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

Table of Contents

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**
>
> 如果您執行可使用 AWS Identity and Access Management (IAM) 服務角色叫用其他服務的自動化工作流程，請注意您必須為該服務角色設定可叫用這些服務的許可。此要求適用於所有 AWS Automation Runbook (`AWS-*` Runbook)，例如 `AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup` 和 `AWS-RestartEC2Instance` Runbook 等。此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 內嵌政策新增至角色，以啟用其他 AWS 服務的許可。如需詳細資訊，請參閱新增自動化內嵌原則以叫用其他 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。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

- 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
- 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. 請在以下位置開啟 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 Gateway

AWS Systems Manager 自動化為 Amazon API Gateway 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

- 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-TroubleshootAWSBatchJobrunbook 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。
- 如果任務需要的 vCPUs 或記憶體資源數量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 GPU 執行個體上執行，但運算環境未設定為使用 GPU 型執行個體。
- 如果運算環境的 Auto Scaling 群組無法啟動執行個體。
- 如果啟動的執行個體可以加入基礎 Amazon Elastic Container Service (Amazon ECS) 叢集；如果沒有，它會執行 AWSSupport-疑難排解ContainerInstance操作手冊。
- 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.

- 此執行手冊可針對AWS Batch在 Amazon ECS AWS Fargate 或亞馬遜彈性運算雲端 (Amazon EC2) 執行個體上排定的任務啟動。如果在 Amazon 彈性 Kubernetes 服務 (亞馬遜 EKS) 上啟動任務的自動化，則啟動將停止。AWS Batch
- 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。有關更多信息，請參考 AWSSupport-疑難解答操作手ContainerInstance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

  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。

- 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 許可

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

- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeScalingActivities
- batch:DescribeComputeEnvironments
- batch:DescribeJobs
- batch:DescribeJobQueues
- batch:ListJobs
- cloudtrail:LookupEvents
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSpotFleetInstances
- ec2:DescribeSpotFleetRequests
- ec2:DescribeSpotFleetRequestHistory
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ecs:DescribeClusters
- ecs:DescribeContainerInstances
- ecs:ListContainerInstances
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy

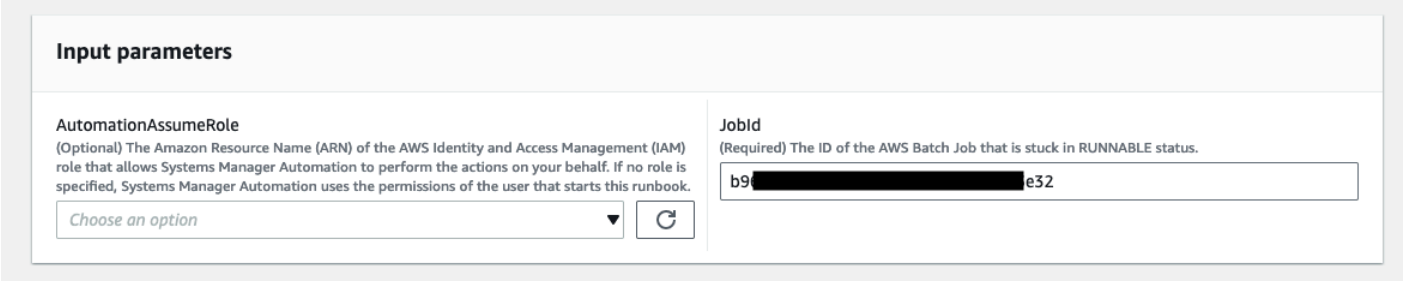
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sts:GetCallerIdentity

指示

1. 導航到AWS Systems Manager控制台AWSBatchJob中的 AWSSupport-疑難解答。
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)：

     (IAM) 角色的 Amazon 資源名稱 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。
   - JobId （必填）：

     停留在RUNNABLE狀態中的 AWS Batch Job ID。



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：

  根據計算環境檢查是否成功進行分支。

- UnderlyingInfraEvaluation:

  對基礎 Auto Scaling 群組或競價型叢集請求執行檢查。

- ProceedOnlyIfInstancesNotJoiningEcs叢集：

  根據是否有執行個體未加入 Amazon ECS 叢集進行分支。

- EcsAutomationRunner:

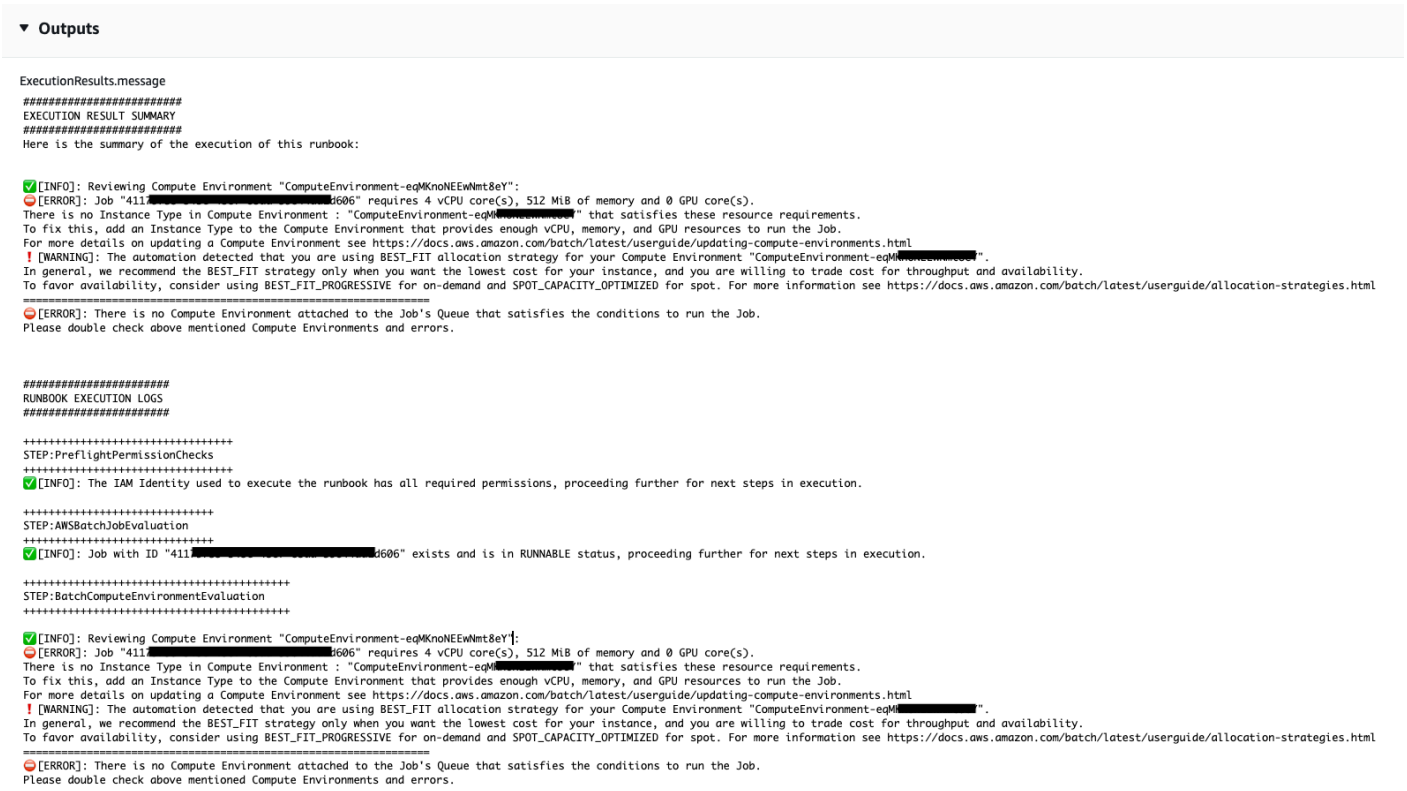
  針對未加入叢集的執行個體執行 Amazon ECS 自動化。

- ExecutionResults:

  根據先前的步驟產生輸出。

7. 完成後，會提供評估報告 HTML 檔案的 URI：

   S3 主控台連結和 Amazon S3 URI，用於成功執行工作手冊的報告



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

AWS-EnableCloudFormationSNSNotificationRunbook 為您指定的 () 堆疊啟用亞馬遜簡單通知服務 AWS CloudFormation (Amazon SNS 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 系統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。
- StackArn

  類型：字串

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

  類型：字串

  說明：(必要) 您要與 AWS CloudFormation 堆疊產生關聯的 Amazon SNS 主題的 ARN。

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

文件步驟

- CheckCfnSnsLimits (AWS：執行腳本)-驗證尚未與您指定的堆疊產生關聯的 Amazon SNS 主題數目上限。 AWS CloudFormation
- EnableCfnSnsNotification (aws:executeAwsApi)-為 AWS CloudFormation 堆疊啟用 Amazon SNS 通知。
- VerificationCfnSnsNotification (AWS：執行指令碼)-確認已為堆疊啟用 Amazon SNS 通知。 AWS CloudFormation

輸出

CheckCfnSnsLimits。 NotificationArnList -接收 AWS CloudFormation 堆疊之 Amazon SNS 通知的 ARN 清單。

VerificationCfnSnsNotification。 VerifySnsTopicsResponse -來自 API 作業的回應，確認已針對 AWS CloudFormation 堆疊啟用 Amazon SNS 通知。

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`runbook 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

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。
- LambdaAssume角色

  類型：字串

  描述：(必要) Lambda 所承擔之角色的 ARN
- 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/DOC-EXAMPLE-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:GetBucketLocation`API 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)。
- 公里 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。
- 公里 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

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 許可

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

- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

文件步驟

- `aws:executeScript`-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

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

  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 | 門 LessThanLowerOrGreaterThanUpper檻 | | 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。

必要的 IAM 許可

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

  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 ClusterResourceId

  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：毫米，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 返回 Amazon DocumentDB 集群標識符。
- VerifyDocDbEngine （aws：assertAwsResource屬性）-驗證 Amazon DocumentDB 引擎類型是docdb為了防止意外更改其他 Amazon RDS 引擎類型。
- VerifyDocDbStatus （AWS：waitAwsResource屬性）-驗證 Amazon DocumentDB 集群狀態為。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：執行指令碼)-驗證 Amazon 文件資料庫叢集的保留期間，以及偏好的備份時段 (如果指定) 已成功設定。

輸出

ModifyDocDbRetentionPeriod。 ModifyDbClusterResponse -來自 ModifyDBCluster API 作業的回應。

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)。
- 公里 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-DeleteAccessKeysFromCodeBuildProjectrunbook 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
- 客戶管理的生命週期事件掛接
- 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-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 CSV 檔案，其中包含無法在時間限制內關聯的所有電話號碼和聯絡流程配對，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的 CSV 檔案，將電話號碼與 Amazon Connect 執行個體中的聯絡流程相關聯。輸入的 CSV 檔案應與下列格式對齊，其PhoneNumber值為 E.164 格式。

輸入 CSV 檔案的範例

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

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

- **automation:EXECUTION_ID/ResourceIdList.csv**：包含AssociatePhoneNumberContactFlow API 所需的PhoneNumberId和ContactFlowId配對的臨時文件。
- **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/連絡人流程無法由於時間限制而處理，runbook 將它們包含在 CSV 檔中，以作為下一個 runbook 執行的輸入。

文件類型

自動化

擁有者

Amazon

平台

Linux,macOS, Windows

參數

必要的 IAM 許可

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[AWSSupport-AssociatePhoneNumbersToConnectContactFlows]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)

(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。

- 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)

  CSV 檔案的 Amazon S3 物件金鑰，其中包含電話號碼和聯絡流程配對。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)

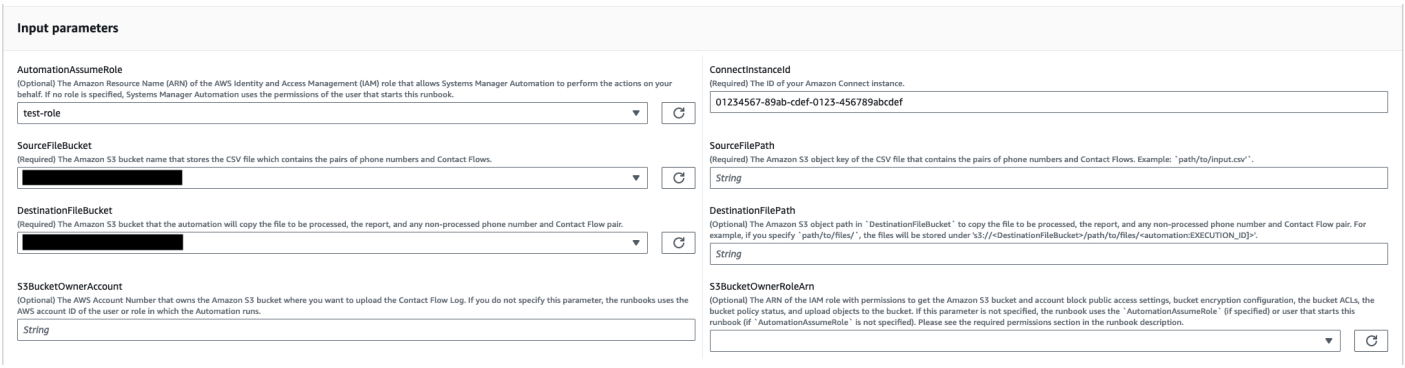
  應存放中繼檔案和結果報告的 Amazon S3 物件路徑。`DestinationFileBucket`例如，如果您指定`path/to/files/`，檔案會儲存在下面`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`。

- 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)

  IAM 角色的 ARN 具有取得 Amazon S3 儲存貯體和帳戶區塊公開存取設定、儲存貯體加密組態、儲存貯體 ACL、儲存貯體政策狀態，以及將物件上傳到儲存貯體的許可。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。



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 的限制。
   - GenerateResourceIdMap

     下載在中指定的來源 CSV 檔案，`SourceFilePath`並`ContactFlowId`為每個資源識別`PhoneNumberId`和。完成後，它會將包含`PhoneNumber`、`PhoneNumberId`和的 CSV 檔案上傳`ContactFlowId`到中指定的目的地 Amazon S3 儲存貯體`DestinationFileBucket`。`ContactFlowName`如果`PhoneNumberId`無法識別特定數字，CSV 檔案中的欄位將為空。
   - 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，`SourceFileBucket``SourceFilePath`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超過了最大數量而無法處理的電話號碼，則會在中上傳[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) 的位置 (Amazon S3 URI 和 Amazon S3 主控台 URL)。

- **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

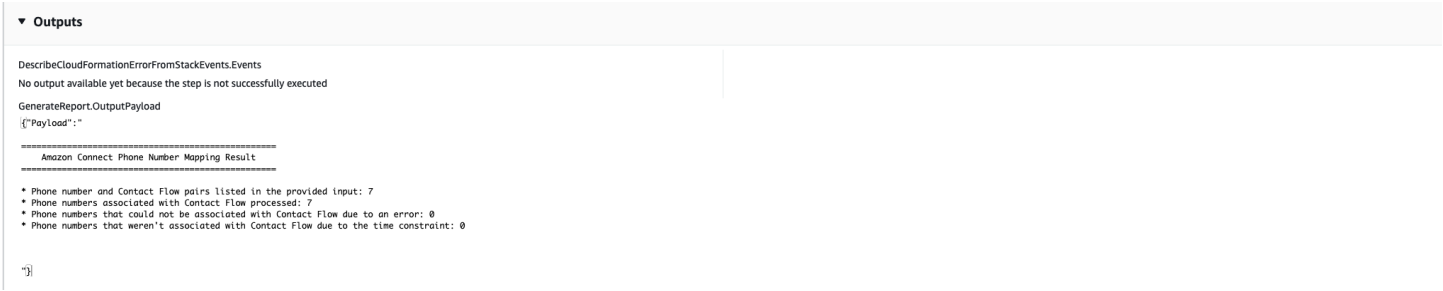
     輸出電話號碼和聯繫流程關聯。此報告包含下列資訊：

     - 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 檔案中指定的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

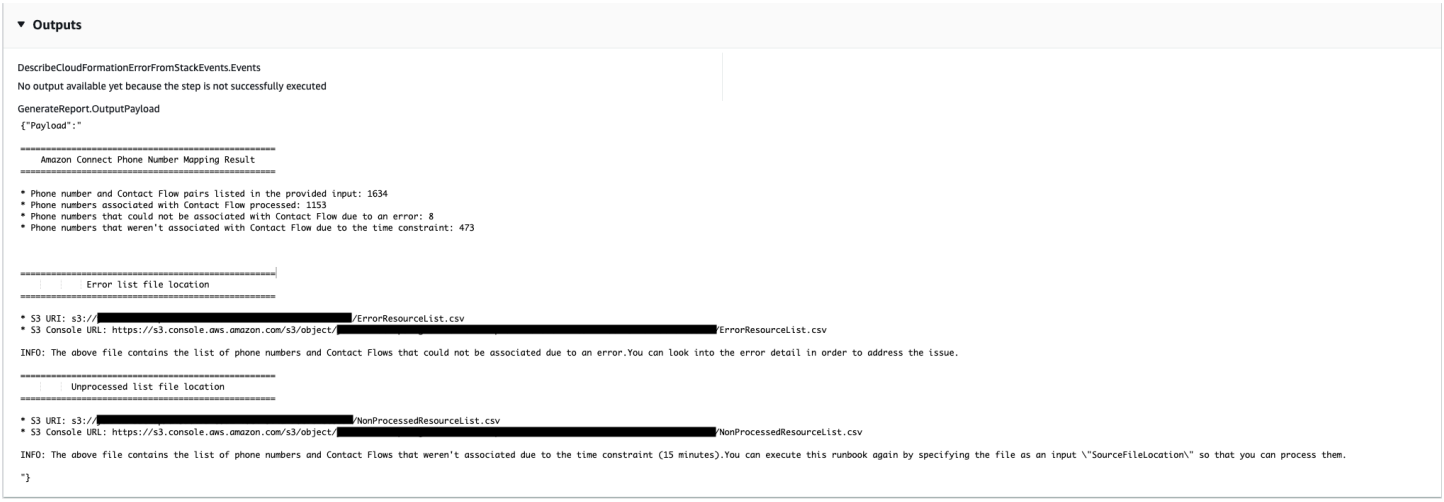
   - DescribeCloudFormationErrorFromStackEvents. 活動。

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



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



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 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
- t3.2xlarge

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 (描述)

AWSSupport-TroubleshootADConnectorConnectivityRunbook 會驗證 AD 連接器的下列必要條件：

- 檢查與 AD 連接器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 ManagerAWS Security Token Service、和 Amazon CloudWatch 界面虛擬私有雲端節點是否存在於與 AD 連接器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 連接器相同的子網路中啟動兩個 Amazon 彈性運算雲端 (Amazon EC2) 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**
>
> 使用此執行手冊可能會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

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。
- 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AmazonSSMManagedInstanceCore原則或同等權限。

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。

- 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 連接器。
- aws:executeAwsApi-收集 AD 連接器的相關資訊。
- aws:executeAwsApi-收集與 AD 連接器相關聯之安全性群組的相關資訊。
- aws:executeAwsApi-收集與 AD 連接器子網路相關聯之網路 ACL 規則的相關資訊。
- aws:executeScript-評估 AD 連接器安全性群組規則，以確認允許所需的輸出流量。
- aws:executeScript-評估 AD 連接器網路 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 Security Token Service和 Amazon CloudWatch 界面端點是否存在於與 AD 連接器相同的 VPC 中。AWS Systems Manager
- 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 ACL 缺少必要的輸出和輸入規則，自動化會在此停止。
- aws:createStack-建立AWS CloudFormation堆疊以啟動 Amazon EC2 執行個體以執行連線測試。
- aws:executeAwsApi-收集新啟動的 Amazon EC2 執行個體的 ID。
- aws:waitForAwsResourceProperty-等待第一個新推出的 Amazon EC2 執行個體報告為受管理的執行個體。AWS Systems Manager
- aws:waitForAwsResourceProperty-等待第二個新推出的 Amazon EC2 執行個體報告為受管理的執行個體。AWS Systems Manager
- aws:runCommand-從第一個 Amazon EC2 執行個體對現場部署 DNS 伺服器 IP 地址執行網路連線測試。
- aws:runCommand-從第二個 Amazon EC2 執行個體對現場部署 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。

- ApiId

  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`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 | 公里

  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

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)。
- 公里 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 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

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。

- 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 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
- 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：睡眠 ）-睡覺以避免 API 節流。
- PutScalingPolicyWrite (aws:executeAwsApi)-設定 DynamoDB 表的目標寫入容量使用率。
- PutScalingPolicyWriteDelay （ aws：睡眠 ）-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：睡眠 ）-睡覺以避免 API 節流。
- PutScalingPolicyRead (aws:executeAwsApi)-設定 DynamoDB 表的目標讀取容量使用率。
- VerifyDynamoDbAutoscalingEnabled (AWS：執行程序檔)-確認已根據您指定的值，針對 DynamoDB 表啟用應用程式自動調整比例。

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

Description

AWSSupport-AnalyzeEBSResourceUsage自動化手冊用於分析亞馬遜彈性區塊商店（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. 收集處於可用狀態的所有 Amazon EBS 磁碟區。
3. 收集已刪除來源磁碟區的所有 Amazon EBS 快照。
4. 收集未被任何未終止的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體使用的所有亞馬遜機器映像 (AMI)。

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，則執行手冊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、封鎖公用存取，並要求使用 SSL/TLS 的請求。

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。
- 僅允許傳送 SSL 要求到您的儲存貯體。
- 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

Linux 系統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。

- 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]$

- CustomerManagedKmsKey阿恩

  類型：字串

  說明：(選用) 自訂 AWS KMS 金鑰 Amazon 資源名稱 (ARN)，用於加密帳戶中指定的儲存貯體不存在時將建立的新 Amazon S3 儲存貯體。如果在未指定自訂 AWS KMS 金鑰 ARN 的情況下嘗試建立值區，則自動化會失敗。

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

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: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

