373ce-2023-06-24_04.08.37.html)

---

**Execution status**

|                |                    |             |
|----------------|--------------------|-------------|
| Overall status | All executed steps | # Succeeded |
| ✔ Success      | 9                  | 9           |
| # Failed       | # Cancelled        | # TimedOut  |
| 0              | 0                  | 0           |

## 參考

### Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化操作](#)
- [Support 自動化工作流程登陸頁](#)

### AWS 服務文件

- [AWS Shield Advanced](#)



# Amazon SNS

AWS Systems Manager 自動化為 Amazon 簡單通知服務提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)
- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

## AWS-EnableSNSTopicDeliveryStatusLogging

### Description

AWS-EnableSNSTopicDeliveryStatusLogging 執行手冊可設定 Amazon 資料 Firehose HTTP、Lambda 或 Amazon 簡單佇列服務 (Amazon) 端點的交付狀態記錄。Platform application SQS 這使 Amazon 可 SNS 以將失敗的提醒和成功警報通知的樣本百分比記錄到 Amazon CloudWatch。如果已針對主題設定傳遞狀態記錄，runbook 會以您為輸入參數指定的新值取代現有的組態。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- EndpointType

類型：字串

有效值：

- HTTP
- Firehose
- Lambda
- 應用程式
- SQS

說明：( 必填 ) 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

說明：(必填) 您要設定交付狀態記錄ARN的 Amazon SNS 主題。

- SuccessFeedbackRoleArn

類型：字串

描述：( 必填 ) Amazon SNS 用來傳送成功通知訊息日誌ARN的IAM角色 CloudWatch。

- SuccessFeedbackSampleRate

類型：字串

有效值：0 至 100

說明：(必填) 指定 Amazon SNS 主題要取樣的成功訊息百分比。

- FailureFeedbackRoleArn

類型：字串

描述：(必填) Amazon SNS 用來傳送失敗通知訊息日誌ARN的IAM角色 CloudWatch。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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參數值套用至 Amazon SNS 主題。
- `aws:executeAwsApi`-將SuccessFeedbackSampleRate參數值套用至 Amazon SNS 主題。
- `aws:executeAwsApi`-將FailureFeedbackRoleArn參數值套用至 Amazon SNS 主題。
- `aws:executeScript`-確認 Amazon SNS 主題上已啟用交付狀態記錄。

## 輸出

VerifyDeliveryStatusLoggingEnabled。GetTopicAttributesResponse -來自GetTopicAttributesAPI操作的響應。

VerifyDeliveryStatusLoggingEnabled。VerifyDeliveryStatusLoggingEnabled -指出成功驗證傳送狀態記錄的訊息。

# AWSConfigRemediation-EncryptSNSTopic

## Description

AWSConfigRemediation-EncryptSNSTopicRunbook 在您使用 () 客戶受管金鑰指定的 Amazon 簡單通知服務 AWS Key Management Service (Amazon SNS AWS KMS) 主題上啟用加密。此 runbook 僅應用作基準，以確保您的 Amazon SNS 主題根據建議的最低安全性最佳實務進行加密。我們建議您使用不同的客戶管理金鑰來加密多個主題。

## [運行此自動化 \(控制台\)](#)

## 文件類型

## 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- KmsKeyArn

類型：字串

描述：(必填) 您要用來加密 Amazon SNS 主題的 AWS KMS 客戶受管金鑰的 Amazon 資源名稱 (ARN)。

- TopicArn

類型：字串

說明：( 必填 ) 您要加密ARN的 Amazon SNS 主題。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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 Amazon SNS 主題上已啟用加密。

## AWS-PublishSNSNotification

### Description

向 Amazon 發布通知SNS。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 訊息

類型：字串

描述：(必要) 要包含在SNS通知中的訊息。

- `TopicArn`

類型：字串

描述：(必要) 要向ARN其發佈通知的SNS主題。

# Amazon SQS

AWS Systems Manager 自動化為 Amazon 簡單隊列服務 ( AmazonSQS ) 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

## 主題

- [AWS-EnableSQSEncryption](#)

## AWS-EnableSQSEncryption

### Description

R AWS-EnableSQSEncryption unbook 為 Amazon 簡單隊列服務 ( AmazonSQS ) 隊列啟用靜態加密。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原則，其中包含授權可使用佇列之所有主體的權限。啟用加密後，會拒絕匿名SendMessage和對加密佇列的ReceiveMessage要求。

### [運行此自動化 \( 控制台 \)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

Linux 系統macOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- QueueUrl

類型：字串

描述：(必填) 您要在URL其上啟用加密的 Amazon SQS 佇列。

- KmsKeyId

類型：字串

說明：(選擇性) 用於加密的 AWS KMS 金鑰。這個值可以是一個全局唯一的標識符，一個別名或一個鍵，或者一個別名名稱前綴ARN為「alias/」。您也可以通過指定別名 aws/sqs 來使用 AWS 託管密鑰。

- KmsDataKeyReusePeriodSeconds

類型：字串

有效值：

預設：300

說明：(選用) Amazon SQS 佇列可以重複使用資料金鑰加密或解密訊息的時間長度 (以秒為單位)，AWS KMS 然後再次呼叫。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sqs:GetQueueAttributes
- sqs:SetQueueAttributes

## 文件步驟

- SelectKeyType ( aws:branch )：根據指定的密鑰進行分支。
- 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 佇列上已啟用加密功能。
- `VerifySqsEncryptionDefault (aws:assertAwsResourceProperty)`-驗證 Amazon SQS 佇列上已啟用加密功能。

## Step Functions

AWS Systems Manager 自動化提供預先定義的手冊 AWS Step Functions (Step Functions)。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [AWS-EnableStepFunctionsStateMachineLogging](#)

## AWS-EnableStepFunctionsStateMachineLogging

### Description

`AWS-EnableStepFunctionsStateMachineLogging`runbook 會啟用或更新您指定的AWS Step Functions狀態機器上的記錄。最低記錄層級必須設定為ALLERROR、或FATAL。

### [運行此自動化 \(控制台\)](#)

### 文件類型

#### 自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- `AutomationAssumeRole`

類型：字串



說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- Level

類型：字串

有效值：全部 | 錯誤 | 嚴重

說明：(必填) 您要在其上啟用加密之 Amazon SQS 佇列的網址。

- LogGroupArn

類型：字串

描述：(必要) 您要將狀態機器 CloudWatch 日誌傳送到的 Amazon 日誌日誌群組的 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) 決定是否要在記錄檔中包含執行資料。

- TracingConfiguration

類型：布林值

預設：False

說明：(選擇性) 決定是否啟用AWS X-Ray追蹤。

## 必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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`)-驗證已啟用指定狀態機器的記錄。

### 輸出

- `EnableStepFunctionsStateMachineLogging`. 回應-來自 `UpdateStateMachine` API 呼叫的回應。

## Systems Manager

AWS Systems Manager 自動化為 Systems Manager 提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 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-BulkDeleteAssociationrunbook 可以幫助您一次刪除多達 50 個 Systems Manager 器狀態管理器關聯。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AssociationIds

類型: StringList

描述：(必要) 您要刪除IDs的關聯清單，以逗號分隔。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-BulkEditOpsItemsrunbook 可協助您編輯的狀態、嚴重性、類別或優先順序。AWS Systems Manager OpsItems此自動化操作一次最多可編輯 50 OpsItems 個。

## [運行此自動化 \( 控制台 \)](#)

## 文件類型

自動化

## 擁有者

Amazon

## 平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 類別

類型：字串

有效值：

- 可用性
- 費用
- 未變更
- 效能
- 復原
- 安全

預設值：無變更

描述：(選擇性) 您要為編輯的項目指定的新類別 OpsItems。

- OpsItemIds

類型: StringList

描述：(必填) OpsItems IDs 您要編輯的逗號分隔清單 (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

預設值：無變更

描述：(選擇性) 編輯項目相對於系統 OpsItems 中其他 OpsItems 項目的重要性。

- 嚴重性

類型：字串

有效值：

- 未變更
- 1
- 2
- 3
- 4

預設值：無變更

描述：(選擇性) 已編輯項目的嚴重性 OpsItems。

- WaitTimeBetweenEditsInSecs

類型：字串

有效值：0.0-2.0

預設：0.8

描述：(選擇性) 自動化呼叫UpdateOpsItems作業之間等待的時間。

- Status

類型：字串

有效值：

- InProgress
- 未變更
- 開啟
- Resolved (已解決)

預設值：無變更

描述：(選擇性) 已編輯項目的新狀態 OpsItems。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

#### 文件步驟

- aws:executeScript-根據 OpsItems 您為Category、和OpsItemIds參數指定的值編輯您在Status參數Priority中Severity指定的值。

## AWS-BulkResolveOpsItems

### Description

AWS-BulkResolveOpsItemsrunbook 會解析 AWS Systems Manager OpsItems 符合您指定之篩選器的問題。您也可以 OpsItems 使用OpsInsightsId參數指定 OpsItemId 要加入至解析的。如果您為S3BucketName參數指定值，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至 Amazon S3 儲存貯體後接收通知，請指定SnsTopicArn參數值。此自動化操作一次最多可解決 1,000 OpsItems 個問題。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

#### 擁有者

Amazon

#### 平台

LinuxmacOS, Windows

#### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 篩選條件

類型：字串

描述：(必要) 篩選器的鍵值配對，以傳回 OpsItems 您要解決的問題。例如，`[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`。若要深入瞭解可用於篩選 OpsItems 回覆的選項，請參閱〈AWS Systems Manager API 參考〉[OpsItemFilters](#) 中的〈〉。

- OpsInsightId

類型：字串

描述：(選用) 您要新增至已解析的相關資源識別碼 OpsItems。

- S3 BucketName

類型：字串

說明：(選用) 您要將結果摘要傳送至的 Amazon S3 儲存貯體的名稱。

- SnsMessage

類型：字串

說明：(選用) 您希望 Amazon 簡易通知服務 (Amazon SNS) 在自動化完成時傳送的通知。

- SnsTopicArn

類型：字串

說明：(選用) 當結果摘要傳送至 Amazon S3 時，您要通知 ARN 的 Amazon SNS 主題。

## 必要的 IAM 權限

此 AutomationAssumeRole 參數需要執行下列動作，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- OpsItems` 根據您指定的篩選器收集和解析。如果您為 `OpsInsightId` 參數指定了值，則會將該值新增為相關資源。
- `aws:executeScript-`如果您為 `S3BucketName` 參數指定了值，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，則在將結果摘要傳送至 Amazon S3 之後，會傳送通知至 Amazon SNS 主題，包括 `SnsMessage` 參數值 (如果已指定)。

## AWS-ConfigureMaintenanceWindows

### Description

`AWS-ConfigureMaintenanceWindowsrunbook` 可以幫助您啟用或禁用多個 Systems Manager 維護窗口。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- `AutomationAssumeRole`

