aws

用户指南

AWS Systems Manager 自动化运行手册参考

AWS Systems Manager 自动化运行手册参考: 用户指南

Table of Contents

Systems Manager 自动化运行手册参考

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

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

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

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

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

主题

- 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
- 亚马逊 OpenSearch 服务
- 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
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- 第三方
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

查看运行手册内容

您可以在 Systems Manager 控制台查看运行手册的内容。

查看运行手册内容

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

   –或者–

   如果首先打开 AWS Systems Manager 主页，请选择菜单图标 (☰)。以打开导航窗格，然后在导航窗格中选择 “文档”。
3. 在类别部分，选择自动化文档。
4. 选择运行手册，然后选择查看详细信息。
5. 选择内容选项卡。

API Gateway

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

主题

- AWSConfigRemediation-DeleteAPIGatewayStage
- AWSConfigRemediation-EnableAPIGatewayTracing
- AWSConfigRemediation-UpdateAPIGatewayMethodCaching

AWSConfigRemediation-DeleteAPIGatewayStage

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

类型：字符串

描述：（必需）要删除的 API 网关的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

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

文档步骤

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

AWSConfigRemediation-EnableAPIGatewayTracing

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要启用跟踪的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

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

文档步骤

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

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：StringList

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

  类型：字符串

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

所需的 IAM 权限

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

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

文档步骤

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

AWS Batch

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

主题

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

描述

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

如何工作？

此运行手册执行以下检查：

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

> **Important**
>
> - 此 Runbook 必须与处于RUNNABLE状态的任务在同一个AWS区域启动。

- 可以为在亚马逊 ECS AWS Fargate 或亚马逊弹性计算云 (Amazon EC2) 实例上安排的AWS Batch任务启动本运行手册。如果在亚马逊 Elastic Kubernetes Service（亚马逊 EKS）上为AWS Batch任务启动自动化，则启动将停止。
- 如果实例可用于运行任务，但无法注册 Amazon ECS 集群，则此运行手册将启动`AWSSupport-TroubleshootECSContainerInstance`自动化运行手册以尝试确定原因。有关更多信息，请参阅 AWSSupport-Troubleshot ContainerInstance ecs 运行手册。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- JobId

  类型：字符串

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

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

所需的 IAM 权限

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

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

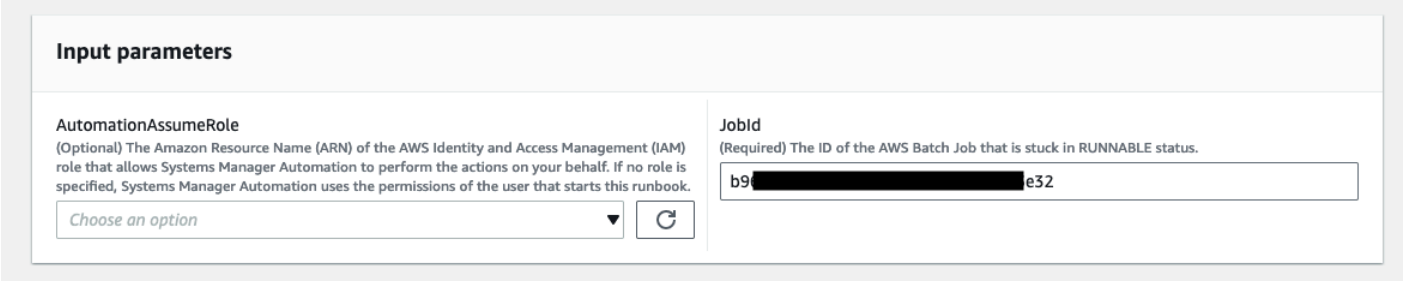
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sts:GetCallerIdentity

说明

1. 导航到AWS Systems Manager控制台AWSBatchJob中的 AWSSupport-疑难解答。
2. 选择 Execute automation（执行自动化）
3. 要输入参数，请输入内容：
   - AutomationAssumeRole （可选）：

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

     处于RUNNABLE状态的 AWS Batch Job 的 ID。



4. 选择执行。
5. 请注意，自动化已启动。
6. 文档将执行以下步骤：
   - PreflightPermissionChecks:

     对初始用户/角色执行预检 IAM 权限检查。如果缺少任何权限，则此步骤将提供全局输出部分中缺少的 API 操作。
   - ProceedOnlyIfUserHasPermission:

根据您是否有权执行运行手册的所有必要操作进行分支。

- AWSBatchJobEvaluation:

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

- ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

  根据任务是否存在以及是否处于RUNNABLE状态进行分支。

- BatchComputeEnvironmentEvaluation:

  对AWS Batch计算环境进行检查。

- ProceedOnlyIfComputeEnvironmentChecksAreOK：

  根据计算环境检查是否成功进行分支。

- UnderlyingInfraEvaluation:

  根据底层 Auto Scaling 组或 Spot 队列请求执行检查。

- ProceedOnlyIfInstancesNotJoiningEcs集群：

  根据是否有未加入 Amazon ECS 集群的实例进行分支。

- EcsAutomationRunner:

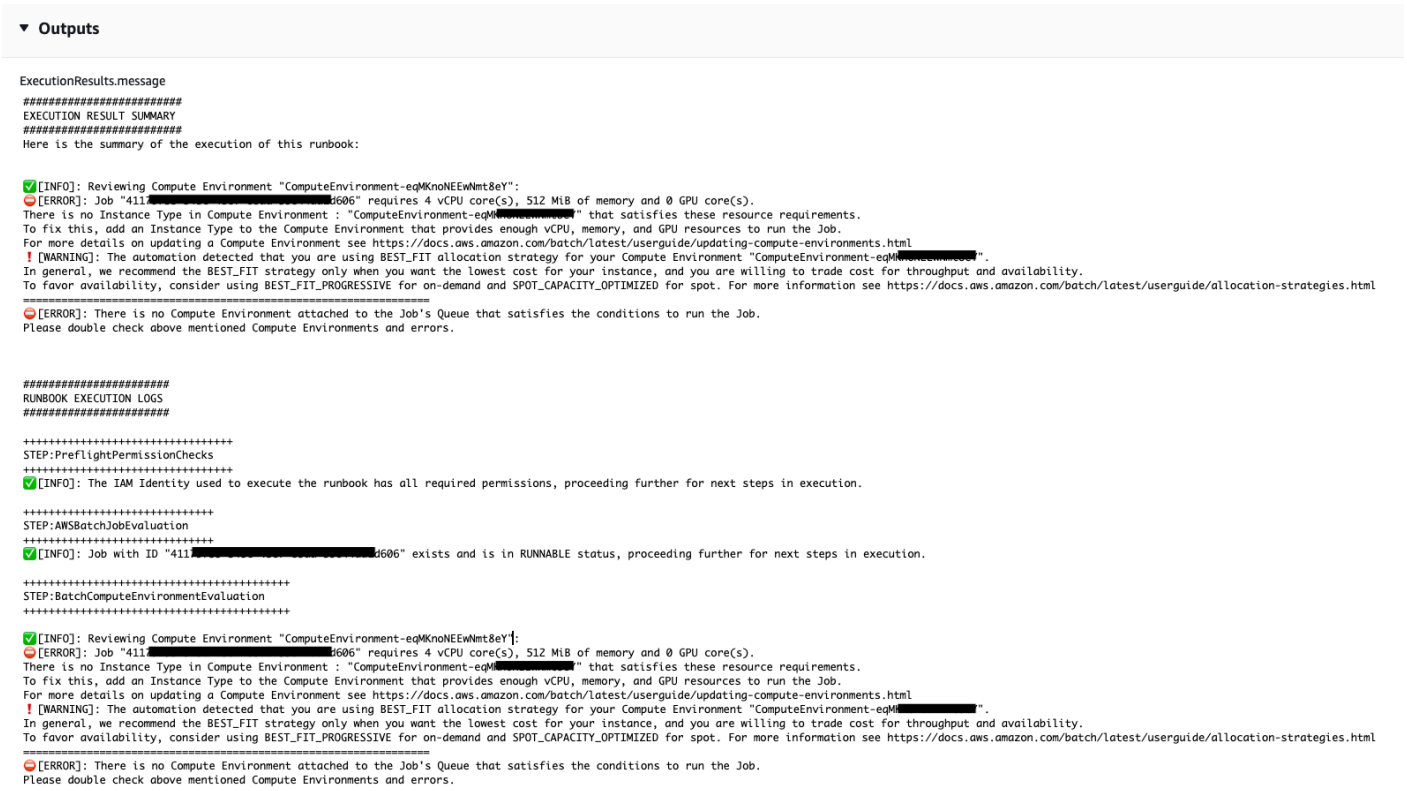
  为未加入集群的实例运行 Amazon ECS 自动化。

- ExecutionResults:

  根据之前的步骤生成输出。

7. 完成后，将提供评估报告 HTML 文件的 URI：

   运行手册成功执行后该报告的 S3 控制台链接和 Amazon S3 URI



参考

Systems Manager Automation

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

AWS CloudFormation

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

主题

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification
- AWS-RunCfnLint

- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

AWS-DeleteCloudFormationStack

描述

删除 AWS CloudFormation 堆栈。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要删除的 CloudFormation 堆栈的名称或唯一 ID

AWS-EnableCloudFormationSNSNotification

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

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

所需的 IAM 权限

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

- ssm：GetAutomationExecution

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

文档步骤

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

输出

CheckCfnSnsLimits。 NotificationArnList -接收堆栈的 Amazon SNS 通知的 AWS CloudFormation ARN 列表。