執行此 Runbook 所需的最低 IAM 許可的範例政策：

```
        {
            "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:::DOC-EXAMPLE-BUCKET1",
                    "arn:aws:s3:::DOC-EXAMPLE-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：

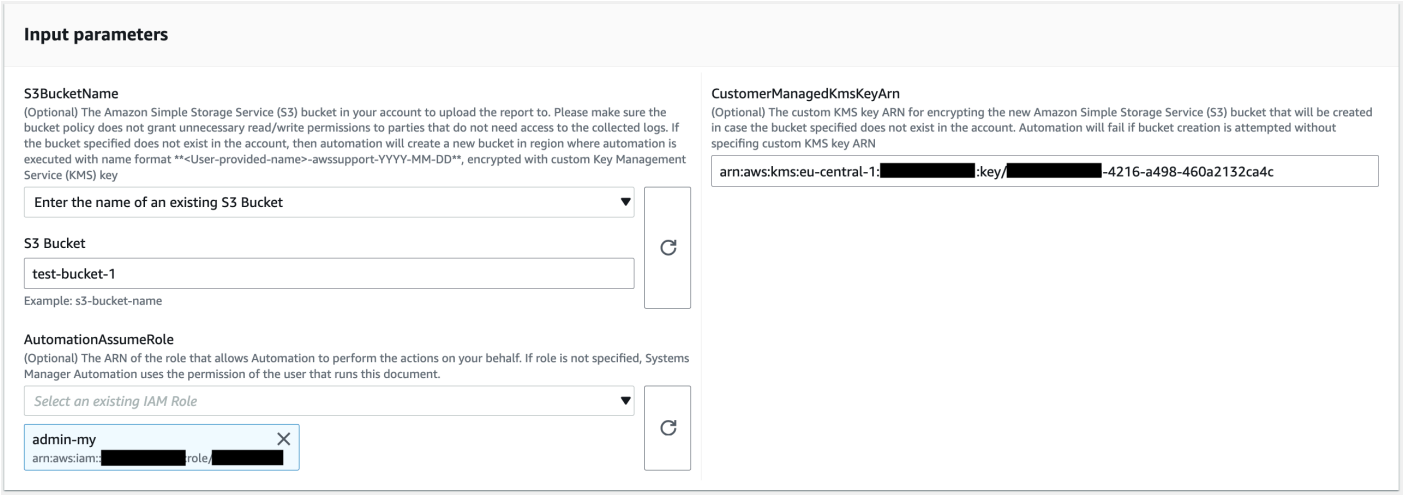
1. 導航到控AWSSupport制台中的分析ResourceUsage。 AWS Systems Manager
2. 對於輸入參數，請輸入以下內容：
   - AutomationAssumeRole (選擇性)：

     (IAM) 角色的 Amazon 資源名稱 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。



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：

   - 並行檢查：

     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。

   - 驗OrCreate證桶：

     驗證 Amazon S3 存儲桶是否存在。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。

   - 聚集AmiDetails：

     搜尋 AMI (未被任何 Amazon EC2 執行個體使用) 產生名稱格式的報告`<region>-images.csv`，並將其上傳到 Amazon S3 儲存貯體。

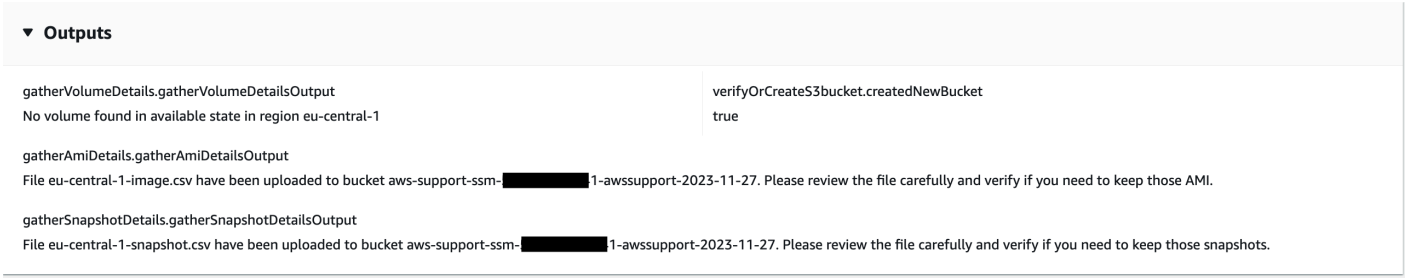
   - 聚集VolumeDetails：

     驗證 Amazon EBS 磁碟區處於可用狀態，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。

   - 聚集SnapshotDetails：

尋找已刪除之 Amazon EBS 磁碟區的 Amazon EBS 快照，以名稱格式產生報告<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。



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-ArchiveEBSSnapshots執行手冊可協助您為 Amazon 彈性區塊存放區 (Amazon EBS) 磁碟區的快照存檔。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

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：(選擇性) 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`。
- SnapshotWith標籤

  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

  類型：字串

  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 許可

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

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

文件步驟

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

AWS-AttachEBSVolume

Description

將亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區連接到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 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 磁碟區的識別碼。磁碟區和執行個體必須位於相同的可用區域內。

AWSSupport-CalculateEBSPerformanceMetrics

Description

AWSSupport-CalculateEBSPerformanceMetrics執行手冊可透過計算效能指標並將效能指標發佈到儀表板，協助診斷 Amazon EBS 效能問題。 CloudWatch 儀表板會顯示目標 Amazon EBS 磁碟區或連接到目標 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的所有磁碟區的預

估平均 IOPS 和輸送量。對於 Amazon EC2 執行個體，它也會顯示執行個體的平均 IOPS 和輸送量。runbook 會將連結輸出至新建立的儀表板，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。
- 驗證資源識別碼 (Amazon EBS 磁碟區或 Amazon EC2 執行個體) 是否有效。
- 當您提供 Amazon EC2 做為 ResourceID 時，它會為該 Amazon EC2 執行個體建立包含實際 IOPS/輸送量的 CloudWatch 儀表板，以及連接至 Amazon EC2 執行個體的所有 Amazon EBS 磁碟區的預估平均 IOPS/輸送量圖形。
- 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/ 輸送量圖形。
- 產生 CloudWatch 儀表板之後，如果「預估平均 IOPS」或「預估平均輸送量」分別大於「最大 IOPS」或「最大輸送量」，則連接至 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)，應該考慮最大 IOPS/ 輸送量，直到您有突發平衡為止。完全利用突發平衡後，即它變為零，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）

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: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)：

(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。

- ResourceID (必要)：

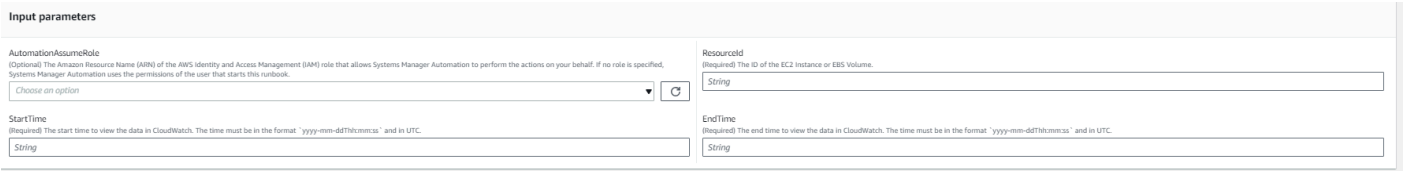
  Amazon EC2 執行個體或亞馬遜 EBS 磁碟區的識別碼。

- 開始時間 (必填):

  檢視資料的開始時間 CloudWatch。時間必須採用 UTC 格式`yyyy-mm-ddThh:mm:ss`。

- 結束時間 (必填):

  檢視資料的結束時間 CloudWatch。時間必須採用 UTC 格式`yyyy-mm-ddThh:mm:ss`。



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 EC2 執行個體的平均 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。
7. 完成後，請查看「輸出」部分以獲取執行的詳細結果：

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

CloudWatch > Dashboards >
AWSSupport-i-0[redacted]-EBS-Performance-40121150-f1be-4418-a[redacted]

Autosave: Off

AWSSupport-i-0[redacted]-EBS-Performance-... | 2024-01-10T17:44:00 > 2024-01-10T18:07:00 | UTC timezone | Actions | Save

Aggregated Metrics for EC2 Instance i-[redacted]

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

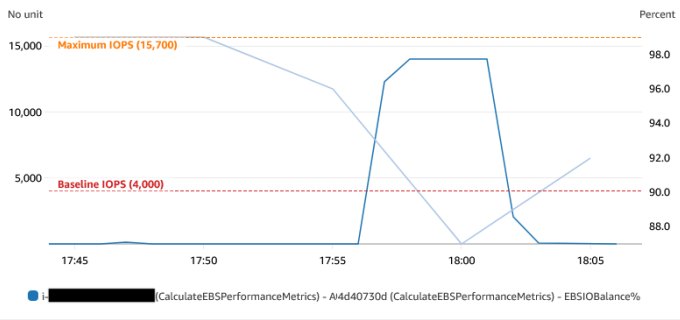
More details on EBS Optimized instances | More details on EBS Volume Types

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

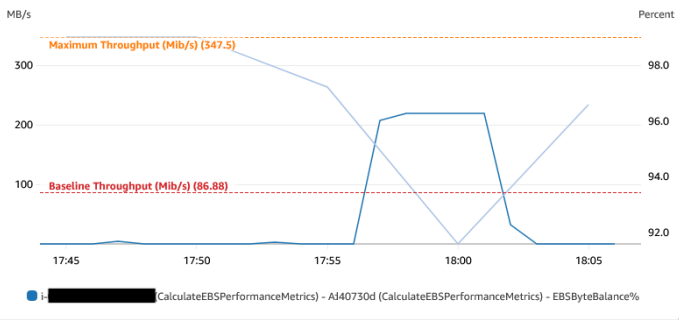
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

Average Total IOPS
2024-01-10 - 2024-01-10



Average Total Throughput
2024-01-10 - 2024-01-10



EBS Volume(s) Metrics

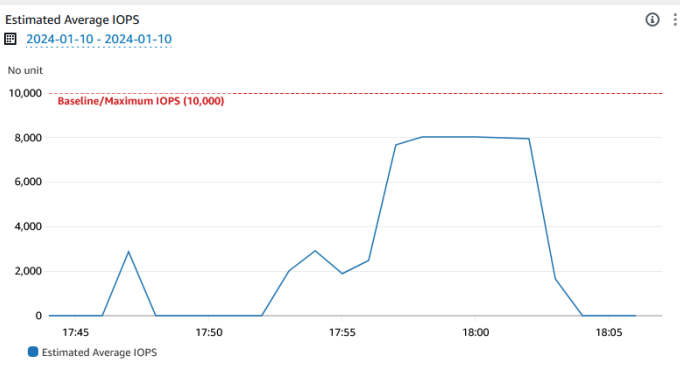
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

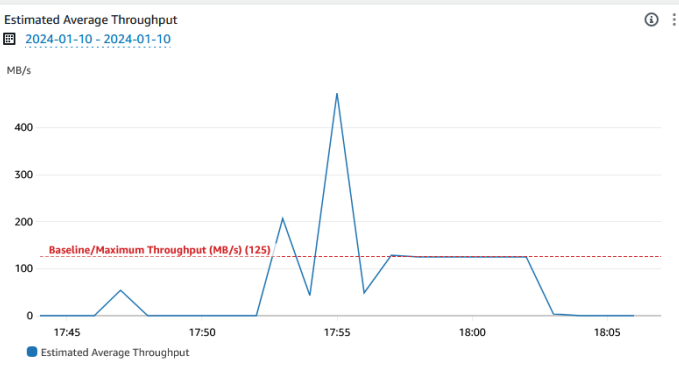
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

Estimated Average IOPS
2024-01-10 - 2024-01-10

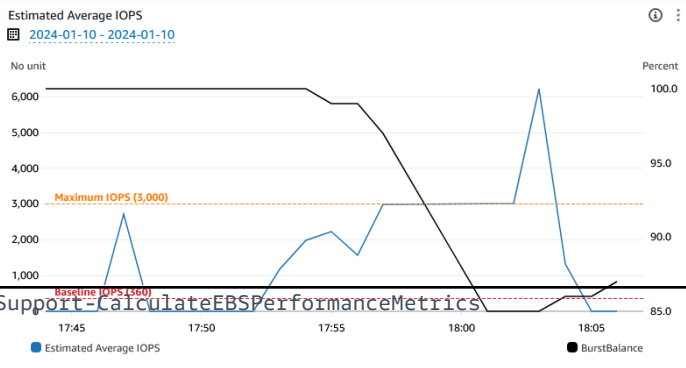


Estimated Average Throughput
2024-01-10 - 2024-01-10

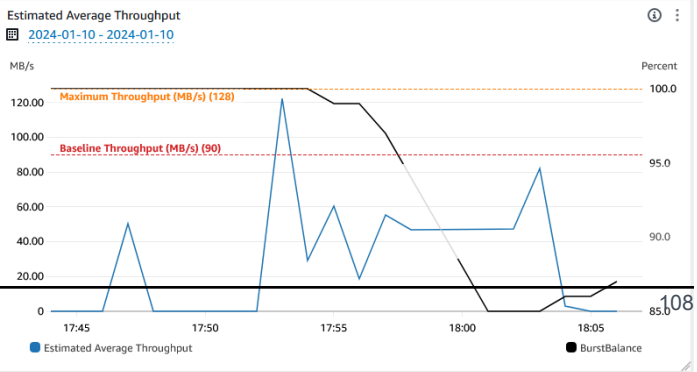


Volume: vol[redacted] | Type: gp2

Estimated Average IOPS
2024-01-10 - 2024-01-10



Estimated Average Throughput
2024-01-10 - 2024-01-10

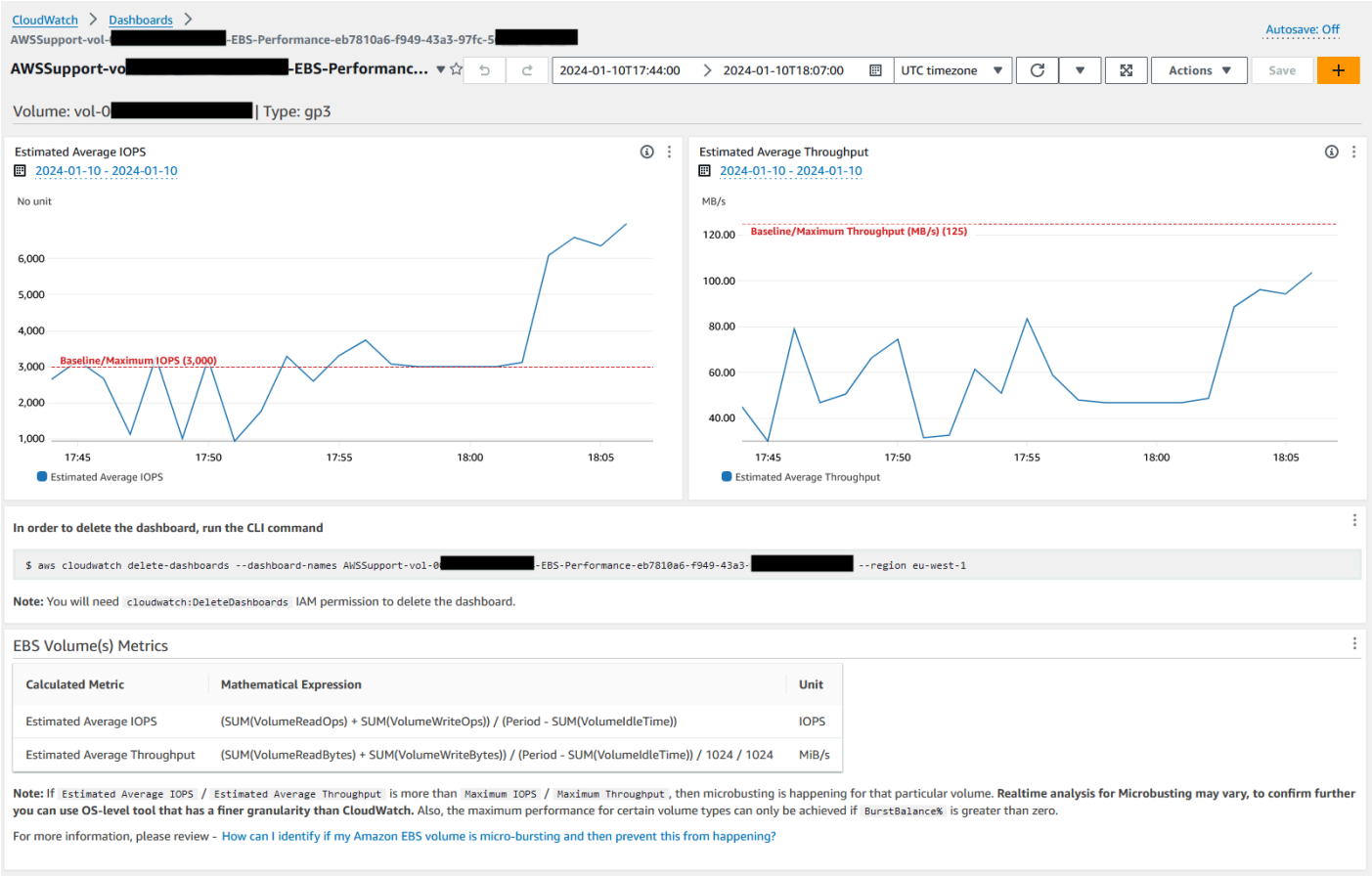


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

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
- 設定自動化操作
- Support 自動化工作流登陸頁

AWS服務文件

- 如何確定我的 Amazon EBS 磁碟區是否微爆裂，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

複製亞馬遜彈性區塊存放區 (Amazon EBS) 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

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：(選擇性) Amazon EBS 快照的說明。
- SnapshotId

  類型：字串

  說明：(必填) 要複製之 Amazon EBS 快照的識別碼。

- 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

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。

- 描述

  類型：字串

  描述：(選用) 快照的描述
- VolumeId

  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

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。
- SnapshotId

類型：字串

描述：(必要) EBS 快照的 ID。

AWSConfigRemediation-DeleteUnusedEBSVolume

Description

手AWSConfigRemediation-DeleteUnusedEBSVolume冊刪除未使用的 Amazon Elastic Block Store (Amazon EBS) 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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。
- VolumeId

  類型：字串

描述：(必填) 您要刪除之 Amazon EBS 磁碟區的識別碼。

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
- 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，並根據您為參數選擇的值建立快照。CreateSnapshot
- 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

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。
- 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AMIs消註冊的標籤值。

必要的 IAM 許可

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

- ec2:DeregisterImage
- ec2:DescribeImages

文件步驟

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

AWS-DetachEBSVolume

Description

從 Amazon 彈性運算雲端 (Amazon EC2) 執行個體分離亞馬遜 EBS 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

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。

- LambdaAssume角色

  類型：字串

  描述：(選用) Lambda 所承擔之角色的 ARN

- VolumeId

  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 Elastic Block Store (Amazon EBS) 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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 許可

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

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

文件步驟

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

AWS-ExtendEbsVolume

Description

AWS-ExtendEbsVolume執行手冊會增加 Amazon EBS 磁碟區的大小，並擴充檔案系統。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

  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。
- 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：(選用) 您要擴充的 Amazon EBS 磁碟區附加到的 Amazon EC2 執行個體識別碼。
- 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：(必要) 您要將 Amazon EBS 磁碟區修改為單位的 GiB 大小。
- VolumeId

  類型：字串

  描述：(必要) 您要擴充的 EBS 磁碟區識別碼。

必要的 IAM 許可

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

- 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

AWSSupport-ModifyEBSSnapshotPermission執行手冊可協助您修改多個 Amazon Elastic Block Store (Amazon EBS) 快照的許可。使用此 runbook，您可以製作快照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

  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。

- AccountIds

  類型: StringList

  預設：none

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

- AccountPermission操作

  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

  說明：(必填) 您要修改其權限的 Amazon EBS 快照識別碼。

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
- ec2:DescribeSnapshots
- ec2:ModifySnapshotAttribute

文件步驟

1. aws:executeScript-驗證SnapshotIds參數中提供的快照 ID。驗證 ID 之後，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

SharewithOther帳戶. 結果

MakePrivate。結果

MakePrivate. 命令。

AWSConfigRemediation-ModifyEBSVolumeType

Description

手AWSConfigRemediation-ModifyEBSVolumeType冊修改 Amazon 彈性區塊存放區 (亞馬遜 EBS) 磁碟區的磁碟區類型。修改磁碟區類型後，磁碟區會進入optimizing狀態。如需監控磁碟區修改進度的相關資訊，請參閱 Amazon EC2 使用者指南中的監控磁碟區修改進度。

運行此自動化（控制台）

文件類型

自動化

擁有者

Amazon

平台

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。
- EbsVolume識別碼

  類型：字串

  描述：(必填) 您要修改之 Amazon EBS 磁碟區的識別碼。
- EbsVolume类型

  類型：字串

  有效值：標準 | IO1 | IO2 | gp3 |

  描述：您想要將 Amazon EBS 磁碟區變更為的磁碟區類型。如需 Amazon EBS 磁碟區類型的相關資訊，請參閱亞馬遜 EC2 使用者指南中的 Amazon EBS 磁碟區類型。

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: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-CreateImage
- AWS-DeleteImage
- AWS-PatchAsgInstance
- AWS-PatchInstanceWithRollback
- AWS-QuarantineEC2Instance
- AWS-ResizeInstance
- AWS-RestartEC2Instance
- AWS-SetupJupyter
- AWS-StartEC2Instance
- AWS-StopEC2Instance
- AWS-TerminateEC2Instance
- AWS-UpdateLinuxAmi
- AWS-UpdateWindowsAmi
- AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck
- AWSConfigRemediation-EnforceEC2InstanceIMDSv2
- AWSEC2-CloneInstanceAndUpgradeSQLServer
- AWSEC2-CloneInstanceAndUpgradeWindows
- AWSEC2-ConfigureSTIG
- AWSEC2-PatchLoadBalancerInstance
- AWSEC2-SQLServerDBRestore
- AWSSupport-ActivateWindowsWithAmazonLicense
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2
- AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

- AWSSupport-CheckXenToNitroMigrationRequirements
- AWSSupport-ConfigureEC2Metadata
- AWSSupport-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-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`

步驟號碼	步驟名稱	自動化動作
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。
- AmiId

  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。
- InstanceId

  類型:StringList

  描述：(必要) 要終止的一個或多個 EC2 執行個體之 ID。

AWS-UpdateLinuxAmi

Description

使用 Linux 發行包和 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：應用程序，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AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck冊可為您指定的 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

LinuxmacOS, 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 (描述)

AMI從 EC2 執行個體建立執Windows Server行個體以執行 SQL Server 2008 年或更新版本，然後將 AMI 升級為較新版本的 SQL 伺服器。

支援下列升級路徑：

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

- SQL Server 2017 升級至 SQL Server 2019

如果您使用的是與 SQL 伺服器 2019 不相容的舊版視窗伺服器，則自動化文件必須將您的視窗伺服器版本升級到 2016 年。

升級為多步驟程序，可能需要 2 小時才能完成。自動化會從執行個體建立 AMI，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 中啟動新功能來測試應用程式功能。結束測試後，在執行另一次升級前，請先安排應用程式停機時間，再完全切換至已升級的執行個體。

> **Note**
>
> 如果要修改從新啟動 EC2 執行個體的電腦名稱AMI，請參閱重新命名託管 SQL Server 獨立執行個體的電腦。

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.
- EC2 執行個體必須使用 Windows Server 2008 R2 (或更新版本) 和 SQL Server 2008 (或更新版本) 的 Windows Server 版本。

- 確認 SSM Agent 安裝於您的執行個體上。如需詳細資訊，請參閱在適用於 Windows 伺服器的 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，請參閱建立 Systems Manager 的 IAM 執行個體設定檔。
- 驗證執行個體在執行個體開機磁碟中有 20 GB 的可用磁碟空間。
- 針對使用自有授權 (BYOL) 的 SQL Server 版本執行個體，適用下列額外的事前準備：
  - 提供包含目標 SQL 伺服器安裝媒體的 EBS 快照集識別碼。若要執行此作業：

    1. 確認 EC2 執行個體執行的是 Windows Server 2008 R2 或更新版本。
    2. 在執行個體執行的相同可用區域中建立 6 GB 的 EBS 磁碟區。將磁碟區連結到執行個體。例如，將其掛載為 D 磁碟機。
    3. 在 ISO 按一下滑鼠右鍵，並將其掛載至執行個體，例如做為 E 磁碟機。
    4. 從磁碟機 E:\ 將 ISO 的內容複製到磁碟機 D:\
    5. 建立步驟 2 中所建立 6 GB 磁碟區的 EBS 快照。

限制

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

參數

- IamInstanceProfile

  類型：字串

  說明：（必填）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) 或 SQL Server 2008 (或更新版本) 的執行個體。
- KeepPreUpgradeImageBackUp

類型：字串

說明：(選擇性) 如果設為`true`，自動化操作不會刪除升級前從執行個體建立的 AMI。如果設定為`true`，則必須刪除 AMI。AMI 預設為刪除。

- SubnetId

  類型：字串

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

- SQL ServerSnapshotId

  類型：字串

  說明：(條件式) 目標 SQL Server 安裝媒體的快照集識別碼。此參數對使用 BYOL SQL Server 版本的執行個體是必要項目。針對包含 SQL Server 授權的執行個體 (即使用 AWS 所提供 Windows Server 與 Microsoft SQL Server Amazon Machine Image 啟動的執行個體)，此為選用參數。

- RebootInstanceBeforeTakingImage

  類型：字串

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

- 目標字址版本

  類型：字串

  說明：(選擇性) 選取目標 SQL Server 版本。

  可能的目標：

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

  預設目標：SQL 伺服器

輸出

AMIID：從升級到較新版本的 SQL 伺服器執行個體所建立的 AMI 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 Server2008 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 (STIG) 是國防資訊系統機構 (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設定。

Amazon EC2 提供了一個 Systems Manager 執行手冊AWSEC2-ConfigureSTIG，您可以使用它將 STIG 設定套用至執行個體。本文件可協助您快速建立符合 STIG 標準的相容影像。STIG Systems Manager 文件會掃描設定錯誤並執行補救指令碼。它也會 InstallRoot 從 Windows AMI 上的國防部 (DoD) 安裝，以安裝和更新 DoD 憑證，並移除不必要的憑證以維持 STIG 相容性。使用 STIG Systems Manager 文件無須額外付費。

> **Important**
>
> 除了少數例外之外，Systems Manager 文件下載的 STIG 強化元件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 支援該套件的相關 STIG，則會套用這些 STIG。

本頁列出 Amazon EC2 支援的 STIG 強化元件適用於您的 EC2 執行個體的所有 STIG。

您可以選擇要套用的 STIG 法規遵循類別。

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

Amazon 會針對每個版本將 STIG 強化元件分組成與作業系統相關的套裝軟體。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 ）。視窗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 資源進行通訊。我們需要 TLS 1.2 並建議使用 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

視窗風格設置

Amazon EC2 視窗 STIG AMI 和強化元件是專為獨立伺服器所設計，並套用本機群組原則。STIG 相容的元件會 InstallRoot 從 Windows AMI 上的 DoD (DoD) 進行安裝，以下載、安裝及更新國防部憑證。他們也會移除不必要的憑證，以維持 STIG 合規性。目前，Amazon EC2 支援以下版本的視窗伺服器 STIG 基準：

本節列出 Amazon EC2 針對您的 Windows 基礎設施所支援的目前 STIG 設定，接著是版本歷史記錄日誌。

您可以套用低、中或高 STIG 設定。

低視窗風格 (類別三)

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

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

- 視窗服務器 2022 STIG 版本 1 版本 1

  V-254335, V-254336, V-254337, V-254338, V-254351, 愿意, 鼎, 和遷 V-254357 V-254363 V-254481
- 視窗服務器 2019 時尚版本 2 發布 5

  V-205691、V-205819、V-205858、V-205859、V-205860、V-205870、V-205871 以及 V-205923
- 視窗服務器 2016 時尚版本 2 發布 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 風格版本 3 版本 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 版本 2 版本 2 版本 2

  沒有任何 STIG 設定適用於 Microsoft .NET 架構的第三類漏洞。
- 視窗防火牆樣式版本 2 版本 1

  V-241994, V-241995, V-241996, V-241999, V-242000, 愿意, 鼎, 朗, 和熱 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

中等視窗風格（第二類）

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

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

> **Note**
>
> 除了 Amazon EC2 針對類別 II 弱點所支援的 STIG 強化設定之外，視窗 STIG 中型類別還包括所有列出的適用於視窗 STIG 低 (類別 III) 的 STIG 強化設定。

- 視窗服務器 2022 STIG 版本 1 版本 1

  包含 Amazon EC2 針對類別 III (低) 弱點支援的所有 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, 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-254321, V-254323, V-254323, 伏特, 254325, V 型, 254326, V-254327, V-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，伏特 -254376，V-254379，V-254382，V-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 254464,V-254468, V-254470, V-254471, V-254472,,, 湧, 球, 蘋果, 她, 節制, 節制, 幕, 蒸氣, 向量, 毫秒, 伏特, 伏特, 卷, V 型, 254495, V 型, V 型 254497, V 型 254499, V 型 254501, V 型 254501, V 型 254502, V 型 254502, V 型 254503, 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 時尚版本 2 發布 5

  包含 Amazon EC2 針對類別 III (低) 弱點支援的所有 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,,V -205729, V-205730, V-205733, V-205747, 電視 -205752, V-205752, V-205756, V-205758, V. V -205770, V-205771, V-205772, V-205773, V-205774, V-205775, V, 205777, V. V-205801, V-205808, V-205809, V-205810, V-205811, 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 205917, 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

- 視窗服務器 2016 時尚版本 2 發布 5

  包含 Amazon EC2 針對類別 III (低) 弱點支援的所有 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, 電視, 電影 -224887, 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-二 24915, V-二 24920, V 型電視 -224927, V-224928, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V, V-224948, V-224949, V-224951, V-224953, 伏特 -224955, 伏特 -224956, 電影 -224957, V-224959, V-224962, 十六、二二二五十七、二二二二五十九、二二二五二十二、二二二五十三、二二二二二五十四、二二二五十九、二五零三四、二五零三三、五五十三三、V 四十一、二百五十四、七五十四、七五十四、四百五十四V-225051, V-225052, V-225055, V-225056,, 保證, 湧, 球, 蘋果, 節制, 節制, 蒸氣, 蒸氣, 毫秒, 伏特, 冰壺, 風格, V-225076, 格魯, V 型 225080, V 型 -225082, V 型 225083, V 型 225084, V 型 225088, V 型 V-236000 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-225078

- 視窗服務器 2012 R2 MS 風格版本 3 版本 5

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

  V-225574, V-225573, V-225572, V-225571, V-225569, 伏特 -225568, 伏特 -225567, V-225566, 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 型, 二五五十八, V 型,伏特 -225506, 伏特 -225503, V-225502, 伏特 -225501, 伏特 -225500, 伏特 -225494, 伏特 -225478, 伏特, V 25463, V-225461, V-225458, V-225457, V-225456, 伏特 -225455, 伏特 -225453, V-225452, V-225448, V 225411, V-225410, V-225409, V-225408, 伏特 -225406, 伏特 -225405, 伏特 -225402, V-225402, V-225393, V, V-225385, V-二 25384, V-二二五八三, V 型伏特 -225379, 伏特 -225378, 伏特 -225375, 伏特 -225374, 伏特 -225373, 伏特 -225372, 伏特 -225371, V, V-225349, V-225348,

V-225347, 伏特 -225346, 伏特 -225345, 伏特 -225341, 伏特 -225340, V-225337, V 314, V-225305, V 型, 二二五三零三, V 型V-225283, V-225282, V-225281, V-225280,,, 搶, 球, 蘋果, 早餐, 四千五百六十一, 蒸汽浴缸, 蘋果,,, 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 框架樣式 4.0 版本 2 版本 2 發布 2

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

  V-225238

- 視窗防火牆樣式版本 2 版本 1

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

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

- 互聯網瀏覽器 11 STIG 版本 2 發布 3

  包含 Amazon EC2 針對類別 III (低) 弱點支援的所有 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,, 向, 湧, 球, 蘋果, 四季, 四千〇一年, 蒸汽, 雞, 冰, 伏特, 冰壺, 風格, 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-235740 V-235742

- 後衛 STIG 版本 2 版本 4（僅限視窗服務器 2022）

  V-213427, V-213429, V-213430, V-213431,, V-213432, 向前, 球, 蘋果, 四季, 節制, 節制, 包括, 臘, 基督徒, 伏特, 冰壺, 風格, V-213446, V-213447, V 型 213448, V 型 213449, V 型 213451, V 型 213455, V 型 213464, V 型 213464, V 型 213465, V 型 213465, 和 V 型 213465, V 型 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

窗戶風格高（類別 I）

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

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

> **Note**
>
> 除了 Amazon EC2 針對類別 I 弱點所支援的 STIG 強化設定外，視窗 STIG 高類別還包含適用於 Windows STIG 中和低類別的所有列出的 STIG 強化設定。

- 視窗服務器 2022 STIG 版本 1 版本 1

  V-254293, V-254352, V-254353, V-254354,, 搶, 鼎, 蘋果, 熱潮, 電視台,, 北, 405, 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 時尚版本 2 發布 5

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

  V-205653、V-205654、V-205711、V-205713、V-205724、V-205725、V-205757、V-205802、V-205804 以及 V-205919
- 視窗服務器 2016 時尚版本 2 發布 5

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

  V-224874、V-224932、V-224933、V-224934、V-224954、V-224958、V-224961、V-225025、V-225044 以及 V-225079
- 視窗服務器 2012 R2 MS 風格版本 3 版本 5

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

  V-225556、V-225552、V-225547、V-225507、V-225505、V-225498、V-225497、V-225496、V-225493 以及 V-225274
- Microsoft. NET 框架樣式 4.0 版本 2 版本 2 發布 2

包括 Amazon EC2 針對 Microsoft .NET 框架的第二類和第三類 (中和低) 弱點所支援的所有 STIG 強化設定。沒有其他 STIG 設定適用於類別 I 弱點。

- 視窗防火牆樣式版本 2 版本 1

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，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 EC2 針對 IE 11 類別 II 和第 III 類 (中和低) 弱點所支援的所有 STIG 強化設定。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)

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

  V-235758 和 V-235759

- 後衛 STIG 版本 2 版本 4 (僅限視窗服務器 2022)

  包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

  V-213426、V-213452 和 V-213453

視窗版本歷史記錄

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 年第一季度變更-2024 年 2 月 23 日 (沒有變動)：

對於 2024 年第一季度發行的 Windows 元件 STIG 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 Windows 元件 STIG 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 年第三季發行的視窗元件 STIG 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 年第二季度發行的 Windows 元件 STIG 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 年第一季度發行的 Windows 元件 STIG 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：

針對 2022 年第四季發行版本的更新 STIG 版本和套用的 STIG，如下所示：

柱狀構建視窗-低版本

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft 邊緣 STIG 版本 1 版本 6 (僅限視窗伺服器 2022)

STIG 構建視窗中型版本

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft 邊緣 STIG 版本 1 版本 6 (僅限視窗伺服器 2022)
- 後衛 STIG 版本 2 版本 4 (僅限視窗服務器 2022)

柱狀構建視窗-高版本

- Windows Server 2022 STIG 版本 1 第 1 版
- Windows Server 2019 STIG 版本 2 第 5 版
- Windows Server 2016 STIG 版本 2 第 5 版
- Windows Server 2012 R2 MS STIG 版本 3 第 5 版
- Microsoft .NET Framework 4.0 STIG 版本 2 第 2 版
- Windows Firewall STIG 版本 2 第 1 版
- Internet Explorer 11 STIG 版本 2 第 3 版
- Microsoft 邊緣 STIG 版本 1 版本 6 (僅限視窗伺服器 2022)
- 後衛 STIG 版本 2 版本 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 年第三季發行的 Windows 元件 STIG 沒有任何變更。

二零二年第二季度變動：

為 2022 年第二季發行版本更新了 STIG 版本和應用的 STIG。

柱狀構建視窗低版本 1.5.0

- 視窗服務器 2019 時尚版本 2 版本 4
- 視窗服務器 2016 時尚版本 2 版本 4
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1
- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建的窗口中版本 1.5.0

- 視窗服務器 2019 時尚版本 2 版本 4
- 視窗服務器 2016 時尚版本 2 版本 4
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1

- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建窗口高版本 1.5.0

- 視窗服務器 2019 時尚版本 2 版本 4
- 視窗服務器 2016 時尚版本 2 版本 4
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1
- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

2022 年第一季度變動（不變）：

對於 2022 年第一季發布的 Windows 組件 STIG 沒有任何更改。

二零二一年第四季度變更：

針對 2021 年第四季發行的更新 STIG 版本和應用了 STIG。

柱狀構建視窗低版本 1.5.0

- 視窗服務器 2019 時尚版本 2 發布 3
- 視窗服務器 2016 時尚版本 2 發布 3
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1
- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建的窗口中版本 1.5.0

- 視窗服務器 2019 時尚版本 2 發布 3
- 視窗服務器 2016 時尚版本 2 發布 3
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1

- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建窗口高版本 1.5.0

- 視窗服務器 2019 時尚版本 2 發布 3
- 視窗服務器 2016 時尚版本 2 發布 3
- 視窗服務器 2012 R2 MS 風格版本 3 版本 3
- Microsoft. NET 框架 4.0 版本 2 版本 1
- Windows Firewall STIG 版本 2 第 1 版
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

二零二一年第三季變更-九月三十日：

針對 2021 年第三季發行的更新 STIG 版本和應用了 STIG。

柱狀構建視窗低版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗服務器 2016 時尚版本 2 發布 2
- 視窗服務器 2012 R2 MS 風格版本 3 版本 2
- Microsoft. NET 框架 4.0 版本 2 版本 1
- 視窗防火牆樣式版本 1 版本 7
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建視窗中版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗服務器 2016 時尚版本 2 發布 2
- 視窗服務器 2012 R2 MS 風格版本 3 版本 2
- Microsoft. NET 框架 4.0 版本 2 版本 1
- 視窗防火牆樣式版本 1 版本 7
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

柱狀構建窗口高版本 1.4.0

- 視窗服務器 2019 STIG 版本 2 發布 2
- 視窗服務器 2016 時尚版本 2 發布 2
- 視窗服務器 2012 R2 MS 風格版本 3 版本 2
- Microsoft. NET 框架 4.0 版本 2 版本 1
- 視窗防火牆樣式版本 1 版本 7
- 互聯網瀏覽器 11 STIG 版本 1 版本 19

STIG 設定

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

- 紅帽企業版 (RHEL) 7 樣式設定
  - RHEL 7
  - CentOS 7
  - Amazon Linux 1 (AL2)
- 風險 8 風格設置
  - RHEL 8
  - CentOS 8
  - Amazon 马逊

低分級 (類別三)

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

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

RHEL 7 風格版本 3 版本 14

- 瑞尔 7/CentOS 7

V-204452、V-204576 和 V-204605

- AL2

  V-204452、V-204576 和 V-204605

RHEL 8 風格版本 1 版本 13

- RHEL 8 /CentOS 8

  V-230241, V-244527, V-230269, V-230270,, 搶, 壓制, 蘋果, 早餐, 卷, 鑼, 蒸氣, 北, V-230486,,,, V-230496, 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-230494 V-230495

Ubuntu 18.04 風格版本 2 版本發布 13

V-219172, V-219173, V-219174, V-219175,, 搶, 鼎, 蘋果, 熱潮, 電梯, 鑼灣, 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 20.04 風格版本 1 版本發布 11

V-238202, V-238234, V-238235, V-238237,, 搶, 鼎, 蘋果, 熱潮, 電梯, 鑼灣, 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

斯蒂格中型 (類別二)

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

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

> **Note**
>
> 除了 Amazon EC2 針對類別 II 弱點所支援的 STIG 強化設定外，Linux STIG 中型類別包含所有適用於 Linux STIG 低 (類別 III) 的所有列出的 STIG 強化設定。

RHEL 7 風格版本 3 版本 14

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

- 瑞尔 7/CentOS 7

  V-204585, V-204490, V-204491, V-, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-, V-204600, V-204602, V-204602, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V 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-204562, V-204563, V 型,, V-204610, V-204611, V-204612, V-204613, V-204614, V-204616, V-204617, V-204617, V.,V-204631、V-204633 和 V-256970

- 其二：

  V-204585, V-204490, V-204491, V-, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-, V-204600, V-204602, V-204602, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V 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-204562, V-204563, V 型,, V-204610, V-204611, V-204612, V-204613, V-204614, V-204616, V-204617, V-204617, V.,V-204631、V-204633 和 V-256970

RHEL 8 風格版本 1 版本 13

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

- RHEL 8 /CentOS 8

  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, 電影 -230314, 電影 -244523, 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, 伏特 -230359, V-230359, V-230361, V-230361, V V-244533, V-251713, V-251717, V-251714, V-251716, 伏特 -230332, 伏特 -230334, 伏特 -230335, V -230340, V, V-230343, V-230345, V-230240, V-230282, V-250316, V-230277, V-230277, V-230278, V-230394, V-230396, V 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 V-244542, V-230503, V-二三四四, V 型V-230296, V-230330,

V-230382, V-230526,,, 向前, 壓制, 蘋果, 四千五百五十, 四季, 蒸汽浴缸,, 伏特,,, V-230488, 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

Ubuntu 18.04 風格版本 2 版本發布 13

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, V -219315, 伏特 -219195, 伏特 -219196, 伏特 -219197, 伏特, 二 19214, V -219215, 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, 玻璃, 伏特, 伏特, V 型, 219287, V 型 219297, V-219298, V 型, 電信 -233780, 電信 -255906, 電子 -219338, 電子 -219344, 電視 -219184, V 型, 電子 -219156, 電子 -219156, 電子 -219160, 電子 -219306, 電子 -219149, V 型 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 V-219279 V-219281

Ubuntu 20.04 風格版本 1 版本發布 11

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-23833, V-238369, V-238341, V-238342, V-238343, V-238343, V-238353, V-238228, 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,, 節制, 蒸氣, 蒸汽, 包, 雞, 伏特, 玻璃, 伏特, 伏特, V 型 238302, V 型 238309, V 型 238309, V 型 238310, V 型 238310, V 型 238315, V 型 238315, V 型 238316, V 型 238316, V 型 238317, V 型 238319 電視 -251505, 電視 -238360, 電視機, 電視 238213, 電視機, 電視 238220, V 型, 電視 -238355, 電視, 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

高分類 (類別一)

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

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

> **Note**
>
> 除了 Amazon EC2 針對類別 I 弱點所支援的 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的 STIG 強化設定。

RHEL 7 風格版本 3 版本 14

包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

- 瑞尔 7/CentOS 7

  V-204425, V-204594, V-204455, V-204424,, 搶, 鼎, 朗, 熱量, 電梯, 和 CHINGS V-204442 V-204443 V-204447 V-204448 V-204502 V-204620 V-204621
- 其二：

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

RHEL 8 風格版本 1 版本 13

包含 Amazon EC2 針對第 II 類和第 III 類 (中和低) 弱點支援的所有 STIG 強化設定，以及：

- RHEL 8 /CentOS 8

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

Ubuntu 18.04 風格版本 2 版本發布 13

V-219157, V-219158, V-219177, V-219212 V-219308, 愿意, 鼎立, 和朋友 V-219314 V-219316 V-251507

Ubuntu 20.04 風格版本 1 版本發布 11

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

歷史版本

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。

2024 年第一季度變更-二零二四年六月二日：

針對 2024 年第一季發行版本更新 STIG 版本和套用的 STIG，如下所示：

標籤構建-亞歷克斯-低版本 2024.1.x

- RHEL 7 風格版本 3 版本 14
- RHEL 8 風格版本 1 版本 13
- Ubuntu 18.04 風格版本 2 版本發布 13
- Ubuntu 20.04 風格版本 1 版本發布 11

標籤構建-亞麻-中型版本 2024.1.x

- RHEL 7 風格版本 3 版本 14
- RHEL 8 風格版本 1 版本 13
- Ubuntu 18.04 風格版本 2 版本發布 13
- Ubuntu 20.04 風格版本 1 版本發布 11

標籤構建-亞麻-高版本 2024.1.x

- RHEL 7 風格版本 3 版本 14
- RHEL 8 風格版本 1 版本 13
- Ubuntu 18.04 風格版本 2 版本發布 13
- Ubuntu 20.04 風格版本 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：

針對 2023 年第四季發行的 STIG 版本和套用的 STIG 更新如下：

標籤構建-亞麻-低版本 2023.4.x

- RHEL 7 風格版本 3 版本 13
- RHEL 8 風格版本 1 版本 12
- Ubuntu 18.04 風格版本 2 版本發布 12
- Ubuntu 20.04 風格版本 1 版本發布 10

標籤構建-亞麻-中型版本 2023.4.x

- RHEL 7 風格版本 3 版本 13
- RHEL 8 風格版本 1 版本 12
- Ubuntu 18.04 風格版本 2 版本發布 12
- Ubuntu 20.04 風格版本 1 版本發布 10

標籤構建-亞麻-高版本 2023.4.x

- RHEL 7 風格版本 3 版本 13
- RHEL 8 風格版本 1 版本 12
- Ubuntu 18.04 風格版本 2 版本發布 12
- Ubuntu 20.04 風格版本 1 版本發布 10

二零二三年第三季變更-二零二三年四月十日：

針對 2023 年第三季發行的 STIG 版本和套用的 STIG 更新，如下所示：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 12
- RHEL 8 風格版本 1 版本 11
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 1 發布版本 9

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 12
- RHEL 8 風格版本 1 版本 11
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 1 發布版本 9

高分類 (類別一)

- RHEL 7 風格版本 3 版本 12

- RHEL 8 風格版本 1 版本 11
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 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：

針對 2023 年第二季發行的 STIG 版本和套用的 STIG 更新如下：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 11
- RHEL 8 風格版本 1 發布 10
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 1 版本發布 8

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 11
- RHEL 8 風格版本 1 發布 10
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 1 版本發布 8

高分類 (類別一)

- RHEL 7 風格版本 3 版本 11
- RHEL 8 風格版本 1 發布 10
- Ubuntu 18.04 風格版本 2 版本發布 11
- Ubuntu 20.04 風格版本 1 版本發布 8

二零二三年第一季度變動-2023 年 3 月 27 日：

針對 2023 年第一季發行的 STIG 版本和套用的 STIG 更新，如下所示：

低分級 (類別三)

- RHEL 7 風格版本 3 發布 10

- RHEL 8 風格版本 1 版本 9
- Ubuntu 18.04 風格版本 2 版本發布 10
- Ubuntu 20.04 風格版本 1 版本發布 7

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 發布 10
- RHEL 8 風格版本 1 版本 9
- Ubuntu 18.04 風格版本 2 版本發布 10
- Ubuntu 20.04 風格版本 1 版本發布 7

高分類 (類別一)

- RHEL 7 風格版本 3 發布 10
- RHEL 8 風格版本 1 版本 9
- Ubuntu 18.04 風格版本 2 版本發布 10
- Ubuntu 20.04 風格版本 1 版本發布 7

二零二二年第四季變更-二零二三年一月二日：

針對 2022 年第四季發布的 STIG 版本和應用的 STIG 更新如下：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 9
- RHEL 8 風格版本 1 版本 8
- Ubuntu 18.04 風格版本 2 版本 9
- Ubuntu 20.04 風格版本 1 發布版本 6

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 9
- RHEL 8 風格版本 1 版本 8
- Ubuntu 18.04 風格版本 2 版本 9
- Ubuntu 20.04 風格版本 1 發布版本 6

高分類 (類別一)

- RHEL 7 風格版本 3 版本 9
- RHEL 8 風格版本 1 版本 8
- Ubuntu 18.04 風格版本 2 版本 9
- Ubuntu 20.04 風格版本 1 發布版本 6

2022 年第三季度變動-二零二二年九月三十日 (不變) :

對於 2022 年第三季發行的 Linux 元件 STIG，並沒有任何變更。

二零二年第二季度變動：

針對 2022 年第二季發行版推出 Ubuntu 支援、更新的 STIG 版本，以及套用 STIG，如下所示：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 7
- RHEL 8 風格版本 1 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)

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 7
- RHEL 8 風格版本 1 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)

高分類 (類別一)

- RHEL 7 風格版本 3 版本 7
- RHEL 8 風格版本 1 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。將先前的 AL2 指令碼與 RHEL 7 結合在一起。針對 2022 年第一季發布的 STIG 版本和應用的 STIG 更新如下：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 6
- RHEL 8 風格版本 1 版本 5

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 6
- RHEL 8 風格版本 1 版本 5

高分類 (類別一)

- RHEL 7 風格版本 3 版本 6
- RHEL 8 風格版本 1 版本 5

二零二一年第四季度變更：

更新了 STIG 版本，並在 2021 年第四季度發布中應用了 STIGS，如下所示：

低分級 (類別三)

- RHEL 7 風格版本 3 發布 5
- RHEL 8 風格版本 1 版本 4

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 發布 5
- RHEL 8 風格版本 1 版本 4

高分類 (類別一)

- RHEL 7 風格版本 3 發布 5

- RHEL 8 風格版本 1 版本 4

二零二一年第三季變更-九月三十日：

更新了 STIG 版本，並在 2021 年第三季度發布中應用了 STIGS，如下所示：

低分級 (類別三)

- RHEL 7 風格版本 3 版本 4
- RHEL 8 風格版本 1 版本 3

斯蒂格中型 (類別二)

- RHEL 7 風格版本 3 版本 4
- RHEL 8 風格版本 1 版本 3

高分類 (類別一)

- RHEL 7 風格版本 3 版本 4
- RHEL 8 風格版本 1 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在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，則自動化會使用提ServerEdition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。
- 是 3 PresignedUrl

  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: 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AWSPremiumSupport-ChangeInstanceTypeIntelToAMD冊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yes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runningpending、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。
10. aws: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。
11. aws:executeAwsApi：傳回具有相同記憶體和 vCPU 數量的 AMD 執行個體類型清單。
12. aws: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。
13. aws: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。
14. aws:branch：根據DryRun參數值是否為分支自動化yes。
15. aws: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。
16. aws:executeAwsApi：取得目前執行個體狀態。
17. aws:changeInstanceState：停止亞馬遜 EC2 實例。
18. aws:changeInstanceState：如果執行個體停留在停止狀態，則強制停止執行個體。
19. aws:executeAwsApi：將執行個體類型變更為目標 AMD 執行個體類型。
20. aws:sleep: 為了達到最終一致性，變更執行個體類型後等待 3 秒。
21. aws: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。

22aws: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:DescribeInstancesTypes

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

AWSSupport-CopyEC2Instance

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 V PC？ 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 E BS？
- 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。
- copyAmiTo區域-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。 DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

Description

手冊可AWSSupport-EnableWindowsEC2SerialConsole協助您在 Amazon EC2 Windows 執行個體上啟用亞馬遜 EC2 序列主控台、特殊管理主控台 (SAC) 和開機功能表。使用 Amazon Elastic Compute Cloud (Amazon EC2) 序列主控台功能，您可以存取 Amazon EC2 執行個體的序列埠，以便對開機、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自動化手冊有助於在運行 Microsoft Windows 服務器的 Amazon EC2 實例上啟用 SAC 和啟動菜單。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，以啟用 SAC 和開機功能表。對於處於停止狀態或未受管理的執行個體 AWS Systems Manager，執行手冊會使用 AWSSupport-StarteC2 RescueWorkflow 建立暫時性的 Amazon EC2 執行個體，以離線執行所需的變更。

如需詳細資訊，請參閱適用於 Windows 執行個體的 Amazon EC2 序列

> **Important**
>
> - 如果您在執行個體上啟用 SAC，依賴密碼擷取的 Amazon EC2 服務將無法從 Amazon EC2 主控台運作。如需詳細資訊，請參閱使用 SAC 疑難排解您的 Windows 執行個體。
> - 若要設定序列主控台的存取權，您必須在帳戶層級授予序列主控台存取權，然後設定 AWS Identity and Access Management (IAM) 政策以授予使用者存取權。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，請參閱設定對 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

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。