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- MaintenanceWindows

類型: StringList

描述：(必要) 您要啟用或停用IDs之維護時段的逗號分隔清單。

- MaintenanceWindowsStatus

類型：字串

有效值：「真」|「假」

預設值：「假」

描述：(必要) 決定是否啟用或停用維護時段。指定「True」以啟用維護時段，指定「False」則停用它們。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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

為 Linux 建EC2立針對「Systems Manager 設定的執行個體。

[運行此自動化 \(控制台\)](#)

## 文件類型

### 自動化

### 擁有者

### Amazon

### 平台

### Linux

### 參數

- Amild

類型：字串

說明：(必要) 用來啟動執行個體的 AMI ID。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- GroupName

類型：字串

預設值：SSMSecurityGroupForLinuxInstances

描述：(必要) 要建立的安全群組之名稱。

- HttpTokens

類型：字串

有效值：可選 | 必填

預設值：選擇性

說明：(選擇性) IMDSv2 使用憑證支援的工作階段。將 HTTP 令牌的使用設置為 optional 或 required 以確定 IMDSv2 是可選的還是必需的。

- 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) 建立安全性群組，其連接埠範圍為 SSH (連接埠範圍 22) 開啟至IPs指定的連接埠 CIDR (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

預設值：SSMManagedInstanceProfileRole

描述：(必要) 要建立的角色之名稱。

- StackName

類型：字串

預設值：CreateManagedInstanceStack{{自動化：EXECUTION\_ID}}

描述：(選擇性) 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

說明：(必填) 新執行個體將部署到此 Amazon Virtual Private Cloud (AmazonVPC) 或預設 Amazon (VPC如果未指定)。

## AWS-CreateManagedWindowsInstance

### Description

為 Systems Manager 設定的EC2執行個體建立執行個體。Windows Server

[運行此自動化 \(控制台\)](#)

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}}`

說明：(必要) 用來啟動執行個體的 AMI ID。

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- GroupName

類型：字串

預設值：SSMSecurityGroupForLinuxInstances

描述：(必要) 要建立的安全群組之名稱。

- HttpTokens

類型：字串

有效值：可選 | 必填

預設值：選擇性

說明：(選擇性) IMDSv2 使用憑證支援的工作階段。將 HTTP 令牌的使用設置為 optional 或 required 以確定 IMDSv2 是可選的還是必需的。

- 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) 建立安全性群組，其連接埠範圍 3389 RDP (連接埠範圍 3389) 的開IPs啟狀態 CIDR (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

預設值：SSMManagedInstanceProfileRole

描述：(必要) 要建立的角色之名稱。

- StackName

類型：字串

預設值：CreateManagedInstanceStack{{自動化：EXECUTION\_ID}}

描述：(選擇性) 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

說明：(必填) 新執行個體將部署到此 Amazon Virtual Private Cloud (AmazonVPC) 或預設 Amazon (VPC如果未指定)。

## AWSConfigRemediation-EnableCWLoggingForSessionManager

### Description

AWSConfigRemediation-EnableCWLoggingForSessionManagerRunbook 可讓 AWS Systems Manager 工作階段管理員 (工作階段管理員) 工作階段將輸出日誌存放到 Amazon CloudWatch (CloudWatch) 日誌群組。

## 運行此自動化 (控制台)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DestinationLogGroup

類型：字串

描述：(必要) 記 CloudWatch 錄群組的名稱。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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`-接受記 CloudWatch 錄群組以更新儲存工作階段管理員工作階段輸出記錄偏好設定的文件，或建立一個 (如果不存在)。

# AWS-ExportOpsDataToS3

## Description

此 Runbook 會擷取 AWS Systems Manager 資源管理器中的 OpsData 摘要清單，並將其匯出到指定的 Amazon Simple Storage Service (Amazon S3) 貯體中的物件。

## [運行此自動化 \(控制台\)](#)

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

## 參數

- AutomationAssumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 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：(選擇性) getOpsSummary 請求的篩選器。

- resultAttribute

類型：字串

描述：(選擇性) 要 getOpsSummary 的結果屬性。

- S3 BucketName

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：(可選) 當 runbook 完成時發送的消息。

- snsTopicArn

類型：字串

說明：(必填) 下載完成時要通知的 Amazon 簡單通知服務 (AmazonSNS) 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

getOpsSummary 步驟 — 立即擷取多達 5,000 個操作摘要以匯出到 CSV 檔案中。

## 輸出

OpsData 對象 — 如果 runbook 運行成功，您將在目標 S3 存儲桶中找到導出的 OpsData 對象。

# AWS-ExportPatchReportToS3

## Description

此 Runbook 會在修補程式管理員中擷取修補程式摘要資料和 AWS Systems Manager 修補程式詳細資料清單，並將其匯出到指定 Amazon Simple Storage Service (Amazon S3) 貯體中的 .csv 檔案。

## [運行此自動化 \( 控制台 \)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- assumeRole

類型：字串

描述：(必要) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。ARN 如果未指定角色，Systems Manager 自動化會使用執行此文件之使用者的權限。

- S3 BucketName

類型：字串

說明：(必要) 您要下載輸出檔案的 S3 儲存貯體。

- snsTopicArn

類型：字串

說明：(可選) Amazon 簡單通知服務 (AmazonSNS) 主題 Amazon 資源名稱 (ARN) 下載完成時通知。

- snsSuccessMessage

類型：字串

描述：(選用) 當 Runbook 完成時要傳送的訊息文字。

- targets

類型：字串

說明：(必要) 執行個體 ID 或萬用字元 (\*), 指出要報告特定執行處理或所有執行處理的修補程式資料。

#### 文件步驟

ExportReportStep — 此步驟的動作取決於targets參數值。如果格式為instanceids=\*, 則targets此步驟會針對您帳戶中的執行個體擷取最多 10,000 個修補程式摘要, 並將資料匯出至 .csv 檔案。

如果targets是格式instanceids=<instance-id>, 則此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/修補程式物件 — 如果 runbook 執行成功, 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

建立一或多個受管理執行個體的系統管理員庫存關聯。系統會根據關聯中的排程, 從您的執行個體收集繼資料。如需詳細資訊, 請參閱[AWS Systems Manager 庫存](#)。

### [運行此自動化 \(控制台\)](#)

#### 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, 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

說明：(選擇性) 用來從代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

預設值：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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AwsComponents

類型：字串

預設：Enabled

說明：(選擇性) 收集 AWS 元件的中繼資料，例如 amazon-ssm-agent。

- 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。如需如何收集此類詳細目錄資料的相關資訊，請參閱[使用檔案和 Windows 登錄詳細目錄](#)。需要 SSMAgent 2.2.64.0 版或更新版本。實

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

說明：(選擇性) 收集執行個體的其他相關資訊，包括CPU型號、速度和核心數目，僅舉幾例。

- InstanceIds

類型：字串

預設：\*

摘要：您要庫存的 (必要) EC2 執行環境。

- LambdaAssumeRole

類型：字串

說明：(選用) 允許自動化建立ARN的 Lambda 代表您執行動作的角色。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。

- 輸出 3 BucketName

類型：字串

說明：(選用) 您要在其中寫入庫存日誌資料的 Amazon S3 儲存貯體的名稱。

- 輸出 3 KeyPrefix

類型：字串

說明：(選用) 您要在其中寫入庫存日誌資料的 Amazon S3 key prefix (子資料夾)。

- OutputS3Region

類型：字串

說明：(選擇性) Amazon S3 所在 AWS 區域 位置的名稱。

- 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

說明：(選用，僅限 Windows 作業系統，需要 2.2.64.0 及以上SSMAgent版本) 收集服務設定的資料。

- WindowsRegistry

類型：字串

描述：(選用) 收集 Microsoft Windows 登錄機碼的中繼資料。如需如何收集此類詳細目錄資料的相關資訊，請參閱[使用檔案和 Windows 登錄詳細目錄](#)。需要SSM代理程式版本 2.2.64.0 或更新版本。示例：[{「路徑」：「HKEY CURRENT \_CONFIG\系統」，「遞歸」：真}，{「路

徑」：」 HKEY LOCAL \_ MACHINESOFTWARE\ 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 版或更新版本。

- 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

為 Systems Manager 存取設定具有 AWS Identity and Access Management (IAM) 角色的執行個體。

### [運行此自動化 \(控制台\)](#)

### 文件類型

自動化

### 擁有者

Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole



類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必要) 要設定的 EC2 執行個體 ID

- LambdaAssumeRole

類型：字串

說明：(選用) 允許自動化建立 ARN 的 Lambda 代表您執行動作的角色。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

預設值：SSMRoleForManagedInstance

說明：(選擇性) 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，請確認角色包含受 AmazonSSMManagedInstanceCore 管理的策略。

## AWS-SetupManagedRoleOnEC2Instance

### Description

為系統管理員存取權限設定具有 SSMRoleForManagedInstance 受管 Systems Manager IAM 角色的執行個體。

### [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

## Amazon

### 平台

LinuxmacOS, Windows

### 參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必要) 要設定的 EC2 執行個體 ID

- LambdaAssumeRole

類型：字串

說明：(選用) 允許自動化建立 ARN 的 Lambda 代表您執行動作的角色。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

預設值：SSMRoleForManagedInstance

說明：(選擇性) 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，請確認角色包含受 AmazonSSMManagedInstanceCore 管理的策略。

## AWSsupport-TroubleshootManagedInstance

### Description

AWSsupport-TroubleshootManagedInstance 執行手冊可協助您判斷為何 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體未報告為受 AWS Systems Manager 管理。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) 執行個體設定檔已附加至執行個體。

### Important

此自動化工作流程簿不會評估 IPv6 規則。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定任何角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 未報告為由系統管理員所管理之 Amazon EC2 執行個體的 ID。

必要的 IAM 許可

此AutomationAssumeRole參數需要執行下列動作，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`-收集實例PingStatus的。
- `aws:branch`-根據執行個體是否已報告為由系統管理員管理的分支。
- `aws:executeAwsApi`-收集執行個體的詳細資料，包括 VPC 組態。
- `aws:executeScript`-如果適用，會收集與已部署以搭配 Systems Manager 搭配使用的 VPC 端點相關的其他詳細資料，並確認連接至 VPC 端點的安全群組允許來自執行個體的 TCP 連接埠 443 上的輸入流量。
- `aws:executeScript`-檢查路由表是否允許傳輸至 VPC 端點或公用 Systems Manager 端點的流量。
- `aws:executeScript`-檢查網路 ACL 規則是否允許流量傳送至 VPC 端點或公用 Systems Manager 端點。
- `aws:executeScript`-檢查與執行個體關聯的安全性群組是否允許進入 VPC 端點或公用 Systems Manager 端點的輸出流量。