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

AWS-RunCfnLint

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

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

  类型：字符串

  描述：（可选）传递给 `--format` 参数以指定输出格式的值。

  有效值：Default | quiet | parseable | json

  默认值：Default
- IgnoreChecksFlag

  类型：字符串

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

  示例：E1001,E1003,W7001

- IncludeChecksFlag

  类型：字符串

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

  示例：E1001,E1003,W7001

- InfoFlag

  类型：字符串

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

  原定设置值：false

- TemplateFileName

  类型：字符串

  描述：S3 存储桶中的模板文件的名称或键。

- TemplateS3BucketName

  类型：字符串

  描述：包含 Packer 模板的 S3 存储桶的名称。

- RegionsFlag

  类型：字符串

  描述：（可选）传递给 `--regions` 参数以根据指定的 AWS 区域 测试模板的值。

  示例：us-east-1,us-west-1

文档步骤

RunCfnLintAgainstTemplate – `cfn-python-lint` 根据指定的 AWS CloudFormation 模板运行 工具。

输出

RunCfnLintAgainstTemplate.output – 来自 `cfn-python-lint` 工具的标准输出。

AWSSupport-TroubleshootCFNCustomResource

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

所需的 IAM 权限

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

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

文档步骤

- validateCloudFormationStack - 验证 AWS CloudFormation 堆栈是否存在于同一个 AWS 账户 和 AWS 区域 中。
- checkCustomResource - 分析 AWS CloudFormation 堆栈，检查失败的自定义资源，并输出有关如何对失败的自定义资源进行故障排除的信息。

AWS-UpdateCloudFormationStack

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- LambdaAssume角色

  类型：字符串

  说明：（必需）Lambda 担任角色的 ARN

- StackNameOrId

  类型：字符串

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

- TemplateUrl

  类型：字符串

  描述：（必填）包含更新 CloudFormation 模板的 S3 存储桶位置（例如 `https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/updated.template`）

CloudFront

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

主题

- AWSConfigRemediation-EnableCloudFrontDefaultRootObject
- AWSConfigRemediation-EnableCloudFrontAccessLogs
- AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity
- AWSConfigRemediation-EnableCloudFrontOriginFailover

- AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

描述

AWSConfigRemediation-EnableCloudFrontDefaultRootObject 运行手册为你指定的 Amazon CloudFront (CloudFront) 分配配置默认的根对象。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

  描述：（必需）当查看者的请求指向您的根 URL 时您希望 CloudFront 返回的对象。

所需的 IAM 权限

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

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

文档步骤

- aws:executeScript - 为您在 CloudFrontDistributionId 中指定的 Amazon CloudFront 分配配置默认的根对象。

AWSConfigRemediation-EnableCloudFrontAccessLogs

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- BucketName

  类型：字符串

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

- CloudFrontId

  类型：字符串

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

- IncludeCookies

  类型：布尔值

  有效值：true | false

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

- Prefix

  类型：字符串

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

所需的 IAM 权限

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

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

- s3:GetBucketAcl
- s3:PutBucketAcl

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

文档步骤

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

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

描述

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity 运行手册为您指定的 Amazon CloudFront (CloudFront) 发行版启用来源访问身份。此自动化会为 Amazon Simple Storage Service (Amazon S3) 来源类型的所有来源分配相同的 CloudFront 来源访问身份，而不会为您指定的 CloudFront 发行版分配来源访问身份。此自动化不会向 CloudFront 授予访问 Amazon S3 存储桶中对象的来源访问身份读取权限。您必须更新 Amazon S3 存储桶权限才能允许访问。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用来源失效转移的 CloudFront 分配的 ID。
- OriginAccessIdentityId

  类型：字符串

  描述：（必需）要与源关联的 CloudFront 源访问身份。

所需的 IAM 权限

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

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

文档步骤

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

AWSConfigRemediation-EnableCloudFrontOriginFailover

描述

`AWSConfigRemediation-EnableCloudFrontOriginFailover`运行手册为您指定的 Amazon CloudFront (CloudFront) 分配启用源站失效转移。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用来源失效转移的 CloudFront 分配的 ID。
- OriginGroupId

  类型：字符串

  说明：（必需）源组的 ID。
- PrimaryOriginId

  类型：字符串

  描述：（必需）源组中主源 ID。
- SecondaryOriginId

  类型：字符串

  描述：（必需）源组中的辅助源 ID。

所需的 IAM 权限

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

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

文档步骤

- aws:executeScript - 为您在CloudFrontDistributionId参数中指定的 CloudFront 分配启用源失效转移，并验证是否已启用失效转移。

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- CloudFrontDistributionId

  类型：字符串

  描述：（必需）要对启用查看者协议策略的 CloudFront 分配的 ID。
- ViewerProtocolPolicy

  类型：字符串

  有效值：https-only、redirect-to-https

  描述：（必需）查看器可用于访问指定的来源中的文件的协议。

所需的 IAM 权限

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

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

文档步骤

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

CloudTrail

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

主题

- AWSConfigRemediation-CreateCloudTrailMultiRegionTrail
- AWS-EnableCloudTrail
- AWS-EnableCloudTrailCloudWatchLogs

- AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS
- AWS-EnableCloudTrailKmsEncryption
- AWSConfigRemediation-EnableCloudTrailLogFileValidation
- AWS-EnableCloudTrailLogFileValidation
- AWS-QueryCloudTrailLogs