```
{
    "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 Amazon EC2 序列主控台 (SAC) 和開機功能表的 Amazon EC2 執行個體識別碼。
   - AutomationAssumeRole: (選擇性)

     IAM 角色的 Amazon 資源名稱 (ARN)，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。
   - HelperInstanceType: (有條件)

     執行手冊佈建用於為離線執行個體設定 Amazon EC2 序列主控台的 Amazon EC2 執行個體類型。
   - HelperInstanceProfileName: (有條件)

     協助程式執行個體的現有 IAM 執行個體設定檔名稱。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 boot 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，則自動化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。

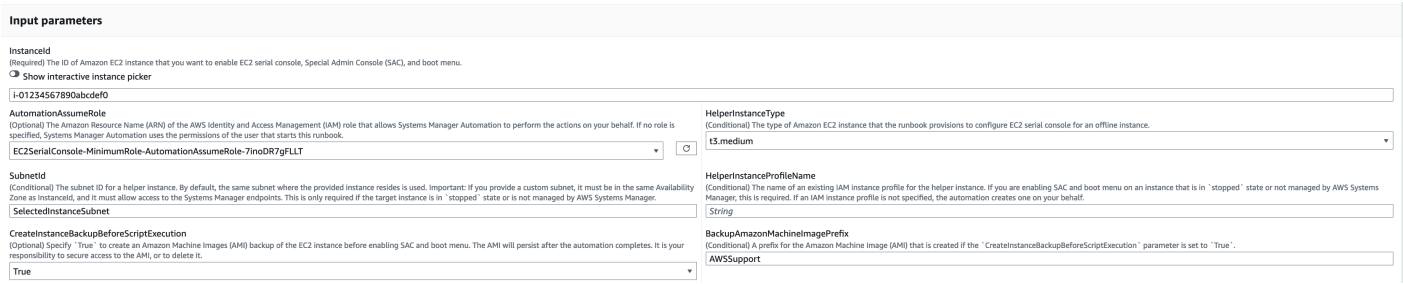
> **Important**
>
> 如果您提供自訂子網路，則該子網路必須與其位於相同的可用區域中 InstanceId，而且必須允許存取 Systems Manager 端點。只有在目標執行處於停止狀態或不受管理時，才需要這樣做 AWS Systems Manager。

- CreateInstanceBackupBeforeScriptExecution: (選擇性)

  指定 True 可在啟用 SAC 和開機功能表之前建立 Amazon EC2 執行個體的亞馬遜機器映像 (AMI) 備份。自動化完成之後，AMI 會持續存在。您有責任保護 AMI 的訪問或刪除它。

- BackupAmazonMachineImagePrefix: (有條件)

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



4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：

   - CheckIfEc2SerialConsoleAccessEnabled:

     檢查是否已在帳戶層級啟用 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。

   - CheckIfEc2InstanceIsWindows:

     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。

   - CheckIfInstanceTypeIsNitro:

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。

- CheckIfInstanceIsInAutoScaling群組：

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

- WaitForEc2InstanceStateStablized:

  等待執行處理處於執行中或已停止狀態。

- 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 InstanceIsManagedBy 特殊傳統管理：

  檢查執行個體是否由管理 AWS Systems Manager。如果受管理，runbook 會使用 PowerShell 執行命令啟用 SAC 和開機功能表。

- BranchOnPreEC2RescueBackup：

  根據`CreateInstanceBackupBeforeScriptExecution`輸入參數進行分支。

- CreateAmazonMachineImageBackup:

  建立執行個體的 AMI 備份。

- 啟用交流：AndBootMenu

  透過執行「 PowerShell 執行命令」指令碼啟用 SAC 和開機功能表。

- RebootInstance:

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

- CheckIfHelperInstanceProfileIsProvided:

在使用臨時 Amazon EC2 執行個體離線啟用 SAC 和開機功能表之前，檢查HelperInstanceProfileName指定項目是否存在。

- RunAutomationToInjectOfflineScriptFor功能包括AndBootMenu：

  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：

   - 啟用輸AndBootMenu出：

     在步驟中執行命令的輸EnableSACAndBootMenu出。

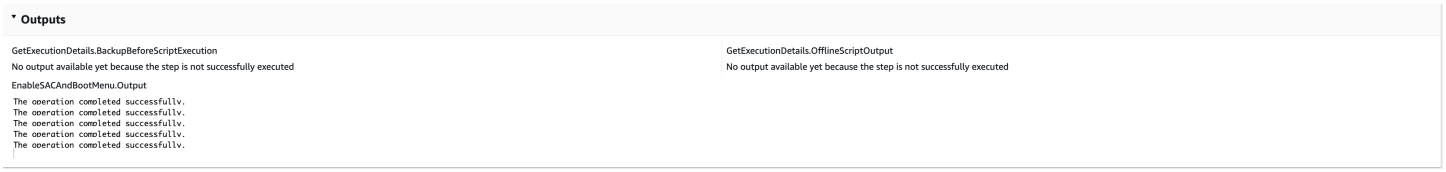
   - GetExecutionDetails.OfflineScriptOutput:

     在步驟中執行的離線指令碼輸RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu出。

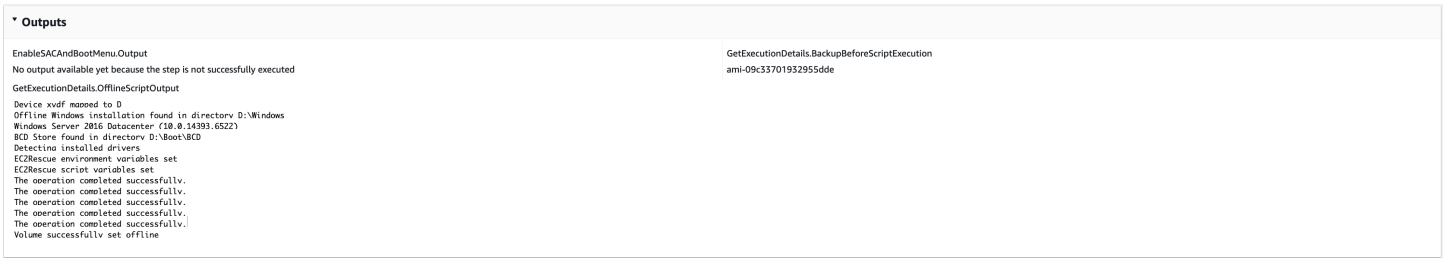
   - GetExecutionDetails.BackupBeforeScriptExecution:

     如果CreateInstanceBackupBeforeScriptExecution輸入參數為 True，則採用 AMI 備份的映像識別碼。

執行及管理的執行個體上的執行輸出 AWS Systems Manager



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



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-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-Classic 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

g etInstanceProperties.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。

AWSSupport-MigrateXenToNitroLinux

Description (描述)

執行手AWSSupport-MigrateXenToNitroLinux冊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AWSSupport-CloneXenEC2InstanceAndMigrateToNitro冊。
- 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。
- getXenInstanceTypeDetails-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Nitro體類型執行。
- checkIfTargetInstanceLifecycleIsSpot-檢查目標執行個體的購買選項是否為 Spot。
- checkIfOperatingSystemIsLinux-檢查目標執行個體作業系統是否為 Linux。
- verifySSMConnectivityForTargetInstance-驗證目標執行個體是否由系統管理員管理。
- checkIfEphemeralVolumeAreSupported-檢查目標執行個體的目前執行個體類型是否支援執行個體儲存磁碟區。
- 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工作流程會執行與工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Nitro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其 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的使用者，此執行手冊特別有用。Runbook 會在您的 AWS Identity and Access Management (IAM) 角色中建立一個暫時的 Amazon EC2 執行個體， AWS 帳戶 並具有擷取包含密碼的 AWS Secrets Manager 秘密值的權限。

執行手冊會停止您的目標 Amazon EC2 執行個體、分離根目錄亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區，並將其附加到暫時的 Amazon EC2 執行個體。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 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 磁碟區使用客戶受管 AWS Key Management Service (AWS KMS) 金鑰加密，請確定金 AWS KMS 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

  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。
- InstanceId

  類型：字串

  說明：(必要) 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。
- LinuxUser姓名

  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：(必要) 包含新密碼的 Secrets Manager 密碼的 ARN。
- SecurityGroup身份證

類型：字串

說明：(選用) 要連接到暫時 Amazon EC2 執行個體的安全群組 ID。如果您未提供此參數的值，則會使用預設的 Amazon Virtual Private Cloud (Amazon VPC) 安全群組。

- SubnetId

  類型：字串

  說明：(選用) 您要在其中啟動 Amazon EC2 臨時執行個體的子網路識別碼。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：(選用) 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 許可

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

- `ssm:DescribeInstanceInformation`
- `ssm:ListTagsForResource`
- `ssm:SendCommand`

- ec2:AttachVolume
- ec2:CreateSnapshot
- ec2:CreateSnapshots
- ec2:CreateVolume
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeSnapshotAttribute
- ec2:DescribeSnapshots
- ec2:DescribeSnapshotTierStatus
- ec2:DescribeVolumes
- ec2:DescribeVolumeStatus
- ec2:DetachVolume
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudformation:CreateStack
- cloudformation:DeleteStack
- cloudformation:DescribeStackResource
- cloudformation:DescribeStacks
- cloudformation:ListStacks
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:PutLogEvents

文件步驟

1. aws:branch— 根據您是否已提供停止目標 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或狀stopped態。否則，自動化結束。
3. aws:executeAwsApi取得亞馬遜 EC2 執行個體屬性。
4. aws:executeAwsApi取得根磁碟區屬性。
5. aws:branch根據是否提供臨時 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 實例架構是arm64或x86_64。
9. aws:assertAwsResourceProperty確保 Amazon EC2 實例關閉行為是stop和不是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。如果執行個體屬於自 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 執行個體正在執行。
14. aws:executeAwsApi取得臨時亞馬遜 EC2 執行個體的識別碼。
15. aws:waitForAwsResourceProperty等待臨時 Amazon EC2 執行個體報告為由系統管理員所管理。
16. aws:changeInstanceState停止目標 Amazon EC2 實例。
17. aws:changeInstanceState強制目標 Amazon EC2 執行個體停止，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建立目標 Amazon EC2 執行個體根目錄 Amazon EBS 磁碟區的快照。
20. aws:waitForAwsResourceProperty等待快照處於某個狀completed態。
21. aws:executeAwsApi從目標 Amazon EC2 執行個體卸離亞馬遜 EBS 根磁碟區。
22. aws:waitForAwsResourceProperty等待 Amazon EBS 根磁碟區從目標亞馬遜 EC2 執行個體分離。
23. aws:executeAwsApi將根 Amazon EBS 磁碟區附加到暫時的亞馬遜 EC2 執行個體。

24 aws:waitForAwsResourceProperty 等待 Amazon EBS 根磁碟區連接到臨時的亞馬遜 EC2 執行個體。

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 從暫時的 Amazon EC2 執行個體卸離亞馬遜 EBS 根磁碟區。

27 aws:waitForAwsResourceProperty 等待 Amazon EBS 根磁碟區從臨時的亞馬遜 EC2 執行個體分離。

28 aws:executeAwsApi 發生錯誤後，將 Amazon EBS 根磁碟區從暫存的 Amazon EC2 執行個體卸離。

29 aws:waitForAwsResourceProperty 發生錯誤後，等待亞馬遜 EBS 根磁碟區從臨時的 Amazon EC2 執行個體中分離。

30 aws: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。

31 aws:executeAwsApi 將根 Amazon EBS 磁碟區重新連接到目標亞馬遜 EC2 執行個體。

32 aws:waitForAwsResourceProperty 等待 Amazon EBS 根磁碟區連接到亞馬遜 EC2 執行個體。

33 aws:executeAwsApi 從目標 Amazon EC2 執行個體根磁碟區快照建立新的 Amazon EBS 磁碟區。

34 aws:waitForAwsResourceProperty 等待直到新的 Amazon EBS 卷處於狀態。available

35 aws:executeAwsApi 將新的 Amazon EBS 磁碟區連接到目標執行個體做為根磁碟區。

36 aws:waitForAwsResourceProperty 等待 Amazon EBS 卷處於一個attached狀態。

37 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。

38 aws: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。

39 aws:changeInstanceState 視需要啟動亞馬遜 EC2 執行個體。

40 aws:waitForAwsResourceProperty 在刪除之前，請等待 AWS CloudFormation 堆棧處於終端狀態。

41 aws:executeAwsApi 刪除包含臨時 Amazon EC2 執行個體的 AWS CloudFormation 堆疊。

AWSPremiumSupport-ResizeNitroInstance

Description (描述)

該手AWSPremiumSupport-ResizeNitroInstance冊提供了一個自動化的解決方案，用於調整在硝基系統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yes為AllowInstanceStoreInstances和AllowCloudFormationInstances參數指定。

runbook 提供兩種不同的方法來指定您要變更為的執行個體類型：

- 對於以單一執行個體為目標的簡單自動化，請使用TargetInstanceTypeFromParameter參數指定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runningpending、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。

15aws: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。

16aws: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。

17aws: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。

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 Amazon EC2 執行個體變更為其原始類型。

iv. aws:sleep: 為了達到最終一致性，變更執行個體類型後等待 3 秒。

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。

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。
15. aws:waitForAwsResourceProperty-等待磁碟區狀態為available。
16. aws:waitForAwsResourceProperty-等待執行個體狀態為stopped。
17. aws:executeAwsApi-分離根磁碟區。
18. aws:waitForAwsResourceProperty-等待根磁碟區分離。
19. aws:executeAwsApi-附加新的根磁碟區。
20. aws:waitForAwsResourceProperty-等待要連接的新磁碟區。
21. aws:executeAwsApi-啟動實例。
22. aws:waitForAwsResourceProperty-等待執行個體狀態為available。
23. aws:waitForAwsResourceProperty-等待系統和執行個體狀態檢查通過執行個體。
24. aws:executeScript-執行指令碼以尋找可用來成功建立磁碟區的快照。
25. aws: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。
26. aws: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 (描述)

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載至協助程式執行個體，也稱為 EC2Rescue 執行個體。如果您的執行個體是 Windows，請提供 Powershell 指令碼。否則，請使用 Bash。runbook 設置一些您可以在腳本中使用的環境變量。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**
>
> 此自動化不支援從商城亞馬遜機器映像 (AMI) 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]::Unicode.GetBytes([System.IO.File]::Rea
```

Bash：

```
base64 PATH_TO_FILE
```

以下為您可在離線指令碼中使用的環境變數清單 (取決於目標作業系統)

Windows：

變數	描述	範例值
$env:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
$env:EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
$env:EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
$env:EC2RESCUE_EC2RW_DIR	適用於 Windows 安裝路徑的 EC2Rescue	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EC2RW_DIR	適用於 Windows 安裝路徑的 EC2Rescue	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b

變數	描述	範例值
$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	離線 Windows 目前控制集路徑	HKLM:\AWSTempSystem\ControlSet001
$env:EC2RESCUE_OFFLINE_DRIVE	離線 Windows 磁碟機字母	D:\
$env:EC2RESCUE_OFFLINE_EBS_DEVICE	離線根磁碟區 EBS 裝置	xvdf
$env:EC2RESCUE_OFFLINE_KERNEL_VER	離線 Windows 核心版本	6.1.7601.24214
$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	離線 Windows 架構	AMD64
$env:EC2RESCUE_OFFLINE_OS_CAPTION	離線 Windows 字幕	Windows Server 2008 R2 Datacenter
$env:EC2RESCUE_OFFLINE_OS_TYPE	離線 Windows 作業系統類型	伺服器
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	離線 Windows 程式檔案目錄路徑	D:\Program Files
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	離線 Windows 程式檔案 x86 目錄路徑	D:\Program Files (x86)
$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	離線 Windows 登錄檔目錄路徑	D:\Windows\System32\config
$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT	離線 Windows 系統根目錄路徑	D:\Windows
$env:EC2RESCUE_REGION	{{ global:REGION }}	us-west-1

變數	描述	範例值
$env:EC2RESCUE_S3_BUCKET	{{S3BucketName}}	mybucket
$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	離線 Windows 安裝中繼資料	客戶 Powershell 物件

Linux：

變數	描述	範例值
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	適用於 Linux 安裝路徑的 EC2Rescue	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	離線裝置名稱	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	離線根磁碟區 EBS 裝置	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	離線根磁碟區掛載點	/mnt/mount

變數	描述	範例值
EC2RESCUE_PYTHON	Python 版本	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3BucketName}}	mybucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

文件類型

自動化

擁有者

Amazon

平台

Linux,macOS, Windows

參數

- AMIPrefix

  類型：字串

  預設：`AWSSupport-EC2Rescue`

  描述：(選用) 備份 AMI 名稱的字首。
- AutomationAssumeRole

  類型：字串

  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。

- CreatePostEC2 RescueBackup

  類型：字串

  有效值：true | false

  預設：false

  說明：(選擇性) 將其設定`true`為在執行指令碼之InstanceId後建立 AMI，然後再啟動指令碼。自動化完成之後，AMI 會持續存在。您有責任保護對 AMI 的存取，或是將其刪除。

- CreatePreEC2 RescueBackup

  類型：字串

  有效值：true | false

  預設：false

  說明：(選擇性) 將其設定`true`為InstanceId在執行指令碼之前建立的 AMI。自動化完成之後，AMI 會持續存在。您有責任保護對 AMI 的存取，或是將其刪除。

- EC2 RescueInstanceType

  類型：字串

  有效值：2. 小 | 2. 中等

  預設：t2.small

  描述：(選用) EC2Rescue 執行個體的 EC2 執行個體類型。

- InstanceId

  類型：字串

  描述：(必要) EC2 執行個體的 ID。重要：AWS Systems Manager 自動化會停止此執行個體。存放在執行個體存放磁碟區的資料會遺失。如果您不是使用彈性 IP，則公有 IP 位址會變更。

- OfflineScript

  類型：字串

  描述：(必要) 對協助程式執行個體執行的 Base64 編碼指令碼。如果您的源代碼實例是 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

  描述：(選用) EC2Rescue 執行個體的子網路 ID。根據預設，會使用與提供的執行個體所在相同的子網路。重要事項：如果您提供自訂子網路，它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：{{ automation:EXECUTION_ID }}

  描述：(選用) 自動化操作的唯一識別碼。

必要的 IAM 許可

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

建議執行自動化的使用者附加了 AmazonSSM AutomationRole IAM 管理政策。除了該政策，使用者必須擁有：

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

```
                    "Action": [
                        "lambda:InvokeFunction",
                        "lambda:DeleteFunction",
                        "lambda:GetFunction"
                    ],
                    "Resource": "arn:aws:lambda:*:An-AWS-Account-
ID:function:AWSSupport-EC2Rescue-*",
                    "Effect": "Allow"
                },
                {
                    "Action": [
                        "s3:GetObject",
                        "s3:GetObjectVersion"
                    ],
                    "Resource": [
                        "arn:aws:s3:::awssupport-ssm.*/*.template",
                        "arn:aws:s3:::awssupport-ssm.*/*.zip"
                    ],
                    "Effect": "Allow"
                },
                {
                    "Action": [
                        "iam:CreateRole",
                        "iam:CreateInstanceProfile",
                        "iam:GetRole",
                        "iam:GetInstanceProfile",
                        "iam:PutRolePolicy",
                        "iam:DetachRolePolicy",
                        "iam:AttachRolePolicy",
                        "iam:PassRole",
                        "iam:AddRoleToInstanceProfile",
                        "iam:RemoveRoleFromInstanceProfile",
                        "iam:DeleteRole",
                        "iam:DeleteRolePolicy",
                        "iam:DeleteInstanceProfile"
                    ],
                    "Resource": [
                        "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
                        "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport-
EC2Rescue-*"
                    ],
                    "Effect": "Allow"
                },
                {
```

```
                    "Action": [
                        "lambda:CreateFunction",
                        "ec2:CreateVpc",
                        "ec2:ModifyVpcAttribute",
                        "ec2:DeleteVpc",
                        "ec2:CreateInternetGateway",
                        "ec2:AttachInternetGateway",
                        "ec2:DetachInternetGateway",
                        "ec2:DeleteInternetGateway",
                        "ec2:CreateSubnet",
                        "ec2:DeleteSubnet",
                        "ec2:CreateRoute",
                        "ec2:DeleteRoute",
                        "ec2:CreateRouteTable",
                        "ec2:AssociateRouteTable",
                        "ec2:DisassociateRouteTable",
                        "ec2:DeleteRouteTable",
                        "ec2:CreateVpcEndpoint",
                        "ec2:DeleteVpcEndpoints",
                        "ec2:ModifyVpcEndpoint",
                        "ec2:Describe*"
                    ],
                    "Resource": "*",
                    "Effect": "Allow"
                }
            ]
        }
```

文件步驟

1. aws:executeAwsApi-描述提供的實例
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-檢查根磁碟區沒有加密
5. aws:assertAwsResourceProperty-檢查提供子網 ID
   a. (使用目前執行個體子網路)-如果 * SubnetId = SelectedInstanceSubnet * 則執行aws:createStack以部署 EC2 CloudFormation Rescue 堆疊
   b. (建立新的虛擬私人雲端)-如果 * SubnetId = CreateNew 虛擬私人雲端 *，則執行aws:createStack以部署 EC2Rescue 堆疊 CloudFormation
   c. (使用自訂子網路) - 所有其他情況：

aws:assertAwsResourceProperty-檢查提供的子網是否與提供的實例位於相同的可用區域

aws:createStack-部署 EC2Rescue 堆疊 CloudFormation

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-說明 EC2Rescue CloudFormation 堆疊輸出，以取得 EC2Rescue 協助程式執行個體識別碼
10. aws:waitForAwsResourceProperty-等待 EC2Rescue 輔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 CreatePre EC2 RescueBackup 輸入值
    a. (建立 EC2 救援前備份)-如果 * EC2 = 真 * CreatePre RescueBackup
    b. aws:executeAwsApi-建立所提供執行個體的 AMI 備份
    c. aws:createTags-標記 AMI 備份
15. aws:runCommand-在 EC2Rescue 輔助程式執行個體上安裝 EC2Rescue
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-將根磁碟區連接至 EC2Rescue 輔助程式執行個體，做為 *xvdf*

       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-將根磁碟區連接至 EC2Rescue 輔助程式執行個體，做為 */dev/sdf*

       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 輔助程式執行個體

19.aws:changeInstanceState-強制停止 EC2Rescue 輔助程式執行個體

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

22.aws:assertAwsResourceProperty-檢查 CreatePost EC2 RescueBackup 輸入值

   a. (建立 EC2 救援後備份)-如果 * EC2 = 真 * CreatePost RescueBackup

   b. aws:executeAwsApi-建立所提供執行個體的 AMI 備份

   c. aws:createTags-標記 AMI 備份

23.aws: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

24.aws:changeInstanceState-恢復提供實例的初始狀態（運行/停止）

25.aws:deleteStack-刪除 EC2 CloudFormation 救援堆疊

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或者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。 ImageId

備份程式視窗。 ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Description

AWSSupport-TroubleshootEC2InstanceConnect自動化有助於分析和偵測錯誤，防止使用 Amazon EC2 執行個體連線到 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的 Connect 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、安全殼層 Connect 埠和亞馬遜資源名稱 (ARN) 作為 IAM 角色或使用者遇到 Amazon EC2 執行個體連接問題的使用者。然後，它會檢查使用 Amazon EC2 執行個體 Connect 連接至 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 EC2 執行個體 Connect 支援的AWS區域中。
- 該實例的 AMI 受到 Amazon EC2 實例 Connect 的支持。
- 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、網路 ACL 和路由表規則) 允許透過 Amazon EC2 執行個體連線至執行個體。
- 用於利用 Amazon EC2 執行個體 Connect 的 IAM 角色或使用者可以存取將金鑰推送到 Amazon EC2 執行個體。

Important

- 若要檢查執行個體 AMI、IMDSv2 可 Connect 性和 Amazon EC2 執行個體連接套件安裝，執行個體必須由 SSM 管理。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 SourceIp CIDR 作為輸入參數提供時，網路檢查才會偵測安全性群組和網路 ACL 規則是否封鎖流量。否則，它只會顯示與 SSH 相關的規則。
- 使用 Amazon EC2 執行個體 Connect 線端點的連線未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 許可

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)：

  IAM 角色的 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。

- 使用者名稱 (必填):

  用於使用 Amazon EC2 執行個體 Connect 連接到 Amazon EC2 執行個體的使用者名稱。它用於評估是否授予此特定用戶的 IAM 訪問權限。

- EC2 InstanceConnectRoleOrUser (必要)：

  正在利用 Amazon EC2 執行個體 Connect 將金鑰推送到執行個體的 IAM 角色或使用者的 ARN。

- 連接埠 (選擇性)：

  在亞馬遜 EC2 執行個體上設定的安全殼層連接埠。預設值為 22。連接埠號碼必須介於之間1-65535。

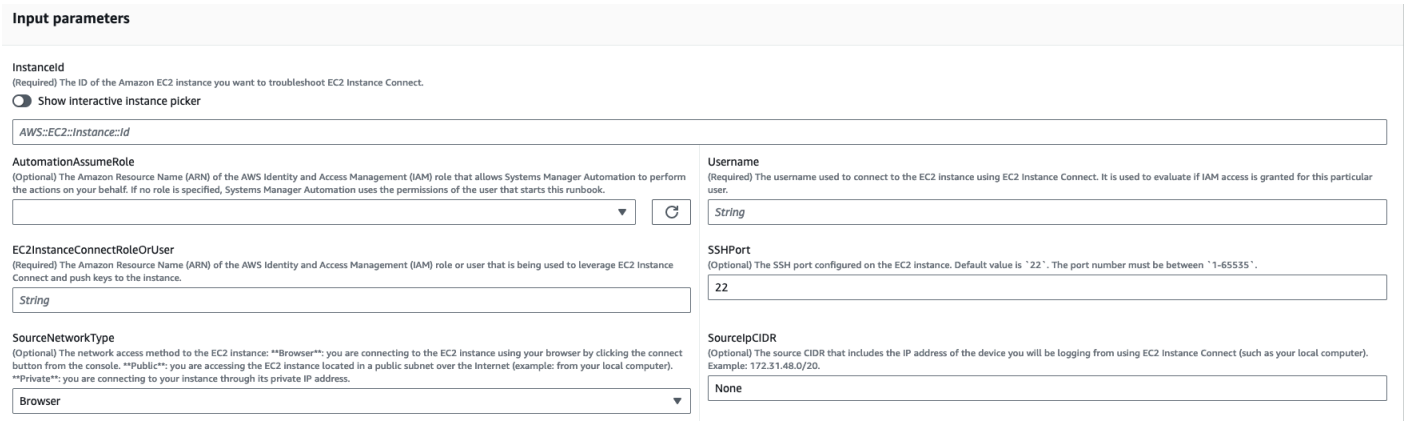
- SourceNetworkType (選擇性)：

  亞馬遜 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 CIDR。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，則執行手冊將不會評估 Amazon EC2 執行個體安全群組和網路 ACL 規則是否允許 SSH 流量。它將改為顯示與 SSH 相關的規則。



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:

     取得目前的 Amazon EC2 執行個體屬性 (PlatformDetails PublicIpAddress VpcId、、 SubnetId 和 MetadataHttpEndpoint)。
   - GatherInstanceInformationFrom特殊音量管理：

     如果執行個體受 SSM 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料。
   - CheckIfAWSRegionSupported:

     檢查 Amazon EC2 執行個體是否位於 Amazon EC2 執行個體 Connect 支援的AWS區域中。
   - BranchOnIfAWSRegionSupported:

     如果 Amazon EC2 執行個體 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。
   - CheckIfInstanceAMIIsSupported：

     檢查 Amazon EC2 執行個體 Connect 是否支援與執行個體相關聯的 AMI。
   - BranchOnIfInstanceAMIIsSupported：

如果支援執行個體 AMI，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 套件安裝和組態。否則，它會檢查 HTTP 中繼資料是否已使用 AWS API 啟用，然後進入網路檢查步驟。

- 檢查ReachabilityFromOs程式：

  在目標 Amazon EC2 Linux 實例上運行一個 Bash 腳本，以檢查它是否能夠訪問 IMDSv2。

- 方格PackageInstallation：

  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。

- 檢查 SSHConfigFromOs：

  在目標 Amazon EC2 Linux 執行個體上執行 Bash 指令碼，以檢查設定的安全殼層連接埠是否與輸入參數 `SSHport 相符。 `

- CheckMetadataHTTPEndpointIsEnabled:

  檢查執行個體中繼資料服務 HTTP 端點是否已啟用。

- 方格NetworkAccess：

  檢查網路組態 (安全群組、網路 ACL 和路由表規則) 是否允許透過 Amazon EC2 執行個體 Connect 到執行個體。

- 跳棋RoleOrUserPermissions:

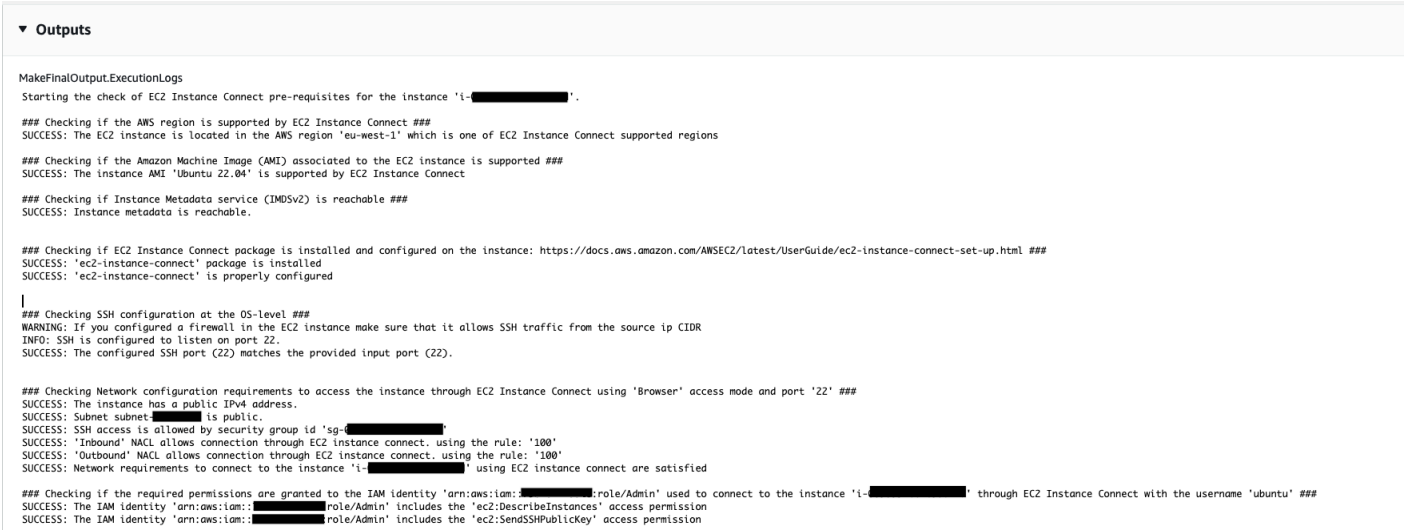
  檢查用於利用 Amazon EC2 執行個體 Connect 的 IAM 角色或使用者是否可以使用提供的使用者名稱將金鑰推送到 Amazon EC2 執行個體。

- MakeFinalOutput:

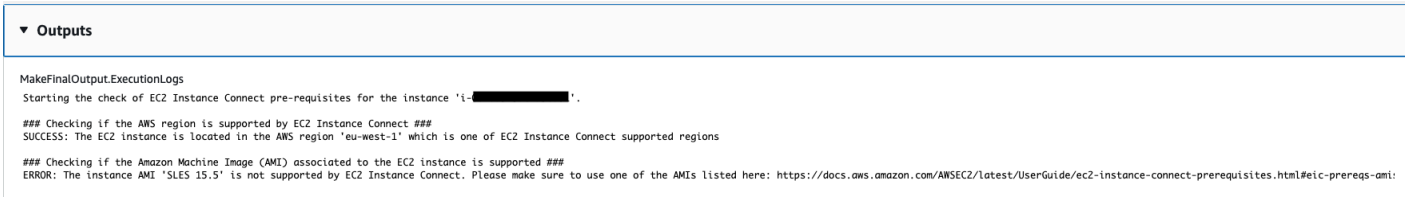
  合併所有先前步驟的輸出。

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：



不支援目標執行個體 AMI 的執行：



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 EC2 執行個體 Connect 連線到 Amazon EC2 執行個體的問題？

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:，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: 以及 ssm: DescribeInstances，GetAutomationExecution才能讀取自動化輸出。 AWSSupport-TroubleshootRDP執AWSSupport-ExecuteEC2Rescue行離線修復的呼叫-請檢閱的權限，以確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執Windows Server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-執行指PowerShell令碼以取得 Windows 防火牆資料檔狀態。

      aws:executeAutomation-獲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:，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: 以及 ssm: 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 Elastic Compute Cloud (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，請將最新EC2Rescue工具安裝到 Amazon EC2 Windows 執行個體以擷取事件和系統日誌，但不會分析所擷取的程序傾印和日誌EC2Rescue。

> **Important**
>
> - 要執行此操作手冊，Amazon EC2 Windows 實例必須由 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工EC2Rescue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 許可

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

- ec2:DescribeInstances
- ssm:DescribeAutomationExecutions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand
- s3:ListBucket

- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:PutObject
- s3:GetBucketAcl
- s3:GetAccountPublicAccessBlock

(選擇性) 附加在執行個體設定檔上的 IAM 角色或在執行個體上設定的 IAM 使用者需要執行下列動作，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)：

     (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)：

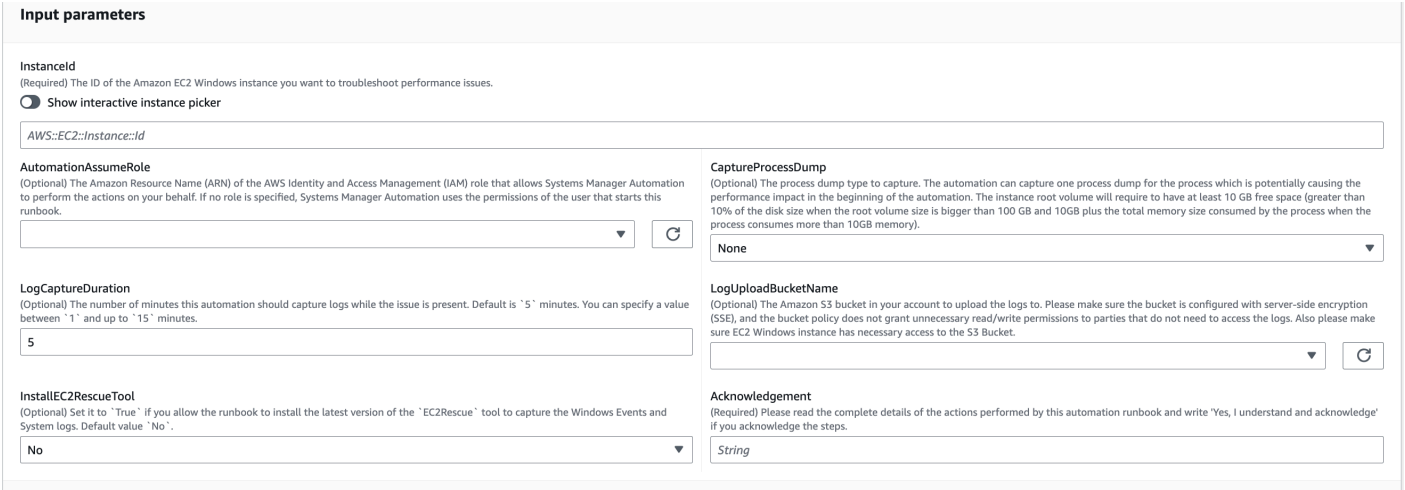
  您帳戶中要上傳日誌的 Amazon S3 儲存貯體。值區必須設定伺服器端加密 (SSE)，且儲存貯體政策不得將不必要的讀取/寫入權限授與不需要存取擷取記錄的對象。Amazon EC2 視窗執行個體必須能夠存取 Amazon S3 儲存貯體。

- 安裝 2RescueTool （ 可選 ）：

  設定為`Yes`以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`。



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:**

  聲明亞馬遜 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:**

  摘要在上一個步驟中產生的 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。它會生成類似的信息 LogicalDisk，網絡接口，內存，TCPv4，IPv4 和 UDpv4 的使用，並將其保存到analysis_output.log輸出文件夾中。

- **BranchOnInstallEC2Rescue:**

  如果您將其設定為在 Amazon EC2 執行個體中安裝最新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。 EC2Rescue僅擷取必要的記錄檔以節省空間。

- **BranchOnIfS3BucketProvided:**

  根據使用者輸入的分支，LogUploadBucketName以查看是否有值區名稱可用於上傳記錄。

- **GetS3BucketPublicStatus:**

  判斷是否提供 Amazon S3 儲存貯體，如果是，請確認 Amazon S3 儲存貯體不是公開的，且已使用 SSE 進行設定。

- **UploadLogResult:**

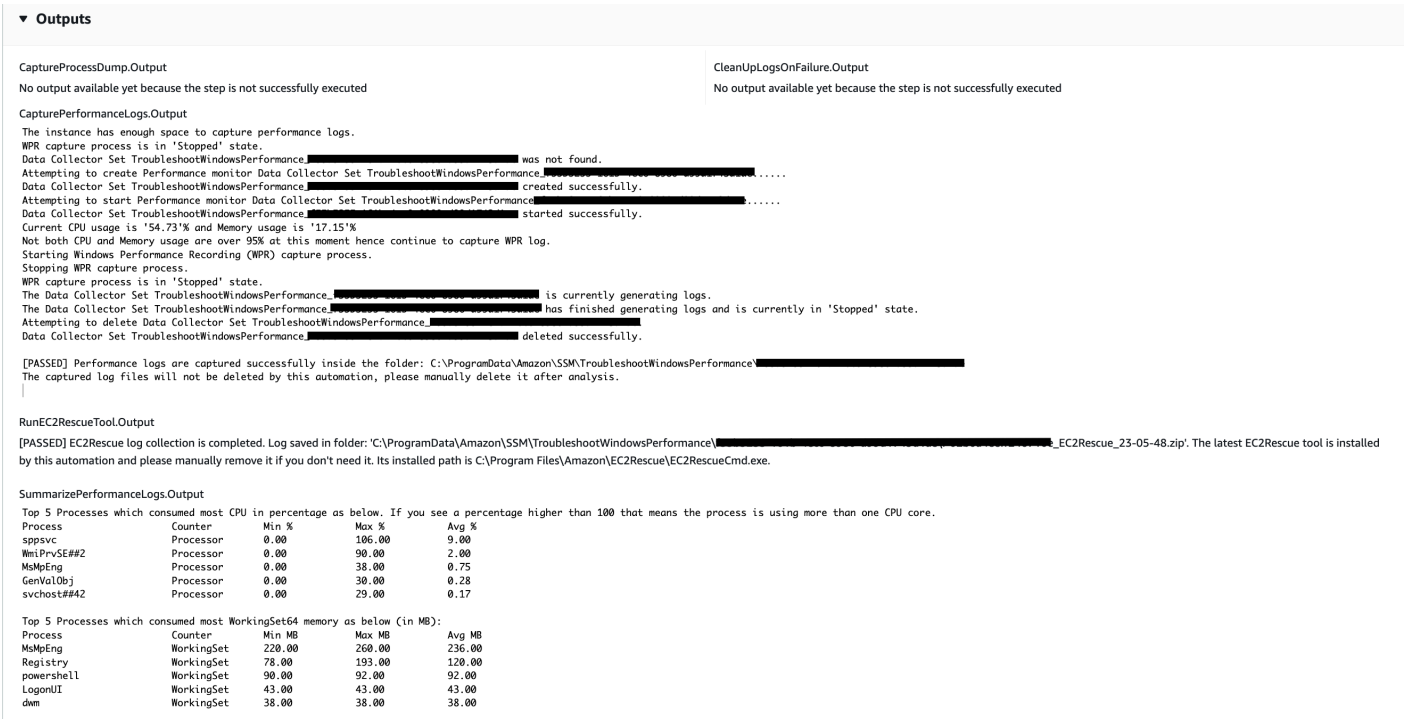
  將日誌上傳到提供的 Amazon S3 儲存貯體。如果 PowerShell 版本為 5.0 或更高版本，它會將日誌壓縮為 ZIP 存檔並上傳它們。它會在上傳完成後刪除 ZIP 文件。如果 PowerShell 版本低於 5.0，它將文件直接上傳到文件夾。

- **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

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