- `aws:executeScript`-檢查連接至執行個體的執行個體設定檔是否包含提供必要權限的受管理政策。
- `aws:branch`-以執行個體作業系統為基礎的分支。
- `aws:executeScript`-提供`ssmagent-toolkit-linux`殼層指令碼的參考。
- `aws:executeScript`-提供`ssmagent-toolkit-windows` PowerShell 指令碼的參考。
- `aws:executeScript`-生成自動化的最終輸出。
- `aws:executeScript`-如果執行個體是Online，則傳回執行個體已由系統管理員管理。PingStatus

## AWSsupport-TroubleshootPatchManagerLinux

### Description

AWSsupport-TroubleshootPatchManagerLinuxrunbook 可疑難排解使用「修補程式管理員」AWS Systems Manager 功能在 Linux 型受管理節點上造成修補程式失敗的常見問題。這個 runbook 的主要目標是確定修補程式命令失敗根本原因，並建議修復計畫。

它是如何工作的？

AWSsupport-TroubleshootPatchManagerLinuxrunbook 會考慮由您提供的幾個執行個體 ID/ 指令 ID 進行疑難排解。如果未提供 Command ID，它會在提供的執行個體上選取過去 30 天內失敗的最新修補程式命令。檢查命令狀態、必要條件履行和作業系統散發之後，runbook 會下載並執行記錄分析程式套件。輸出包括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 AL2
- 紅帽企業版工作系統 8.X 和 9.X
- CENTOS 8.X 及 9.X

- SUSE15.X

## 參數

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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操作：

1. 導覽至主 AWS Systems Manager 控制台 [AWSSupport-TroubleshootPatchManagerLinux](#) 中的。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：

- InstanceId ( 必填 )：

使用互動式執行個體選擇器選擇修補程式命令失敗的 Linux SSM 受管節點 (Amazon 彈性運算雲端 (AmazonEC2) 或混合啟動伺服器) 的識別碼，或手動輸入SSM受管執行個體的 ID。

- AutomationAssumeRole (選擇性)：

輸入允許「自動化」代表您執行動作ARN的IAM角色。如果未指定角色，自動化會使用啟動此 runbook 之使用者的權限。

- RunCommandId (選擇性)：

輸入AWS-RunPatchBaseline文件的「失敗的執行命令 ID」。如果您未提供命令 ID，runbook 會在選取的執行個體上尋找最近 30 天內失敗的最新修補程式命令。

**Input parameters**  

---

**InstanceId**  
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.  
 Show interactive instance picker

---

**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.

**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.

4. 選取執行。

5. 自動化啟動。

6. 文件會執行下列步驟：

- CheckConcurrency:

確保只有一個執行此 runbook 針對相同的實例。如果 runbook 發現另一個正在進行中針對相同執行個體的執行，它會傳回錯誤並結束。

- ValidateCommand識別碼:

驗證是否為AWS-RunPatchBaselineSSM文檔執行提供的命令 ID (作為輸入參數)。如果未提供指令 ID，runbook 會考慮在選取的執行個體上最近 30 天AWS-RunPatchBaseline內執行失敗的情況。

- BranchOnCommandStatus:

確認所提供指令的狀態為失敗。否則，runbook 結束執行並生成一個報告，指出所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) 發行版本和版本。

- GetDownloadURL:

擷取 PatchManager 記錄分析器套件的下載URL。

- EvaluatePatchManagerLogs:

下載並在執行個體上執行 PatchManager 日誌分析器 python 套件，以評估記錄檔。

- GenerateReport:

生成 runbook 執行的最終報告，其中包括識別的問題和建議的解決方案。

7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

```
▼ 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

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流登陸頁](#)

## AWSsupport-TroubleshootSessionManager

### Description

AWSsupport-TroubleshootSessionManagerRunbook 可協助您疑難排解使用工作階段管理員連線到受管 Amazon 彈性運算雲端 (AmazonEC2) 執行個體的常見問題。工作階段管理員是的功能 AWS Systems Manager。此手冊檢查以下內容：

- 檢查執行個體是否正在執行，並以系統管理員的方式回報。
- 如果AWSsupport-TroubleshootManagedInstance執行個體未報告為由系統管理員管理，則執行 Runbook。



- 檢查執行個體上安裝的SSM代理程式版本。
- 檢查包含工作階段管理員建議 AWS Identity and Access Management (IAM) 政策的執行個體設定檔是否附加至 Amazon EC2 執行個體。
- 從執行個體收集SSM代理程式記錄檔。
- 分析工作階段管理員偏好設定
- 執行 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 Runbook 以分析工作階段管理員、AWS Key Management Service (AWS KMS)、Amazon 簡單儲存服務 (Amazon S3) 和 Amazon CloudWatch 日誌 (CloudWatch 日誌) 的執行個體與端點的連線。

## 考量

- 不支援混合式受管節點。
- 此 runbook 只會檢查建議的受管理IAM策略是否附加至執行個體設定檔。它不會分析IAM或包含在您的執行個體設定檔中的 AWS KMS 權限。

### Important

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2runbook 使用可 [VPCReachability Analyzer](#) 來分析來源和服務端點之間的網路連線。系統會根據來源與目標之間執行的分析收費。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- InstanceId

類型：字串

說明：(必填) 您無法使用工作階段管理員連線到的 Amazon EC2 執行個體 ID。

- SessionPreferenceDocument

類型：字串

預設值：SSM-SessionManagerRunShell

描述:(選擇性) 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權限

此AutomationAssumeRole參數需要執行下列動作，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` : 等待最多 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` : 取得附加至執行個體ARN的執行個體設定檔。
4. `aws:executeAwsApi` : 檢查您的執行個體是否報告為由系統管理員管理。
5. `aws:branch` : 根據您的執行個體是否報告為由系統管理員管理而定的分支。
6. `aws:executeScript` : 檢查執行個體上安裝的SSM代理程式是否支援工作階段管理員。
7. `aws:branch` : 根據您的實例平台收集`ssm-cli`日誌的分支。
8. `aws:runCommand` : 從`ssm-cliLinux`或執行個體`macOS`收集記錄輸出。
9. `aws:runCommand` : 從`ssm-cliWindows`執行個體收集記錄輸出。
10. `aws:executeScript` : 剖析`ssm-cli`記錄檔。
11. `aws:executeScript` : 檢查建議的IAM政策是否已附加至執行個體設定檔。

- 12aws:branch : 決定是否根據ssm-cli記錄檔評估ssmmessages端點連線。
- 13aws:executeAutomation : 評估執行個體是否可以連線到ssmmessages端點。
- 14aws:branch : 決定是否根據ssm-cli日誌和工作階段偏好評估 Amazon S3 端點連線。
- 15aws:executeAutomation : 評估執行個體是否可以連接到 Amazon S3 端點。
- 16aws:branch : 決定是否要根據ssm-cli記錄檔和工作階段偏好設定評估 AWS KMS 端點連線。
- 17aws:executeAutomation : 評估執行個體是否可以連線到 AWS KMS 端點。
- 18aws:branch : 決定是否要根據 CloudWatch 記錄檔和工作階段喜好設定評估 ssm-cli Logs 端點連線。
- 19aws:executeAutomation : 評估執行個體是否可以連線至 CloudWatch Logs 端點。
- 20aws:executeAutomation : 執AWSsupport-TroubleshootManagedInstance行手冊。
- 21aws:executeScript : 編譯先前步驟的輸出並輸出報告。

## 輸出

- generateReport.EvalReport-以純文本執行的 runbook 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。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

## 主題

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

## AWS-CreateJiraIssue

### Description

在 Jira 建立問題。

[運行此自動化 \(控制台\)](#)

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, 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

說明：(選擇性) 問題的到期日 (以 yyyy-mm-dd格式表示)。

- 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)。

- 吉拉 URL

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

說明：(必要) 包含 Jira 使用者API金鑰或密碼的加密SSM參數名稱。

## 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 函數以建立吉拉問題

`aws:deleteStack`-刪除建立的 CloudFormation 堆疊。

## 輸出

Issued：新建立的 Jira 問題的識別碼

# AWS-CreateServiceNowIncident

## Description

在事件資料表中建立 ServiceNow 事件。

[運行此自動化 \(控制台\)](#)

## 文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 類別

類型：字串

描述：(選用) 事件的類別。

有效值：無 | 查詢/幫助 | 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

說明：(必要) 包含 ServiceNow 使用者密碼的加密SSM參數名稱。

- ServiceNowInstanceURL

類型：字串

描述：(必要) ServiceNow 執URL行處理的

- 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 | CPU 作業系統 | 磁碟 | 鍵盤 | 硬體 | 記憶體 | 監視器  
DHCP DNS | 滑鼠 | IP 位址 VPN | 無線 DB2 | MS SQL 伺服器 | Oracle

預設值：無

## 文件步驟

推送事件 — 將事件資訊推送至。 ServiceNow

## 輸出

推送未預期事件識別 — 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封裝程式範本。本手冊使用封隔器 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 公開位址屬性，否則您也必須設 `associate_public_ip_address` 定為 `true`。

## [運行此自動化 \(控制台\)](#)

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssumeRole

類型：字串

描述：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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BuildValidate、和Fix。

- TemplateFileName

類型：字串

描述：S3 儲存貯體中範本檔案的名稱或鍵。

- 範本 3 BucketName

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 — 使用封裝程式工具針對範本執行選取的模式。

## 輸出

RunPackerProcessTemplate.output — 來自「封裝器」工具的標準輸出。

RunPackerProcessTemplate.fixed\_template\_key — 存放在 S3 儲存貯體中的範本名稱，僅在「修正」模式下執行時使用。

RunPackerProcessTemplate.s3\_bucket — S3 儲存貯體的名稱，該儲存貯體包含僅在「修復」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 提供預先定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

## 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 會從您指定的安全性群組中移除所有輸入和輸出規則。

[運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- SecurityGroupId

類型：字串

描述：(必要) 您要關閉的安全性群組識別碼。

必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

文件步驟

- aws:executeScript-從您在參數中指定的安全性群組移除所有輸入和輸出規則。SecurityGroupId

# AWSSupport-ConfigureDNSQueryLogging

## Description

AWSSupport-ConfigureDNSQueryLogging執行手冊會針對來自虛擬私有雲端 (VPC) 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到 Amazon CloudWatch 日誌、Amazon 簡單儲存服務 (Amazon S3) 或亞馬遜資料 Firehose。如需有關查詢記錄和解析器查詢記錄檔的詳細資訊，請參閱[公用DNS查詢記錄](#)和[解析器查詢記錄](#)。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LogDestinationArn

類型：字串

說明：(選用) 您要傳送查詢 CloudWatch 日誌ARN的目標日誌群組、Amazon S3 儲存貯體或 Firehose 串流的資料流。請注意，Route 53 公用DNS查詢記錄僅支援記 CloudWatch 錄檔群組。如果您未指定此參數的值，則自動化操作會建立具有該格式的 CloudWatch 記錄群組 `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID}`，並建立IAM資源策略以發佈查詢記錄。由自動化操作建立的「CloudWatch 記錄」群組的保留期為 14 天。

- QueryLogType

類型：字串

描述：(選擇性) 您要記錄的查詢類型。

有效值：公開 | 解析器/私有

預設值：公開

- ResourceId

類型：字串

描述：( 必填 ) 您要記錄其查詢的資源 ID。如果Public為QueryLogType參數指定，則資源必須是 Route 53 私有主控區域的 ID。如果您Resolver/Private為QueryLogType參數指定，則資源必須是VPC。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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參數指定的資源存在，並檢查資源類型是否符合所需QueryLogType項。
- aws:executeScript-驗證您為LogDestinationArn參數指定的值是否符合所需QueryLogType的值。
- aws:executeScript-驗證 Route 53 將記錄發佈至記錄檔記 CloudWatch 錄群組的必要權限，並建立必要的IAM資源原則 (如果不存在)。



- `aws:executeScript`-啟用所選目的地的DNS查詢記錄。

## AWSSupport-ConfigureTrafficMirroring

### Description

AWSSupport-ConfigureTrafficMirroring執行手冊可設定流量鏡像，以協助您疑難排解負載平衡器和 Amazon 彈性運算雲端 (AmazonEC2) 執行個體之間的連線問題。流量鏡像會複製來自連接至執行個體之網路介面的入站和輸出流量。若要設定流量鏡像，此 Runbook 會建立必要的目標、篩選器和工作階段。依預設，Runbook 會為除 Amazon 以外的所有通訊協定設定所有入站和輸出流量的鏡像。DNS如果您想要鏡像來自特定來源和目的地的流量，可以在自動化完成後修改輸入和輸出規則。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 來源 ENI

類型：字串

描述：(必要) 您要設定流量鏡像的 elastic network interface。

- 目標

類型：字串

描述：(必要) 鏡像流量的目的地。您必須指定網路介面、Network Load Balancer 或閘道 Load Balancer 端點的識別碼。如果您指定 Network Load Balancer，則連接埠 4789 上必須有接UDP聽程式。

- SessionNumber

類型：字串

有效值：

描述：(必要) 您要使用的鏡像工作階段數目。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-執行指令碼以建立目標。
- aws:executeAwsApi-建立篩選規則。
- aws:executeAwsApi-為所有輸入流量建立鏡像篩選規則。
- aws:executeAwsApi-為所有輸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`-如果篩選器或工作階段建立失敗，則刪除篩選器。
- `aws:executeAwsApi`-如果篩選器或工作階段建立失敗，則刪除目標。

## 輸出

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.TargetIDOutput

## AWSsupport-ConnectivityTroubleshooter

### Description

AWSsupport-ConnectivityTroubleshooterRunbook 會診斷下列項目之間的連線問題：

- AWS Amazon Virtual Private Cloud ( AmazonVPC ) 中的資源
- AWS 使用對VPC等連接的相同VPCs AWS 區域 內部不同 Amazon 中的資源
- AWS 使用互聯網閘道的 Amazon VPC 和互聯網資源中的資源
- AWS 使用網絡地址翻譯 ( NAT ) 網關的 Amazon VPC 和互聯網資源中的資源

### [運行此自動化 \( 控制台 \)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 目的地 IP

類型：字串

描述：( 必填 ) 您要連線到的資源IPv4位址。

- DestinationPort

類型：字串

預設：true

描述：(必要) 您要在目的地資源上連線到的連接埠號碼。

- DestinationVpc

類型：字串

預設值：全部

說明：(選用) VPC 您要測試連線的 Amazon ID。

- SourceIP

類型：字串

描述：( 必填 ) 您要測試連線能力的 Amazon VPC 中 AWS 資源的私有IPv4地址。

- SourcePortRange

類型：字串

說明：(選用) 您要測試連線能力的 Amazon 中 AWS 資源VPC使用的連接埠範圍。

- SourceVpc

類型：字串

預設值：全部

說明：(選用) VPC 您要從中測試連線的 Amazon ID。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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-使用從上一步收集的路由確定來自 AWS 資源的網絡流量的目的地。
- aws:branch-基於網絡流量目的地的分支。
- aws:executeAwsApi-收集有關目標資源的詳細資訊。
- aws:executeScript-確認針對目的地 Amazon 傳回的 ID VPC 與DestinationVpc參數中指定的值 (如果有的話) 相符。
- aws:executeAwsApi-收集來源和目標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標資源之間所需的流量。
- aws:executeAwsApi-收集與來源和目標資源之子網NACLs路相關聯的網路存取控制清單 ()。
- aws:executeScript-確認是否NACLs允許來源和目標資源之間的所需流量。
- aws:executeScript-確認來源是否具有與資源關聯的公用 IP 位址 (如果路由目的地為網際網路閘道)。
- 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標資源的所需流量。
- aws:executeAwsApi-收集與來源資源之子網路NACLs相關聯的資訊。
- aws:executeScript-確認是否NACLs允許來自來源資源所需的流量。
- aws:executeAwsApi-收集有關NAT閘道的詳細資料。

- `aws:executeAwsApi`-收集與NAT閘道之子網路NACLs相關聯的資訊。
- `aws:executeScript`-確認是否NACLs允許來自NAT閘道子網路的所需流量。
- `aws:executeScript`-收集與NAT閘道子網路相關聯的路由。
- `aws:executeScript`-確認NAT閘道是否具有通往網際網路閘道的路由。
- `aws:executeAwsApi`-收集有關VPC對等連接的詳細信息。
- `aws:executeScript`-確認兩者VPCs都在相同的區域中，並且為目標傳回的 ID VPC 與DestinationVpc參數中指定的值 (如果有的話) 相符。
- `aws:executeAwsApi`-傳回目標資源的子網路。
- `aws:executeScript`-收集與對等VPC子網路相關聯的路由。
- `aws:executeScript`-確認對等連接是否具VPC有通往對等連接的路由。
- `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-TroubleshootVPNrunbook 可以幫助您跟踪和解決 AWS Site-to-Site VPN 連接中的錯誤。該自動化包括幾個自動化檢查，旨在跟踪IKEv1或與 AWS Site-to-Site VPN 連接通道相關的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的清單。

注意：此自動化操作不能糾正錯誤。它會在上述時間範圍內執行，並掃描記錄群組中的[VPN CloudWatch 記錄檔](#)群組中是否有錯誤。

### 它是如何工作的？

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對應於VPN通道記錄的日誌串流、VPN連線 ID 是否存在，以及是否存在通道 IP 位址。它會在設定用於記錄的記 CloudWatch 錄群組上進行VPN記錄深入分析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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- LogGroupName

類型：字串

說明：(必要) 為 AWS Site-to-Site VPN 連線記錄設定的 Amazon CloudWatch 日誌群組名稱

允許的模式：`^[\\.\-_\/#A-Za-z0-9]{1,512}`

- VpnConnectionId

類型：字串

描述：(必要) 要進行疑難排解的 AWS Site-to-Site VPN 連線 ID。

允許的模式：`^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

類型：字串

描述：(必填) 與您關聯的隧道號碼 1 IPv4 位址 AWS Site-to-Site VPN。

允許的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}$`

- TunnelBIPAddress

類型：字串

描述：(選擇性) 與您關聯的通道號碼 2 IPv4 位址 AWS Site-to-Site VPN。

允許的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

類型：字串

描述：(必填) 選擇您正在使用的IKE版本。允許的值：IKEv1 , IKEv2

有效值：['IKEv1', 'IKEv2']

- StartTimeinEpoch

類型：字串

描述：(選擇性) 記錄檔分析的開始時間。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 進行日誌分析

允許的模式：^\d{10}\$

- EndTimeinEpoch

類型：字串

描述：(選擇性) 記錄檔分析的結束時間。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 進行日誌分析。如果同時給出 StartTimeinEpoch/EndTimeinEpoch LookBackPeriod 然後 LookBackPeriod 優先

允許的模式：^\d{10}\$

- LookBackPeriod

類型：字串

說明：(選擇性) 回頭查看記錄分析的兩位數時間 (以小時為單位)。有效範圍：1-99。如果您還給予 StartTimeinEpoch和，則此值優先 EndTime

允許的模式：^(\d?[1-9]|[1-9]0)\$

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- logs:DescribeLogGroups
- logs:GetQueryResults
- logs:DescribeLogStreams



- logs:StartQuery
- ec2:DescribeVpnConnections

## 指示

附註：當記 CloudWatch 錄輸出格式為時，此自動化作業適用於為VPN通道記錄所設定的記錄群組 JSON。

請依照下列步驟設定自動化操作：

1. 導航到 AWS Systems Manager 控制台VPN中的 [AWSsupport-疑難解答](#)。
2. 對於輸入參數，請輸入以下內容：
  - AutomationAssumeRole (選擇性)：

( ) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
  - LogGroupName ( 必填 )：

要驗證的 Amazon CloudWatch 日誌群組名稱。這必須是設定要將記錄檔傳送VPN至的記錄群組。 CloudWatch
  - VpnConnectionId ( 必填 )：

追蹤其記錄群組是否VPN發生錯誤的 AWS Site-to-Site VPN 連線識別碼。
  - TunnelAIPAddress (必填):

通道與您的 AWS Site-to-Site VPN 連線相關聯的 IP 位址。
  - TunnelBIPAddress (選擇性):

與您的 AWS Site-to-Site VPN 連線相關聯的通道 B IP 位址。
  - IKEVersion ( 必填 )：

選擇IKEversion您正在使用的內容。允許的值：IKEv1、IKEv2。
  - StartTimeinEpoch (選擇性)：

要查詢錯誤的時間範圍的開頭。該範圍包含在內，因此查詢中包含指定的開始時間。指定為紀元時間，即自 1970 年 1 月 1 日 00: UTC 00:00 以來的秒數。
  - EndTimeinEpoch (選擇性)：

查詢錯誤的時間範圍結束時間。範圍包含在內，因此查詢中會包含指定的結束時間。指定為紀元時間，即自 1970 年 1 月 1 日 00: UTC 00:00 以來的秒數。

- LookBackPeriod ( 必填 ) :

回顧查詢錯誤的時間 ( 以小時為單位 ) 。

附註：設定 StartTimeEpoch EndTimeEpoch、或 LookBackPeriod 以修正記錄分析的時間範圍。給一個以小時為單位的兩位數字，以檢查自動化開始時間過去的錯誤。或者，如果錯誤在特定時間範圍內過去，請包含 StartTimeEpoch 和 EndTimeEpoch，而不是 LookBackPeriod。

| Input parameters  |  |
|---|--|
| <b>AutomationAssumeRole</b><br><small>(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.</small><br><input type="text" value="Choose an option"/>               | <b>LogGroupName</b><br><small>(Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs</small><br><input type="text" value="vpnlog"/> |
| <b>VpnConnectionId</b><br><small>(Required) The AWS Site-to-Site VPN connection id to be validated.</small><br><input type="text" value="vpn-123abc456zxc"/>  | <b>Tunnel1IPAddress</b><br><small>(Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated.</small><br><input type="text" value="1.1.1.1"/>                             |
| <b>Tunnel2IPAddress</b><br><small>(Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated.</small><br><input type="text" value="String"/>                     | <b>IKEVersion</b><br><small>(Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both</small><br><input type="text" value="IKEv1"/>  |
| <b>StartTimeEpoch</b><br><small>(Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis</small><br><input type="text" value="String"/> | <b>EndTimeEpoch</b><br><small>(Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis</small><br><input type="text" value="String"/>              |
| <b>LookBackPeriod</b><br><small>(Required) Time in hours to look back for log analysis</small><br><input type="text" value="05"/>   |  |

3. 選取執行。

4. 自動化啟動。

5. 自動化工作流程簿執行下列步驟：

- parameterValidation:

對自動化中包含的輸入參數執行一系列驗證。

- branchOnValidationOfLogGroup:

檢查參數中提到的日誌組是否有效。如果無效，它會停止進一步啟動自動化步驟。

- branchOnValidationOfLogStream:

檢查記錄資料流是否存在於包含的 CloudWatch 記錄群組中。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連接 ID 是否有效。如果無效，它會停止進一步啟動自動化步驟。

- branchOnValidationOfVpnIp:

檢查參數中提到的隧道 IP 地址是否有效。如果無效，那麼它會停止自動化步驟的進一步執行。

- `traceError`:

在包含 CloudWatch 的日誌組中進行日誌洞察API調用，並搜索與IKEv1/IKEv2相關的建議解決方案相關的錯誤。

## 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
{"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-flx-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:
[3] 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.
Step 5: Choose or enter new values for the tunnel options.
Step 6: Choose Save.
}