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

描述

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail 运行手册将创建一个AWS CloudTrail (CloudTrail) 跟踪，将来自多个 AWS 区域 的日志文件发送到您选择的 Amazon Simple Storage Service (Amazon S3) 存储桶。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要将日志上传到的 Amazon S3 存储桶的名称。

- KeyPrefix

  类型：字符串

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

  类型：字符串

  描述：（必需）要创建的 CloudTrail 跟踪的名称。

所需的 IAM 权限

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

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

文档步骤

- aws:executeAwsApi - 接受跟踪名称和 Amazon S3 存储桶名称作为输入，并创建一个 CloudTrail 跟踪。
- aws:executeAwsApi - 对创建的跟踪启用日志记录，并开始将日志传输到您指定的 Amazon S3 存储桶。
- aws:assertAwsResourceProperty - 验证 CloudTrail 跟踪是否已创建。

AWS-EnableCloudTrail

描述

创建 AWS CloudTrail 跟踪并配置日志记录到 S3 存储桶。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- S3BucketName

  类型：字符串

  说明：（必需）为发布日志文件指定的 S3 存储桶的名称。

  > **Note**
  >
  > S3 存储桶必须存在且存储桶策略必须授予 CloudTrail 对此存储桶执行写入操作的权限。有关信息，请参阅适用于 CloudTrail 的 Amazon S3 存储桶策略。

- TrailName

  类型：字符串

  说明：（必需）新跟踪的名称。

AWS-EnableCloudTrailCloudWatchLogs

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

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

  类型: StringList

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

所需的 IAM 权限

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

- cloudtrail:UpdateTrail
- iam:PassRole

文档步骤

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

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

描述

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 运行手册使用您指定的 AWS Key Management Service (AWS KMS) 客户托管密钥加密一个 AWS CloudTrail (CloudTrail) 跟踪。此运行手册应仅用作基准，以确保您的 CloudTrail 跟踪按照建议的最低安全最佳实践进行加密。我们建议使用不同的 KMS 密钥加密多个跟踪。CloudTrail 摘要文件未加密。如果您之前已将跟踪的 EnableLogFileValidation 参数设置为 true，则参阅AWS CloudTrail《用户指南》中 CloudTrail 预防性安全最佳实践主题中的“使用 AWS KMS 托管密钥的服务器端加密”部分，了解更多信息。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

  描述：（必需）要升级加密的跟踪的 ARN 或名称。

所需的 IAM 权限

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

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

文档步骤

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

AWS-EnableCloudTrailKmsEncryption

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型: StringList

  描述：（必填）要更新以加密的跟踪列表，以逗号分隔。

所需的 IAM 权限

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

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

文档步骤

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

AWSConfigRemediation-EnableCloudTrailLogFileValidation

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

所需的 IAM 权限

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

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

文档步骤

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

AWS-EnableCloudTrailLogFileValidation

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

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

- TrailNames

  类型: StringList

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

所需的 IAM 权限

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

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

文档步骤

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

AWS-QueryCloudTrailLogs

描述

`AWS-QueryCloudTrailLogs` 运行手册从您选择的 Amazon Simple Storage Service (Amazon S3) 存储桶创建一个包含 AWS CloudTrail(CloudTrail) 日志的 Amazon Athena 表。创建表后，此自动化将运行您指定的 SQL 查询，然后删除该表。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要运行的 SQL 查询。
- SourceBucketPath

  类型：字符串

  描述：（必需）包含要查询的 CloudTrail 日志文件的 Amazon S3 存储桶的名称。
- TableName

  类型：字符串

  描述：（可选）自动化创建的 Athena 表的名称。

  默认：cloudtrail_logs

所需的 IAM 权限

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

- `athena:GetQueryResults`
- `athena:GetQueryExecution`
- `athena:StartQueryExecution`
- `glue:CreateTable`
- `glue:DeleteTable`

- glue:GetDatabase
- glue:GetPartitions
- glue:GetTable
- s3:AbortMultipartUpload
- s3:CreateBucket
- s3:GetBucketLocation
- s3:GetObject
- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject

文档步骤

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

CloudWatch

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

主题

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

AWS-ConfigureCloudWatchOnEC2Instance

描述

启用或禁用对托管实例的 Amazon CloudWatch 详细监控。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要为其启用 CloudWatch 监控的 Amazon EC2 实例的 ID。
- 属性

  类型：字符串

  说明：（可选）不支持此参数。此处列出它是为了实现向后兼容性。
- 状态

  有效值：启用 | 禁用

  说明：（可选）指定启用还是禁用 CloudWatch。

  默认值：Enabled

文档步骤

configureCloudWatch - 在 Amazon EC2 实例上使用给定的状态配置 CloudWatch。

输出

此自动化没有输出。

AWS-EnableCWAlarm

描述

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

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ComparisonOperator

  类型：字符串

  有效值： GreaterThanOrEqualToThreshold | GreaterThanThreshold GreaterThanUpperThreshold | Thres LessThanLowerOrGreaterThanUpper hol | | | LessThanLowerThreshold LessThanOrEqualToThreshold LessThanThreshold