```
The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance_[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

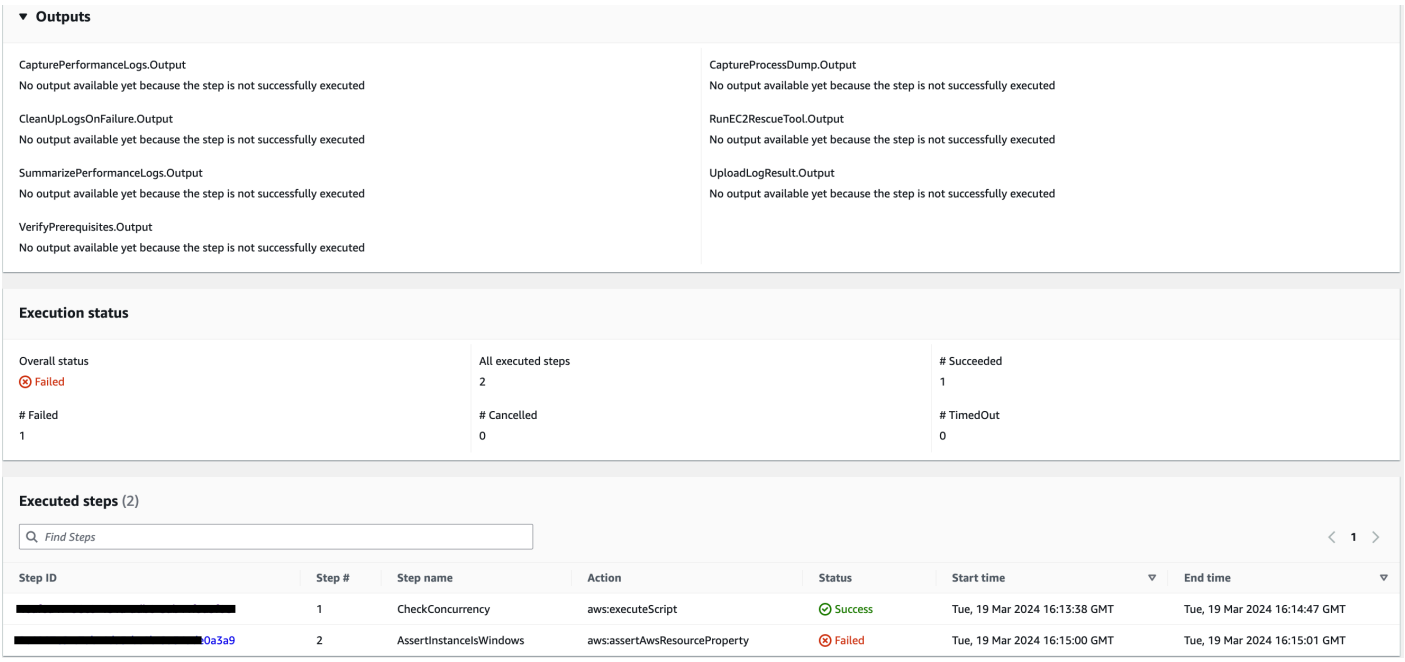
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]_EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program 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 %
sppsvc                  Processor       0.00            106.00          9.00
WmiPrvSE##2             Processor       0.00            90.00           2.00
MsMpEng                 Processor       0.00            38.00           0.75
GenValObj               Processor       0.00            30.00           0.28
svchost##42             Processor       0.00            29.00           0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):
Process                 Counter         Min MB          Max MB          Avg MB
MsMpEng                 WorkingSet      220.00          260.00          236.00
Registry                WorkingSet      78.00           193.00          120.00
powershell              WorkingSet      90.00           92.00           92.00
LogonUI                 WorkingSet      43.00           43.00           43.00
dwm                     WorkingSet      38.00           38.00           38.00
```

目標執行個體在 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

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output

No output available yet because the step is not successfully executed

UploadLogResult.Output

No output available yet because the step is not successfully executed

VerifyPrerequisites.Output

No output available yet because the step is not successfully executed

Execution status

Overall status	All executed steps	# Succeeded
Failed	2	1
# Failed	**# Cancelled**	**# TimedOut**
1	0	0

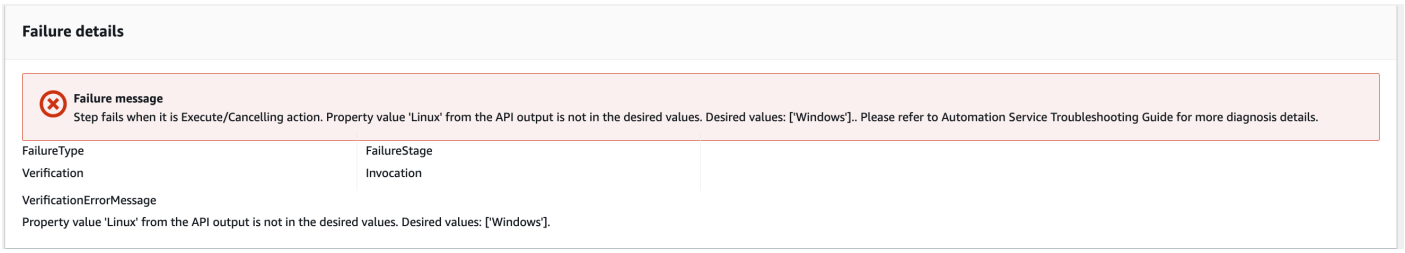
Executed steps (2)

Find Steps

1

Step ID	Step #	Step name	Action	Status	Start time	End time
[redacted]	1	CheckConcurrency	aws:executeScript	Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
[redacted]0a3a9	2	AssertInstancesIsWindows	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。



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-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 GetDeployablePatchSnapshotForInstanceAPI 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AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2冊的選項，以分析執行個體與 Amazon S3 端點的連線。

- 驗證 Windows 更新組態並測試 Windows 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：

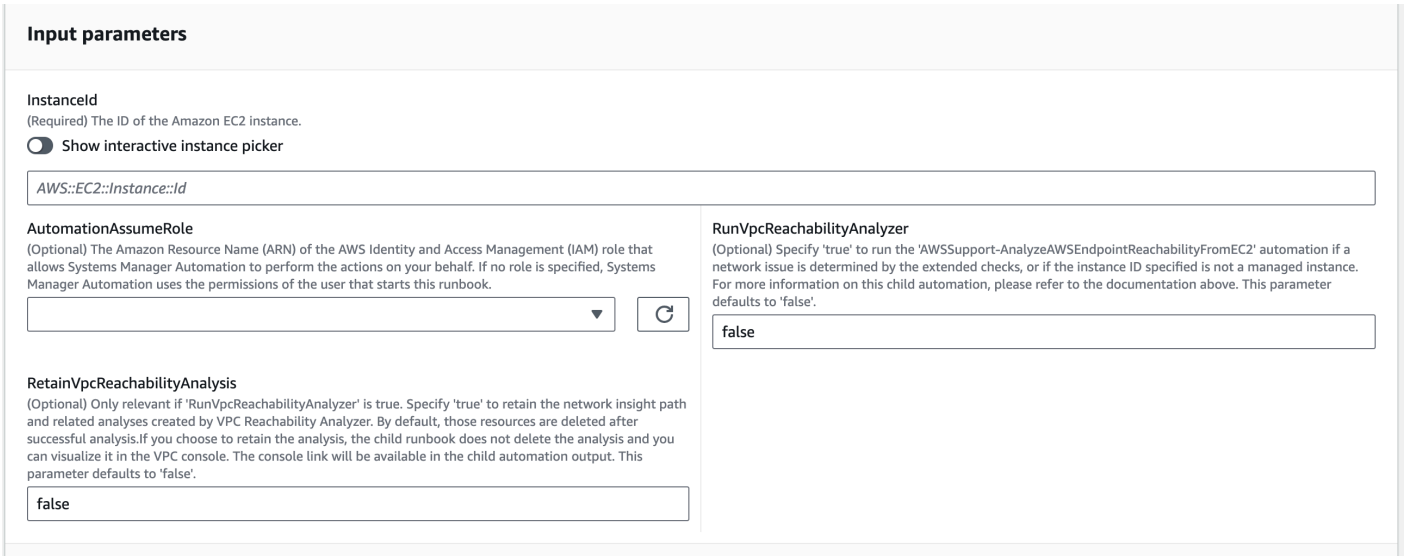
1. 瀏覽至「文件」下AWSSupport-TroubleshootWindowsUpdate的「Systems Manager」。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
   - AutomationAssumeRole （ 可選 ）：

     (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。



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\\Adminisrative 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 自動化工作流登陸頁

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 AmazonSSMManagedInstanceCore Amazon 受管政策附加到 IAM 角色以提供這些許可。不過，建議您針對此目的使用自動化 IAM 角色 AmazonSSMAutomationRole。如需詳細資訊，請參閱使用 IAM 設定自動化的角色。

如果您要執行離線升級，請參閱 AWSSupport-StartEC2RescueWorkflow 所需的許可。

文件步驟

1. aws:assertAwsResourceProperty-驗證輸入實例是否為 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`-斷言國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

執行手AWSSupport-CollectECSInstanceLogs冊會從 Amazon 彈性運算雲端 (Amazon EC2) 執行個體收集作業系統和 Amazon 彈性容器服務 (Amazon ECS) 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。為了協助確保從 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) 授予 All Users Amazon S3 預先定義群組的READ|WRITE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

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。

- ECS InstanceId

  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 許可

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

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- ssm:DescribeInstanceInformation

我們建議您在ECSInstanceId參數中指定的 Amazon EC2 執行個體具有 IAM 角色，並附加了 AmazonSSMManagedInstanceCore Amazon 受管政策。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，並在目錄中建立封存檔案。/var/log/collectECSlogs
- runLogCollectionScriptOnWindows-在 Windows 執行個體上收集作業系統和 Amazon ECS 相關的日誌檔案，並在目錄中建立封存檔案。C:\ProgramData\collectECSlogs
- 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

執行手AWS-InstallAmazonECSAgent冊會在您指定的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體上安裝亞馬遜 Elastic Container Service (Amazon ECS) 代理程式。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

  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。

- InstanceIds

  類型: StringList

  說明：(必填) 您要在其上安裝 Amazon ECS 代理程式的亞馬遜 EC2 執行個體識別碼。

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
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

文件步驟

aws:executeScript-在您在InstanceIds參數中指定的亞馬遜 EC2 執行個體上安裝 Amazon ECS 代理程式。

輸出

InstallAmazon電子代理。 SuccessfulInstances -Amazon ECS 代理程式安裝成功的執行個體識別碼。

InstallAmazon電子代理。 FailedInstances -安裝 Amazon ECS 代理程式失敗的執行個體識別碼。

InstallAmazon電子代理。 InProgressInstances -正在安裝 Amazon ECS 代理程式的執行個體識別碼。

AWS-ECSRunTask

Description

執行手AWS-ECSRunTask冊執行您指定的 Amazon Elastic Container Service (Amazon ECS) 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

  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。
- 容量 ProviderStrategy

  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) 要在其上執行工作的叢集的簡短名稱或 ARN。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。

- 啟用 ECs ManagedTags

  類型：布林值

  描述：(選用) 指定是否針對任務使用 Amazon ECS 受管標籤。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的標記您的 Amazon ECS 資源。

- 啟用 ExecuteCommand

  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`。

- 啟動類型

  類型：字串

  有效值：EC2 | 遠門 | 外部

  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

  說明：(選擇性) JSON 格式的容器覆寫清單，用來指定指定工作定義中的容器名稱，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。

- 放置約束

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。

- 放置策略

  類型：字串

  描述：(選用) 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。

- 由開始

  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 ListTasks API 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。

- 任務定義

  類型：字串

  描述：(選擇性) 要執行之作業定義的 AND `revision` (`family:revision`) 或完整 ARN。`family`如果未指定修訂，則會使用最新的`ACTIVE`修訂版本。

必要的 IAM 許可

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

- `ecs:RunTask`

文件步驟

`aws:executeScript`-根據您為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 (Amazon EC2) 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`ACTIVE`為。

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。
- ClusterName

  類型：字串

  說明：(必要) 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 許可

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

- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- iam:GetInstanceProfile

- iam:GetRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy

文件步驟

AWS：執行指令碼：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

AWSSupport-TroubleshootECSTaskFailedToStart執行手冊可協助您疑難排解 Amazon ECS 叢集中的亞馬遜彈性容器服務 (Amazon ECS) 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 許可
- VPC 端點連線能力
- 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 函數和必要的 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

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。
- ClusterName

  類型：字串

  描述：(必填) 任務無法啟動的 Amazon ECS 叢集名稱。
- CloudwatchRetention期間

  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

  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 許可

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

- `cloudtrail:LookupEvents`

- ec2:DeleteNetworkInterface
- ec2:DescribeInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ecr:DescribeImages
- ecr:GetRepositoryPolicy
- ecs:DescribeContainerInstances
- ecs:DescribeServices
- ecs:DescribeTaskDefinition
- ecs:DescribeTasks
- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:CreateFunction
- lambda:DeleteFunction

- lambda:GetFunctionConfiguration
- lambda:InvokeFunction
- lambda:TagResource
- logs:DescribeLogGroups
- logs:PutRetentionPolicy
- secretsmanager:DescribeSecret
- ssm:DescribeParameters
- sts:GetCallerIdentity

文件步驟

- aws:executeScript-驗證啟動自動化的使用者或角色是否具有必要的 IAM 許可。如果您沒有足夠的權限來使用此 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-如果分析確定需要測試的網路連線能力，請在 VPC 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-格式化自動化的輸出，以將分析結果返回到控制台。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進行分支。
- 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

執行手AWS-UpdateAmazonECSAgent冊會更新您指定的亞馬遜彈性運算雲端 (Amazon EC2) 執行個體上的亞馬遜彈性容器服務 (Amazon ECS) 代理程式。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

  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。
- 集群集

  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 許可

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeImage
- ec2:DescribeInstance
- ec2:DescribeInstanceAttribute

- ecs:DescribeContainerInstances
- ecs:DescribeClusters
- ecs:ListContainerInstances
- ecs:UpdateContainerAgent

文件步驟

aws:executeScript-更新您在參數中指定的 Amazon ECS 叢集上的 Amazon ECS 代理程式。ClusterARN

輸出

UpdateAmazon電子代理。 UpdatedContainers -Amazon ECS 代理程式更新成功的執行個體識別碼。

UpdateAmazon電子代理。 FailedContainers -Amazon ECS 代理程式更新失敗的執行個體識別碼。

UpdateAmazon電子代理。 InProgressContainers -正在進行 Amazon ECS 代理程式更新的執行個體識別碼。

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 (Amazon EFS) 檔案系統的先決條件，並將檔案系統掛接到您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。此執行手冊支援使用 DNS 名稱或使用掛接目標的 IP 位址掛接您的 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

  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。
- 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) 您要在其上掛載檔案系統之 Amazon EC2 執行個體的 ID。
- MountOptions

  類型：字串

  說明：(選擇性) 您要在掛載檔案系統時使用的 Amazon EFS 掛載協助程式支援的選項。如果您指定選`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 位址掛接可在停用 DNS 的環境中運作，例如停用 DNS 主機名稱的虛擬私有雲端 (VPC)。此外，如果您的環境使用 Amazon 路線 53（路線 53）以外的 DNS 提供商，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 許可

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

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:StartAutomationExecution
- iam:ListRoles

- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- elasticfilesystem:DescribeFileSystemPolicy
- elasticfilesystem:DescribeMountTargets
- elasticfilesystem:DescribeMountTargetSecurityGroups
- resource-groups:*

文件步驟

- aws:executeScript-收集有關您在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 上的流量來自您在參數中指定的 Amazon EC2 執行個體。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EfsId參InstanceId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-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup

- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups

AWSSupport-CollectEKSInstanceLogs

Description

執行手AWSSupport-CollectEKSInstanceLogs冊會從 Amazon 彈性運算雲端 (Amazon EC2) 執行個體收集作業系統和 Amazon 彈性 Kubernetes 服務 (Amazon EKS) 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 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) 授予 All Users Amazon S3 預先定義群組的READ|WRITE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 (Amazon EBS) 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

  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。
- EKS InstanceId

  類型：字串

  說明：(必填) 您要從中收集日誌的 Amazon EKS EC2 執行個體識別碼。
- 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 許可

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`

我們建議接收命令的 EC2 執行個體具有 IAM 角色，並附加了 Amazon SSM ManagedInstance 核心亞馬遜受管政策。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`-確認作業系統的`EKSInstanceId`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 (Amazon EKS) 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

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。
- ClusterName

  類型：字串

  描述：(必要) 叢集的唯一名稱。

- ClusterRole阿恩

  類型：字串

  說明：(必要) IAM 角色的 ARN，可為 Kubernetes 控制平面提供許可，以代表您呼叫 AWS API 作業。

- FargateProfile姓名

  類型：字串

  描述：(必要)「Fargate」設定檔的名稱。

- FargateProfileRoleArn

  類型：字串

  說明：(必要) Amazon EKS 網繭執行 IAM 角色的 ARN。

- FargateProfile选择器

  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

  說明：(必填) 您要用於 Amazon EKS 叢集的子網路識別碼。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 ID。

- EKS 訪問 EndpointPrivate

  類型：布林值

  預設：True

  說明：(選擇性) 將此值設定為`True`允許叢集的 Kubernetes API 伺服器端點進行私人存取。如果您啟用私有存取，叢集 VPC 中的 Kubernetes API 請求將使用私有 VPC 端點。如果停用私人存取，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。

- EKS 訪問 EndpointPublic

  類型：布林值

預設：False

描述：(選擇性) 將此值設為以停False用對叢集 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 VPC 內接收要求。

- PublicAccessCIDR

  類型: StringList

  說明：(選用) 允許存取叢集公用 Kubernetes API 伺服器端點的 CIDR 區塊。從您指定的 CIDR 區塊之外的地址與端點的通訊遭拒。如果您已停用私人端點存取，且叢集中有節點或 Fargate 網繭，請確定您已指定必要的 CIDR 區塊。

- SecurityGroup身份證

  類型: StringList

  說明：(選擇性) 指定要與 Amazon EKS 在您帳戶中建立的彈性網路界面建立關聯的一或多個安全群組。

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
- 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

- 建立檔叢集 (aws: 執行AwsApi)-建立 Amazon EKS 叢集。
- 驗證 ClusterIsActive (aws: 等待 ForAwsResourceProperty)-驗證叢集狀態為。ACTIVE
- CreateFargateProfile （ aws：執行AwsApi ）-為集群創建一個 Fargate。
- VerifyFargateProfileIsActive （ aws：等待 ForAwsResourceProperty ）-驗證 Fargate 配置文件狀態為。ACTIVE

輸出

CreateEKSCluster.CreateClusterResponse

說明：從 CreateCluster API 呼叫收到的回應。

CreateFargateProfile.CreateFargateProfileResponse

說明：從 CreateFargateProfile API 呼叫收到的回應。

AWS-CreateEKSClusterWithNodegroup

Description

AWS-CreateEKSClusterWithNodegroup執行手冊會使用節點群組來建立亞馬 Amazon Elastic Kubernetes Service (Amazon EKS) 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

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。

- ClusterName

  類型：字串

  描述：(必要) 叢集的唯一名稱。

- ClusterRole阿恩

  類型：字串

  說明：(必要) IAM 角色的 ARN，可為 Kubernetes 控制平面提供許可，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。

- NodegroupRole阿恩

  類型：字串

  描述：(必要) 要與節點群組建立關聯的 IAM 角色的 ARN。Amazon EKS 工作者節點 Kubelet 精靈會代表您呼叫 AWS API。節點透過 IAM 執行個體描述檔和關聯的政策，取得這些 API 呼叫的許可。啟動節點並在叢集中註冊之前，您必須先為那些節點建立啟動時要使用的 IAM 角色。

- SubnetIds

  類型: StringList

  說明：(必填) 您要用於 Amazon EKS 叢集的子網路識別碼。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 ID。

- EKS 訪問 EndpointPrivate

  類型：布林值

  預設：True

說明：(選擇性) 將此值設定為True允許叢集的 Kubernetes API 伺服器端點進行私人存取。如果您啟用私有存取，叢集 VPC 中的 Kubernetes API 請求將使用私有 VPC 端點。如果停用私人存取，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。

- EKS 訪問 EndpointPublic

  類型：布林值

  預設：False

  描述：(選擇性) 將此值設為以停False用對叢集 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 VPC 內接收要求。

- PublicAccessCIDR

  類型: StringList

  說明：(選用) 允許存取叢集公用 Kubernetes API 伺服器端點的 CIDR 區塊。從您指定的 CIDR 區塊之外的地址與端點的通訊遭拒。如果您已停用私人端點存取，且叢集中有節點或 Fargate 網繭，請確定您已指定必要的 CIDR 區塊。

- SecurityGroup身份證

  類型: StringList

  說明：(選擇性) 指定要與 Amazon EKS 在您帳戶中建立的彈性網路界面建立關聯的一或多個安全群組。

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:DescribeSubnets
- eks:CreateCluster
- eks:CreateNodegroup
- eks:DescribeCluster
- eks:DescribeNodegroup

- iam:CreateServiceLinkedRole
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:PassRole

文件步驟

- 建立檔叢集 (aws: 執行AwsApi)-建立 Amazon EKS 叢集。
- 驗證 ClusterIsActive (aws: 等待 ForAwsResourceProperty)-驗證叢集狀態為。ACTIVE
- CreateNodegroup （ aws：執行AwsApi ）-為集群創建一個節點組。
- VerifyNodegroupIsActive （ aws：等待 ForAwsResourceProperty ）-驗證節點組的狀態。ACTIVE

輸出

- CreateEKSCluster.CreateClusterResponse：從 CreateCluster API 呼叫收到的回應。
- CreateNodegroup.CreateNodegroupResponse：從 CreateNodegroup API 呼叫收到的回應。

AWS-DeleteEKSCluster

Description

此執行手冊會刪除與 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 指令行公用程式。kubectl如需詳細資訊，請參閱 Amazon E KS 使用者指南中的安裝 kubectl。
2. 執行下列命令以列出叢集中執行的所有服務。