```

## 參考

## Systems Manager Automation

- [運行此自動化 \(控制台\)](#)
- [執行自動化](#)
- [設定自動化](#)
- [Support 自動化工作流程登陸頁](#)

## AWS 服務文件

- [網站對站台VPN記錄檔的內容](#)

# AWSConfigRemediation-DeleteEgressOnlyInternetGateway

## Description

AWSConfigRemediation-DeleteEgressOnlyInternetGatewayrunbook 會刪除您指定的僅輸出網際網路閘道。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- EgressOnlyInternetGatewayId

類型：字串

說明：(必要) 您要刪除的僅限輸出的網際網路閘道 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

### 文件步驟

- `aws:executeScript`-刪除參數中指定的僅限輸出的`EgressOnlyInternetGatewayId`網際網路閘道。
- `aws:executeScript`-驗證僅限輸出的網際網路閘道已刪除。

## AWSConfigRemediation-DeleteUnusedENI

### Description

AWSConfigRemediation-DeleteUnusedENIRunbook 會刪除具有附件狀態為的 `detached elastic network interface (ENI)`。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `NetworkInterfaceId`

類型：字串

說明：(必要) 您ENI要刪除的 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

### 文件步驟

- `aws:executeAwsApi`-刪除ENI您在NetworkInterfaceId參數中指定的。
- `aws:executeScript`-驗證ENI已刪除。

## AWSConfigRemediation-DeleteUnusedSecurityGroup

### Description

AWSConfigRemediation-DeleteUnusedSecurityGrouprunbook 會刪除您在GroupId參數中指定的安全性群組。如果您嘗試刪除與 Amazon 彈性運算雲端 (AmazonEC2) 執行個體關聯的安全性群組，或被另一個安全群組參考的安全性群組，則自動化會失敗。此自動化操作不會刪除預設安全性群組。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- GroupId

類型：字串

描述：(必要) 您要刪除之安全性群組的識別碼。

## 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，才能成功使用 Runbook。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2>DeleteSecurityGroup

## 文件步驟

- aws:executeAwsApi-使用您在參數中提供的值傳回安全群組名GroupId稱。
- aws:branch-確認群組名稱不是「預設」。
- aws:executeAwsApi-刪除GroupId參數中指定的安全性群組。
- aws:executeScript-確認已刪除安全性群組。

## AWSConfigRemediation-DeleteUnusedVPCNetworkACL

### Description

AWSConfigRemediation-DeleteUnusedVPCNetworkACLrunbook 會刪除未與子網路相關聯的網路存取控制清單 (ACL)。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- NetworkAcId

類型：字串

描述：(必要) 您要刪除ACL的網路 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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ACL指定的網路。



- `aws:executeScript`-確認已刪除`NetworkAclId`參數中ACL指定的網路。

## AWSConfigRemediation-DeleteVPCFlowLog

### Description

AWSConfigRemediation-DeleteVPCFlowLogrunbook 會刪除您指定的虛擬私有雲 (VPC) 流程記錄。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `FlowLogId`

類型：字串

描述：( 必填 ) 您要刪除的流程日誌 ID。

#### 必要的IAM權限

此`AutomationAssumeRole`參數需要執行下列動作，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`參數中指定的流程記錄。
- `aws:executeScript`-驗證流程記錄已刪除。

## AWSConfigRemediation-DetachAndDeleteInternetGateway

### Description

`AWSConfigRemediation-DetachAndDeleteInternetGatewayRunbook` 會分離並刪除您指定的網際網路閘道。如果虛擬私有雲 (VPC) 中的任何 Amazon EC2 執行個體具有彈性 IP 地址或與其相關的公有IPv4地址，則執行手冊會失敗。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- `InternetGatewayId`

類型：字串

說明：(必要) 您要刪除的網際網路閘道 ID。

### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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內容變更為`available`或逾時。
- `aws:executeAwsApi`-擷取指定的虛擬私人閘道組態。
- `aws:branch`-以 `VpcAttachments .state` 參數值為基礎的分支。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID，並等待虛擬私人閘道的 `VpcAttachments .state` 內容變更為`attached`或逾時。
- `aws:executeAwsApi`-接受虛擬私有閘道的 ID 和 Amazon 的 ID VPC 作為輸入，並將虛擬私有閘道從 Amazon VPC 分離。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID，並等待虛擬私人閘道的 `VpcAttachments .state` 內容變更為`detached`或逾時。
- `aws:executeAwsApi`-接受虛擬私有閘道的 ID 作為輸入並將其刪除。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID 作為輸入，並驗證其刪除。
  - `aws:executeAwsApi`-從網際網路閘道 VPC ID 收集 ID。
- `aws:executeAwsApi`-將網際網路閘道 ID 從中分離。VPC

- `aws:executeAwsApi`-刪除網際網路閘道。

## AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

### Description

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGatewayRunbook 會分離並刪除連接到使用 Amazon 虛擬私有雲 (AmazonEC2) 建立的虛擬私有雲端 () 的指定 Amazon 彈性運算雲端 (AmazonVPC) 虛擬私有閘道。VPC

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- VpnGatewayId

類型：字串

描述：(必要) 要刪除之虛擬私有閘道的 ID。

#### 必要的IAM權限

此AutomationAssumeRole參數需要執行下列動作，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內容變更為`available`或逾時。
- `aws:executeAwsApi`-擷取指定的虛擬私人閘道組態。
- `aws:branch`-以 `VpcAttachments .state` 參數值為基礎的分支。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID，並等待虛擬私人閘道的 `VpcAttachments .state` 內容變更為`attached`或逾時。
- `aws:executeAwsApi`-接受虛擬私有閘道的 ID 和 Amazon 的 ID VPC 作為輸入，並將虛擬私有閘道從 Amazon VPC 分離。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID，並等待虛擬私人閘道的 `VpcAttachments .state` 內容變更為`detached`或逾時。
- `aws:executeAwsApi`-接受虛擬私有閘道的 ID 作為輸入並將其刪除。
- `aws:waitForAwsResourceProperty`-接受虛擬私有閘道的 ID 作為輸入，並驗證其刪除。

## AWS-DisableIncomingSSHOnPort22

### Description

AWS-DisableIncomingSSHOnPort22runbook 會移除允許安全性群組TCP連接埠 22 上不受限制傳入SSH流量的規則。

### [運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- SecurityGroupIds

類型：字串

描述：(必要) 您要限制SSH流量IDs的安全性群組清單 (以逗號分隔)。

### 必要的IAM權限

此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參數中指定的安全性群組移除允許TCP連接埠 22 上傳入SSH流量的所有規則。

### 輸出

DisableIncomingSSHTemplate。RestrictedSecurityGroupIds -已移除輸入SSH規則IDs的安全性群組清單。

## AWS-DisablePublicAccessForSecurityGroup

### Description

此 Runbook 禁用默認SSH和打開到所有 IP 地址的RDP端口。

#### Important

此手冊失敗，並顯示「InvalidPermission. NotFound符合下列兩項準則的安全性群組發生 "錯誤：1) 安全性群組位於非預設值中VPC；以及 2) 安全性群組的輸入規則未使用下列四種模式來指定開啟的連接埠：

- 0.0.0.0/0
- ::/0
- SSH or RDP port + 0.0.0.0/0
- SSH or RDP port + ::/0

#### Note

這本手冊在中國境 AWS 區域 內不可用。

### [運行此自動化 \( 控制台 \)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 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

說明：(選擇性) 應封鎖存取的其他 IPv4 位址 (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 公用位址屬性。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- SubnetId

類型：字串

描述：(必要) 您要停用自動指派公用IPv4位址屬性的子網路識別碼。

## 必要的IAM權限

此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用IPv4位址屬性。
- aws:assertAwsResourceProperty-驗證屬性已停用。

# AWSsupport - EnableVPCFlowLogs

## Description

AWSsupport-EnableVPCFlowLogs Runbook 為您的. 中的子網路、網路界面和 VPC 建立 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌。AWS 帳戶如果您為子網路或 VPC 建立流程記錄，則會監控該子網路或 Amazon VPC 中的每個彈性網路界面。流程日誌資料會發佈到您指定的 Amazon CloudWatch 日誌日誌群組或 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**

將 CloudWatch 流程日誌發佈到日誌或 Amazon S3 時，需支付費用日誌的資料擷取和存檔費用。如需詳細資訊，請參閱[流程記錄定價](#)

**運行此自動化 (控制台)****📘 Note**

選取s3做為記錄目的地時，請確定儲存貯體政策允許記錄傳遞服務存取值區。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

說明：(選用) 允許 Systems Manager 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- DeliverLogsPermissionArn

類型：字串

說明：(選用) IAM 角色的 ARN，該角色允許 Amazon Elastic Compute Cloud (Amazon EC2) 將流程日誌發佈到您帳戶中的 CloudWatch 日誌日誌群組。如果您s3為LogDestinationType參數指定，