  描述：（必填）比较指定统计量和阈值时使用的算术运算。

- MetricName

  类型：字符串

  描述：（必填）与警报关联的指标的名称。

- 周期

  类型：整数

  有效值：10 | 30 | 60 | 60 的倍数

  描述：（必填）应用统计数据的周期（以秒为单位）。

- 资源收益

  类型: StringList

  描述：（必填）用逗号分隔的用于创建警报的资源 ARN 列表 CloudWatch

- Statistic

  类型：字符串

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

  描述：（必填）与警报关联的指标的统计信息。

- Threshold

  类型：整数

描述：（必填）要与指定统计数据进行比较的值。

所需的 IAM 权限

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

- cloudwatch:PutMetricAlarm

文档步骤

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

输出

启用 Walarm。 FailedResources：未为其创建 CloudWatch 警报的资源 ARN 的映射列表以及失败的原因。

启用 Walarm。 SuccessfulResources：已成功创建 CloudWatch 警报的资源 ARN 列表。

Amazon DocumentDB

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

主题

- AWS-EnableDocDbClusterBackupRetentionPeriod

AWS-EnableDocDbClusterBackupRetentionPeriod

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：整数

  描述：（必填）保留自动备份的天数。必须是 7-35 天之间的值。
- PreferredBackupWindow

  类型：字符串

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

- `ssm:GetAutomationExecution`

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

文档步骤

- GetDocDbClusterIdentifier (aws:executeAwsApi)-使用提供的资源 ID 返回亚马逊文档数据库集群标识符。
- VerifyDocDbEngine (aws: P assertAwsResource roperty)-验证 Amazon DocumentDB 引擎类型`docdb`是为了防止无意中更改其他 Amazon RDS 引擎类型。
- VerifyDocDbStatus (aws: Pro waitAwsResource perty)-验证 Amazon DocumentDB 集群的状态为。`available`
- ModifyDocDbRetentionPeriod (aws:executeAwsApi)-使用为指定的 Amazon DocumentDB 集群提供的值设置保留期。
- VerifyDocDbBackupsEnabled (aws: executeScript)-验证 Amazon DocumentDB 集群的保留期和首选备份窗口（如果已指定）已成功设置。

输出

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

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

CodeBuild

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

主题

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

  描述：（必填）要加密其构建工件的 CodeBuild 项目的 ID。

所需的 IAM 权限

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

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

文档步骤

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

输出

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

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

所需的 IAM 权限

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

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

文档步骤

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

AWS CodeDeploy

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

主题

- AWSSupport-TroubleshootCodeDeploy

AWSSupport-TroubleshootCodeDeploy

描述

AWSSupport-TroubleshootCodeDeploy 运行手册可帮助您确定 Amazon Elastic Compute Cloud（Amazon EC2）实例上 AWS CodeDeploy 部署失败的原因。运行手册将输出相关步骤，以帮助解决问题或进一步排查问题。CodeDeploy 还会提供最佳实践，帮助您在将来避免类似问题。

此运行手册可帮助您解决以下问题：

- Amazon EC2 实例上未安装或未运行 CodeDeploy 代理
- Amazon EC2 实例没有附加 AWS Identity and Access Management (IAM) 实例配置文件
- 附到加 Amazon EC2 实例的 IAM 实例配置文件没有所需的 Amazon Simple Storage Service (Amazon S3) 权限
- 存储在 Amazon S3 中的修订版缺失，或者使用的 Amazon S3 存储桶位于与 Amazon EC2 实例不同的 AWS 区域
- 应用程序规范 (AppSpec) 文件问题
- “文件已存在于某个位置”错误
- CodeDeploy 托管生命周期事件钩子失败
- 客户托管生命周期事件钩子失败
- 部署期间的横向缩减事件

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）失败的部署的 ID。
- InstanceId

  类型：字符串

  说明：（必需）部署失败处的 Amazon EC2 实例的 ID。

所需的 IAM 权限

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

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

文档步骤

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

AWS Config

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

主题

- AWSSupport-SetupConfig

AWSSupport-SetupConfig

描述

AWSSupport-SetupConfig 运行手册将创建了一个 AWS Identity and Access Management (IAM) 服务相关角色、一个由 AWS Config 提供支持的配置记录器，以及一个带有 Amazon Simple Storage Service (Amazon S3) 存储桶的交付渠道，AWS Config 将向其发送配置快照和配置历史记录文件。如果您为 AggregatorAccountId 和 AggregatorAccountRegion 参数指定值，则运行手册还会为数据聚合创建授权，以便从多个 AWS 账户 和多个 AWS 区域 收集 AWS Config 配置和合规性数据。要详细了解如何汇总来自多个账户和区域的数据，请参阅AWS Config《开发者指南》中的多账户多区域数据聚合。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  说明：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。

- AggregatorAccountId

类型：字符串

描述：（可选）将向其中添加聚合器的 AWS 账户 的 ID，用于聚合来自多个账户和 AWS 区域 的 AWS Config 配置和合规性数据。聚合器还使用此账户对源账户进行授权。