```
kubectl 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。

```
kubectl 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

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。

- EKS ClusterName

  類型：字串

  描述：(必填) 要刪除的 Amazon EKS 叢集名稱。

- VPC 堆疊 CloudFormation

  類型：字串

  描述：(選用) 要刪除之 EKS 叢集之 VPC 的 AWS CloudFormation 堆疊名稱。這會刪除 VPC 的 AWS CloudFormation 堆疊以及堆疊所建立的任何資源。

- VPC CloudFormation StackRole

  類型：字串

  說明：(選用) AWS CloudFormation 假設刪除 VPC 擬私 CloudFormation 人雲端堆疊的 IAM 角色的 ARN。 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。

- SelfManagedNodeStacks角色

  類型：字串

  說明：(選用) AWS CloudFormation 假設刪除自我管理節點堆疊的 IAM 角色的 ARN。 AWS CloudFormation 使用角色的認證代表您撥打電話。

必要的 IAM 許可

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

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`

- eks:DeleteCluster
- cfn:DescribeStacks
- cfn:DeleteStack

文件步驟

- aws:executeScript- DeleteNodeGroups：尋找並刪除 EKS 叢集中的所有節點群組。
- aws:executeScript- DeleteFargateProfiles：查找並刪除 EKS 叢集中的所有 Fargate 設定檔。
- aws:executeScript- DeleteSelfManagedNodes：刪除所有自我管理節點以及用於建立節點的 CloudFormation 堆疊。
- aws:executeScript-刪除叢集：刪除 EKS 叢集。
- aws:executeScript-刪除 VPC CloudFormation 堆疊：刪除虛擬私人雲端堆疊。 CloudFormation

AWS-MigrateToNewEKSSelfManagedNodeGroup

Description

AWS-MigrateToNewEKSSelfManagedNodeGroup執行手冊可協助您建立新的 Amazon Elastic Kubernetes Service (Amazon EKS) 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 使用者指南中的遷移到新節點群組。

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

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。

- OldStack姓名

  類型：字串

  說明：（必填）現有堆疊的名稱或 AWS CloudFormation 堆疊 ID。

- NewStack姓名

  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*。

- ClusterControlPlaneSecurity集團

  類型：字串

  說明：(選用) 您希望節點用於與 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。

- NodeInstance类型

  類型：字串

  說明：(選擇性) 要用於新節點群組的執行個體類型。如果您沒有為此參數指定值，則會使用在現有 AWS CloudFormation 堆疊中指定的執行個體類型。

- NodeGroup姓名

  類型：字串

  描述：(選擇性) 新節點群組的名稱。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的節點群組名稱。

- NodeAutoScalingGroupDesiredCapacity

  類型：字串

描述：(選擇性) 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。

- NodeImage識別碼

  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。

- NodeImageIDSSParam

  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

- NodeVolume大小

  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。

- NodeVolume類型

  類型：字串

  說明：(選擇性) 您要用於節點根磁碟區的 Amazon EBS 磁碟區類型。如果您未指定此參數的值，則會使用現有 AWS CloudFormation 堆疊中指定的磁碟區類型。

- KeyName

類型：字串

描述：(選擇性) 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) 要用於新節點群組的子網路 ID 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。

- 停用模式 1

  類型：布林值

  說明：(選擇性) 指定停`true`用執行個體中繼資料服務版本 1 (IMDSv1)。根據預設，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 許可

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `autoscaling:CreateAutoScalingGroup`
- `autoscaling:CreateOrUpdateTags`
- `autoscaling:DeleteTags`
- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `autoscaling:DescribeScheduledActions`
- `autoscaling:SetDesiredCapacity`

- autoscaling:TerminateInstanceInAutoScalingGroup
- autoscaling:UpdateAutoScalingGroup
- cloudformation:CreateStack
- cloudformation:DescribeStackResource
- cloudformation:DescribeStacks
- cloudformation:UpdateStack
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateLaunchTemplateVersion
- ec2:CreateLaunchTemplate
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteLaunchTemplate
- ec2:DeleteSecurityGroup
- ec2:DescribeAvailabilityZones
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2: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：執行程序檔)-收集要用於新節點群組的參數值。
- CreateStack (AWS：建立堆疊)-為新節點群組建立 AWS CloudFormation 堆疊。
- GetNewStackNodeInstanceRole （aws：執行AwsApi）-獲取節點實例角色。
- GetNewStackSecurityGroup （aws：執行AwsApi）-該步驟獲取節點安全組。
- AddIngressRulesToNewNodeSecurityGroup (aw: executeAwsApi)-將輸入規則新增至新建立的安全性群組，以便接受來自指派給先前節點群組的流量。
- AddIngressRulesToOldNodeSecurityGroup (aw: executeAwsApi)-將輸入規則新增至先前的安全性群組，以便它可以接受來自指派給新建立節點群組的流量。
- VerifyStackComplete （aws：斷言AwsResource屬性）-驗證新的堆棧狀態。CREATE_COMPLETE

輸出

DetermineParameterValuesForNewNode群組。 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。

GetNewStackSecurity群組。 NewNodeSecurityGroup -新節點群組的安全性群組識別碼。

DetermineParameterValuesForNewNode群組。 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 (Amazon EKS) 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 upport 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) 授予 All Users Amazon S3 預先定義群組的READ|WRITE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

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。
- 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 許可

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeVpcs
- ec2:DescribeNetworkAcls
- iam:GetInstanceProfile
- iam:ListInstanceProfiles
- iam:ListAttachedRolePolicies
- eks:DescribeCluster
- eks:ListNodegroups
- eks:DescribeNodegroup
- autoscaling:DescribeAutoScalingGroups

此外，連接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 參數進行ssm:GetParameter操作，才能取得工作者節點的最新建議 Amazon EKS Amazon Machine Image (AMI)。

- arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2/recommended/image_id
- arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-*/image_id
- arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-EKS_Optimized-*/image_id
- arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-1909-English-Core-EKS_Optimized-*/image_id
- arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2-gpu/recommended/image_id

若要將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 Elastic Compute Cloud (Amazon EC2) 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 叢集的虛擬私有雲端 (VPC)、子網路、網路位址轉譯 (NAT) 閘道、子網路路由、安全群組和網路存取控制清單 (ACL) 的詳細資料。
- aws:executeScript-收集連接的 IAM 實例配置文件和角色政策的詳細信息。
- 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 子網路分類為公有或私有。
- aws:executeScript-檢查 Amazon VPC 子網路是否有屬於 Amazon EKS 叢集一部分所需的標籤。
- 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 實例是否使用最新的 Amazon EKS 優化 AMI

- aws:executeScript-檢查 Amazon VPC 安全群組是否連接到工作者節點是否有必要的標籤。
- 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從 Amazon EKS 叢集建議的輸出規則。
- 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-TroubleshootEKSWorkerNode

Description

AWSSupport-TroubleshootEKSWorkerNode執行手冊會分析 Amazon Elastic Compute Cloud (Amazon EC2) 工作者節點和 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集，以協助您識別並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ACTIVE為。

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)。如果未指定任何角色，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

  說明：(必填) 無法加入叢集之 Amazon EC2 工作者節點的 ID。

必要的 IAM 許可

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

- ec2:DescribeDhcpOptions
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- eks:DescribeCluster
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand

文件步驟

- aws:assertAwsResourceProperty-確認您在ClusterName參數中指定的 Amazon EKS 叢集存在且處於ACTIVE狀態。
- aws:assertAwsResourceProperty-確認您在WorkerID參數中指定的 Amazon EC2 工作者節點存在且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 (Amazon EKS) 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

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。
- ClusterName

  類型：字串

  說明：(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 許可

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

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

文件步驟

- `aws:executeAwsApi`-更新 Amazon EKS 叢集所使用的 Kubernetes 版本。
- `aws:waitForAwsResourceProperty`-等待更新狀態為`Successful`。

AWS-UpdateEKSManagedNodeGroup

Description

AWS-UpdateEKSManagedNodeGroup執行手冊可協助您更新 Amazon Elastic Kubernetes Service (Amazon EKS) 受管節點群組。您可以選擇Version或Configuration更新。

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。
- ClusterName

  類型：字串

  描述：(必要) 您要更新其節點群組的叢集名稱。
- NodeGroup姓名

  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：

- AMI ReleaseVersion

  類型：字串

  說明：(選用) 您要使用的最佳化 AMI Amazon EKS 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。
- LaunchTemplate識別碼

  類型：字串

  描述：(選擇性) 啟動範本的 ID。
- LaunchTemplate姓名

  類型：字串

  描述：(選擇性) 啟動範本的名稱。
- LaunchTemplate版本

  類型：字串

  說明：（可選）Amazon Elastic Compute Cloud (Amazon EC2) 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。

- MaxUnavailablePercentageNode集團

  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 許可

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

- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

文件步驟

- aws:executeScript-根據您為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 (Amazon EKS) 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。

將部署擴展到兩個複本

1. 安裝 Kubernetes 指令行公用程式。kubectl如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的安裝 kubectl。
2. 執行下列命令。

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. 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

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。

- ClusterName

  類型：字串

描述：(必填) Amazon EKS 叢集的名稱。

- NodeGroup姓名

  類型：字串

  描述：(必要) 受管理節點群組的名稱。

- ClusterControlPlaneSecurity集團

  類型：字串

  描述：(必要) 控制平面安全性群組的識別碼。

- 停用模式 1

  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。

- NodeInstance类型

  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。

- NodeImage識別碼

  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。

- NodeImageIDSSParam

  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) 您要叢集使用之子網路 ID 的逗號分隔清單。

- VpcId

  類型：字串

  預設：Default

  描述：(必要) 部署叢集的虛擬私人雲端 (VPC)。

必要的 IAM 許可

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 Elastic Compute Cloud (Amazon Windows Server EC2) 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。為了協助確保從 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) 授予 All Users Amazon S3 預先定義群組的READ|WRITE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* 。*##*和 *accountID* 值會根據「區域」而有所不同，而且 AWS 帳戶 您在中執行自動化操作。記錄服務包將儲存到目 resources/environments/logs/bundle/ *environmentID* / *instanceID* 錄中。*## ID ##### ID ###### Elastic Beanstalk ######## Amazon EC2 #####*有所不同。

依預設，連接至 Elastic Beanstalk 環境之 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 EC2 執行個體的執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 Amazon EC2 執行個體的根亞馬遜彈性區塊存放區 (Amazon EBS) 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

  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。
- 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。如果未指定參數值，則會忽略此`S3BucketName`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: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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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 許可

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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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) 您要傳送通知的亞馬遜簡單通知服務 (Amazon SNS) 主題的 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`
- `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 Elastic Compute Cloud (Amazon EC2) 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 (ACL) 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

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。

- 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

  說明：(選擇性) 提供給您的 URL，供您將記錄檔服務包從 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 許可

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) 主體具有執行 runbook 中定義的所有動作的必要許可。
- 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-檢查與 VPC 中子網路相關聯的路由表和 ACL 的網路連線問題。
- aws:executeScript-檢查與 Amazon EC2 執行個體相關聯的安全群組規則的網路連線問題。
- 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

Description

AWSConfigRemediation-DropInvalidHeadersForALBRunbook 可讓您指定的應用程式負載平衡器移除含有無效標頭的 HTTP 標頭。

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

- AutomationAssume角色

  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)。
- LoadBalancer阿恩

  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 許可

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LoadBalancerArn定。
- `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

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。

- 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)。

- LoadBalancer名稱

  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 許可

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

啟用 CLB AccessLogs。 SuccessesLoadBalancers -成功啟用存取記錄的負載平衡器名稱清單。

啟用 CLB AccessLogs。 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。連線耗盡可能讓 CLB 完成對已取消註冊或運作狀態不良的執行中要求，而指定的逾時是在將執行個體報告為已取消註冊之前，連線保持作用中的時間。如需 CLB 上連線排除的詳細資訊，請參閱 C lassic Load Balancer 使用者指南中的設定傳統負載平衡器的連線排除。

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

  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。
- LoadBalancer姓名

  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 許可

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 (aw: executeAwsApi)：啟用連線排除，並為您指定的負載平衡器設定指定的逾時值。
- VerifyLoadBalancerConnectionDrainingEnabled（aws：斷言AwsResource屬性）：驗證負載平衡器是否啟用了連接排除。
- VerifyLoadBalancerConnectionDrainingTimeout(aws：assert AwsResource 屬性)：驗證負載平衡器的連線逾時值是否符合您指定的值。

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Description

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancingRunbook 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。
- LoadBalancer姓名

  類型：字串

描述：(必要) 您要啟用跨區域負載平衡的 CLB 名稱。

必要的 IAM 許可

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-為您在參數中指定的 CLB 啟用跨區域負載平衡。LoadBalancerName
- aws:assertAwsResourceProperty-驗證 CLB 上已啟用跨區域負載平衡。

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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。

- LoadBalancer阿恩

  類型：字串

  描述：(必填) 您要在其上啟用刪除保護之 ELB 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`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文件步驟

- `aws:executeScript`-對您在LoadBalancerArn參數中指定的 ELB 啟用刪除保護。

AWSConfigRemediation-EnableLoggingForALBAndCLB

Description

AWSConfigRemediation-EnableLoggingForALBAndCLBrunbook 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。
- LoadBalancer識別碼

  類型：字串

  描述：(必要)「Classic Load Balancer」名稱或「應用程式負載平衡器」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 許可

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 Elastic Compute Cloud (Amazon EC2) 執行個體之間的連線問題。此外，會檢閱用戶端與 CLB 之間的連線問題。此 Runbook 也會檢閱 CLB 的健康狀態檢查、驗證是否遵循最佳做法，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

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。

- 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。

- LoadBalancer姓名

  類型：字串

  描述：(必要) CLB 的名稱。

- 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)。*###############################/S3 LocationPrefix/{{}} _ {###### ID InvestigationType}} .txt#*

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:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`

- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerPolicies
- elasticloadbalancing:DescribeInstanceHealth
- elasticloadbalancing:DescribeLoadBalancerAttributes
- iam:ListRoles
- cloudwatch:PutDashboard
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:SendCommand
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetPublicAccessBlock
- s3:PutObject

文件步驟

- aws:executeScript-驗證您在LoadBalancerName參數中指定的 CLB 是否存在。

- aws:branch-根據為InvestigationType參數指定的值進行分支。
- aws:executeScript-對 CLB 執行連線檢查。
- aws:executeScript-驗證 CLB 組態是否遵循 Elastic Load Balancing 最佳作法。
- aws:executeScript-為您的 CLB 創建 Amazon CloudWatch 儀表板。
- 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

RunBest練習。摘要

RunConnectivity檢查. 摘要

CreateTroubleshooting儀表板輸出

UploadOutput支持 3. 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。

- LoadBalancer阿恩

  類型：字串

  描述：(必要) 您要啟用跨區域負載平衡之 NLB 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`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文件步驟

- `aws:executeAwsApi`-針對您在`LoadBalancerArn`參數中指定的 NLB 啟用跨區域負載平衡。
- `aws:executeScript`-驗證已在 NLB 上啟用跨區域負載平衡。

AWS 更新模式 DesyncMitigation

Description

`AWS-UpdateALBDesyncMitigationMode`runbook 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

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。
- LoadBalancer阿恩

  類型：字串

  說明：(必要) 您要修改的不同步緩和模式之 ALB 的 Amazon 資源名稱 (ARN)。
- DesyncMitigation模式

  類型：字串

  有效值：監控 | 防守 | 最嚴格

  描述：(必要) 您希望 ALB 使用的緩和模式。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 許可

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 (aw: assert AwsResource 屬性)-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：執行AwsApi ）-更新 ALB 以使用指定的。DesyncMitigationMode
- VerifyLoadBalancerDesyncMitigationMode (AWS：執行程序檔)-確認目標 ALB 的不同步緩和模式是否已更新。

輸出

VerifyLoadBalancerDesyncMitigationMode。 ModificationResult -驗證 ALB 修改的腳本的消息有效負載。

AWS 更新 CLB 模式 DesyncMitigation

Description

AWS-UpdateCLBDesyncMitigationModeRunbook 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。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

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。

- LoadBalancer姓名

  類型：字串

  描述：(必要) 您要修改其不同步緩和模式之 CLB 的名稱。

- DesyncMitigation模式

  類型：字串

  有效值：監控 | 防守 | 最嚴格

  描述：(必要) 您希望 CLB 使用的緩和模式。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 許可

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：執行AwsApi ）-更新 CLB 以使用指定的。`DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (AWS：執行程序檔)-確認目標 CLB 的不同步緩和模式是否已更新。

輸出

VerifyLoadBalancerDesyncMitigationMode。 ModificationResult -驗證 CLB 修改的腳本的消息有效負載。

Amazon EMR

AWS Systems Manager 自動化為 Amazon EMR 提供預先定義的操作手冊。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

此執行手冊可協助識別在 Amazon EMR 叢集上執行任務時的錯誤。runbook 會分析檔案系統上定義的記錄清單，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：

- 記憶體容器 — YARN 容器記憶體不足，執行作業可能會失敗。
- yarn_nodemanager 健康：核心或任務節點的磁盤空間不足，將無法運行任務。
- 節點狀態更改：主節點無法訪問核心或任務節點。
- 步驟失敗：EMR 步驟失敗。
- 正在執行的核心節點：目前沒有執行中的核心節點，叢集狀況不佳。
- 缺少 HDFS 塊：缺少 HDFS 塊可能導致數據丟失。
- 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_黑名單：YARN 已將核心或任務節點列入黑名單，無法執行任務。

- yarn_node_lost：核心或任務節點已被紗線標記為丟失，可能出現的連接問題。

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

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。
- ClusterID (ClusterID)

  類型：字串

  描述：(必要) 您要分析其節點記錄之叢集的 ID。
- 作業

  類型：字串

  有效值：「運行一次」|「計划」|「刪除計划

  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。

- LogToCloudWatch日誌

  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。

- CreateMetric過濾器

  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 許可

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-收集參數中指定之 Amazon EMR 叢集的ClusterID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-收集叢集中執行之所有執行個體的 ID。
    - 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

GetCluster信息。 ClusterName

GetCluster信息。 ClusterState

ListingCluster執行個體. 執行個體

CreatingScheduleCloudFormation堆疊。 StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroup現有輸出

FindLogPatternOn電子節點。 CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Description

使用 AWSSupport-DiagnoseEMRLogsWithAthena Amazon 雅典娜與 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 EMR 日誌檔，並針對特定日期範圍或以關鍵字為基礎的搜尋提供選用參數。

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 EMR Amazon S3 日誌位置建立資料 AWS Glue 庫並執行 Amazon 雅典娜資料定義語言 (DDL) 查詢，以建立叢集日誌的表格和已知問題清單。
- 執行資料操縱語言 (DML) 查詢，以搜尋 Amazon EMR 日誌中的已知問題模式。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 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：

- 使用叢集 ID 或輸入 Amazon S3 位置取得 Amazon EMR 叢集日誌位置，以擷取日誌位置和大小。
- 根據記錄位置大小提供 Athena 成本估算。
- 在執行 Athena 查詢之前，請先向指定 IAM 主體申請核准，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

/

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

- 雅典娜：GetQuery執行
- 雅典娜：StartQuery執行
- 雅典娜：GetPrepared聲明
- 雅典娜：CreatePrepared聲明
- 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：GetBucket版本控制
- S3：ListBucket版本
- S3：GetBucketPublicAccess阻止
- S3：GetBucketPolicyStatus
- S3：GetObject
- S3：GetBucket位置
- 定價：GetProducts
- 定價：價GetAttribute值
- 定價：DescribeServices
- 定價：ListPrice清單

Important

若要限制只存取此自動化所需的資源，請將下列政策附加至信任 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-診斷 LogsWith Athena 先生在下面的文件。 AWS 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)：

     (IAM) 角色的 Amazon 資源名稱 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。
   - ClusterID D (必要)：

     Amazon EMR 叢集識別碼。
   - S3 LogLocation (選擇性)：

     Amazon S3 Amazon EMR 日誌位置。輸入路徑樣式網址 Amazon S3 位置，例如：`s3://mybucket/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體：使用者名稱、使用者 ARN、IAM 角色 ARN 或 IAM 假設角色 ARN。核准者的數量上限為 10。
   - FetchNodeLogsOnly (選擇性)：

     如果設定為`true`，則自動化會診斷 Amazon EMR 應用程式容器記錄。預設值為 `false`。
   - FetchContainersLogsOnly (選擇性)：

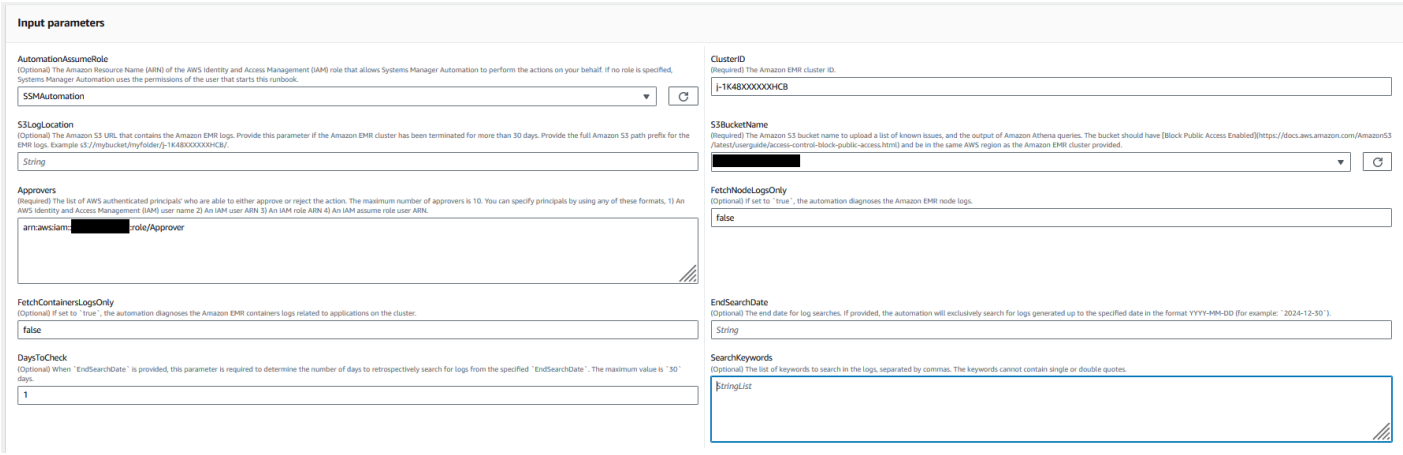
     如果設定為`true`，則自動化會診斷 Amazon EMR 容器日誌。預設值為 `false`。
   - EndSearchDate (選擇性)：

     記錄搜尋的結束日期。如果有提供，自動化操作會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。



4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：
   - 得到LogLocation：

     透過查詢指定的 Amazon EMR 叢集識別碼來擷取 Amazon S3 日誌位置。如果自動化無法從 Amazon EMR 叢集 ID 查詢日誌位置，則執行手冊會使用S3LogLocation輸入參數。
   - 分支OnValid日誌：

     驗證 Amazon EMR 日誌位置。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。
   - 估計AthenaCosts：

     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。
   - 批准自動化：

     等待指定的 IAM 主體核准，以繼續執行自動化的後續步驟。核准通知包含 Amazon EMR 日誌上 Amazon Athena 掃描的估計成本，以及自動化佈建資源的詳細資料。
   - 上傳KnownIssuesExecuteAthena查詢：

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。

- 獲取QueryExecution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。

- 分析AthenaResults：

  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。

- 得到AnalyzeResults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

- 得到AnalyzeResults查詢 2：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。

- 打印AthenaQueries信息：

  列印 Amazon Athena DML 查詢結果的連結。

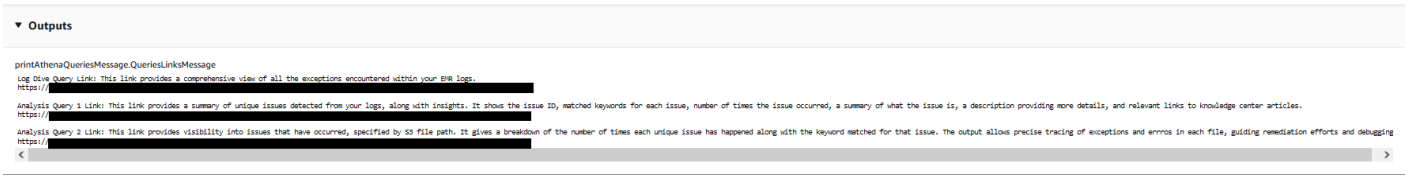
- 清除來源：

  刪除建立的資 AWS Glue 料庫，並刪除 Amazon EMR 記錄儲存貯體中建立的已知問題檔案，以清理資源。

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。



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 DeleteDomainAPI 給定的 Amazon OpenSearch 服務域。

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

  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。
- AutomationAssume角色

  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 許可

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AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain冊使用 UpdateDomainConfig API EnforceHTTPS 在給定的 Amazon OpenSearch 服務域上啟用。

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

- DomainName

  類型：字串

  允許的值：(\ d {12}/)? [a 至 Z] {1} [a-z0-9-] {2,28}

  說明：(必要) 您要用來強制執行 HTTPS 的 Amazon OpenSearch 服務網域名稱。
- AutomationAssume角色

  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 許可

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執行手冊會使用組態 API 更新指定 Amazon OpenSearch 服務網域上的安全群組組態。UpdateDomain

> **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。
- SecurityGroup清單

  類型: StringList

  描述：(必填) 您要指派給 Amazon OpenSearch 服務網域的安全群組 ID。
- AutomationAssume角色

  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 許可

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：

- 針對目標網域呼叫 DescribeDomainAPI 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 人雲端電腦 AWS Lambda 功能。備註：Lambda 函數包含針對叢集執行 OpenSearch 服務 API 的疑難排解程式碼，以判斷叢集為何處於紅色或黃色狀態。
- 刪除 Lambda 函數。
- 顯示執行的檢查以及解決紅色或黃色叢集問題的下一個建議步驟。

文件類型

自動化

擁有者

Amazon

平台

Linux,macOS, Windows

參數

必要的 IAM 許可

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

- cloudformation:CreateStack
- cloudformation:DescribeStacks

- cloudformation:DescribeStackEvents
- cloudformation:DeleteStack
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:InvokeFunction
- lambda:GetFunction
- es:DescribeDomain
- es:DescribeDomainConfig
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:DeleteNetworkInterface
- ec2:DescribeInstances
- ec2:AttachNetworkInterface
- cloudwatch:GetMetricData
- iam:PassRole

LambdaExecutionRole參數需要下列動作才能成功使用 runbook：

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface

LambdaExecutionRole政策概述：

以下是 Lambda 函數的執行角色 (AWS Identity and Access Management (IAM) 角色) 範例，該角色授予函數存取此執行手冊所需 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 服務叢集是以 Amazon 虛擬私人雲端為基礎 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：

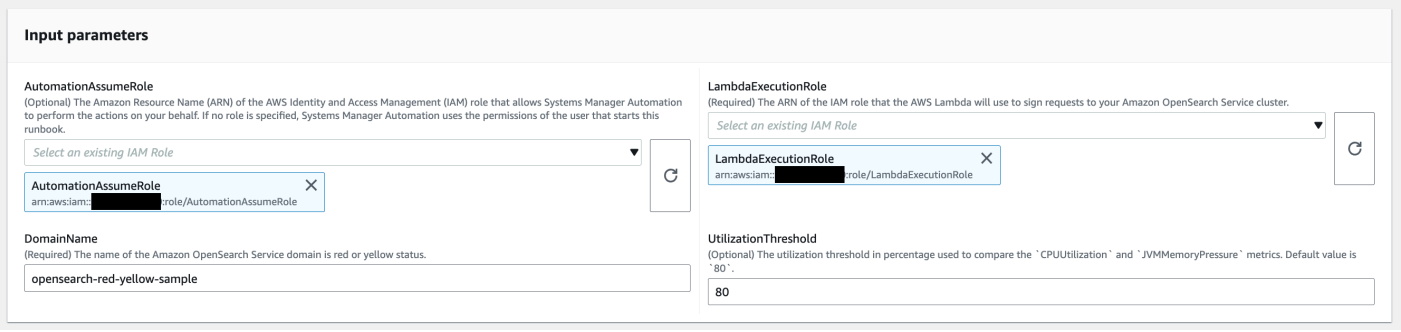
1. 導覽至主 AWS Systems Manager 控台TroubleshootOpenSearchRedYellowCluster中的 AWSSupport-。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
   - AutomationAssumeRole (選擇性)：

     (IAM) 角色的 Amazon 資源名稱 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。
   - LambdaExecutionRole （必填）：

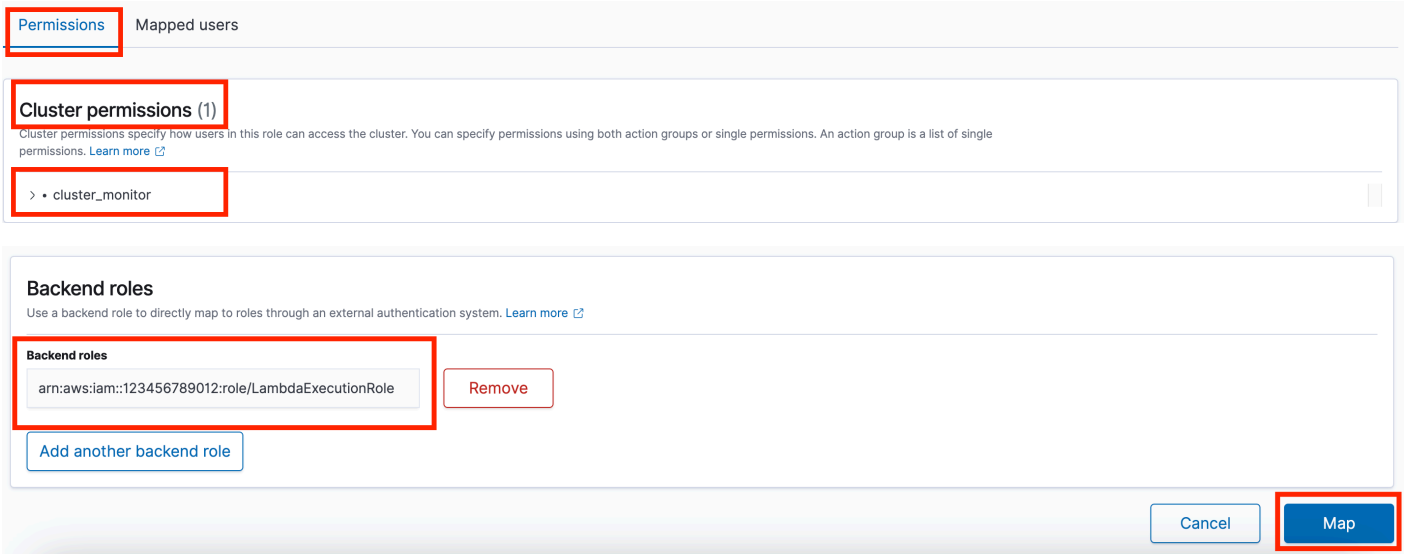
     Lambda 將用來向您的 Amazon OpenSearch 服務叢集簽署請求的 IAM 角色的 ARN。
   - DomainName （必填）：

     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 CPU 使用率和 JVM MemoryPressure 測量結果的使用率臨界值百分比。預設值為 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。



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。
   - 建立AWSLambdaFunctionStack：

     使用建立帳戶中的臨時 Lambda 函數 AWS CloudFormation。Lambda 函數是用來執行 OpenSearch 服務 API。
   - WaitForAWSLambdaFunctionStack:

     等待 CloudFormation 堆棧完成。
   - GetClusterMetricsFromCloudWatch:

     取得 Amazon CloudWatch ClusterStatus、CPU 使用率和 JVM MemoryPressure OpenSearch 服務叢集相關指標及其建立日期。
   - RunOpenSearchAPI：

     使用 Lambda 函數呼叫 OpenSearch 服務 API 並分析叢集指標資料，以診斷紅色或黃色叢集狀態的原因。
   - 刪除AWSLambdaFunctionStack：

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
- 設定自動化操作
- 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 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，以對 CPU 高問題進行疑難排解。

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 CPU 使用率過高。

執行手冊執行下列步驟：

- 針對提供的 Amazon OpenSearch 服務網域執行 DescribeDomainAPI，以取得叢集中繼資料。

- 檢查 Amazon OpenSearch 服務網域是公有網域還是以 Amazon 虛擬私人雲端為基礎 AWS CloudFormation，並在的協助下建立公用或以 Amazon V AWS Lambda PC 為基礎的函數。
- 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)。

必要的 IAM 許可

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

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 服務叢集是以 Amazon 虛擬私人雲端為基礎 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. 瀏覽至主 AWS Systems Manager 控台中的 AWSSupport-TroubleshootOpenSearchHigh CPU。
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)：

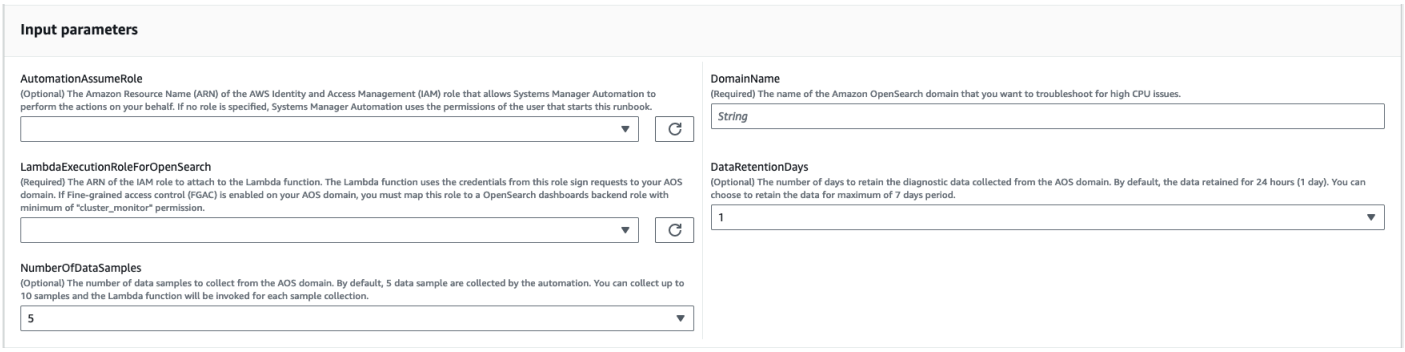
     (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
   - DomainName （必填）：

     您要針對 CPU 過高問題進行疑難排解的 Amazon OpenSearch 服務網域名稱。
   - LambdaExecutionRoleForOpenSearch （必填）：

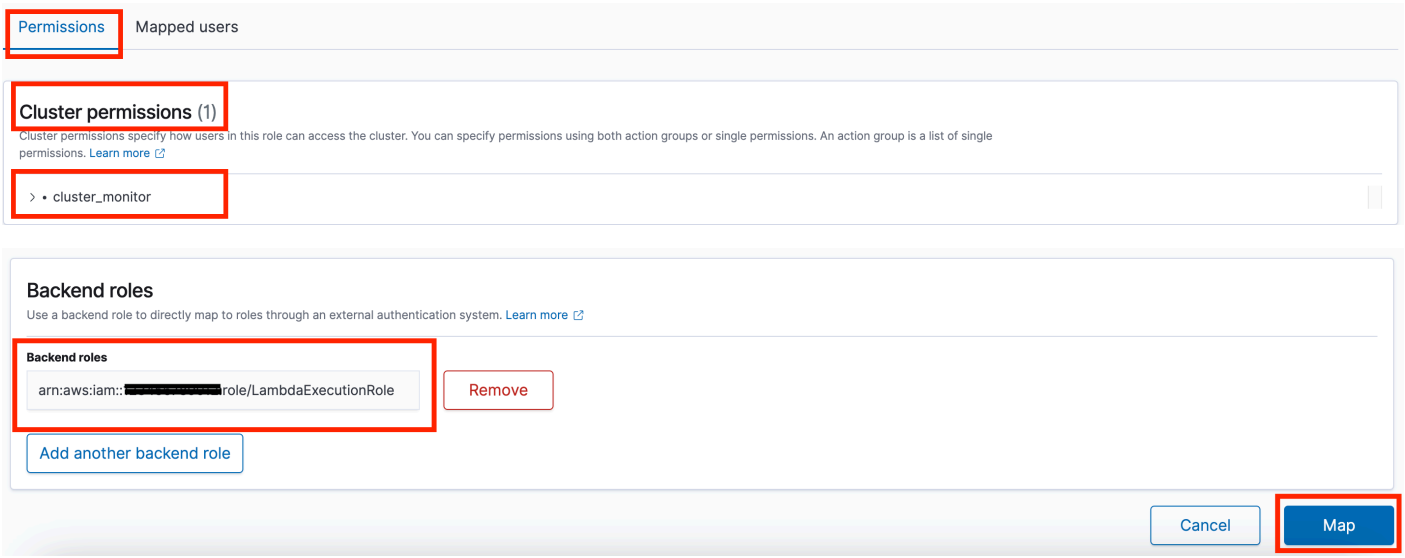
     要連接至 Lambda 函數的 IAM 角色的 ARN。Lambda 函數使用此角色的登入資料，將請求簽署到 Amazon OpenSearch 服務網域。如果在 Amazon OpenSearch 服務網域上啟用了精細的存取控制，則必須將此角色對應至少具有「cluster_monitor」權限的 OpenSearch 服務儀表板後端角色。
   - DataRetentionDays (選擇性)：

     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。



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。



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：
   - 並行檢查：

     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。
   - 佈建資源：

     規定資源使用的數據收集 AWS CloudFormation.
   - waitForStack創作：

等待 AWS CloudFormation 堆棧完成。

- describeStackResources:

  描述 AWS CloudFormation 堆疊並取得狀態機器的 ARN。

- 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。

- unstageOpenSearch高 CPU 自動化:

  刪除AWSSupport-TroubleshootOpenSearchHighCPU AWS CloudFormation 堆疊。

- describeErrorsFromStackDeletion:

  說明刪除 AWS CloudFormation 堆疊時遇到的錯誤。

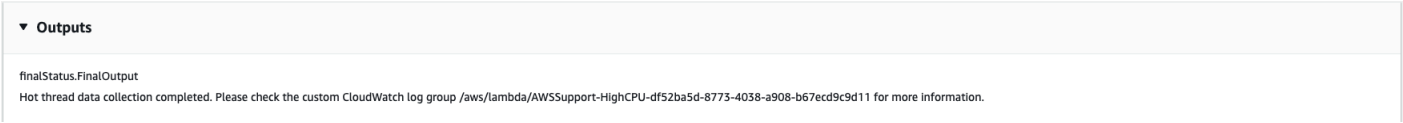
- 最終狀態：

  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。

   - 最終狀態。 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 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

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。

- DedupString

  類型：字串

  描述：(必要) 您要新增至規則的重複資料刪除字串。

- RuleName

  類型：字串

  描述：(必要) 您要新增重複資料刪除字串的規則名稱。

必要的 IAM 許可

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。EventBridge

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。
- EventBus姓名

  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 許可

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。

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

- AutomationAssume角色

  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 許可

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) 角色附加到代管執行個體。

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

  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。
- ForceReplace

  類型：布林值

  說明：(選用) 指定是否要取代現有的 IAM 設定檔的旗標。

  預設：true
- InstanceId

  類型：字串

  說明：(必填) 您要指派 IAM 角色的執行個體 ID。
- RoleName

類型：字串

說明：(必填) 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 EC2 實例的 IAM 實例配置文件。
2. aws:branch- CheckInstanceProfileAssociations -檢查連接到 EC2 實例的 IAM 實例配置文件。
   a. 如果 IAM 執行個體設定檔已附加ForceReplace且設定為true：
      i. aws:executeAwsApi- DisassociateIamInstanceProfile -取消 IAM 執行個體設定檔與 EC2 執行個體的關聯。
   b. aws:executeAwsApi- ListInstanceProfilesForRole -列出提供的 IAM 角色的執行個體設定檔。
   c. aws:branch- CheckInstanceProfileCreated -檢查提供的 IAM 角色是否具有關聯的執行個體設定檔。
      i. 如果 IAM 角色具有關聯的執行個體設定檔：
         A. aws:executeAwsApi-執行個體 ProfileToInstance -將 IAM 執行個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 -為指定的 IAM 角色建立執行個體設定檔角色。
         B. aws:executeAwsApi- AddRoleToInstanceProfile -將執行個體設定檔角色附加到指定的 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-執行個體 ProfileToInstanceWithRetry -將 IAM 執行個體設定檔角色附加至 EC2 執行個體。

輸出

速度重試ProfileToInstanceWith。 AssociationId

GetInstance設定檔。 InstanceProfile姓名

GetInstance設定檔。 InstanceProfile阿恩

速度實例ProfileTo。 AssociationId

ListInstanceProfilesFor角色。 InstanceProfile姓名

ListInstanceProfilesFor角色。 InstanceProfile阿恩

AWS-DeleteIAMInlinePolicy

Description

AWS-DeleteIAMInlinePolicyRunbook 會刪除您指定的 IAM 身分附加的所有 AWS Identity and Access Management (IAM) 內嵌政策。

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。
- IamArns

  類型：字串

  說明：(必填) 您要從中刪除內嵌政策的 IAM 身分的 ARN 清單 (以逗號分隔)。此清單可包括 IAM 使用者、群組或角色。

必要的 IAM 許可

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 內嵌政策。

AWSConfigRemediation-DeleteIAMRole

Description

AWSConfigRemediation-DeleteIAMRole執行簿會刪除您指定的 AWS Identity and Access Management (IAM) 角色。此自動化操作不會刪除與 IAM 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

- AutomationAssume角色

  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

  說明：（必填）您要刪除的 IAM 角色的 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
- 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 角色的名稱。
- 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

AWSConfigRemediation-DeleteIAMUser執行手冊會刪除您指定的 AWS Identity and Access Management (IAM) 使用者。此自動化操作會刪除或卸離與 IAM 使用者相關聯的下列資源：

- 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

- AutomationAssume角色

  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)。
- IAM UserId

  類型：字串

  說明：（必填）您要刪除的 IAM 使用者的 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
- 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、登入資料、MFA 裝置和 SSH 金鑰。
- aws:executeScript-收集 IAM 使用者的群組成員資格和政策。
- aws:executeScript-刪除與 IAM 使用者關聯的存取金鑰、憑證、登入資料、MFA 裝置和 SSH 金鑰。
- aws:executeScript-刪除 IAM 使用者的群組成員資格和政策。
- aws:executeScript-刪除 IAM 使用者並驗證使用者已刪除。

AWSConfigRemediation-DeleteUnusedIAMGroup

Description

AWSConfigRemediation-DeleteUnusedIAMGroup執行手冊會刪除不包含任何使用者的 IAM 群組。

AWSConfigRemediation-DeleteUnusedIAMGroup執行手冊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

- AutomationAssume角色

  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

說明：(必要) 您要刪除的 IAM 群組名稱。

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
- iam:DeleteGroup
- iam:DeleteGroupPolicy
- iam:DetachGroupPolicy

文件步驟

- aws:executeScript-移除附加至目標 IAM 群組的受管和內嵌 IAM 政策，然後刪除 IAM 群組。

AWSConfigRemediation-DeleteUnusedIAMPolicy

Description

AWSConfigRemediation-DeleteUnusedIAMPolicyRunbook 會刪除未 AWS Identity and Access Management 附加至任何使用者、群組或角色的 (IAM) 政策。

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

- AutomationAssume角色

  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)。

- IAM ResourceId

  類型：字串

  說明：(必填) 您要刪除之 IAM 政策的資源識別碼。

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
- 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執行簿會分離您指定的 AWS Identity and Access Management (IAM) 政策。

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

- AutomationAssume角色

  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)。
- IAM ResourceId

  類型：字串

  說明：（必填）您要卸離的 IAM 政策的 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`
- `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 政策。

AWSConfigRemediation-EnableAccountAccessAnalyzer

Description

該手AWSConfigRemediation-EnableAccountAccessAnalyzer冊創建一個 AWS Identity and Access Management (IAM) 訪問分析器在您的 AWS 帳戶. 如需存取分析器的相關資訊，請參閱 AWS IAM 使用者指南中的使用 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。
- AutomationAssume角色

  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 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
- 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 會將指定的許可授與 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。若要為 IAM 啟用帳單存取，請記得也要啟用 IAM 使用者和聯合身分使用者對帳單與成本管理頁面的存取。

> **Important**
>
> 如果您提供現有的 IAM 群組，群組中所有目前的 IAM 使用者都會收到新的許可。

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。

- IAM GroupName

  類型：字串

  預設值： ExampleSupportAndBillingGroup

  描述：(必要) 可以是新的或現有的群組。必須遵守 IAM 實體名稱限制。

- IAM UserName

  類型：字串

  預設值： ExampleUser

  描述：(必要) 必須是現有的使用者。

- LambdaAssume角色

  類型：字串

  描述：(選用) 由 lambda 擔任之角色的 ARN。

- 許可

  類型：字串

  有效值： SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  預設值： 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授予帳單控制面板的完整存取權。 SupportAndBillingFullAccess授予支 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 許可

此AutomationAssumeRole參數需要執行下列動作，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

建議您已附加 AmazonSSMAutomationRole Amazon 受管政策，並具備下列其他許可，以便能夠建立 Lambda 函數和 IAM 角色以傳遞給 Lambda：

```
{
                    "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

使用者必須擁有傳遞為AutomationAssume角色和角色的 IAM 角色PassRole上的 ssm:StartAutomation 執行許可，以及 LambdaAssume iam:。以下為各 IAM 角色需要的許可：

```
AutomationAssumeRole

                    {
                        "Version": "2012-10-17",
                        "Statement": [
                            {
                                "Action": [
                                    "lambda:InvokeFunction",
                                    "lambda:CreateFunction",
                                    "lambda:DeleteFunction",
                                    "lambda:GetFunction"
                                ],
                                "Resource":
 "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
                                "Effect": "Allow"
                            }
                        ]
```

```
                    }
```

LambdaAssumeRole

```
                {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:CreateGroup",
                                "iam:AddUserToGroup",
                                "iam:ListAttachedGroupPolicies",
                                "iam:GetGroup",
                                "iam:GetUser"
                            ],
                            "Resource" : [
                                "arn:aws:iam::*:user/*",
                                "arn:aws:iam::*:group/*"
                            ]
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:AttachGroupPolicy"
                            ],
                            "Resource": "*",
                            "Condition": {
                                "ArnEquals": {
                                    "iam:PolicyArn": [
                                        "arn:aws:iam::aws:policy/job-function/Billing",
                                        "arn:aws:iam::aws:policy/AWSSupportAccess"
                                    ]
                                }
                            }
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:ListAccountAliases",
                                "iam:GetAccountSummary"
                            ],
```

```
                        "Resource" : "*"
                    }
                ]
            }
```

文件步驟

1. aws:createStack-執行 AWS CloudFormation 範本以建立 Lambda 函數。
2. aws:invokeLambdaFunction-執行 Lambda 以設定 IAM 許可。
3. aws:deleteStack-刪除 CloudFormation 模板。

輸出

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

Description

AWSConfigRemediation-RemoveUserPoliciesrunbook 會刪除 AWS Identity and Access Management (IAM) 內嵌政策，並分離任何附加到您指定使用者的受管政策。

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

- AutomationAssume角色

  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)。

- iamUser

  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

  說明：(必要) 您要從使用者移除的 IAM 政策類型。

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
- 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卸離 IAM 政策。

AWSConfigRemediation-ReplaceIAMInlinePolicy

Description

AWSConfigRemediation-ReplaceIAMInlinePolicyRunbook 會以複寫的受管身分與存取權管理政策取代內嵌 AWS Identity and Access Management (IAM) 政策。對於連接到使用者、群組或角色的內嵌政策，內嵌政策許可會複製到受管 IAM 政策中。受管 IAM 政策會新增至資源，並移除內嵌政策。 AWS Config 必須在您執行此自動化操作的 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

- AutomationAssume角色

  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)。
- InlinePolicy姓名

  類型: StringList

  說明：(必填) 您要取代的內嵌 IAM 政策。
- ResourceId

  類型：字串

  說明：(必要) 您要取代其內嵌政策之 IAM 使用者、群組或角色的 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
- iam:AttachGroupPolicy
- iam:AttachRolePolicy
- iam:AttachUserPolicy
- iam:CreatePolicy
- iam:CreatePolicyVersion
- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:GetGroupPolicy
- iam:GetRolePolicy
- iam:GetUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

文件步驟

- aws:executeScript-將內嵌 IAM 政策取代為您指定資源的 AWS 複寫政策。

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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。
- IAM ResourceId

  類型：字串

  說明：(必要) 您要撤銷未使用登入資料的 IAM 資源 ID。
- MaxCredentialUsageAge

  類型：字串

  預設：90

  說明：(必要) 必須使用認證的天數。

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: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 登入資料。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：存取金鑰旋轉。

AWSConfigRemediation-SetIAMPasswordPolicy

Description

AWSConfigRemediation-SetIAMPasswordPolicy執行手冊會 AWS Identity and Access Management 為您 AWS 帳戶的.