請勿提供此參數的值。有關詳情，請參閱 Amazon VPC 使用者指南中的[將流程 CloudWatch 日誌發佈到日誌](#)。

- LogDestinationARN

類型：字串

描述：(選擇性) 流程記錄資料發佈至的資源 ARN。如果cloud-watch-logs為LogDestinationType參數指定，請提供您要將流程 CloudWatch 記錄資料發佈至的記錄檔群組的 ARN。或者，請改用 LogGroupName。如果s3為LogDestinationType參數指定，則必須為此參數指定要向其發佈流程日誌資料的 Amazon S3 儲存貯體的 ARN。您也可以在此值區中指定資料夾。

 Important

選擇s3為時，LogDestinationType您應確保所選儲存貯體遵循 [Amazon S3 儲存貯體安全性最佳實務](#)，並遵守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 | 3

描述：(必要) 決定發佈流程記錄資料的位置。如果指定LogDestinationType為s3，請勿指定DeliverLogsPermissionArn或LogGroupName。

- LogFormat

類型：字串

說明：(選用) 要包含在流程記錄中的欄位，以及它們在記錄中的顯示順序。如需可用欄位的清單，請參閱 Amazon VPC 使用者指南中的[流程記錄](#)。如果您未為此參數提供值，則會使用預設格式建立流程記錄。如果您指定此參數，則必須至少指定一個欄位。

- LogGroupName

類型：字串

說明：(選用) 發佈流程 CloudWatch 記錄資料的記錄檔群組名稱。如果您s3為LogDestinationType參數指定，請勿提供此參數的值。

- ResourceIds

類型: StringList

說明 : (必要) 您要為其建立流程記錄的子網路、彈性網路介面或 VPC ID 的逗號分隔清單。

- TrafficType

類型 : 字串

有效值 : 接受 | 拒絕 | 全部

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

此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

## 樣品政策

```
{
  "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) 是否可能授與其物件的讀 `public` 取或寫入存取權限。
- `aws:executeScript`-如果未為參數指定值且已為 `LogDestinationARN` 參數指定，`cloud-watch-logs` 則建立記錄群組。 `LogDestinationType`
- `aws:executeScript`-根據 `runbook` 參數中指定的值建立流程記錄。

## AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

### Description

`AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` 執行手冊將 VPC 流程日誌資料發佈到 Amazon 簡單儲存服務 (Amazon S3) 取代現有的 Amazon 流程日誌，該日誌會將流程日誌資料發佈到您指定的 Amazon CloudWatch 日誌 (日誌) 日誌群組。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DestinationLogGroup

類型：字串

描述：(必填) 您要將流程記 CloudWatch 錄資料發佈到其中的記錄記錄群組名稱。

- DeliverLogsPermissionArn

類型：字串

描述：(必要) 您要使用ARN的 AWS Identity and Access Management (IAM) 角色，該角色為 Amazon 彈性運算雲端 (AmazonEC2) 提供將流程日誌資料發佈到 CloudWatch 日誌的必要許可。

- FlowLogId

類型：字串

說明：(必填) 發佈到您要取代的 Amazon S3 的流程日誌 ID。

- MaxAggregationInterval

類型：整數

有效值：

說明：(選擇性) 擷取封包流程並彙總到流程記錄中的最大時間間隔 (以秒為單位)。

- TrafficType

類型：字串



有效值：ACCEPT| REJECT | ALL

描述：( 必填 ) 您要記錄和發佈的流程記錄資料類型。

### 必要的IAM權限

此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-VPC 從您在FlowLogId參數中指定的值收集有關您的詳細信息。
- aws:executeAwsApi-根據您為 runbook 參數指定的值建立流程記錄。
- aws:assertAwsResourceProperty-驗證新建立的流程記錄發佈至 CloudWatch 記錄。
- aws:executeAwsApi-刪除發佈到 Amazon S3 的流程日誌。
- aws:executeScript-確認已刪除發佈到 Amazon S3 的流程日誌。

## AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

### Description

使用AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket流程日誌取代現有的 Amazon VPC 流程日誌，該日誌將流程日誌資料發佈到 Amazon CloudWatch 日 CloudWatch 誌 (日誌)，該日誌會將流程日誌資料發佈到您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- 目的地 3 BucketArn

類型：字串

說明：(必填) 您要將流程日誌資料發佈到ARN的 Amazon S3 儲存貯體。

- FlowLogId

類型：字串

描述：( 必填 ) 發佈到要取代的 CloudWatch 日誌中的流程日誌 ID。

- MaxAggregationInterval

類型：整數

有效值：

說明：(選擇性) 擷取封包流程並彙總到流程記錄中的最大時間間隔 (以秒為單位)。

- TrafficType

類型：字串

有效值：ACCEPT| REJECT | ALL

描述：( 必填 ) 您要記錄和發佈的流程記錄資料類型。

### 必要的IAM權限

此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-VPC` 從您在 `FlowLogId` 參數中指定的值收集有關您的詳細信息。
- `aws:executeAwsApi`-根據您為 `runbook` 參數指定的值建立流程記錄。
- `aws:assertAwsResourceProperty`-驗證新建立的流程日誌發佈到 Amazon S3。
- `aws:executeAwsApi`-刪除發佈至 CloudWatch 記錄的流程記錄檔。
- `aws:executeScript`-確認已刪除發佈至 CloudWatch 防護記錄的流程記錄。

## AWS-ReleaseElasticIP

### Description

使用分配 ID 釋出指定的彈性 IP 地址。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AllocationId

類型：字串

描述：(必要) 彈性 IP 地址的分配 ID。

## AWS-RemoveNetworkACLUnrestrictedSSHRDP

### Description

AWS-RemoveNetworkACLUnrestrictedSSHRDP runbook 會從指定的網路移除所有網路存取控制清單 (ACL) 規則，ACL 這些規則允許從所有來源位址傳輸到預設值 SSH 和 RDP 連接埠的輸入流量。不會移除包含與預設值 SSH 和 RDP 通訊埠重疊的通訊埠範圍的規則。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- NetworkACLId

類型：字串

描述：(必要) 您要移除不受限制規則ACL的網路 ID，這些規則允許從所有來源位址輸入流量傳輸至預設值SSH和RDP連接埠。

### 必要的IAM權限

此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-移除所有輸入規則，這些規則允許來自您在SecurityGroupId參數中指定的安全性群組中的所有來源位址的流量。

### 輸出

RemoveNaclEntriesAndVerify。 VerificationMessage -成功刪除網路ACL規則的驗證訊息。

RemoveNaclEntriesAndVerify。 RulesDeletedAndApiResponses -已刪除的網路ACL規則，以及作DeleteNetworkAclEntryAPI業回應。

## **AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules**

### Description

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRulesrunbook 會從您指定的安全性群組中移除所有輸入規則，以允許來自所有來源位址的流量。

### [運行此自動化 \( 控制台 \)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- SecurityGroupId

類型：字串

描述：(必要) 您要移除允許來自所有來源位址之流量的輸入規則之安全性群組識別碼。

## 必要的IAM權限

此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-移除所有輸入規則，這些規則允許來自您在SecurityGroupId參數中指定的安全性群組中的所有來源位址的流量。

# AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

## Description

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRulesrunbook 會從您指定的虛擬私人雲端 (VPC) 的預設安全性群組中移除所有規則。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- GroupId

類型：字串

描述：(必要) 您要從中移除所有規則的安全性群組識別碼。

### 必要的IAM權限

此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名為 `default`。
- `aws:executeScript`-從您在`GroupId`參數中指定的安全性群組中移除所有規則。

# AWSSupport-SetupIPMonitoringFromVPC

## Description

AWSSupport-SetupIPMonitoringFromVPC在指定的子網路中建立 Amazon 彈性運算雲端 (AmazonEC2) 執行個體，並透過持續執行 ping、MTR追蹤路徑和 `tracertcp` 測試來監控所選目標 IPs (IPv4或IPv6)。結果會儲存在 Amazon CloudWatch Logs 日誌中，而且會套用指標篩選器，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 日誌數據可用於網絡故障排除和模式/趨勢的分析。此外，當封包遺失和/或延遲達到閾值時，您還可以使用 Amazon SNS 通知設定 CloudWatch 警示。在使用開啟案例時，也可以使用這些資料 AWS Support，以協助快速找出問題，並縮短調查網路問題時的解決時間。

### Note

若要清理所建立的資源AWSSupport-SetupIPMonitoringFromVPC，您可以使用 `runbook AWSSupport-TerminateIPMonitoringFromVPC`。如需詳細資訊，請參閱 [AWSSupport-TerminateIPMonitoringFromVPC](#)。

## 運行此自動化 (控制台)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- CloudWatchLogGroupNamePrefix

類型：字串

預設值：/AWSSupport-SetupIPMonitoringFromVPC

說明：(選擇性) 針對測試結果建立的每個 CloudWatch 記錄群組使用的前置詞。

- CloudWatchLogGroupRetentionInDays

類型：字串

有效值：1 | 3 | 5 | 七

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：微型 | t2. 小 | t2. 中 | t2. 大 | t3. 微 | 微型 | t3. 小 | t3. 大 | 微型 | t4 公克。

預設：t2.micro

說明：(選擇性) EC2 執行處理的執行EC2Rescue個體類型。建議大小：t2.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，則必須確定有網際網路存取權，以允許監視器執行個體設定測試 (也就是說，安裝 CloudWatch 記錄代理程式、與 Systems Manager 互動 以及 CloudWatch)。

- TargetIPs

類型：字串

說明：( 必填 ) 以逗號分隔的IPv4s和/或IPv6s要監控的列表。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。

### 必要的IAM權限

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

建議執行自動化操作的使用者附加 AmazonSSMAutomation Role IAM 受管理的原則。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:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::
        AWS_account_ID
        :role/AWSSupport/SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::
        AWS_account_ID
        :instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```
    },
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudwatch:DeleteDashboards"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ssm:GetParameter",
```

```

        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]
}

```

## 文件步驟

1. **aws:executeAwsApi**-描述提供的子網。

2. **aws:branch**-評估 T argetIPs 輸入。

( IPv6 ) 如果 T argetIPs 包含IPv6 :

**aws:assertAwsResourceProperty**-檢查提供的子網路是否有關聯的IPv6池

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 從參數存儲中獲取最新的 Amazon Linux 2。

5. **aws:executeAwsApi**-為子網路中的測試建立安全群組VPC。

(清除) 如果安全群組建立失敗 :

**aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

6. **aws:executeAwsApi**-允許測試安全性群組中的所有輸出流量。

(清除) 如果安全群組輸出規則建立失敗 :

**aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

7. **aws:executeAwsApi**-為測試EC2實例創建IAM角色

(清除) 如果角色建立失敗 :

a. **aws:executeAwsApi**-刪除由自動化操IAM作建立的角色 (如果存在的話)。

b. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

8. **aws:executeAwsApi**-附加受amazonSSMManagedInstanceCore 管理策略

(清除) 若政策連接失敗：

- a. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的策略與自動化建立的角色中斷連接 (如果附加)。
- b. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- c. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