- AggregatorAccountRegion

  类型：字符串

  描述：（可选）将向其中添加聚合器的区域，用于聚合来自多个账户和区域的 AWS Config 配置和合规性数据。

- IncludeGlobalResourcesRegion

  类型：字符串

  默认：us-east-1

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

- 分区

  类型：字符串

  默认值：aws

  描述：（必需）要从中收集AWS Config配置和合规性数据的分区。

- S3BucketName

  类型：字符串

  默认值：aws-config-delivery-channel

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

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

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

文档步骤

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

Amazon Connect

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

主题

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

描述

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

如何工作？

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

输入 CSV 文件的示例

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

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

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

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

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

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketAcl",
                "s3:GetObject",
                "s3:GetObjectAttributes",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
            "arn:aws:s3:::YOUR-BUCKET/*",
            "arn:aws:s3:::YOUR-BUCKET"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DeleteStack",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
```

```
                    "lambda:InvokeFunction",
                    "lambda:TagResource",
                    "connect:AssociatePhoneNumberContactFlow",
                    "logs:CreateLogGroup",
                    "logs:TagResource",
                    "logs:PutRetentionPolicy",
                    "logs:DeleteLogGroup",
                    "s3:GetAccountPublicAccessBlock"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "connect:DescribeInstance",
                    "connect:ListPhoneNumbers",
                    "connect:ListContactFlows",
                    "ds:DescribeDirectories"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Condition": {
                    "StringLikeIfExists": {
                        "iam:PassedToService": [
                            "ssm.amazonaws.com",
                            "lambda.amazonaws.com"
                        ]
                    }
                },
                "Action": [
                    "iam:PassRole"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
```

说明

按照这些步骤对自动化进行配置：

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

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

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

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

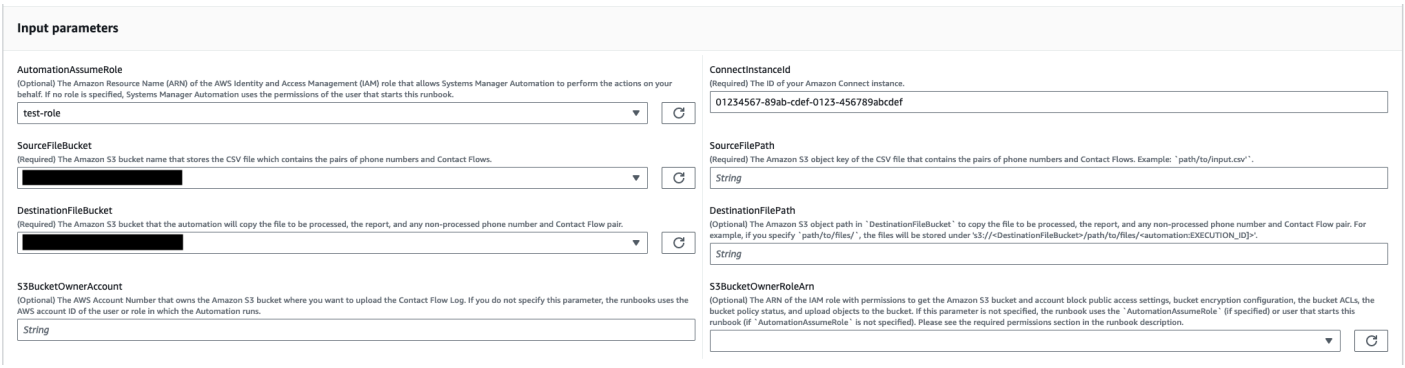
     包含电话号码和联系流程对的 CSV 文件的 Amazon S3 对象密钥。例如，`path/to/input.csv`。
   - DestinationFileBucket （必填）