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

- AutomationAssume角色

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)。

- AllowUsersToChange密碼

  類型：布林值

  預設：false

  說明：(選用) 如果設定為`true`，您中的所有 IAM 使用者都 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：(選用) 如果設為`true`，IAM 使用者將無法在密碼到期後重設密碼。

- MaxPassword年齡

  類型：整數

  預設：0

  說明：(選用) IAM 使用者密碼有效的天數。

- MinimumPassword長度

  類型：整數

  預設：6

  說明：(選用) IAM 使用者密碼可以包含的字元數下限。

- PasswordReuse預防

  類型：整數

  預設：0

  說明：(選用) IAM 使用者無法重複使用的先前密碼數目。

- RequireLowercase人物

  類型：布林值

  預設：false

  說明：(選用) 如果設定為`true`，IAM 使用者的密碼必須包含 ISO 基本拉丁字母 (a 到 z) 中的小寫字元。
- RequireNumbers

  類型：布林值

  預設：false

  說明：(選用) 如果設定為`true`，IAM 使用者的密碼必須包含數字字元 (0-9)。
- RequireSymbols

  類型：布林值

  預設：false

  說明：(選用) 如果設定為`true`，IAM 使用者的密碼必須包含非英數字元 (! @ # $ % ^ * ( ) _ +-= [] {} | ')。
- RequireUppercase人物

  類型：布林值

  預設：false

  說明：(選用) 如果設定為`true`，IAM 使用者的密碼必須包含 ISO 基本拉丁字母 (A 到 Z) 中的大寫字元。

必要的 IAM 許可

此`AutomationAssumeRole`參數需要執行下列動作，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 使用者密碼政策。 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 系統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。

- 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。此值可以是全域唯一識別名、別名或索引鍵的 ARN，或是以「alias/」為前置詞的別名名稱。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 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`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

文件步驟

- VerifyKinesisStreamStatus （aws：waitforAwsResource屬性）-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: assertAwsResource 屬性)-驗證 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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 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
- 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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 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`
- `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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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) 啟用追蹤之 Lambda 函數的名稱或 ARN。

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。

- lambda:UpdateFunctionConfiguration
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文件步驟

- aws:executeAwsApi-對您在參數中指定的 Lambda 函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 UpdateFunctionConfiguration API 呼叫的回應。

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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。
- LambdaFunction姓名

  類型：字串

  說明：(必要) 您要刪除的 Lambda 函數名稱。

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`
- `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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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之 Lambda 函數的名稱或 ARN。
- 公里 KeyArn

  類型：字串

  說明：(必要) 您要用來加密 Lambda 函數環境變數之 AWS KMS 客戶受管金鑰的 ARN。

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
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文件步驟

- aws:waitForAwsResourceProperty-等待物LastUpdateStatus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（Amazon 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

- AutomationAssume角色

  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) 要移至 Amazon VPC 的 Lambda 函數名稱。

- SecurityGroup身份證

  類型：字串

  描述：(必要) 您要指派給與 Lambda 函數相關聯之彈性網路介面 (ENI) 的安全性群組 ID。
- SubnetIds

  類型：字串

  描述：(必要) 您要建立與 Lambda 函數相關聯之彈性網路介面 (ENI) 的子網路 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`
- `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 SNS) 和亞馬遜簡單佇列服務 (Amazon 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。如果在使用執行手冊之後，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

  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。

- LambdaFunction阿恩

  類型：字串

  說明：(必要) Lambda 函數的 ARN。

- 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 許可

此AutomationAssumeRole參數需要執行下列動作，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 (Amazon VPC) 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

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。
- 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 許可

此AutomationAssumeRole參數需要執行下列動作，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 函數的 VPC 中各種資源的組態。
- `aws:branch`-根據指定的 Lambda 函數是否在 VPC 中進行分支。
- `aws:executeScript`-檢閱啟動 Lambda 函數之子網路的路由表路由，並驗證是否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 閘道會根據為和參數指定的值允許輸出網際網路存取。destinationIp destinationPort

輸出

VPC-啟動 Lambda 函數所在的虛擬私人雲端識別碼。

子網路-啟動 Lambda 函數的子網路識別碼。

安全性群組-與 Lambda 函數相關聯的安全性群組。

檢查 NACL-含有資源名稱的分析訊息。 LambdaIp指的是 Lambda 函數 elastic network interface 的私有 IP 位址。只有具有通往 NAT 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 / destionation 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 / destionation port in Ingress rule"
   }
}
```

檢查 SecurityGroups .secgrps-分析與您的 Lambda 函數相關聯的安全群組。下面的內容是輸出的一個例子。

```
{
   "sg-123456789":{
```

```
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

子網路-分析 VPC 中與 Lambda 函數相關聯的子網路。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"
   }
}
```

AWSSupport-TroubleshootLambdaS3Event

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 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

  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。
- LambdaFunction阿恩

  類型：字串

  說明：(必要) Amazon S3 事件通知觸發的 Lambda 函數的 ARN。
- 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 許可

此AutomationAssumeRole參數需要執行下列動作，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) 命令以新增所需的許可，如果政策中缺少必要的許可。驗證屬於相同 S3 儲存貯體事件通知一部分的其他 Lambda 函數資源政策，並在缺少所需權限時產生 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-TroubleshootMWAAEnvironmentCreation執行手冊提供針對 Apache Airflow (Amazon MWAA) 環境建立問題進行 Amazon 受管工作流程偵錯的資訊，並以最佳方式執行檢查以及記錄的原因，以協助識別故障。

它是如何工作的？

執行手冊執行下列步驟：

- 擷取 Amazon MWAA 環境的詳細資訊。
- 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 許可

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

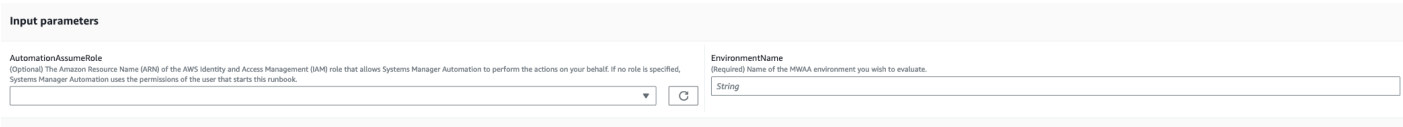
指示

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)：

     (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。



4. 選取執行。
5. 自動化啟動。
6. 文件會執行下列步驟：
   - **GetMWAAEnvironmentDetails:**

     擷取 Amazon MWAA 環境的詳細資訊。如果此步驟失敗，自動化過程將停止並顯示為Failed。
   - **CheckIAMPermissionsOnExecutionRole:**

     驗證執行角色具有 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 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:SimulateCustomPolicy API 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 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 日誌群組的存在進行分支。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 ACL、子網路和路由表組態。

- **CheckEndpointsConnectivity:**

  呼叫`AWSSupport-ConnectivityTroubleshooter`子系自動化以驗證 Amazon MWAA 與所需端點的連線。

- **CheckS3BlockPublicAccess:**

  檢查 Amazon MWAA 環境的 Amazon S3 儲存貯體是否已`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 金鑰政策：

  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 日誌群組：

  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 路由表是否已正確設定。

- 檢查 Amazon MWAA 環境安全群組：

  檢查 Amazon MWAA 環境 Amazon VPC 安全群組是否已正確設定。

- 檢查 Amazon MWAA 環境網路 ACL：

  檢查 Amazon MWAA 環境中的 Amazon VPC 安全群組是否已正確設定。

- 檢查 Amazon MWAA 環境子網路：

  驗證 Amazon MWAA 環境的子網路是否為私有。

- 檢查 Amazon MWAA 環境所需的端點連線能力：

  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`AWSSupport-ConnectivityTroubleshooter`化。

- 檢查 Amazon MWAA 環境 Amazon S3 存儲桶：

  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 Amazon S3 區塊公開存取設定。

- 檢查 Amazon MWAA 環境 CloudWatch 日誌群組錯誤：

  剖析 Amazon MWAA 環境的現有 CloudWatch 日誌群組以找出錯誤。

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

  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。
- 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 許可

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）-返回 Neptune 數據庫集群的 ID。
- VerifyNeptuneDbEngine （aws：assertAwsResource屬性）-驗證 Neptune 數據庫引擎類型是neptune。
- EnableNeptuneDbAuditLogs (aws:executeAwsApi)-啟用要傳送日誌的 Neptune 資料庫叢集的稽核 CloudWatch 日誌。
- VerifyNeptuneDbStatus （aws：waitAwsResource屬性）-驗證 Neptune 數據庫群集狀態為available。
- VerifyNeptuneDbAuditLogs (AWS：執行程序檔)-驗證稽核記錄是否已成功設定為傳送至記錄。CloudWatch

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

  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。
- 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。該值必須是世界協調時間 (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 許可

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）-返回 Neptune 數據庫集群的 ID。
- VerifyNeptuneDbEngine（aws：assertAwsResource屬性）-驗證 Neptune 數據庫引擎類型是neptune。
- VerifyNeptuneDbStatus（aws：waitAwsResource屬性）-驗證 Neptune 數據庫群集狀態為available。
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi)-設定 Neptune 資料庫叢集的保留期。
- VerifyNeptuneDbBackupsEnabled (AWS：執行命令檔)-驗證保留期間和備份時段是否已順利設定。

AWS-EnableNeptuneClusterDeletionProtection

Description

AWS-EnableNeptuneClusterDeletionProtection執行手冊為您指定的 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

  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。
- 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 許可

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）-返回 Neptune 數據庫集群的 ID。
- VerifyNeptuneDbEngine（aws：assertAwsResource屬性）-驗證指定數據庫集群的引擎類型。`neptune`
- VerifyNeptuneStatus（aws: waitForAwsResourceProperty）-驗證叢集的狀態是`available`否為。
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi)-在 Neptune 資料庫叢集上啟用刪除保護。
- VerifyNeptuneDbDeletionProtection (aws: assertAwsResource 屬性)-驗證資料庫叢集上已啟用刪除保護。

輸出

- EnableNeptuneDbDeletionProtection。 EnableNeptuneDbDeletionProtectionResponse -來自 API 作業的輸出。

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-CreateEncryptedRdsSnapshot執行手冊會從未加密的 Amazon 關聯式資料庫服務 (Amazon RDS) 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

  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。
- 資料庫 InstanceIdentifier

  類型：字串

說明：(必填) 您要建立快照的 Amazon RDS 執行個體的識別碼。

- 資料庫 SnapshotIdentifier

  類型：字串

  說明：(選擇性) Amazon RDS 快照的名稱範本。默認的名稱模板是*### InstanceIdentifier-## #*.

- 加密分析 SnapshotIdentifier

  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 = 標記鍵 1，值 = 標籤值 1; 鍵 = 標記鍵 2，值 = 標籤值 2）'

- KmsKey識別碼

  類型：字串

  預設：`alias/aws/rds`

  說明：(選擇性) 您要用來加密快照之客戶管理金鑰的 ARN、金鑰 ID 或金鑰別名。

- SnapshotTags

  類型：字串

  說明：(選擇性) 要新增至快照的標籤。（例如：鍵 = 標記鍵 1，值 = 標籤值 1; 鍵 = 標記鍵 2，值 = 標籤值 2）'

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。

- `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

CopyRdsSnapshotToEncryptedRds快照。 EncryptedSnapshotId -加密的 Amazon RDS 快照的識別碼。

AWS-CreateRdsSnapshot

Description

為 Amazon RDS 執行個體建立 Amazon Relational Database Service 服務 (Amazon RDS) 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

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。

- 資料庫 InstanceIdentifier

  類型：字串

  說明：(必要) 要從中建立快InstanceId 照的 RDS 執行個體的資料庫識別碼。

- 資料庫 SnapshotIdentifier

  類型：字串

  說明：(選擇性) 要建立之 RDS 快照的資料庫SnapshotIdentifier 識別碼。

- 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 快照並傳回快照識別碼。

verifyRDSSnapshot — 檢查在上一個步驟中建立的快照是否存在。

輸出

createRDSSnapshot。 SnapshotId — 已建立快照的 ID。

AWSConfigRemediation-DeleteRDSCluster

Description

AWSConfigRemediation-DeleteRDSCluster執行手冊會刪除您指定的 Amazon Relational Database Service 服務 (Amazon RDS) 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

- AutomationAssume角色

  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)。
- 資料庫 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 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
- rds:DeleteDBCluster

- rds:DeleteDBInstance
- rds:DescribeDBClusters

文件步驟

- aws:executeScript-刪除您在DBClusterId參數中指定的資料庫叢集。

AWSConfigRemediation-DeleteRDSClusterSnapshot

Description

AWSConfigRemediation-DeleteRDSClusterSnapshot執行手冊會刪除指定的 Amazon Relational Database Service 服務 (Amazon RDS) 叢集快照。

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

- AutomationAssume角色

  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)。
- 資料庫ClusterSnapshot代碼

  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 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
- 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) 叢集快照識別碼刪除指定的 Amazon RDS 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 (Amazon RDS) 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

- AutomationAssume角色

  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)。
- DbiResource識別碼

  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。
- SkipFinal快照

  類型：布林值

  預設：false

  說明：(選擇性) 如果設為`true`，則在刪除資料庫執行個體之前，不會建立最終快照。

必要的 IAM 許可

此`AutomationAssumeRole`參數需要執行下列動作，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 (Amazon RDS) 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

- AutomationAssume角色

  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)。
- DbSnapshot識別碼

  類型：字串

  說明：(必要) 您要刪除之快照的 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
- 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-DisablePublicAccessToRDSInstance執行手冊會停用您指定之 Amazon Relational Database Service (Amazon RDS) 資料庫 (資料庫) 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

- AutomationAssume角色

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)。

- DbiResource識別碼

  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 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
- 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 服務 (Amazon RDS) 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。
- AutomationAssume角色

  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) 您要啟用此`CopyTagsToSnapshot`設定之資料庫叢集的資源識別碼。

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
- 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 (Amazon RDS) 執行個體上啟用CopyTagsToSnapshot設定。啟用此設定會將資料庫執行個體的所有標籤複製到資料庫執行個體的快照。預設為不複製它們。AWS Config 必須在您執行此自動化操作的 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。

- AutomationAssume角色

  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)。

- DbiResource識別碼

  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 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`
- `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-EnableEnhancedMonitoringOnRDSInstance執行手冊會在您指定的 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

- AutomationAssume角色

  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)。
- MonitoringRole阿恩

  類型：字串

說明：(必填) IAM 角色的 Amazon 資源名稱 (ARN)，該角色允許 Amazon RDS 將增強型監控指標傳送到 Amazon CloudWatch 日誌。

- 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 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
- 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-在資料庫執行個體上啟用增強型監控。
- aws:executeScript-確認資料庫執行個體已啟用增強型監控。

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

- AutomationAssume角色

  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)。
- DbiResource識別碼

  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 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
- 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-EnableMultiAZOnRDSInstance執行手冊會將您的 Amazon Relational Database Service (Amazon RDS) 資料庫 (資料庫) 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，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

Linux,macOS, 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。
- AutomationAssume角色

  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)。
- DbiResource識別碼

  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 許可

此AutomationAssumeRole參數需要執行下列動作，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

- AutomationAssume角色

  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)。
- DbiResource識別碼

  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。
- PerformanceInsights公里 KeyId

  類型：字串

  預設：`alias/aws/rds`

  說明：(選用) Amazon 資源名稱 (ARN)、金鑰 ID 或您希望 Performance Insights 用來加密所有潛在敏感資料的 AWS Key Management Service (AWS KMS) 客戶受管金鑰的金鑰別名。如果您輸入此參數的關鍵別名，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 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
- 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-收集參數中指定的 AWS KMS 客戶管理金鑰的 ARN。PerformanceInsightsKMSKeyId
- 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 (Amazon RDS) 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

- AutomationAssume角色

  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 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
- 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-EnableRDSInstanceBackup執行手冊可為您指定的 Amazon Relational Database Service (Amazon RDS) 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。
- AutomationAssume角色

  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)。
- BackupRetention期間

  類型：整數

  有效值：1-35

  說明：(必要) 保留備份的天數。
- DbiResource識別碼

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。

- PreferredBackup視窗

  類型：字串

  說明：(選擇性) 建立備份期間的每日時間範圍 (以 UTC 為單位)。

  約束:

  - 必須為格式 hh24:mi-hh24:mi
  - 必須為國際標準時間 (UTC)
  - 不得和慣用的維護時段衝突
  - 必須至少 30 分鐘

必要的 IAM 許可

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執行手冊會在您指定的 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`PreferredMaintenanceWindow`置的修改。
- AutomationAssume角色

  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) 您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 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`
- `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上已啟用刪除保護。

AWSConfigRemediation-ModifyRDSInstancePortNumber

Description

AWSConfigRemediation-ModifyRDSInstancePortNumber執行手冊會修改 Amazon 關聯式資料庫服務 (Amazon RDS) 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

- AutomationAssume角色

  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。

- RDSDB 識InstanceResource別碼

  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 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
- 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-ModifyRDSSnapshotPermission執行手冊可協助您修改多個 Amazon Relational Database Service (Amazon RDS) 快照的許可。使用此 runbook，您可以製作快照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

  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。
- AccountIds

  類型: StringList

  預設：none

  說明：(選擇性) 您要共用快照的帳戶 ID。如果您輸入No參數值，則需要此Private參數。
- AccountPermission操作

  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

  說明：(必填) 您要修改其權限的 Amazon RDS 快照的名稱。

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
- rds:DescribeDBSnapshots
- rds:ModifyDBSnapshotAttribute

文件步驟

1. aws:executeScript-驗證SnapshotIdentifiers參數中提供的快照 ID。驗證 ID 之後，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

SharewithOther帳戶. 結果

MakePrivate。結果。

MakePrivate. 命令。

AWSPremiumSupport-PostgreSQLWorkloadReview

Description

AWSPremiumSupport-PostgreSQLWorkloadReview執行手冊會擷取您的 Amazon Relational Database Service 服務 (Amazon RDS) PostgreSQL 資料庫使用量統計資料的多個快照。 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。統計資料是使用一組自訂 SQL 和殼層指令碼收集的。這些指令碼會下載到由此執行手冊建立的暫時性 Amazon 彈性運算雲端 (Amazon EC2) 執行個體中。 AWS 帳戶 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。使用者名稱必須具有查詢標準 PostgreSQL 統計資料檢視和函數的權限。

這個 runbook 會自動在您 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 VPC 的私有子網路中啟動的虛擬私有雲端 (VPC) 和 Amazon EC2 執行個體，可選擇使用 NAT 閘道連線至網際網路。
- 附加到臨時 Amazon EC2 執行個體的 AWS Identity and Access Management (IAM) 角色，具有擷取機 Secrets Manager 碼值的許可。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。
- VPC 對等連接，可讓您的資料庫執行個體和暫時的 Amazon EC2 執行個體之間進行連線。
- 連接到臨時 VPC 的 Systems Manager 管理員、秘密管理員和 Amazon S3 VPC 人雲端端點。
- 包含已註冊任務的維護時段，可定期啟動和停止暫時 Amazon EC2 執行個體、執行資料收集指令碼，以及將檔案上傳到 Amazon S3 儲存貯體。也會為維護時段建立 IAM 角色，以提供執行已註冊工作的許可。

當 runbook 完成時，會刪除用於建立必要 AWS 資源的 AWS CloudFormation 堆疊，並將報告上傳到您選擇的 Amazon S3 儲存貯體，並選擇性地將 AWS Support 案例上傳。

> **Note**
>
> 依預設，暫時性 Amazon EC2 執行個體的根 Amazon EBS 磁碟區會保留下來。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。在使用本手冊之前，請聯絡您的技術客戶經理 (TAM) 或 TAM 專家 (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 配額請確保您尚未達到可在帳戶和使用此手冊的區域中建立的 Amazon EC2 執行個體或 VPC 數量上限。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 PostgreSQL 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 for PostgreSQL 資料庫執行個體上使用參數。
  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，但此參數可提供與每個查詢 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。

資料安全性與控管本執行手冊透過查詢 PostgreSQL 統計資料檢視和函數來收集統計資料。請確定SecretId參數中提供的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，並可位於中s3://*DOC-EXAMPLE-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。請聯絡您的 AWS TAM，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 VPC 對等連線傳輸臨時 Amazon EC2 執行個體的流量。

使用者建立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下列許可會新增至與臨時 Amazon EC2 執行個體關聯的 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:::DOC-EXAMPLE-BUCKET",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/automation execution id/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account id:secret:secret id",
            "Effect": "Allow"
        },
        {
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:DescribeCases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

此 Systems Manager 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

  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。
- 資料庫 InstanceIdentifier

  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

  說明：(必要) 秘密的 ARN 包含使用者名稱和密碼金鑰值配對的秘密。 AWS CloudFormation 堆疊會建立具有此 ARN `GetSecretValue` 作業許可的 IAM 政策。證明資料是用來允許暫時執行處理收集資料庫統計資料。請連絡您的 TAM 或 STAM，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。我們建議您在執行此自動化操作之前聯絡您的 TAM 或 STAM。

- SupportCase

  類型：字串

  說明：（可選）TAM 或 STAM 提供的 AWS Support 案例編號。如果提供，runbook 會更新案例並附加收集的資料。此選項要求臨時 Amazon EC2 執行個體具有網際網路連線能力，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:PutObject` API 作業的許可。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 VPC 的 IP 位址範圍 (例如)，`172.31.0.0/16`以 CIDR 標記法表示。請確定您選取的 CIDR 不會與資料庫執行個體連線的任何現有 VPC 重疊或相符。您可以建立的最小 VPC 使用 /28 子網路遮罩，而最大的 VPC 則使用 /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。系統會新增 IPv4 路由，透過新建立的 VPC 對等連線將流量路由到暫時的 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 端點進行通訊。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

- EbsVolumeDeleteOn終止

  類型：字串

  說明：(選用) 如果設定為`true`，則會在執行手冊完成後刪除暫存 Amazon EC2 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 許可

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 執行個體執行中為止。
7. aws:executeAwsApi-取得由建立之臨時 Amazon EC2 執行個體和 VPC 對等連線的 ID。 AWS CloudFormation
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能力。
9. aws:executeAwsApi-標記連接到臨時 Amazon EC2 實例的亞馬遜 EBS 磁碟區。
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-等待直到臨時的 Amazon EC2 執行個體由系統管理員管理。如果此步驟逾時或失敗，則 runbook 會重新啟動執行個體。
    a. aws:executeAwsApi-如果上一個步驟失敗或逾時，請重新啟動臨時 Amazon EC2 執行個體。
    b. aws:waitForAwsResourceProperty-等待暫時的 Amazon EC2 執行個體在重新開機後由系統管理員管理。
12. aws:runCommand-在暫時的 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-獲取維護窗口的 ID 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-等待直到臨時的 Amazon EC2 執行個體由系統管理員管理。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-等待暫時的 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-停止暫時性 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。

24aws:waitForAwsResourceProperty-等待 AWS CloudFormation 堆疊處於終端機狀態後再刪除。

25aws:executeAwsApi-刪除維護時段以外的 AWS CloudFormation 堆疊。如果EbsVolumeDeleteOnTermination參數值設定為，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 (Amazon RDS) 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

  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) 您要重新開機之 Amazon RDS 資料庫執行個體的識別碼。

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 (Amazon RDS) 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

  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。
- InstanceId

  類型：字串

  說明：要啟動的 Amazon RDS 執行個體的識別碼 (必填)。

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

  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。

- 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 許可

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 (Amazon RDS) 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

  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。
- InstanceId

  類型：字串

  說明：要停止的 Amazon RDS 執行個體識別碼 (必填)。

AWSSupport-TroubleshootConnectivityToRDS

Description

AWSSupport-TroubleshootConnectivityToRDS執行手冊會診斷 EC2 執行個體和 Amazon Relational Database Service 執行個體之間的連線問題。自動化會確認資料庫執行個體可用，然後會檢查關聯的安全群組規則、網路存取控制清單 (網路 ACL)，以及路由表來檢查是否有潛在的連線能力問題。

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。
- 資料庫 InstanceIdentifier

  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}$

  描述：(必要) 要測試連線能力的來源 EC2 執行個體 ID。

必要的 IAM 許可

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 ACL 的相關資訊。
- aws:executeAwsApi-取得資料庫執行個體子網路 CIDR。
- aws:executeAwsApi-取得 EC2 執行個體的相關資訊。
- aws:executeAwsApi-取得 EC2 執行個體網路 ACL 的相關資訊。
- aws:executeAwsApi-取得與 EC2 執行個體相關聯之安全群組的相關資訊。
- aws:executeAwsApi-取得與資料庫執行個體相關聯之安全群組的相關資訊。
- aws:executeAwsApi-取得與 EC2 執行個體相關聯之路由表的相關資訊。
- aws:executeAwsApi-取得與 EC2 執行個體之 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-取得與資料庫執行個體之 Amazon VPC 相關聯之主路由表的相關資訊。
- aws:executeScript-評估安全性群組規則。
- aws:executeScript-評估網路 ACL。
- aws:executeScript-評估路由表。
- aws:sleep-結束自動化

輸出

GetRDs InstanceProperties .DB InstanceIdentifier -自動化中使用的資料庫執行個體。

GetRDS 的 InstanceProperties .DB InstanceStatus -數據庫實例的當前狀態。

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網路 ACL 與資料庫執行個體網路 ACL 的結果。

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

這項功能AWSSupport-TroubleshootRDSIAMAuthentication可協助針對 Amazon RDS for PostgreSQL 於 MySQL、Amazon RDS for MySQL、Amazon RDS for MariaDB 極光 PostgreSQL 和 Amazon Aurora MySQL 執行個體進行疑難排解 AWS Identity and Access Management (IAM) 身份驗證。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**
>
> 此手冊不支持 Amazon RDS for Oracle 或 Amazon RDS for Microsoft SQL Server。

> **Important**
>
> 如果提供來源 Amazon EC2 執行個體，而目標資料庫是 Amazon RDS，則會叫用子系自動化來AWSSupport-TroubleshootConnectivityToRDS對 TCP 連線進行故障排除。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 身分驗證連接到 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：驗證輸入：驗證輸入到自動化。
- 步驟 2： branchOnSource提供 EC2：驗證輸入參數中是否提供來源 Amazon EC2 執行個體 ID。
- 步驟 3：驗證器連線能力：驗證來源 Amazon EC2 執行個體的 Amazon RDS 連線 (若有提供)。

- 步驟 4：驗證機制：驗證 IAM 身份驗證功能是否已啟用。
- 步驟 5：驗證 Iam 政策：驗證所提供的 IAM 使用者/角色中是否存在所需的 IAM 許可。
- 第 6 步：生成報告：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

  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。
- 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.`
- 資料庫 InstanceIdentifier

  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：(選用) 如果您要從在相同帳戶和區域中執行的 Amazon EC2 執行個體連線至 Amazon RDS 資料庫執行個體，則為 Amazon EC2 執行個體 ID。如果來源不是 Amazon EC2 執行個體，或目標 Amazon RDS 類型為 Aurora 資料庫叢集，請勿指定此參數。

  預設：""

- 雙向投資 RoleName

  類型：字串

  說明：(選用) 用於以 IAM 為基礎的驗證的 IAM 角色名稱。僅在未提供參數DBIAMUserName時提供，否則將其保留空白。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：""

- 雙向投資 UserName

  類型：字串

  說明：(選用) 用於以 IAM 為基礎的驗證的 IAM 使用者名稱。僅在未提供DBIAMRoleName參數時提供，否則將其保留空白。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：""

- 資料庫 UserName

  類型：字串

  描述：(選用) 對應至 IAM 角色/使用者的資料庫使用者名稱，以便在資料庫中進行以 IAM 為基礎的驗證。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 許可

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

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- iam:GetPolicy
- iam:GetRole
- iam:GetUser
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies
- iam:SimulatePrincipalPolicy
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

指示

1. 導航到控制AWSSupport台中的故障排除功能。AWS Systems Manager
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)：

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

- RDST 類型 (必要)：

  選取您嘗試連線並進行驗證的 Amazon RDS 類型。從兩個允許的值中選擇：`Amazon RDS`或`Amazon Aurora Cluster.`

- 資料庫 InstanceIdentifier (必要)：

  輸入您嘗試連線的目標 Amazon RDS 資料庫執行個體或 Aurora 叢集的識別碼，然後使用 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 執行個體連線至 Amazon RDS 資料庫執行個體，請提供 Amazon EC2 執行個體識別碼。如果來源不是 Amazon EC2 或目標 Amazon RDS 類型是 Aurora 叢集，請保留空白。

- 美國海外投資調查 RoleName (可選):

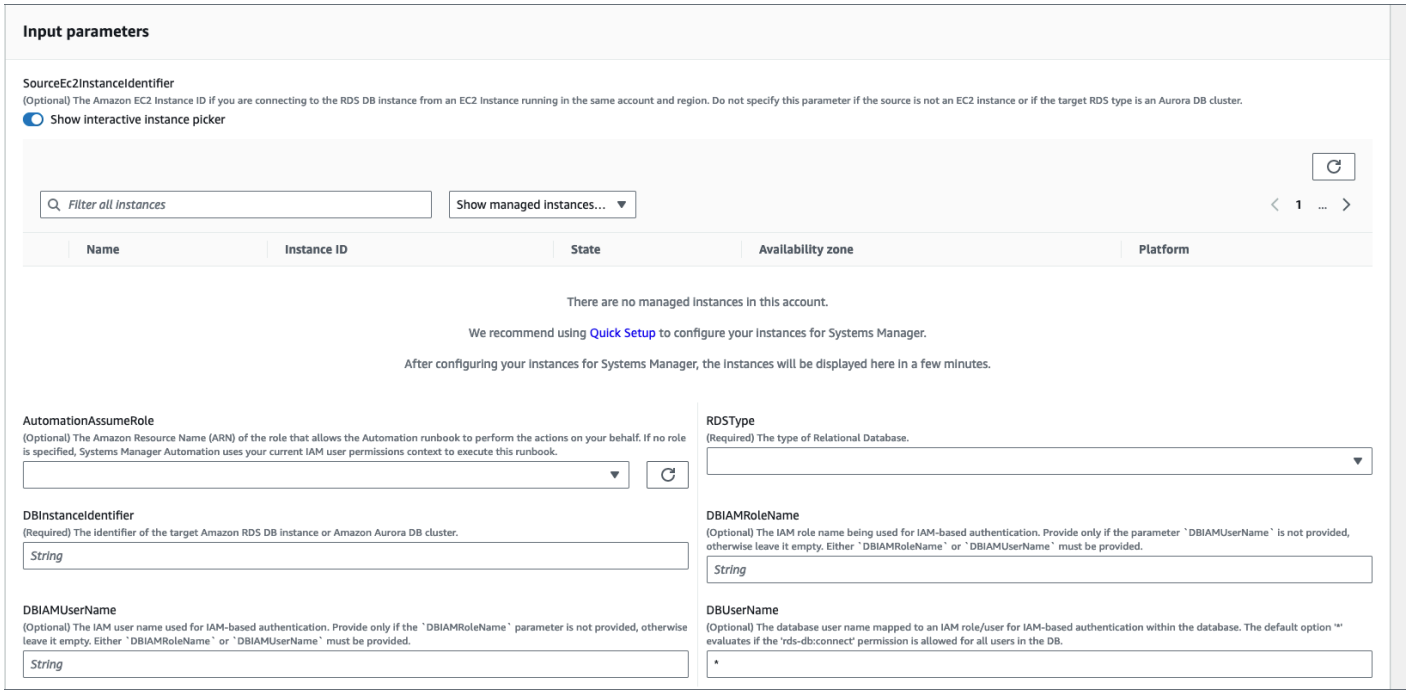
  輸入用於以 IAM 為基礎的身份驗證的 IAM 角色名稱。僅在未提`DBIAMUserName`供時提供；否則，請留空。`DBIAMRoleName`或`DBIAMUserName`必須提供。

- 美國海外投資調查 UserName (可選):

  輸入用於以 IAM 為基礎的身份驗證的 IAM 使用者。僅在未提`DBIAMRoleName`供時提供，否則保留空白。`DBIAMRoleName`或`DBIAMUserName`必須提供。

- 數據庫UserName （ 可選 ）：

  輸入對應至 IAM 角色/使用者的資料庫使用者，以便在資料庫中進行以 IAM 為基礎的驗證。預設選項用*於評估；此欄位中未提供任何內容。



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：
   - 第 1 步：驗證輸入：

     驗證輸入到自動化-SourceEC2InstanceIdentifier（可選），DBInstanceIdentifier或ClusterID，和DBIAMRoleName或DBIAMUserName。它驗證輸入的輸入參數是否存在於您的帳戶和地區。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。
   - 第二步：提供 branchOnSource EC2：

     驗證輸入參數中是否提供來源 Amazon EC2，而資料庫是否為 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，即 Amazon EC2-亞馬遜 RDS 連接驗證，並繼續進行步驟 4。
   - 步驟 3：驗證器連線：

     如果輸入參數中提供了來源 Amazon EC2，而資料庫是 Amazon RDS，則步驟 2 會啟動步驟 3。在此步驟中，系統會叫用子系自動化AWSSupport-TroubleshootConnectivityToRDS來驗證來自來源 Amazon Amazon EC2 RDS 連線能力。子自動化執行手冊AWSSupport-TroubleshootConnectivityToRDS會驗證所需的網路組態 (Amazon Virtual Private Cloud

[Amazon VPC]、安全群組、網路存取控制清單 [NACL]、Amazon RDS 可用性) 是否已就位，以便您可以從 Amazon EC2 執行個體連線到 Amazon RDS 執行個體。

- 步驟 4：驗證系統認證：

  驗證是否已在 Amazon RDS 執行個體或 Aurora 叢集上啟用 IAM 身份驗證功能。

- 步驟 5：驗證策略：

  驗證傳遞的 IAM 使用者/角色中是否存在必要的 IAM 許可，以便讓 IAM 登入資料在指定資料庫使用者 (如果有的話) 的 Amazon RDS 執行個體中進行身份驗證。

- 步驟 6：生成報告：

  取得先前步驟的所有資訊，並列印每個步驟的結果或輸出。它還列出了使用 IAM 登入資料連接到 Amazon RDS 執行個體所需參考和執行的步驟。

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 IAM 用戶/角色權限以連接到數據庫：

  驗證傳遞的 IAM 使用者/角色中是否存在必要的 IAM 許可，以便讓 IAM 登入資料在指定資料庫使用者 (如果有的話) 的 Amazon RDS 執行個體中進行身份驗證。

- 檢查數據庫的基於 IAM 的身份驗證屬性：

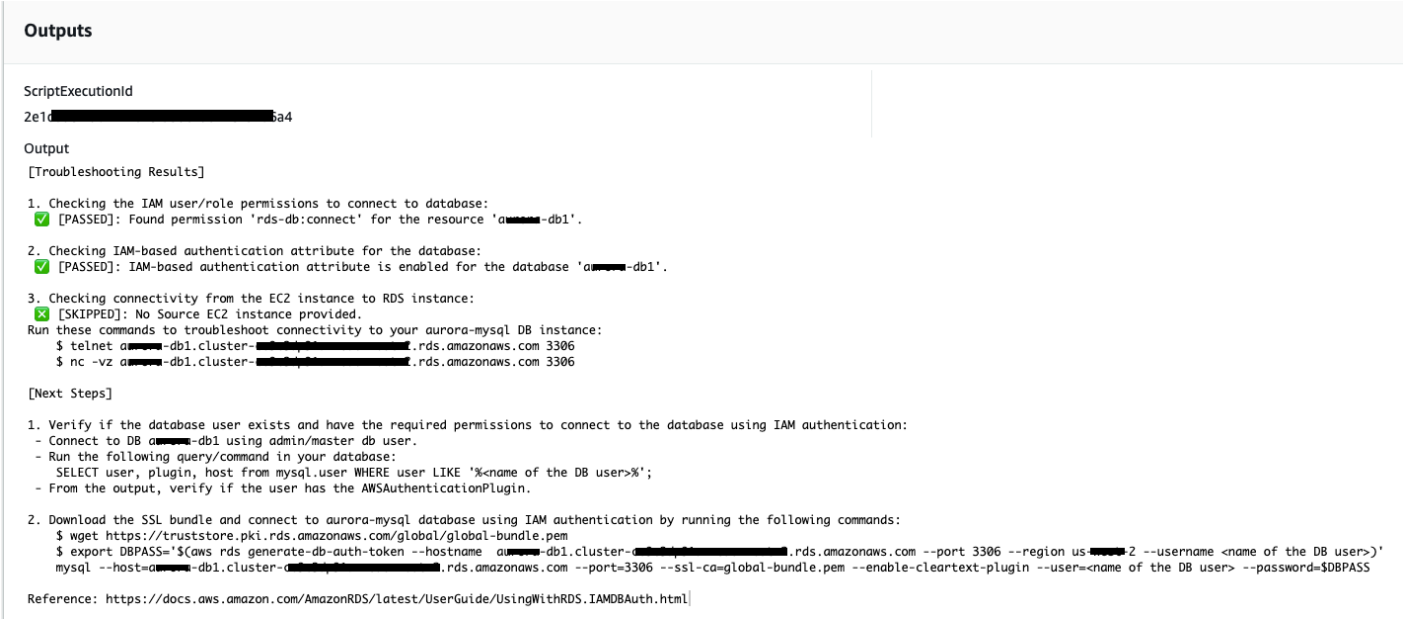
  驗證是否為指定的 Amazon RDS 資料庫/Aurora 叢集啟用 IAM 身份驗證的功能。

- 檢查從 Amazon EC2 執行個體到 Amazon RDS 執行個體的連線能力：

  驗證是否已設置所需的網路組態 (Amazon VPC、安全群組、NACL、Amazon RDS 可用性)，以便您可以從 Amazon EC2 執行個體連線到 Amazon RDS 執行個體。

- 後續步驟:

  列出使用 IAM 登入資料連接到 Amazon RDS 執行個體時所要參考和執行的命令和步驟。



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 (Amazon RDS)/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？

此執行手冊會判斷 Amazon RDS 資料庫執行個體是否會進入不相容的網路狀態，或者如果有，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：

- 每個區域的 Amazon 彈性網路界面 (ENI) 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 (`enableDnsSupport`和`enableDnsHostnames`) 的設定。

> **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，文檔將在第一步中失敗。

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 許可

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

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

樣本政策：

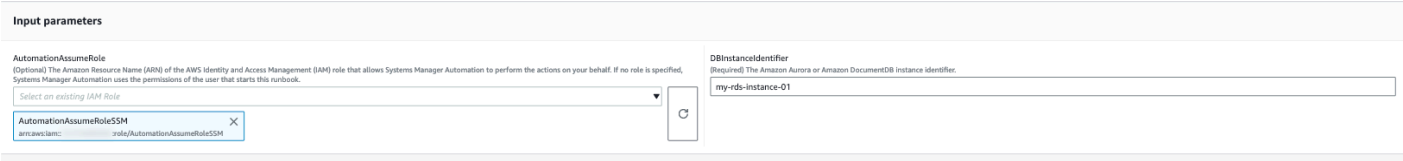
```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "ValidateRdsNetwork",
                    "Effect": "Allow",
                    "Action": [
                        "rds:DescribeDBInstances",
                        "servicequotas:GetServiceQuota",
                        "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)：