9. **aws:executeAwsApi**-附加內嵌政策以允許設置 CloudWatch 日誌組保留和創建儀表板  
CloudWatch

(清除) 若內嵌政策連接失敗：

- a. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策 (如果已建立)。
- b. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的策略與自動化建立的角色中斷連結。
- c. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- d. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

10 **aws:executeAwsApi**-建立 IAM 執行個體設定檔。

(清除) 如果執行個體描述檔建立失敗：

- a. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 執行個體設定檔 (如果存在)。
- b. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- c. **aws:executeAwsApi**-從自動化建立的角色中刪除 AmazonSSMManaged InstanceCore 受管理的原則。
- d. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- e. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

11 **aws:executeAwsApi**-將 IAM 執行個體設定檔與 IAM 角色相關聯。

(清除) 如果執行個體描述檔和角色關聯失敗：

- a. **aws:executeAwsApi**-從角色中移除 IAM 執行個體設定檔 (如果有關聯)。
- b. **aws:executeAwsApi**-刪除自動化操作建立的 IAM 執行個體設定檔。
- c. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- d. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的策略與自動化建立的角色中斷連結。
- e. **aws:executeAwsApi**-刪除自動化操作所建立的角色。

f. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

12 **aws:sleep**-等待執行個體設定檔可用。

13 **aws:runInstances**-在指定的子網中創建測試實例，並附加了先前創建的實例配置文件。

(清除) 如果步驟失敗：

a. **aws:changeInstanceState**-終止測試實例。

b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。

c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。

d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。

e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。

f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。

g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

14 **aws:branch**-評估 TargetIPs 輸入。

( IPv6 ) 如果 TargetIPs 包含IPv6：

**aws:executeAwsApi**-將一個IPv6指派給測試執行個體。

15 **aws:waitForAwsResourceProperty**-等待測試執行個體成為代管執行個體。

(清除) 如果步驟失敗：

a. **aws:changeInstanceState**-終止測試實例。

b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。

c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。

d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。

e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。

f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。

g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

16 **aws:runCommand**-安裝測試先決條件：

(清除) 如果步驟失敗：

a. **aws:changeInstanceState**-終止測試實例。

b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。

- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

17 **aws:runCommand**-驗證提供的語法IPs正確IPv4和/或IPv6地址：

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

18 **aws:runCommand**-為每個提供的定義MTR測試IPs。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

19 **aws:runCommand**-為每個提供的定義第一個 ping 測試IPs。

(清除) 如果步驟失敗：

17 **aws:runCommand**-驗證提供的語法IPs正確IPv4和/或IPv6地址：

(清除) 如果步驟失敗：

18 **aws:runCommand**-為每個提供的定義MTR測試IPs。

(清除) 如果步驟失敗：

19 **aws:runCommand**-為每個提供的定義第一個 ping 測試IPs。

- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

20 **aws:runCommand**-為每個提供的定義第二個 ping 測試IPs。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

21 **aws:runCommand**-為每個提供的定義追蹤路徑測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

22 **aws:runCommand**-為每個提供的定義追蹤路由測試。IPs



- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

23 **aws:runCommand**-配置 CloudWatch 日誌。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

24 **aws:runCommand**-安排 cronjobs 以每分鐘運行每個測試。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

25 **aws:sleep**-等待測試生成一些數據。

26 **aws:runCommand**-設定所需的 CloudWatch 記錄群組保留。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

27 **aws:runCommand**-設定記 CloudWatch 錄群組指標篩選器。

(清除) 如果步驟失敗：

- a. **aws:changeInstanceState**-終止測試實例。
- b. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- c. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- d. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- e. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- f. **aws:executeAwsApi**-刪除自動化操作所建立的角色。
- g. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

28 **aws:runCommand**-創建 CloudWatch 儀表板。

(清除) 如果步驟失敗：

- a. **aws:executeAwsApi**-刪除 CloudWatch 儀表板 (如果存在)。
- b. **aws:changeInstanceState**-終止測試實例。
- c. **aws:executeAwsApi**-從角色中移除IAM執行個體設定檔。
- d. **aws:executeAwsApi**-刪除自動化操作建立的IAM執行個體設定檔。
- e. **aws:executeAwsApi**-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
- f. **aws:executeAwsApi**-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
- g. **aws:executeAwsApi**-刪除自動化操作所建立的角色。

h. `aws:executeAwsApi`-刪除由自動化建立的安全性群組 (如果存在)。

## 輸出

`createCloudWatch儀表板`. 輸出-儀表板的URL。 CloudWatch

`createManagedInstance`. `InstanceIds` -測試實例 ID。

## AWSSupport-TerminateIPMonitoringFromVPC

### Description

AWSSupport-TerminateIPMonitoringFromVPC終止先前啟動的 IP 監視測試。AWSSupport-SetupIPMonitoringFromVPC與指定測試 ID 相關的資料都會刪除。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AutomationExecutionId

類型：字串

描述：(必要) 您先前執行 `AWSSupport-SetupIPMonitoringFromVPC` runbook 時的自動化執行識別碼。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權限

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

建議執行自動化操作的使用者附加 AmazonSSMAutomation Role IAM 受管理的原則。此外，使用者必須將下列原則附加至其使用者、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` 並與 `InstanceId` 相同的測試相關。
2. `aws:assertAwsResourceProperty`-檢查 `SubnetId` 並與 `InstanceId` 相同的測試相關。
3. `aws:executeAwsApi`-擷取測試安全性群組。
4. `aws:executeAwsApi`-刪除 CloudWatch 儀表板。
5. `aws:changeInstanceState`-終止測試實例。
6. `aws:executeAwsApi`-從角色中移除IAM執行個體設定檔。

7. `aws:executeAwsApi`-刪除自動化操作建立的IAM執行個體設定檔。
8. `aws:executeAwsApi`-從自動化操作建立的角色中刪除 CloudWatch 內嵌政策。
9. `aws:executeAwsApi`-將 AmazonSSMManaged InstanceCore 受管理的政策與自動化建立的角色中斷連結。
10. `aws:executeAwsApi`-刪除自動化操作所建立的角色。
11. `aws:executeAwsApi`-刪除由自動化建立的安全性群組 (如果存在)。

## 輸出

無

## AWS WAF

AWS Systems Manager 自動化提供預先定義的 AWS WAF 手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱 [檢視工作手冊內容](#)。

## 主題

- [AWS-AddWAFRegionalRuleToRuleGroup](#)
- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

## AWS-AddWAFRegionalRuleToRuleGroup

### Description

`AWS-AddWAFRegionalRuleToRuleGroup` runbook 將現有的 AWS WAF 地區規則新增至 AWS WAF 地區規則群組。僅支援 AWS WAF 傳統地區規則群組。AWS WAF 傳統區域規則群組最多可以有 10 個規則。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- RuleGroupId

類型：字串

描述：(必要) 您要更新之規則群組的識別碼。

- RulePriority

類型：整數

描述：(必要) 新規則的優先順序。規則優先順序決定區域群組中規則的評估順序。值較低的規則的優先順序高於具有較高值的規則。值必須是唯一的整數。如果您將多個規則新增至地區規則群組，則這些值不一定是連續的。

- RuleId

類型：字串

描述：(必要) 您要新增至地區規則群組之規則的 ID。

- RuleAction

類型：字串

描述：(必要) 指定當 Web 要求符合規則條件時所 AWS WAF 採取的動作。

有效值：ALLOW | BLOCK | COUNT

## 必要的IAM權限

此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

- `GetWAFChange` 令牌 ( `aws:executeAwsApi` ) -檢索 AWS WAF 更改令牌以確保 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` ) -驗證更改令牌的狀態為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` -驗證新規則是否已連接至區域規則群組的步驟輸出。
- `VerifyRuleAddedToRuleGroup`。 `ListActivatedRulesInRuleGroupResponse` -`ListActivatedRulesInRuleGroup` API 操作的輸出。

# AWS-AddWAFRegionalRuleToWebACL

## Description

`AWS-AddWAFRegionalRuleToWebACL`runbook 會將現有的 AWS WAF 地區規則、規則群組或速率型規則新增至 AWS WAF 傳統區域網路存取控制清單 ( ) ACL。此 runbook 不會更新由 AWS Firewall Manager管理ACL的現有 AWS WAF 經典區域網路。



## 運行此自動化 ( 控制台 )

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- WebACLId

類型：字串

說明：(必要) 您要更新 ACL 之網站的 ID。

- ActivatedRulePriority

類型：整數

描述：(必要) 新規則的優先順序。規則優先順序決定評估 Web 中規則 ACL 的順序。值較低的規則的優先順序高於具有較高值的規則。值必須是唯一的整數。如果您將多個規則新增至地區網站 ACL，則值不一定是連續的。

- ActivatedRuleRuleId

類型：字串

描述：(必要) 您要新增至 Web ACL 的一般規則、以速率為基礎的規則或群組的 ID。

- ActivatedRuleAction

類型：字串

有效值：ALLOW| BLOCK | COUNT

描述：(選擇性) 指定當 Web AWS WAF 要求符合規則條件時所採取的動作。

- ActivatedRuleType

類型：字串

有效值：REGULAR| RATE \_ BASED | GROUP

預設值：REGULAR

說明：(選擇性) 您要新增至網路的規則類型ACL。雖然此欄位為選擇性欄位，但請注意，如果您嘗試在未設定類型的ACL情況下將RATE\_BASED規則新增至 Web，則要求會失敗，因為要求預設為REGULAR規則。

## 必要的IAM權限

此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 ( awsexecuteScript:)-驗證 AWS WAF Web ACL 是否在 Firewall Manager 器安全策略中，並驗證優先級 ID 與現有 ID 不衝突。ACL
- AddRuleOrRuleGroupToWebACL ( aws:executeScript ) -將指定的規則添加到 AWS WAF 網絡 ACL。
- VerifyRuleOrRuleGroupAddedToWebAcl ( aws:executeScript ) -驗證指定的 AWS WAF 規則已添加到目標網站ACL。

## 輸出

- DetermineWebACLNotInFMSAndRulePriority。 PrereqResponse : 從DetermineWebACLNotInFMSAndRulePriority步驟輸出。
- VerifyRuleOrRuleGroupAddedToWebAcl。 VerifyRuleOrRuleGroupAddedToWebACLResponse : 從AddRuleOrRuleGroupToWebACL步驟輸出。
- VerifyRuleOrRuleGroupAddedToWebAcl。  
ListActivatedRulesOrRuleGroupsInWebACLResponse : VerifyRuleOrRuleGroupAddedToWebAcl步驟的輸出。

## AWSConfigRemediation-EnableWAFClassicLogging

### Description

AWSConfigRemediation-EnableWAFClassicLogging執行手冊可讓您針對您指定的 AWS WAF 網路存取控制清單 (網路) 記錄到 Amazon 資料防火軟管 (FirehoseACL)。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- DeliveryStreamName