     Amazon S3 存储桶，自动化将在其中放置中间文件和结果报告。
   - DestinationFilePath （可选）

     存储中间文件和结果报告`DestinationFileBucket`的 Amazon S3 对象路径。例如，如果您指定`path/to/files/`，则文件存储在下`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`。
   - S3BucketOwnerAccount （可选）

     拥有您要上传联系流日志的 Amazon S3 存储桶的 AWS 账号。如果您未指定此参数，则运行手册将使用运行自动化的用户或角色的 AWS 账户 ID。
   - S3BucketOwnerRoleArn （可选）

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



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
   - CheckConnectInstanceExistance

     检查中提供的 Amazon Connect 实例`ConnectInstanceId`是否存在。
   - checkS3 BucketPublicStatus

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

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

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

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

败，它将进入该DescribeCloudFormationErrorFromStackEvents步骤以显示 AWS CloudFormation 堆栈事件失败的原因。

- WaitForPhoneNumberContactFlowAssociationCompletion

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

- GenerateReport

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

- **DeleteCloudFormationStack**

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

- **DescribeCloudFormationErrorFromStackEvent**

  描述AssociatePhoneNumbersToContactFlows步骤 AWS CloudFormation 堆栈中的错误。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

   - GenerateReport.OutputPayload

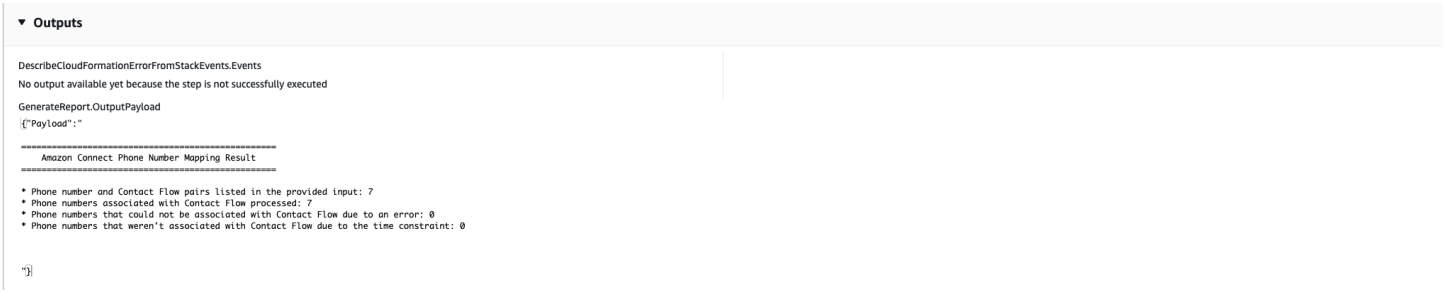
     电话号码和联系流关联的输出。该报告包含以下信息：

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

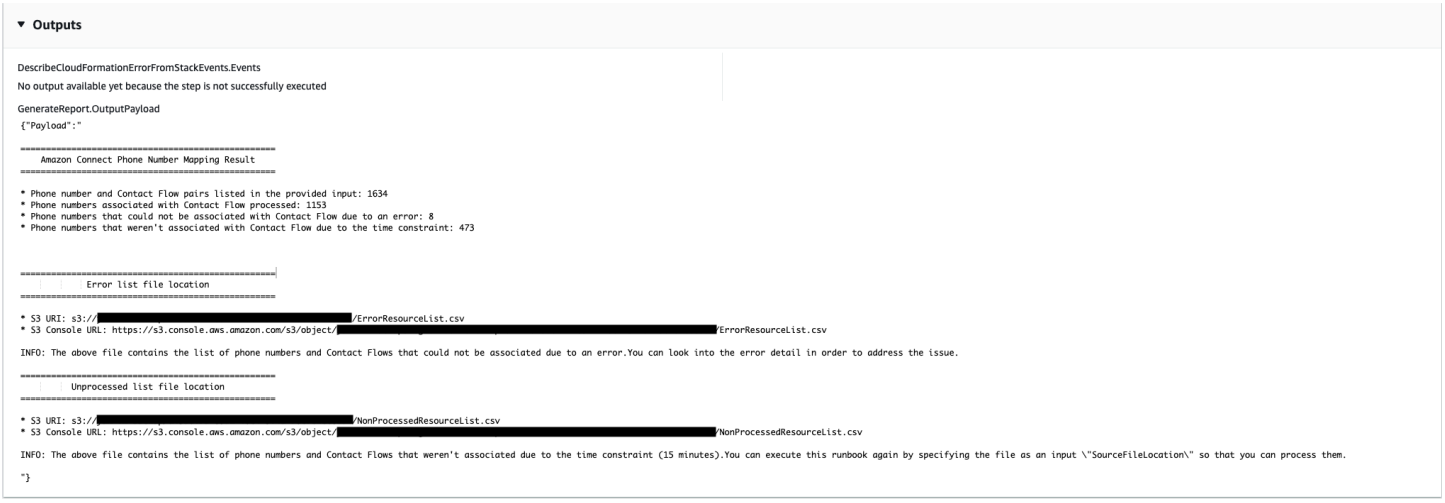
   - DescribeCloudFormationErrorFromStackEvents. 活动

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

使用少量电话号码和联系人流执行的输出



执行输出包含大量电话号码和联系人流以及由于错误或时间限制而未关联的电话号码



参考

Systems Manager Automation

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

AWS Directory Service

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

主题

- AWS-CreateDSManagementInstance

- AWSSupport-TroubleshootADConnectorConnectivity
- AWSSupport-TroubleshootDirectoryTrust

AWS-CreateDSManagementInstance

描述

AWS-CreateDSManagementInstance 运行手册可创建一个 Amazon Elastic Compute Cloud (Amazon EC2) Windows 实例，您可以用它来管理目录 AWS Directory Service。该管理实例不能用于管理 AD Connector 目录。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- AmiID

  类型：字符串

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

描述：（必需）要用于启动管理实例的 Amazon Machine Image (AMI) 的 ID。

- DirectoryId

  类型：字符串

  描述：（必需）要管理的 AWS Directory Service 目录的 ID。该实例已加入您指定的目录。

- IamInstanceProfileName

  类型：字符串

  描述：（必需）您指定的名称将应用于由自动化创建的并附加到管理实例的 IAM 实例配置文件。

- InstanceType

  类型：字符串

  默认：t3.medium

  允许的值：

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

  描述：（必需）要启动的实例类型。

- KeyPairName

类型：字符串

描述：（可选）要在创建 实例时使用的密钥对。如果您没有指定一个值，则不会与该实例关联任何密钥对。

- RemoteAccessCidr

  类型：字符串

  描述：（必需）允许 RDP 流量（端口 3389）来自其的 CIDR 块。您指定的 CIDR 块将应用于添加到由自动化创建的安全组的入站规则。

- SecurityGroupName

  类型：字符串

  描述：（必需）您指定的名称将应用于由自动化创建的并关联到管理实例的安全组。

- 标签

  类型：MapList