     (IAM) 角色的 Amazon 資源名稱 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。
   - 資料庫 InstanceIdentifier (必要)：

     輸入 Amazon Relational Database Service 執行個體識別碼。



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:

     檢查提供的實例標識符是否存在，並具有以下任何狀態：`available`、`stopped`、或`incompatible-network`。

   - 步驟二 gatherRdsInformation：

     收集有關 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:

     檢查該地區目前的 Amazon ENI 可用配額。

   - 步驟四 validateVpcAttributes:

     驗證 Amazon VPC 的 DNS 參數 (`enableDnsSupport`和`enableDnsHostnames`) 是否設定為 true (如果 Amazon RDS 執行個體是`PubliclyAccessible`否設定為)。

   - 步驟五 validateSubnetAttributes:

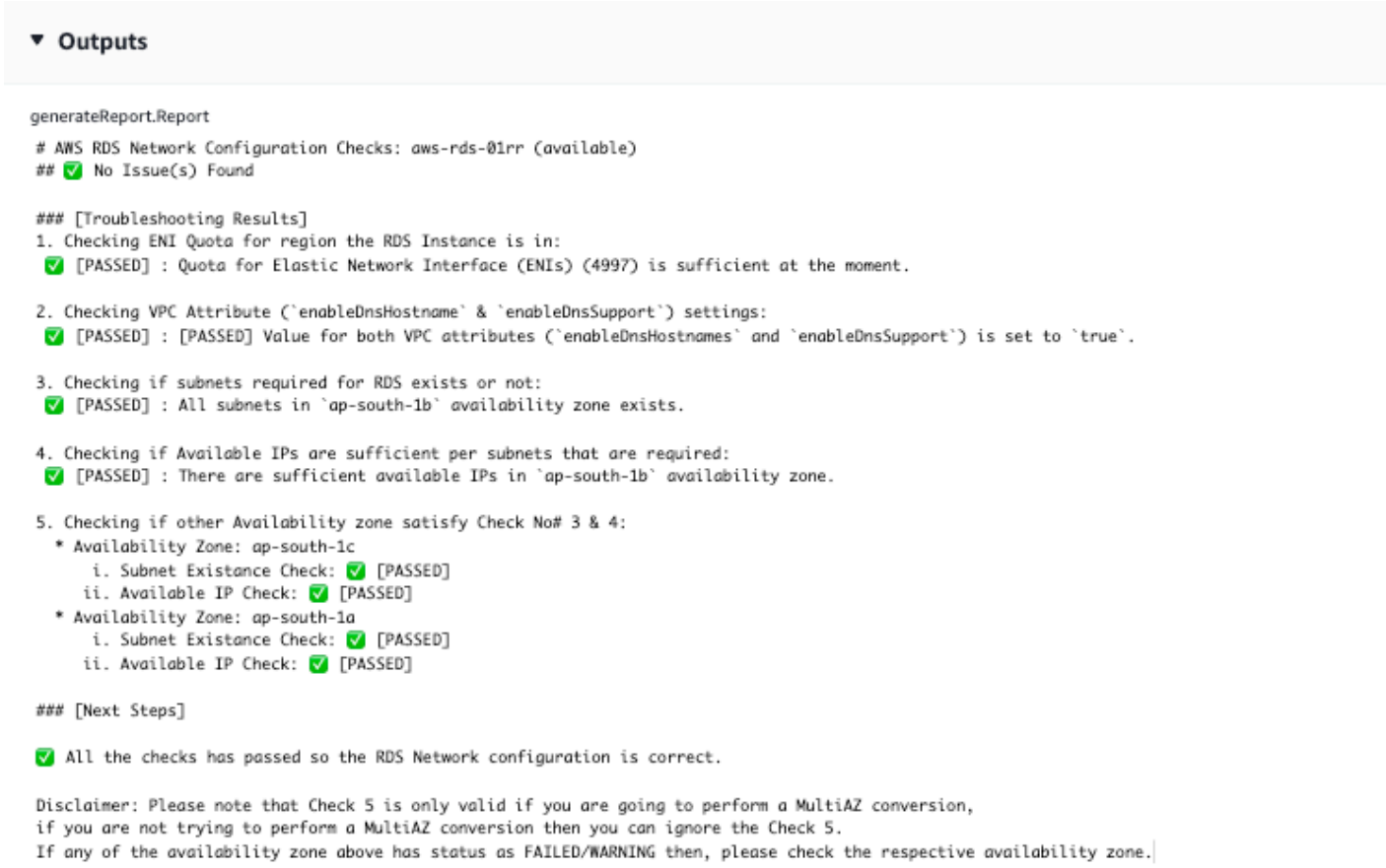
     驗證中是否存在子網路，`DBSubnetGroup`並檢查每個子網路是否有可用的 IP。

   - 步驟 6：生成報告：

     取得先前步驟的所有資訊，並列印每個步驟的結果或輸出。它還列出了使用 IAM 登入資料連接到 Amazon RDS 執行個體的參考和執行步驟。

7. 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：



具有錯誤網路組態的 Amazon RDS 執行個體 (VPC 屬性設定 enableDnsHostnames 為 false)：

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服務文件

- 如何解決處於不相容網路狀態的 Amazon RDS 資料庫的問題？
- 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

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

- AutomationAssume角色

  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 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`
- `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

- AutomationAssume角色

  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 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
- 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

- AutomationAssume角色

  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 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
- 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

- AutomationAssume角色

  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 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
- 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

- AutomationAssume角色

  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) 您要啟用加密之叢集的唯一識別碼。
- KMSKEARN

  類型：字串

  描述：(必填) 您要用來加密叢集資料之 AWS KMS 客戶受管金鑰的 Amazon 資源名稱 (ARN)。

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
- 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。如需增強型虛擬私人雲端路由的相關資訊，請參閱亞馬 Amazon Redshift 管理指南中的增強型 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

- AutomationAssume角色

  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) 您要在其上啟用增強型 VPC 路由的叢集的唯一識別碼。

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`
- `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，才能針對您指定的 Amazon Redshift 叢集使用 SSL。

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

- AutomationAssume角色

  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) 您要在其上啟用增強型 VPC 路由的叢集的唯一識別碼。

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
- 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

- AllowVersion升級

  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。
- AutomationAssume角色

  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) 您要在其上啟用增強型 VPC 路由的叢集的唯一識別碼。

- PreferredMaintenance視窗

類型：字串

說明：（必要）可以進行系統維護的每週時間範圍（以 UTC 為單位）。

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
- 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

- AutomationAssume角色

  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。

- NumberOf節點

  類型：整數

  有效值：

  描述：(選擇性) 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 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`
- `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

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。

- 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) 智慧型分層組態的識別碼。這可以是新的組態識別碼，也可以是現有組態的識別碼。

- NumberOfDaysTo封存

  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 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
- s3:GetIntelligentTieringConfiguration
- s3:PutIntelligentTieringConfiguration

文件步驟

- PutsBucketIntelligentTieringConfiguration (AWS：執行指令碼)-為指定儲存貯體建立或更新 Amazon S3 智慧型分層組態。
- VerifyBucketIntelligentTiering組態 (aws: 斷言AwsResource屬性)-驗證 S3 儲存貯體智慧型組態已套用至指定的儲存貯體。

AWS-ConfigureS3BucketLogging

Description

在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

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。
- 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：完整控制 | 讀取 | 寫入

  描述：(選用) 指派給儲存貯體之被授予者的記錄許可。
- GranteeEmail地址

  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：(選用) 被授予者群組的 URI。
- TargetBucket

  類型：字串

  描述：(必要) 指定您希望 Amazon S3 存放伺服器存取日誌的儲存貯體。您可以將日誌傳送到您擁有的任何儲存貯體。您也可以設定多個儲存貯體，以將其日誌傳送至相同的目標儲存貯體。在這種情況下，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

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。
- 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 | 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。
- BlockPublicACL

  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 (ACL)，以及您在`BucketName`參數中指定之 S3 儲存貯體中存放的物件。

- BlockPublic政策

  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。

- IgnorePublicACL

  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`參數中指定之 S3 儲存貯體的所有公有 ACL。

- RestrictPublic鏟斗

  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 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`
- `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

Linux,macOS, 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。

- AutomationAssume角色

  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)。

- BlockPublicACL

  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 (ACL)。

- BlockPublic政策

  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。

- IgnorePublicACL

  類型：布林值

  預設：true

  說明：(選擇性) 如果設定為`true`，Amazon S3 會忽略 AWS 帳戶 您在`AccountId`參數中指定之 S3 儲存貯體所擁有的所有公有 ACL。

- RestrictPublic鏟斗

  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。

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
- 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

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。

- BucketName

  類型：字串

  說明：(必要) 您要設定的 S3 儲存貯體名稱。

- DaysUntil到期

  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 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`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

文件步驟

- ConfigureExpireMultipartUploads (AWS：執行程序檔)-設定值區的生命週期政策。

- VerifyExpireMultipartUploads (AWS：執行程序檔)-驗證儲存貯體已設定生命週期原則。

輸出

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

Description

使用 Amazon Simple Storage Service (Amazon S3) 停`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

  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。
- 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

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。
- BucketName

  類型：字串

  描述：(必要) 您想要加密內容的 S3 儲存貯體之名稱。
- SSEAlgorithm

  類型：字串

  預設：AES256

描述：(選用) 用於預設加密的伺服器端加密演算法。

AWS-EnableS3BucketKeys

Description

AWS-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 () 金鑰 (DSSE-KMS AWS 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

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。

- 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。

- 公里 KeyId

  類型：字串

  說明：(選用) Amazon 資源名稱 (ARN)、金鑰 ID 或您要用於伺服器端加密之 AWS Key Management Service (AWS KMS) 客戶受管金鑰的金鑰別名。

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
- s3:GetEncryptionConfiguration
- s3:PutEncryptionConfiguration

文件步驟

- ChooseEncryptionType (aws: 分支)-評估為KmsKeyId參數提供的值，以確定將使用 SSE-S3 (AES256) 還是 SSE KMS。
- PutBucketKeySKM (aws: 執行AwsApi)-將BucketKeyEnabled屬性設定true為使用指定的指定 S3 儲存貯體。KmsKeyId
- PutBucket金鑰儲存貯體 256 (aws：執行AwsApi)-將具有 AES256 加密的指定 S3 儲存貯體的BucketKeyEnabled屬性設定true為。
- 驗證 3 BucketKeysEnabled (aws: 斷言AwsResource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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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 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
- 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 會建立一個亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體政策聲明，明確拒絕向您指定的 Amazon S3 儲存貯體發出 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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 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
- 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，明確拒絕 HTTP 要求。

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

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。

- CloudWatchLogGroup名稱

  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。

- CloudWatchLogStream名稱

  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作`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 HTTP 標頭傳回。

- 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 許可

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:::awsexamplebucket1/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::awsexamplebucket1",
            "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 S3 儲存貯體政策中是否存在 GetObject API 動作的明確拒絕。
- 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 HTTP 標頭傳回。
- 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。
- 檢查物件的 ACL 是否授與匿名使用者READ或FULL_CONTROL權限。
- 傳回與物件相關聯的標籤。
- 使用模擬的 IAM 政策來確認在 S3 儲存貯體政策中該物件是否有針對 GetObject API 動作的明確拒絕。
- 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

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。

- NotebookInstance姓名

  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 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
- sagemaker:DescribeNotebookInstance
- sagemaker:StartNotebookInstance
- sagemaker:StopNotebookInstance
- sagemaker:UpdateNotebookInstance

文件步驟

- CheckNotebookInstanceStatus (aws：執行AwsApi)：檢查筆記本執行個體的目前狀態。
- StopOrUpdateNotebookInstance （aws：分支）：根據筆記本實例的狀態進行分支。
- StopNotebookInstance （aws：執行AwsApi）：如果狀態為，則啟動實例。stopped
- WaitForInstanceToStop （aws：等待 ForAwsResourceProperty）：驗證實例是。stopped
- UpdateNotebookInstance （aws：執行AwsApi）：禁用筆記本實例上的根訪問權限。
- WaitForNotebookUpdate （aws：wait ForAwsResourceProperty）：驗證根訪問權限已被禁用，並且實例具有狀態。stopped
- ChooseInstanceStart （aws：分支）：根據是否應該啟動實例的分支。
- StartNotebookInstance （aws：執行AwsApi）：啟動筆記本實例。
- VerifyNotebookInstanceStatus （aws：wait ForAwsResourceProperty）：available在禁用根訪問權限之前驗證實例是否處於狀態。
- VerifyNotebookInstanceRootAccess （aws：斷言AwsResource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-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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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 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
- 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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。
- RotationLambda阿恩

  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）您要旋轉的秘密的 Amazon 資源名稱（ARN）。

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`
- `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-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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。

- EnableDefault標準

  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 許可

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

- 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. 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 IP，根據建議的AWS Shield Advanced保護最佳實務來為其組態設定執行。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 包含一系列對啟用公開存取的各種資源類型的檢查，以及是否根據 AWSDDoS 最佳做法白皮書中的建議設定了保護。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 HTML 報告形式傳回發現項目，儲存在提供的 Amazon S3 儲存貯體中。

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

  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。
- AssessmentType

  類型：字串

  說明：(選擇性) 決定要評估 DDoS 彈性評估的資源類型。默認情況下，runbook 將評估全球和區域資源。對於區域資源，runbook 會描述所有應用程式 (ALB) 和網路 (NLB) 負載平衡器，以及 /區域中所有的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 IAM 角色的 ARN，用於描述 Amazon S3 儲存貯體，並在儲存貯體位於不同AWS 帳戶的情況下AWS 帳戶封鎖公用存取組態。如果未指定此參數，runbook 會使用啟動此 runbook 的AutomationAssumeRole或 IAM 使用者 (如果AutomationAssumeRole未指定)。請參閱 runbook 描述中所需的權限部分。