類型：字串

描述：(必要) 您要傳送記錄檔的 Firehose 傳送串流名稱。

- WebACLIId

類型：字串

說明：(必要) 您要啟用登入的 AWS WAF 網路 ACL ID。

### 必要的IAM權限

此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DeliveryStreamName在存在中指定的傳送串流。
- aws:executeAwsApi-收集WebACLIId參ARN數中ACL指定的 AWS WAF Web。
- aws:executeAwsApi-啟用 Web 的日誌記錄ACL。
- aws:assertAwsResourceProperty-驗證日誌記錄已在 AWS WAF 網路ACL上啟用。

## AWSConfigRemediation-EnableWAFClassicRegionalLogging

### Description

AWSConfigRemediation-EnableWAFClassicRegionalLogging執行手冊可讓您針對您指定的 AWS WAF 網路存取控制清單 () 記錄到 Amazon 資料防火管 (FirehoseACL)。

[運行此自動化 \(控制台\)](#)

## 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 (ARN)。

- LogDestinationConfigs

類型：字串

描述：(必填) 您要傳送日誌的 Firehose 交付串流的 Amazon 資源名稱 (ARN)。

- WebACLId

類型：字串

說明：(必要) 您要啟用登入的 AWS WAF 網路 ACL ID。

### 必要的IAM權限

此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ARN數中ACL指定的 AWS WAF Web。
- `aws:executeAwsApi`-啟用 Web 的日誌記錄ACL。
- `aws:assertAwsResourceProperty`-驗證日誌記錄已在 AWS WAF 網絡ACL上啟用。

## AWSConfigRemediation-EnableWAFV2Logging

### Description

AWSConfigRemediation-EnableWAFV2Logging執行手冊使用指定的 Amazon 資料火管 AWS WAF (Firehose) 交付串流，為 (AWS WAF V2ACL) Web 存取控制清單 (網路) 啟用記錄功能。

### [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- LogDestinationConfigs

類型：字串

描述：(必要) 您要與網路ACL產生關聯ARN的 Firehose 傳送串流。

**Note**

Firehose 傳送串流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 資料 Firehose](#)。

- WebAclArn

類型：字串

描述：將啟用記錄ARNACL的 Web 的 ( 必要 )。

### 必要的IAM權限

此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 的記錄功能，ACL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 提供預定義的手冊。如需有關工作手冊的詳細資訊，請參閱[使用手冊](#)。若要取得有關如何檢視 runbook 內容的資訊，請參閱〈[檢視工作手冊內容](#)〉。

### 主題

- [AWS-CreateWorkspace](#)

- [AWSsupport-RecoverWorkSpace](#)

## AWS-CreateWorkSpace

### Description

AWS-CreateWorkSpacerunbook 會根據您為輸入參數指定的值 WorkSpace，建立新的 Amazon WorkSpaces 虛擬桌面 (稱為 a)。有關詳細信息 WorkSpaces，請參閱[什麼是 Amazon WorkSpaces?](#) 在 Amazon WorkSpaces 管理指南。

### [運行此自動化 \(控制台\)](#)

#### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- BundleId

類型：字串

描述：(必要) 要用於的套裝軟體 ID WorkSpace。

- ComputeTypeName

類型：字串



有效值：VALUESTANDARD| PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

說明：(選用) 您的 Workspace。

- DirectoryId

類型：字串

描述：(必填) 要添加到的目錄的 ID。 Workspace

- RootVolumeEncryptionEnabled

類型：布林值

有效值：true | false

預設：false

說明：(選擇性) 決定 Workspace 是否加密的根磁碟區。

- RootVolumeSizeGib

類型：整數

描述：(必要) 根磁碟區的大小 Workspace。

- RunningMode

類型：字串

有效值：ALWAYS\_開 | AUTO \_ STOP

描述：(必要) 的執行模式 Workspace。

- RunningModeAutoStopTimeoutInMinutes

類型：整數

說明：(選擇性) 使用者登出後 WorkSpaces停止的時間。以 60 分鐘的間隔指定一個值。

- 標籤

類型：字串

說明：(選擇性) 您要套用至的標籤 Workspace。

- **UserName**

類型：字串

描述：(必要) 要與之關聯的使用者名稱 Workspace。

- **UserVolumeEncryptionEnabled**

類型：布林值

有效值：true | false

預設：false

說明：(選擇性) 決定的使用者磁碟區 Workspace 是否已加密。

- **UserVolumeSizeGib**

類型：整數

描述：(必要) 的使用者磁碟區大小 Workspace。

- **VolumeEncryptionKey**

類型：字串

說明：(選用) 您 AWS Key Management Service 要用來加密儲存 Workspace 在。

### 必要的IAM權限

此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 Workspace 據您為輸入參數指定的值建立。
- `aws:waitForAwsResourceProperty`-驗證是的狀態。 Workspace AVAILABLE

### 輸出

CreateWorkspace.WorkspaceId

## AWSsupport-RecoverWorkSpace

### Description

AWSsupport-RecoverWorkSpaceRunbook 會在 Amazon WorkSpaces 虛擬桌面上執行復原步驟，也就是 WorkSpace 您指定的。runbook 會重新啟動 WorkSpace，如果狀態仍然存在 UNHEALTHY，則會 WorkSpace 根據您為輸入參數指定的值還原或重建。在使用本 runbook 之前，我們建議您查看 Amazon WorkSpaces 管理指南中的 [疑難排解 WorkSpaces 問題](#)。

#### Important

還原或重建 WorkSpace 是一種潛在的破壞性動作，可能會導致資料遺失。這是因為會從最後一個可用的快照還原，而從快照復原的資料最久可達 12 小時。WorkSpace 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 WorkSpace 從與建立的套裝軟體相關聯的影像重新建立 WorkSpace 磁碟區。安裝的應用程式或在建立之後變更的 WorkSpace 系統設定都會遺失。如需有關還原和重建的詳細資訊 WorkSpaces，請參閱 Amazon WorkSpaces 管理指南 WorkSpace 中的 [還原 WorkSpace](#) 和 [重建 a](#)。

### [運行此自動化 \(控制台\)](#)

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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN 如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- 確認

類型：字串

有效值：是

描述：(必要) 輸入 yes 表示您瞭解還原與重建動作會嘗試 Workspace 從最近的快照復原，而且從這些快照還原的資料可能是 12 小時。

- 重新開機

類型：字串

有效值：是 | 否

預設值：是

描述：(必要) 決定 Workspace 是否重新啟動。

- 重建

類型：字串

有效值：是 | 否

預設值：否

描述：(必要) 決定 Workspace 是否重新建立。

- 還原

類型：字串

有效值：是 | 否

預設值：否

描述：(必要) 決定 Workspace 是否要還原。

- `WorkspaceId`

類型：字串

說明：(必要) `WorkSpace` 您要復原的 ID。

### 必要的IAM權限

此`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 `WorkSpace` 定的狀態。
- `aws:assertAwsResourceProperty`-驗證 `WorkSpace` 是`AVAILABLE`、`ERRORIMPAIRED`、`STOPPED`或`UNHEALTHY`的狀態。
- `aws:branch`-基於狀態的分支 `WorkSpace`。
- `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`-等待狀 `WorkSpace` 態變更為`AVAILABLE`、`ERRORIMPAIRED`、或啟動`UNHEALTHY`後。
- `aws:executeAwsApi`-收集啟動 `WorkSpace` 後的狀態。
- `aws:branch`-基於啟動 `WorkSpace` 後狀態的分支。
- `aws:executeAwsApi`-收集可用的快照以還原或重建。 `WorkSpace`
- `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`-收集啟動 `WorkSpace` 後的狀態。
- `aws:waitForAwsResourceProperty`-等待的狀態變更 `WorkSpace` 為 `REBOOTING`。
- `aws:waitForAwsResourceProperty`-等待 `WorkSpace` 狀態變更為 `AVAILABLEERROR`、或重新啟動 `UNHEALTHY` 後。
- `aws:executeAwsApi`-重新啟動 `WorkSpace` 後收集的狀態。
- `aws:branch`-基於重新啟動 `WorkSpace` 後狀態的分支。
- `aws:branch`-根據您為 `Restore` 參數指定的值進行分支。
- `aws:executeAwsApi`-恢復 `WorkSpace`。如果還原失敗，執行本會嘗試重建 `WorkSpace`
- `aws:waitForAwsResourceProperty`-等待的狀態變更 `WorkSpace` 為 `RESTORING`。
- `aws:waitForAwsResourceProperty`-等待狀 `WorkSpace` 態變更為 `AVAILABLEERROR`、或恢復 `UNHEALTHY` 之後。
- `aws:executeAwsApi`-收集恢復 `WorkSpace` 後的狀態。
- `aws:branch`-基於恢復 `WorkSpace` 後狀態的分支。
- `aws:branch`-根據您為 `Rebuild` 參數指定的值進行分支。
- `aws:executeAwsApi`-重建 `WorkSpace`
- `aws:waitForAwsResourceProperty`-等待的狀態變更 `WorkSpace` 為 `REBUILDING`。
- `aws:waitForAwsResourceProperty`-等待狀 `WorkSpace` 態變更為 `AVAILABLEERROR`、或重建 `UNHEALTHY` 之後。
- `aws:executeAwsApi`-收集重建 `WorkSpace` 後的狀態。
- `aws:assertAwsResourceProperty`-確認是的狀態 `WorkSpace` 態 `AVAILABLE`。

## X-Ray

AWS Systems Manager 自動化提供預先定義的 AWS X-Ray 手冊。如需有關工作手冊的詳細資訊，請參閱 [使用手冊](#)。若要取得有關如何檢視 `runbook` 內容的資訊，請參閱 [〈〉 檢視工作手冊內容](#)。

### 主題

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

# AWSConfigRemediation-UpdateXRayKMSKey

## Description

AWSConfigRemediation-UpdateXRayKMSKeyRunbook 使用 AWS Key Management Service (AWS KMS) 密鑰啟用對您的 AWS X-Ray 數據進行加密。此 runbook 應該只用作基準，以確保您的 AWS X-Ray 資料根據建議的最低安全性最佳做法加密。我們建議您使用不同的KMS金鑰加密多組資料。

## [運行此自動化 \(控制台\)](#)

### 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 自動化代表您執行動作的 AWS Identity and Access Management (IAM) 角色的 Amazon 資源名稱 ()。ARN

- KeyId

類型：字串

描述：(必填) Amazon 資源名稱 (ARN)、金鑰 ID 或您要用 AWS X-Ray 來加密資料之KMS金鑰的金鑰別名。

### 必要的IAM權限

此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`-使用您在參數中指定的密KMS鑰對 X-Ray KeyId 數據啟用加密。
- `aws:waitForAwsResourceProperty`-等待 X-Ray 的加密配置狀態。ACTIVE
- `aws:executeAwsApi`-收集您在KeyId參數中指定ARN的金鑰。
- `aws:assertAwsResourceProperty`-驗證 X-Ray 上已啟用加密功能。



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。