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 許可

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 IAM 政策範例

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetAccountPublicAccessBlock"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicyStatus",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": "arn:aws:s3:::<bucket-name>",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::<bucket-name>/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "cloudfront:ListDistributions",
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkAcls",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "globalaccelerator:ListAccelerators",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "route53:ListHostedZones",
                "route53:GetHealthCheck",
                "shield:ListProtections",
                "shield:GetSubscriptionState",
                "shield:DescribeSubscription",
                "shield:DescribeEmergencyContactSettings",
                "shield:DescribeDRTAccess",
                "waf:GetWebACL",
                "waf:GetRateBasedRule",
                "wafv2:GetWebACL",
                "wafv2:GetWebACLForResource",
                "waf-regional:GetWebACLForResource",
                "waf-regional:GetWebACL"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
                            {
                                "Action": "iam:PassRole",
                                "Resource": "arn:aws:iam::123456789012:role/
<AutomationAssumeRole-Name>",
                                "Effect": "Allow"
                            }
                        ]
                    }
```

指示

1. 導航到控AWS Systems Manager制台ResiliencyAssessment中的 AWSPremiumSupport-DDoS。
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)：

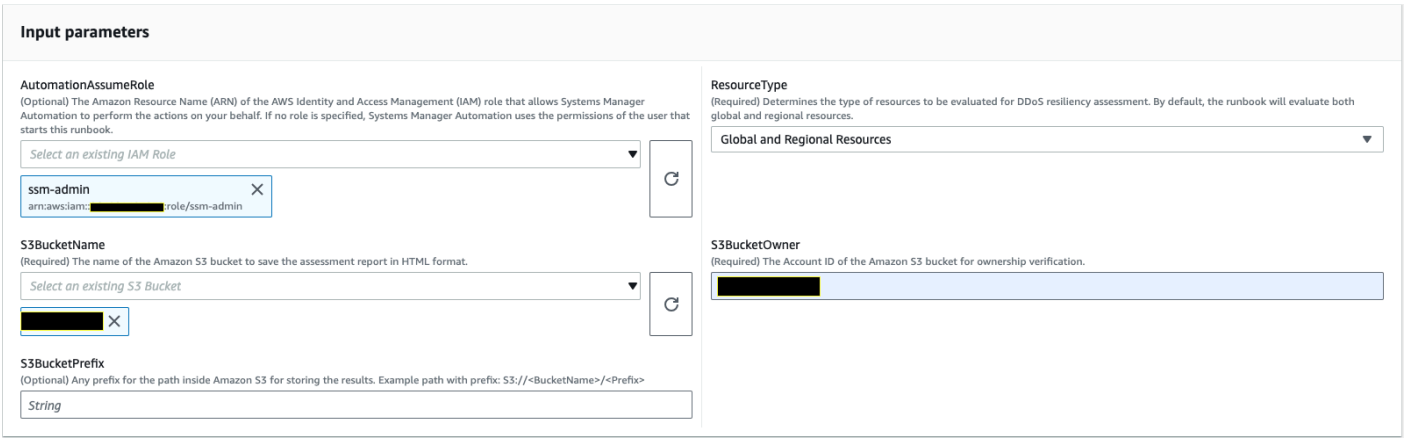
     (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓 Systems Manager 自動化代表您執行動作。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
   - AssessmentType (選擇性)：

     決定要評估 DDoS 彈性評估的資源類型。默認情況下，runbook 評估全球和區域資源。
   - S3 BucketName (必要)：

     用於以 HTML 格式儲存評估報告儲存的 Amazon S3 儲存貯體的名稱。
   - 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。



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：AWS Shield回應團隊 (SRT) 團隊的 IAM 存取權限、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:

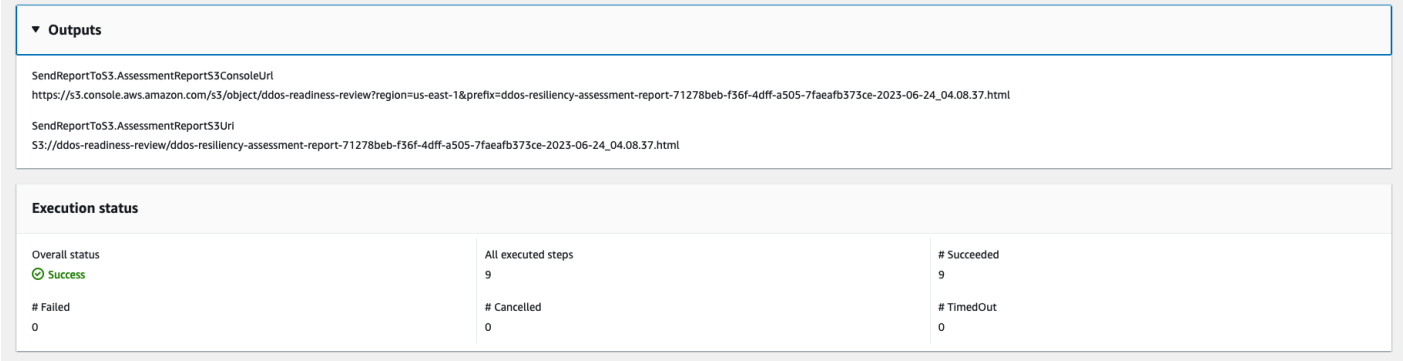
  檢閱 Shield 進階受保護的區域資源，例如應用程式負載平衡器、網路負載平衡器、傳統負載平衡器、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體 (彈性 IP)。

- SendReportTo中三：

  將 DDoS 評估報告詳細資料上傳到 Amazon S3 儲存貯體。

7. 完成後，評估報告 HTML 檔案的 URI 會提供在 Amazon S3 儲存貯體中：

   S3 主控台連結和 Amazon S3 URI，用於成功執行工作手冊的報告



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 或亞馬遜 Amazon Simple Queue Service (Amazon SQS) 端點的交付狀態記錄。Platform application這可讓 Amazon SNS 將失敗的警示和成功警示通知的範例百分比記錄到 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

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。

- EndpointType

  類型：字串

  有效值：

  - HTTP
  - Firehose
  - Lambda
  - 應用程式
  - SQS

  說明：(必填) 您要記錄其交付狀態通知訊息的 Amazon SNS 主題端點類型。

- TopicArn

  類型：字串

  說明：(必要) 您要設定傳送狀態記錄的 Amazon SNS 主題的 ARN。

- SuccessFeedbackRoleArn

  類型：字串

  描述：(必要) Amazon SNS 用來將成功通知訊息的日誌傳送至該角色的 IAM 角色的 ARN。CloudWatch

- SuccessFeedbackSampleRate

  類型：字串

  有效值：0 至 100

  說明：(必要) 指定 Amazon SNS 主題要取樣的成功訊息百分比。

- FailureFeedbackRoleArn

  類型：字串

描述：(必要) Amazon SNS 用來傳送失敗通知訊息日誌的 IAM 角色的 ARN。 CloudWatch

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
- 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

VerifyDeliveryStatusLogging已啟用。 GetTopicAttributesResponse -來自 GetTopicAttributes API 操作的響應。

VerifyDeliveryStatusLogging已啟用。 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 應該只用作基準，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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。
- KmsKey阿恩

  類型：字串

  說明：(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) 您要加密之 Amazon SNS 主題的 ARN。

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`

- 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-確認在 Amazon SNS 主題上啟用了加密。

AWS-PublishSNSNotification

Description

將通知發佈到 Amazon SNS。

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。
- 訊息

  類型：字串

描述：(必要) 要包含在 SNS 通知的訊息。

- TopicArn

  類型：字串

  描述：(必要) 要發佈通知之 SNS 主題的 ARN。

Amazon SQS

AWS Systems Manager 自動化為 Amazon Simple Queue Service (Amazon SQS) 提供預先定義的手冊。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

AWS-EnableSQSEncryption執行手冊為 Amazon Simple Queue Service (Amazon SQS) 啟用靜態加密。Amazon SQS 佇列可以使用 Amazon SQS 受管金鑰 (SSE-SQS) 或 () 受管金鑰 AWS Key Management Service (SSE-KMSAWS 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,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。

- QueueUrl

  類型：字串

  說明：(必填) 您要在其上啟用加密之 Amazon SQS 佇列的網址。

- KmsKeyId

  類型：字串

  說明：(選擇性) 用於加密的AWS KMS金鑰。此值可以是全域唯一識別名、別名或索引鍵的 ARN，或是以「alias/」為前置詞的別名名稱。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 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`
- `sqs:GetQueueAttributes`

- `sqs:SetQueueAttributes`

文件步驟

- SelectKeyType （ aws：分支 ）：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：assertAwsResource屬性 ）-驗證 Amazon SQS 隊列上已啟用加密。
- VerifySqsEncryptionDefault （ aws：assertAwsResource屬性 ）-驗證 Amazon SQS 隊列上已啟用加密。

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

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。

- AssociationIds

  類型: StringList

  說明：(必要) 您要刪除之關聯 ID 的逗號分隔清單。

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:DeleteAssociation`

文件步驟

- `aws:executeScript`-刪除您在`AssociationIds`參數中指定的關聯。

AWS-BulkEditOpsItems

Description

`AWS-BulkEditOpsItems`runbook 可協助您編輯的狀態、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

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。
- 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。
- OpsItem身份證

  類型: StringList

  描述：(必要) 您想要編輯的 OpsItems 識別碼清單 (例如，OI-XXXXXXXX，OI)，以逗號分隔。
- 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 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
- 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。

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

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。

- 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 回應的選項，請參閱 AWS Systems Manager API 參考資料中的篩選OpsItem器。

- OpsInsight身份證

  類型：字串

  描述：(選擇性) 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 Simple Notification Service (Amazon SNS) 在自動化完成時傳送的通知。

- SnsTopic阿恩

  類型：字串

  說明：(選擇性) 您要在結果摘要傳送至 Amazon S3 時通知的 Amazon SNS 主題的 ARN。

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。

- 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 (包含SnsMessage參數值) 之後，系統會傳送通知至 Amazon SNS 主題 (如有指定)。

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

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。

- MaintenanceWindows

  類型: StringList

  描述：(必要) 您要啟用或停用之維護時段 ID 的逗號分隔清單。

- MaintenanceWindows狀態

  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 許可

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 Systems Manager 設定的 Linux 建立 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

- AmiId

  類型：字串

  說明：(必要) 用來啟動執行個體的 AMI ID。
- 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。
- GroupName

  類型：字串

  預設值：SSM 執SecurityGroupForLinux行個體

  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 權杖的使用設定為`optional`或`required`以判斷 ImDSv2 是選用的還是必要的。

- 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。

- KeyPair姓名

  類型：字串

  描述：(必要) 建立執行個體時要使用的金鑰對。

- RemoteAccessCidr

  類型：字串

  預設：0.0.0.0/0

  描述：(必要) 建立安全群組，並將 SSH 連接埠 (連接埠範圍 22) 開放給 CIDR 指定的 IP (預設為 0.0.0.0/0)。如果安全群組已存在，則不會修改，規則也不會變更。

- RoleName

  類型：字串

  預設值：超音波 ManagedInstance ProfileRole

  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：執行 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 (Amazon VPC) 或預設 Amazon VPC (如果未指定) 中。

AWS-CreateManagedWindowsInstance

Description

為 Systems Manager 設定的 Windows Server EC2 執行個體建立。

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

- AmiId

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

  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。

- GroupName

  類型：字串

  預設值：SSM 執SecurityGroupForLinux行個體

  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 權杖的使用設定為optional或required以判斷 ImDSv2 是選用的還是必要的。

- 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。

- KeyPair姓名

  類型：字串

描述：(必要) 建立執行個體時要使用的金鑰對。

- RemoteAccessCidr

  類型：字串

  預設：0.0.0.0/0

  描述：(必要) 建立安全群組，並將 RDP 連接埠 (連接埠範圍 3389) 開放給 CIDR 指定的 IP (預設為 0.0.0.0/0)。如果安全群組已存在，則不會修改，規則也不會變更。

- RoleName

  類型：字串

  預設值：超音波 ManagedInstance ProfileRole

  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：執行 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 (Amazon VPC) 或預設 Amazon VPC (如果未指定) 中。

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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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)。
- DestinationLog集團

  類型：字串

  描述：(必要) 記 CloudWatch 錄群組的名稱。

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

- 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

Linux,macOS, Windows

參數

- AutomationAssume角色

  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求的結果屬性。
- S3 BucketName

  類型：字串

  描述：(必要) 要下載輸出檔案的 S3 儲存貯體。
- SNS SuccessMessage

  類型：字串

  描述：（可選）當 runbook 完成時發送的消息。
- SNS TopicArn

  類型：字串

  說明：(必填) Amazon Simple Notification Service (Amazon SNS) 主題 ARN，以在下載完成時通知。
- syncName

  類型：字串

  描述：(選用) 資源資料同步的名稱。

文件步驟

取得 OpsSummaryStep — 擷取多達 5,000 個作業摘要，以便匯出成 CSV 檔案。

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

Linux,macOS, 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)。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。
- SNS TopicArn

  類型：字串

說明：(選用) Amazon Simple Notification Service (Amazon SNS) 主題 Amazon 資源名稱 (ARN)，以在下載完成時通知。

- SNS SuccessMessage

  類型：字串

  描述：(選擇性) 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 成功執行，匯出的修補程式報告物件會下載到您的目標 S3 儲存貯體。

AWS-SetupInventory

Description

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中繼資料。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

Linux,macOS, Windows

參數

- 應用程式

  類型：字串

  預設：Enabled

  描述：(選用) 收集已安裝之應用程式的中繼資料。
- AssociatedDoc姓名

  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。
- AssocWait時間

  類型：字串

  預設：PT5M

  描述：(選用) 庫存收集在庫存關聯開始時間到達時應暫停的時間量。時間使用 ISO 8601 格式。
- AutomationAssumeRole

  類型：字串

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。

- `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 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}]`

- InstanceDetailed信息

  類型：字串

  預設：Enabled

  描述：(選用) 收集執行個體的其他資訊，包括 CPU 型號、速度和核心數量等。

- InstanceIds

  類型：字串

  預設：*

描述：(必要) 您想要清查的 EC2 執行個體。

- LambdaAssume角色

  類型：字串

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

- NetworkConfig

  類型：字串

  預設：Enabled

  描述：(選用) 收集網路組態的中繼資料。

- 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

描述：(選用，僅 Windows 作業系統，需要 SSMAgent 2.2.64.0 及更新版本) 收集服務組態的資料。

- WindowsRegistry

  類型：字串

  描述：(選用) 收集 Microsoft Windows 登錄機碼的中繼資料。如需如何收集此類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 2.2.64.0 或更新版本。例如：[{"路徑」："HKEY_CURRENT_CONFIG\ 系統」，"遞歸」：真}, {"路徑」："HKEY_LOCAL_ 機器\ 軟體\ Amazon\「," ": [" 導引名 "]}] MachineImage ValueNames

- WindowsRoles

  類型：字串

  預設：Enabled

  描述：(選用) 收集執行個體上的 Windows 角色相關資訊。僅適用於 Windows 作業系統。需要 SSMAgent 2.2.64.0 或更新版本。

- WindowsUpdates

  類型：字串

  預設：Enabled

  描述：(選用) 收集執行個體上所有 Windows Update 的資料。

AWS-SetupManagedInstance

Description

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

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。
- InstanceId

  類型：字串

  描述：(必要) 要設定的 EC2 執行個體之 ID
- LambdaAssume角色

  類型：字串

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

  類型：字串

  預設值：超音波 RoleFor ManagedInstance

  描述：(選用) EC2 執行個體的 IAM 角色名稱。如果此角色不存在，則會建立此角色。指定此值時，請確認角色包含 AmazonSSM ManagedInstance 核心受管原則。

AWS-SetupManagedRoleOnEC2Instance

Description

為 Systems Manager 員存取權限設定具有 SSM RoleForManagedInstance 受管 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

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。
- InstanceId

  類型：字串

  描述：(必要) 要設定的 EC2 執行個體之 ID
- LambdaAssume角色

  類型：字串

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

  類型：字串

  預設值：超音波 RoleFor ManagedInstance

  描述：(選用) EC2 執行個體的 IAM 角色名稱。如果此角色不存在，則會建立此角色。指定此值時，請確認角色包含 AmazonSSM ManagedInstance 核心受管原則。

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 的主要目標是找出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
- 紅帽企業版工作系統 8.X 和 9.X
- CENTOS 8.X 及 9.X
- 速度 15.X

參數

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: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：

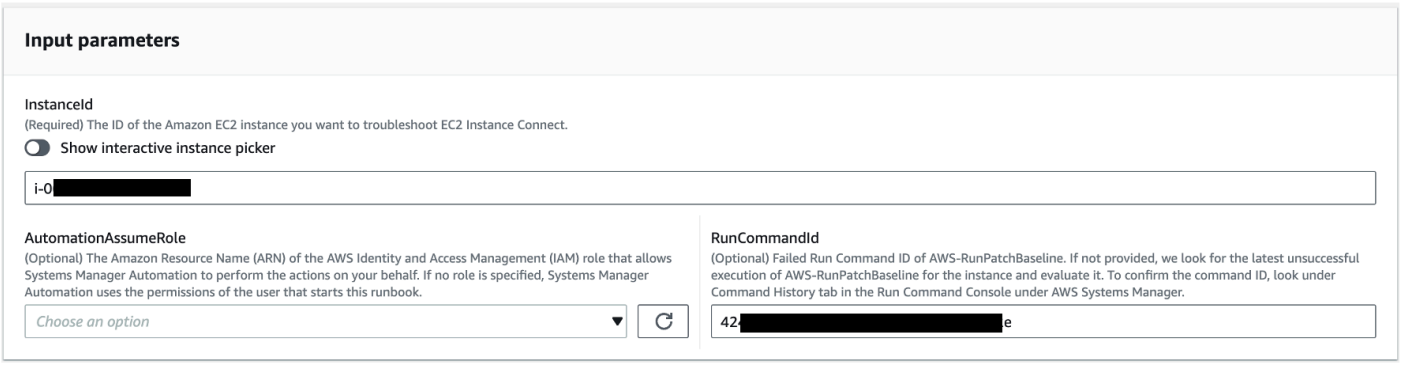
1. 導覽至主AWS Systems Manager控台AWSSupport-TroubleshootPatchManagerLinux中的。
2. 選擇 Execute automation (執行自動化)。
3. 對於輸入參數，請輸入以下內容：
   - InstanceId （必填）：

     使用互動式執行個體選擇器選擇修補程式命令失敗的 Linux 型 SSM 受管節點 (Amazon 彈性運算雲端 (Amazon EC2) 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 IAM 角色的 ARN，該角色允許自動化代表您執行動作。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。



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:

     驗證所提供的命令 ID (作為輸入參數) 是否已針對 AWS-RunPatchBaseline SSM 文件執行。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，指出提供的命令已成功執行。

   - VerifyPrerequistes:

     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。

- GetDownload網址：

  擷取 PatchManager 記錄分析器套件的下載 URL。

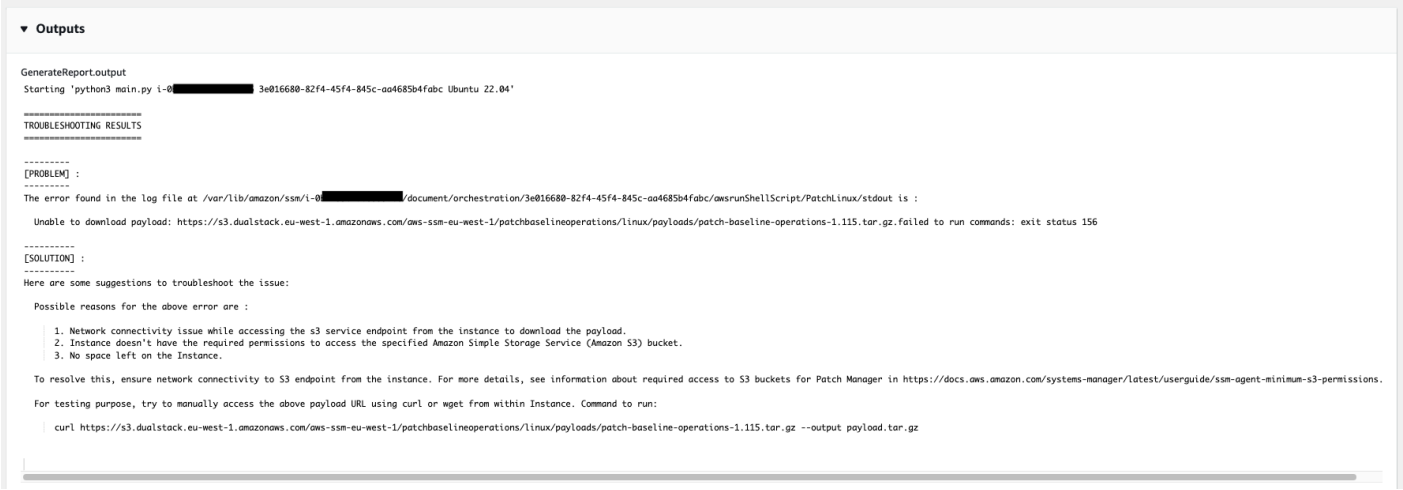
- EvaluatePatchManagerLogs:

  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：



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 Elastic Compute Cloud (Amazon EC2) 執行個體的常見問題。工作階段管理員是的功能 AWS Systems Manager。此 Runbook 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已連接至 Amazon EC2 執行個體。
- 從執行個體收集 SSM 代理程式記錄。
- 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 IAM 政策是否附加至執行個體設定檔。它不會分析執行個體設定檔中包含的 AWS KMS IAM 或許可。

> **Important**
>
> AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2runbook 使用 VPC 可 Reachability Analyzer 來分析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。

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。
- InstanceId

  類型：字串

  說明：(必填) 您無法使用工作階段管理員連線的 Amazon EC2 執行個體 ID。
- SessionPreference文件

  類型：字串

  預設值：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 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: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：獲取附加到實例的實例配置文件的 ARN。
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macOS體收集記錄輸出。
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。
12. aws:branch：決定是否根據ssm-cli記錄檔評估ssmmessages端點連線。
13. aws:executeAutomation：評估執行個體是否可以連線到ssmmessages端點。
14. aws:branch：決定是否根據ssm-cli日誌和您的工作階段偏好評估 Amazon S3 端點連線。
15. aws:executeAutomation：評估執行個體是否可以連接到 Amazon S3 端點。
16. aws: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。
17. aws:executeAutomation：評估執行個體是否可以連線到 AWS KMS 端點。
18. aws: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。
19. aws:executeAutomation：評估執行個體是否可以連線至 CloudWatch Logs 端點。
20. aws:executeAutomation：執AWSSupport-TroubleshootManagedInstance行手冊。
21. aws: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

Linux,macOS, Windows

參數

- AssigneeName

  類型：字串

  描述：(選用) 應指派問題之人員的使用者名稱。
- DueDate

  類型：字串

  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。

- IssueType姓名

  類型：字串

  描述：(必要) 您要建立的問題類型名稱 (例如，任務、子任務、錯誤等)。

- JiraURL

  類型：字串

  描述：(必要) Jira 執行個體的 URL。

- JiraUsername

  類型：字串

  描述：(必要) 要建立問題的使用者名稱。

- PriorityName

  類型：字串

  描述：(選用) 問題優先順序的名稱。

- ProjectKey

  類型：字串

  描述：(必要) 應該在其中建立問題之專案的金鑰。

- 超音波 ParameterName

  類型：字串

  描述：(必要) 包含 Jira 使用者 API 金鑰或密碼之加密 SSM 參數的名稱。

文件步驟

aws:createStack-建立 CloudFormation 堆疊以建立 Lambda IAM 角色和函數。

aws:invokeLambdaFunction-叫用 Lambda 函數以建立吉拉問題

aws:deleteStack-刪除建立的 CloudFormation 堆疊。

輸出

IssueId：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

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。
- 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。

- ServiceNow執行個體網址

  類型：字串

  說明：(必填) 執 ServiceNow 行個體的 URL

- ShortDescription

  類型：字串

  描述：(必要) 事件的簡短描述。

- Subcategory

  類型：字串

  描述：(選用) 事件的子類別。

  有效值：無 | 防病毒 | 電子郵件 | 內部應用程序 | 操作系統 | 中央處理器 | 磁盤 | 鍵盤 | 硬件 | 內存 | 顯示器 | 鼠標 | DHCP | IP 地址 | VPN | 無線網絡連接 | DB2 | MS SQL 服務器 | 甲骨文

  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 公用定址屬性，否則您也必須將 associate_public_ip_address 設定為 true。

運行此自動化（控制台）

文件類型

自動化

擁有者

Amazon

平台

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。

- 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`。
- TemplateFile姓名

  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

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

  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。
- SecurityGroup身份證

  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 許可

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

  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。

- LogDestination阿恩

  類型：字串

  說明：(選用) 您要傳送查詢 CloudWatch 日誌的日誌群組、Amazon S3 儲存貯體或 Firehose 串流的 ARN。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，則自動化會建立具有該格式的 CloudWatch Logs 群組 AWSSupport-ConfigureDNSQueryLogging-{automation: *EXECUTION_ID* } ，以及用於發佈查詢記錄的 IAM 資源政策。由自動化操作建立的「 CloudWatch 記錄」群組的保留期為 14 天。

- QueryLog类型

  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 私用主控區域的 ID。如果Resolver/Private為QueryLogType參數指定，則資源必須是 VPC 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。

- 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選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 所需的許可，以將日誌發佈到日 CloudWatch 誌日誌群組，並在不存在的情況下創建所需的 IAM 資源策略。

- aws:executeScript-在選取的目的地啟用 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 Elastic Compute Cloud (Amazon EC2) 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，執行簿會為除 Amazon DNS 以外的所有通訊協定設定所有入站和輸出流量的鏡像。如果您想要鏡像來自特定來源和目的地的流量，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

- AutomationAssume角色

  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)。
- 源

  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 UDP 接聽程式。

- 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 許可

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. 目標輸出

AWSSupport-ConnectivityTroubleshooter

Description

AWSSupport-ConnectivityTroubleshooterRunbook 會診斷下列項目之間的連線問題：

- AWS Amazon Virtual Private Cloud（Amazon VPC）中的資源
- AWS 相同內部不同 Amazon VPC 中的資源 AWS 區域 ，這些資源使用 VPC 對等連接
- AWS Amazon VPC 中的資源和使用網際網路閘道的網際網路資源
- AWS Amazon VPC 中的資源和使用網路位址轉譯 (NAT) 閘道的網際網路資源

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

  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。
- 目的地 IP

  類型：字串

  描述：(必要) 您要連線的資源 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) 您要測試連線的 Amazon VPC 識別碼。
- SourceIP

  類型：字串

  描述：(必填) 您要從中測試連線的 Amazon VPC 中 AWS 資源的私有 IPv4 位址。
- SourcePort範圍

  類型：字串

  說明：(選用) 您要測試連線能力的 Amazon VPC 中 AWS 資源使用的連接埠範圍。
- SourceVpc

  類型：字串

  預設值：全部

說明：(選用) 您要從中測試連線的 Amazon VPC 識別碼。

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:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

文件步驟

- aws:executeScript-收集有關您在SourceIP參數中指定的 AWS 資源的詳細信息。
- 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 VPC 傳回的 ID 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路相關聯的網路存取控制清單 (NACL)。
- aws:executeScript-確認 NACL 是否允許來源和目標資源之間所需的流量。
- aws:executeScript-確認來源是否具有與資源相關聯的公用 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相關聯的 NACL。
- aws:executeScript-確認 NACL 是否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 閘道之子網路相關聯的 NACL。
- aws:executeScript-確認 NACL 是否允許 NAT 閘道的子網路所需的流量。
- aws:executeScript-收集與 NAT 閘道子網路相關聯的路由。
- aws:executeScript-確認 NAT 閘道是否具有通往網際網路閘道的路由。
- aws:executeAwsApi-收集 VPC 對等連線的詳細資料。
- aws:executeScript-確認兩個 VPC 位於相同區域，且為目的地 VPC 傳回的 ID 與參數中指定的值 (如果有的話) 相DestinationVpc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 VPC 是否具有通往對等連線的路由。
- aws:executeScript-確認如果自動化不支援目的地，是否允許來自來源資源的流量。

AWSSupport-TroubleshootVPN

Description

AWSSupport-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至 VPN 通道記錄的日誌串流、是否存在 VPN 連線識別碼，以及是否存在通道 IP 位址。它會在設定用於 VPN 記錄的記 CloudWatch 錄群組上進行記錄洞見 API 呼叫。

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 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。

- 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}$`

- 隧道通道地址

  類型：字串

  描述：(必要) 與您AWS Site-to-Site VPN關聯的通道號碼 1 IPv4 位址。

  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}$`

- 隧道交換地址

  類型：字串

  描述：(選擇性) 通道編號 2 IPv4 位址與您的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}|^$`

- 池版

  類型：字串

  說明：(必要) 選取您使用的 IKE 版本。允許的值：

  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 許可

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

備註：當記 CloudWatch 錄輸出格式為 JSON 時，此自動化操作適用於為 VPN 通道記錄設定的記錄群組。

請依照下列步驟設定自動化操作：

1. 導航到控AWSSupport制台中的故障排除 VPN。AWS Systems Manager
2. 對於輸入參數，請輸入以下內容：
   - AutomationAssumeRole (選擇性)：

     (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓 Systems Manager 自動化代表您執行動作。如果未指定任何角色，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。這必須是為 VPN 設定要將記錄檔傳送至的記錄群組。 CloudWatch
   - VpnConnectionId （必填）：

     追蹤其記錄群組是否有 VPN 錯誤的AWS Site-to-Site VPN連線識別碼。
   - 隧道通道位址 (必填)：

     通道與您的AWS Site-to-Site VPN連線相關聯的 IP 位址。
   - 隧道位址（可選）：

     與您的AWS Site-to-Site VPN連線相關聯的通道 B IP 位址。
   - 版本 (必填):

     選擇您正在使用的版本。允許的值：
   - StartTimeinEpoch (選擇性)：

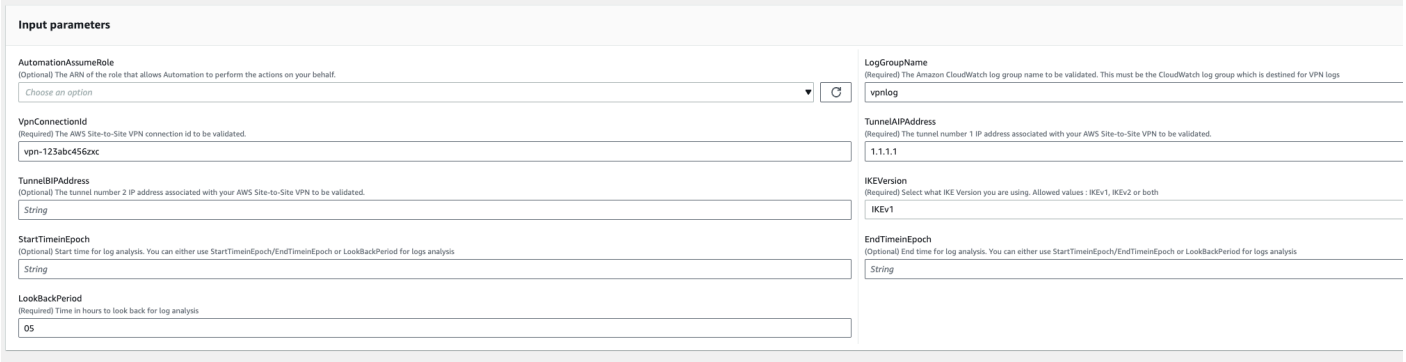
     要查詢錯誤的時間範圍的開頭。該範圍包含在內，因此查詢中包含指定的開始時間。指定為紀元時間，即世界標準時間 1970 年 1 月 1 日 00:00:00 以來的秒數。
   - EndTimeinEpoch (選擇性)：

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，即世界標準時間 1970 年 1 月 1 日 00:00:00 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 StartTimeinEpoch EndTimeinEpoch、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 StartTimeinEpoch 和 EndTimeinEpoch，而不是 LookBackPeriod。



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：

   - 參數驗證：

     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 連線 ID 是否有效。如果無效，它會停止進一步啟動自動化步驟。

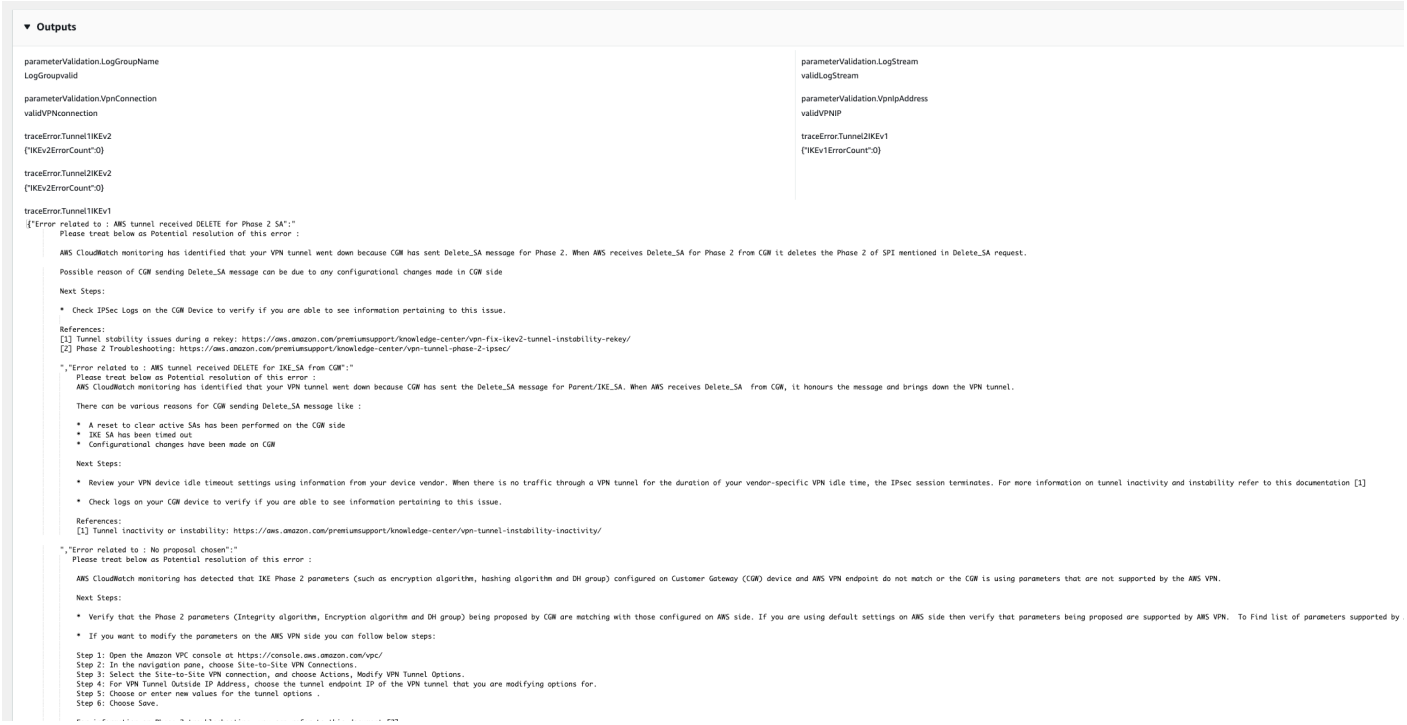
   - branchOnValidationOfVpnIp:

     檢查參數中提到的隧道 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。

- 追蹤錯誤：

  在包含 CloudWatch 的日誌組中進行日誌洞察力 API 調用，並搜索與 IKEV1/IKEv2 相關的錯誤以及相關的建議解決方案。

6. 完成後，請檢閱「輸出」區段以取得執行的詳細結果。



參考

Systems Manager Automation

- 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

- Site-to-Site 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

- AutomationAssume角色

  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)。
- EgressOnlyInternetGateway識別碼

  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 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: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

R AWSConfigRemediation-DeleteUnusedENI unbook 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

- AutomationAssume角色

  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)。
- NetworkInterface身份證

類型：字串

說明：（必填）您要刪除的 ENI 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
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

文件步驟

- aws:executeAwsApi-刪除您在NetworkInterfaceId參數中指定的 ENI。
- aws:executeScript-驗證 ENI 已被刪除。

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 Elastic Compute Cloud (Amazon EC2) 執行個體相關聯的安全群組，或被另一個安全群組參考，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

- AutomationAssume角色

  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 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: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

R AWSConfigRemediation-DeleteUnusedVPCNetworkACL unbook 會刪除與子網路無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

- AutomationAssume角色

  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)。
- NetworkAcl身份證

  類型：字串

  描述：(必要) 您要刪除之網路 ACL 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
- ec2:DeleteNetworkAcl
- ec2:DescribeNetworkAcls

文件步驟

- aws:executeAwsApi-刪除NetworkAclId參數中指定的網路 ACL。

- aws:executeScript-確認已刪除NetworkAclId參數中指定的網路 ACL。

AWSConfigRemediation-DeleteVPCFlowLog

Description

AWSConfigRemediation-DeleteVPCFlowLogRunbook 會刪除您指定的虛擬私人雲端 (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

- AutomationAssume角色

  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)。
- FlowLog身份證

  類型：字串

  描述：（必填）您要刪除的流程日誌 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
- 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 地址或與其相關聯的公有 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

- AutomationAssume角色

  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)。
- InternetGateway身份證

類型：字串

說明：(必要) 您要刪除的網際網路閘道 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
- 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識別碼和 Amazon VPC 的識別碼做為輸入，並將虛擬私有閘道從 Amazon VPC 中分離。
- 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-從網際網路閘道識別碼收集 VPC ID。
- aws:executeAwsApi-將網際網路閘道識別碼從虛擬私人 VPC 分離。

- aws:executeAwsApi-刪除網際網路閘道。

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Description

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway執行手冊會分離並刪除指定的 Amazon Elastic Compute Cloud (Amazon EC2) 虛擬私有閘道，連接到使用 Amazon Virtual Private Cloud (Amazon VPC) 建立的虛擬私有雲端 (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

- AutomationAssume角色

  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)。
- VpnGateway身份證

  類型：字串

  描述：（必要）要刪除之虛擬私有閘道的 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
- 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識別碼和 Amazon VPC 的識別碼做為輸入，並將虛擬私有閘道從 Amazon VPC 中分離。
- 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 會移除允許在 TCP 連接埠 22 上針對安全性群組進行不受限制的傳入 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

  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。
- SecurityGroup身份證

  類型：字串

  說明：(必要) 您要限制 SSH 流量之安全性群組 ID 的逗號分隔清單。

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: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

DisableIncomingSSHM 模板。 RestrictedSecurityGroupIds -已移除輸入 SSH 規則的安全群組 ID 清單。

AWS-DisablePublicAccessForSecurityGroup

Description

此執行手冊會停用開啟至所有 IP 位址的預設 SSH 和 RDP 連接埠。

> **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 VPC 中；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

  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。

- 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`1.2.3.4/32`為)。

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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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 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:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

文件步驟

- `aws:executeAwsApi`-針對您在參數中指定的子網路停用自動指派公用 IPv4 位址屬性。`SubnetId`
- `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執行手冊將流程日誌資料發佈到 Amazon 簡單儲存服務 (Amazon S3) 取代現有的 Amazon VPC 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 (CloudWatch 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。
- DestinationLog集團

  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) 您要使用的 AWS Identity and Access Management (IAM) 角色的 ARN，該角色為 Amazon Elastic Compute Cloud (Amazon EC2) 提供將流程日誌資料發佈到 CloudWatch 日誌的必要許可。
- FlowLog身份證

  類型：字串

  說明：(必填) 發佈到您要取代的 Amazon S3 的流程日誌 ID。
- MaxAggregation間隔

  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：接受 | 拒絕 | 全部

描述：（必填）您要記錄和發佈的流程記錄資料類型。

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:CreateFlowLogs
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs

文件步驟

- aws:executeAwsApi-從您在參數中指定的值收集有關 VPC 的詳細資訊。FlowLogId
- 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

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket執行手冊將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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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：(必要) 您要將流程日誌資料發佈到的 Amazon S3 儲存貯體的 ARN。
- FlowLog身份證

  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。
- MaxAggregation間隔

  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：接受 | 拒絕 | 全部

  描述：（必填）您要記錄和發佈的流程記錄資料類型。

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:CreateFlowLogs
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs

文件步驟

- aws:executeAwsApi-從您在參數中指定的值收集有關 VPC 的詳細資訊。FlowLogId
- 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

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

R AWS-RemoveNetworkACLUnrestrictedSSHRDP unbook 會從指定的網路 ACL 移除所有網路存取控制清單 (ACL) 規則，這些規則允許從所有來源位址傳輸到預設 SSH 和 RDP 連接埠的輸入流量。包含與預設 SSH 和 RDP 連接埠重疊的連接埠範圍的規則不會遭到移除。

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

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。

- NetworkAcl身份證

  類型：字串

  描述：(必要) 您要移除不受限制規則的網路 ACL 識別碼，這些規則允許從所有來源位址輸入流量傳輸至預設 SSH 和 RDP 連接埠。

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: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

RemoveNaclEntriesAnd驗證。 VerificationMessage -成功刪除網路 ACL 規則的驗證訊息。

RemoveNaclEntriesAnd驗證。 RulesDeletedAndApiResponses -已刪除的網路 ACL 規則，以及 `DeleteNetworkAclEntry` API 作業回應。

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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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)。
- SecurityGroup身份證

  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 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: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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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 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: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 (Amazon EC2) 執行個體，並透過持續執行偵測、地鐵、追蹤路徑和跟蹤器 CP 測試來監控所選目標 IP (IPv4 或 IPv6)。結果會儲存在 Amazon CloudWatch 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

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。
- CloudWatchLogGroupRetentionIn天

  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 公斤。

  預設：t2.micro

  描述：(選用) EC2Rescue 執行個體的 EC2 執行個體類型。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

  描述：(必要) 要監控的 IPv4 及/或 IPv6 逗號分隔清單。不可使用空格。大小上限為 255 字元。請注意，如果您提供無效的 IP，則自動化會失敗並轉返測試設定。

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。

建議執行自動化操作的使用者附加了 AmazonSSM AutomationRole IAM 受管政策。此外，使用者必須將以下政策連接至其使用者帳戶、群組或角色：

```
            {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreateInstanceProfile",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:DetachRolePolicy",
                "iam:AttachRolePolicy",
                "iam:PassRole",
                "iam:AddRoleToInstanceProfile",
                "iam: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 TargetIPs 輸入。

   (IPv6) 若 TargetIPs 包含 IPv6：

   aws:assertAwsResourceProperty-檢查提供的子網路是否有關聯的 IPv6 集區
3. **aws:executeScript**-取得最新 Amazon Linux 2 的執行個體類型架構和公有參數路徑AMI。
4. **aws:executeAwsApi**-AMI 從參數存儲中獲取最新的 Amazon Linux 2。
5. **aws:executeAwsApi**-在子網路的 VPC 中建立測試的安全群組。

   (清除) 如果安全群組建立失敗：

   aws:executeAwsApi-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**-刪除由自動化建立的 IAM 角色 (如果存在)。

   b. **aws:executeAwsApi**-刪除由自動化建立的安全性群組 (如果存在)。

8. **aws:executeAwsApi**-附加亞馬遜 SS ManagedInstanceCore M 管理策略

   (清除) 若政策連接失敗：

   a. **aws:executeAwsApi**-將 AmazonSSM ManagedInstanceCore 管理的政策與自動化建立的角色分離 (如果附加)。

   b. **aws:executeAwsApi**-刪除自動化建立的 IAM 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

   c. **aws:executeAwsApi**-刪除自動化建立的 IAM 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 AmazonSSM ManagedInstanceCore 管理的政策。

    d. **aws:executeAwsApi**-刪除自動化建立的 IAM 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 (如果相關聯)。

b. **aws:executeAwsApi**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

e. **aws:executeAwsApi**-刪除自動化建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除自動化建立的 IAM 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) 若 TargetIPs 包含 IPv6：

aws:executeAwsApi-將 IPv6 指派給測試執行個體。

15 **aws:waitForAwsResourceProperty**-等待測試執行個體成為代管執行個體。

(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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除自動化建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除自動化建立的 IAM 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 IP 在語法上是否正確 IPv4 和/或 IPv6 位址：

(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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除自動化建立的 IAM 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 IP 定義 MTR 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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 IP 定義第一個 ping 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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 IP 定義第二個 ping 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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 IP 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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 IP 定義追蹤路由測試。

(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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

f. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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**-刪除由自動化操作建立的 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 AmazonSSM ManagedInstanceCore 受管理的原則與自動化建立的角色分離。

g. **aws:executeAwsApi**-刪除由自動化操作建立的 IAM 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

創建CloudWatch儀表板. 輸出-儀表板的 URL。 CloudWatch

創建ManagedInstance。 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

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)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。

- AutomationExecution身份證

  類型：字串

  描述：(必要) 您先前執行 AWSSupport-SetupIPMonitoringFromVPC runbook 時的自動化執行 ID。與此執行 ID 相關聯的所有資源都會遭到刪除。

- InstanceId

  類型：字串

  描述：(必要) 監控執行個體的執行個體 ID。

- SubnetId

  類型：字串

  描述：(必要) 監控執行個體的子網路 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。

建議執行自動化操作的使用者附加了 AmazonSSM AutomationRole IAM 受管政策。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-刪除由自動化操作建立的 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 AmazonSSM ManagedInstance 核心受管原則與自動化建立的角色分離。
10. aws:executeAwsApi-刪除由自動化操作建立的 IAM 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-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Description

AWS-AddWAFRegionalRuleToRuleGrouprunbook 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

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)。如果未指定角色，Systems Manager 自動化會使用啟動此 runbook 的使用者的權限。
- RuleGroup身份證

  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：允許 | 封鎖 | 計數

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`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

文件步驟

- GetWAFChangeToken （aws：執行AwsApi）-檢索 AWS WAF 更改令牌以確保執行本不會向服務提交衝突的請求。
- AddW RuleTo AF RegionalRuleGroup (AWS: 執行程序檔)-將指定的規則新增至區域規則群組。AWS WAF
- VerifyChangeTokenPropagating （aws：等待 ForAwsResourceProperty）-驗證更改令牌的狀態為或。`PENDING` `INSYNC`
- VerifyRuleAddedToRuleGroup (AWS：執行程序檔)-驗證指定的規則已新增至目標區域 AWS WAF 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 作業的輸出。

AWS-AddWAFRegionalRuleToWebAcl

Description

`AWS-AddWAFRegionalRuleToWebAcl`runbook 會將現有的 AWS WAF 地區規則、規則群組或以速率為基礎的規則新增至 AWS WAF 傳統地區 Web 存取控制清單 (ACL)。此手冊不會更新由 AWS Firewall Manager管理的現有 AWS WAF 經典地區性 Web ACL。

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

  描述：(必要) 您要更新之 Web ACL 的識別碼。

- ActivatedRule優先

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 ACL 中規則的順序。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 Web ACL，則這些值不一定是連續的。

- 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。

- ActivatedRule動作

  類型：字串

  有效值：允許 | 封鎖 | 計數

  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。

- ActivatedRule类型

  類型：字串

  有效值：一般 | 以匯率為基礎 | 群組

  預設值：一般

  描述：(選擇性) 您要新增至 Web ACL 的規則類型。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情況下將RATE_BASED規則新增至 Web ACL，則要求會失敗，因為要求預設為REGULAR規則。

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
- waf-regional:GetChangeToken
- waf-regional:GetWebACL
- waf-regional:UpdateWebACL

文件步驟

- DetermineWebACL NotIn FMS AndRulePriority (AWS: 執行腳本)-驗證 AWS WAF Web ACL 是否在 Firewall Manager 員安全策略中，並驗證優先順序 ID 與現有 ACL 沒有衝突。
- AddRuleOrRuleGroupToWebACL (AW: 執行程序檔)-將指定的規則新增至網路 ACL。 AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (AW: 執行程序檔)-驗證指定的 AWS WAF 規則已新增至目標網頁 ACL。

輸出

- DetermineWebACL NotIn FMS AndRule 優先順序。 PrereqResponse：從`DetermineWebACLNotInFMSAndRulePriority`步驟輸出。
- VerifyRuleOrRuleGroupAddedToWeb十字韌帶。 VerifyRuleOrRuleGroupAddedToWebACL 回應：來自步驟的輸出。`AddRuleOrRuleGroupToWebACL`
- VerifyRuleOrRuleGroupAddedToWeb十字韌帶。 ListActivatedRulesOrRuleGroupsInWebACL 回應：步驟的輸出。`VerifyRuleOrRuleGroupAddedToWebAcl`

AWSConfigRemediation-EnableWAFClassicLogging

Description

`AWSConfigRemediation-EnableWAFClassicLogging`執行手冊可讓您記錄到您指定的 AWS WAF 網路存取控制清單 (網路 ACL) 的 Amazon 資料防火軟管 (Firehose)。

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

- AutomationAssume角色

  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)。

- DeliveryStream姓名

  類型：字串

  描述：(必要) 您要傳送記錄檔的 Firehose 傳送串流名稱。

- WebACLId

  類型：字串

  描述：(必要) 您要啟用登入之 AWS WAF Web ACL 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`
- `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`-收集在參數中指定的 AWS WAF Web ACL 的 ARN。`WebACLId`
- `aws:executeAwsApi`-啟用網頁 ACL 的記錄功能。
- `aws:assertAwsResourceProperty`-驗證已在 AWS WAF 網頁 ACL 上啟用記錄。

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Description

AWSConfigRemediation-EnableWAFClassicRegionalLogging執行手冊可讓您記錄到您指定的 AWS WAF 網路存取控制清單 (ACL) 的 Amazon 資料防火軟管 (Firehose)。

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

- AutomationAssume角色

  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)。
- LogDestination配置

  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

  描述：(必要) 您要啟用登入之 AWS WAF Web ACL 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
- iam:CreateServiceLinkedRole
- waf-regional:GetLoggingConfiguration
- waf-regional:GetWebAcl
- waf-regional:PutLoggingConfiguration

文件步驟

- aws:executeAwsApi-收集在參數中指定的 AWS WAF Web ACL 的 ARN。WebACLId
- aws:executeAwsApi-啟用網頁 ACL 的記錄功能。
- aws:assertAwsResourceProperty-驗證已在 AWS WAF 網頁 ACL 上啟用記錄。

AWSConfigRemediation-EnableWAFV2Logging

Description

AWSConfigRemediation-EnableWAFV2Logging執行手冊會使用指定的 Amazon 資料火管 AWS WAF (Firehose) 交付串流，為 (AWS WAF V2) Web 存取控制清單 (Web ACL) 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

LinuxmacOS, Windows

參數

- AutomationAssume角色

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)。

- LogDestination配置

  類型：字串

  描述：(必要) 您要與網頁 ACL 建立關聯的 Firehose 傳送串流 ARN。

  > **Note**
  >
  > Firehose 傳送串流 ARN 必須以字首開頭。`aws-waf-logs-`例如，`aws-waf-logs-us-east-2-analytics`。如需詳細資訊，請參閱 Amazon 資料 Firehose。

- WebAcl阿恩

  類型：字串

  描述：(必要) 將啟用記錄之 Web ACL 的 ARN。

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`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

文件步驟

- `aws:executeScript`-啟用 AWS WAF V2 Web ACL 的記錄功能，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

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。
- ComputeType姓名

  類型：字串

  有效值：值 | 標準 | 效能 | 電源 | 顯示卡 | 力專業 | 繪圖技術

  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：永遠 _ 開 | 自動 _ 停止

  描述：(必要) 的執行模式 WorkSpace。
- RunningModeAutoStopTimeoutIn分鐘

  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。

- VolumeEncryption關鍵

  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 許可

此AutomationAssumeRole參數需要執行下列動作，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。重建選項會從最近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 WorkSpace 立該磁碟區。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

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 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
- 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 WorkSpace 態AVAILABLE。

X-Ray

AWS Systems Manager 自動化提供預先定義的 AWS X-Ray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-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。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

LinuxmacOS, Windows

參數

- AutomationAssume角色

  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) Amazon 資源名稱 (ARN)、金鑰識別碼或您要用 AWS X-Ray 來加密資料之 KMS 金鑰的金鑰別名。

必要的 IAM 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
- kms:DescribeKey
- xray:GetEncryptionConfig
- xray:PutEncryptionConfig

文件步驟

- aws:executeAwsApi-使用您在KeyId參數中指定的 KMS 金鑰對 X-Ray 資料啟用加密。
- aws:waitForAwsResourceProperty-等待 X-Ray 的加密配置狀態。ACTIVE
- aws:executeAwsApi-收集您在參數中指定的金鑰的 ARN。KeyId
- 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。