  描述：（可选）要应用于由自动化创建的资源的键值对。

所需的 IAM 权限

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

- ds:DescribeDirectories
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances

- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution

文档步骤

- aws:executeAwsApi - 收集有关您在 DirectoryId 参数中指定的类别的详细信息。

- aws:executeAwsApi - 获取启动目录所在的虚拟私有云（VPC）的 CIDR 块。
- aws:executeAwsApi - 使用您在 SecurityGroupName 参数中指定的值创建一个安全组。
- aws:executeAwsApi - 为新创建的安全组创建一个入站规则，允许来自您在 RemoteAccessCidr 参数中指定的 CIDR 的 RDP 流量。
- aws:executeAwsApi - 使用您在 IamInstanceProfileName 参数中指定的值创建一个 IAM 角色和实例配置文件。
- aws:executeAwsApi - 根据您在运行手册参数中指定的值一个启动 Amazon EC2 实例。
- aws:executeAwsApi - 创建一个 AWS Systems Manager 文档以便将新启动的实例加入您的目录。
- aws:runCommand - 将新实例加入您的目录。
- aws:runCommand - 在新实例上安装远程服务器管理工具。

AWSSupport-TroubleshootADConnectorConnectivity

描述

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

- 检查与 AD Connector 关联的安全组和网络访问控制列表（ACL）规则是否允许所需的流量。
- 检查 AWS Systems Manager、AWS Security Token Service 和 Amazon CloudWatch 接口 VPC 端点是否与 AD Connector 位于同一虚拟私有云（VPC）。

成功完成先决条件检查后，运行手册将在与您的 AD Connector 相同的子网中启动两个 Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro 实例。然后使用 netcat 和 nslookup 实用程序执行网络连接测试。

运行此自动化（控制台）

> **Important**
>
> 使用此运行手册可能会对您的 AWS 账户 产生自动化期间创建的 Amazon EC2 实例、Amazon Elastic Block Store 卷和 Amazon Machine Image (AMI) 的额外费用。有关更多信息，请参阅 Amazon Elastic Compute Cloud 定价和 Amazon Elastic Block Store 定价。
> 如果 aws:deletestack 步骤失败，则转到 AWS CloudFormation 控制台手动删除该堆栈。此运行手册创建的堆栈名称以 AWSSupport-TroubleshootADConnectorConnectivity

开头。有关删除 AWS CloudFormation 堆栈的信息，请参阅AWS CloudFormation《用户指南》中的删除堆栈。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- DirectoryId

  类型：字符串

  描述：（必需）要排除连接问题的 AD Connector 目录的 ID。

- Ec2InstanceProfile

  类型：字符串

  最多 128 个字符

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

所需的 IAM 权限

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

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

文档步骤

- aws:assertAwsResourceProperty - 确认 DirectoryId 参数中指定的目录是 AD Connector。
- aws:executeAwsApi - 收集有关 AD Connector 的信息。
- aws:executeAwsApi - 收集与 AD Connector 关联的安全组的相关信息。
- aws:executeAwsApi - 收集与 AD Connector 子网关联的网络 ACL 规则的相关信息。
- aws:executeScript - 评价 AD Connector 安全组规则，以验证是否允许所需的出站流量。

- aws:executeScript - 评价 AD Connector 网络 ACL 规则，以验证是否允许所需的出站和入站网络流量。
- aws:executeScript - 检查 AWS Systems Manager、AWS Security Token Service和 Amazon CloudWatch 接口端点是否与 AD Connector 位于同一个 VPC。
- aws:executeScript - 编译在先前步骤执行的检查的输出。
- aws:branch - 根据先前步骤的输出对自动化进行分支。如果安全组和网络 ACL 缺少所需的出站和入站规则，自动化将在此处停止。
- aws:createStack - 创建 AWS CloudFormation 堆栈以启动 Amazon EC2 实例来执行连接测试。
- aws:executeAwsApi - 收集新启动的 Amazon EC2 实例的 ID。
- aws:waitForAwsResourceProperty - 等待第一个新启动的 Amazon EC2 实例报告为由 AWS Systems Manager 管理。
- aws:waitForAwsResourceProperty - 等待第二个新启动的 Amazon EC2 实例报告为由 AWS Systems Manager 管理。
- aws:runCommand - 对第一个 Amazon EC2 实例的本地 DNS 服务器 IP 地址执行网络连接测试。
- aws:runCommand - 对第二个 Amazon EC2 实例的本地 DNS 服务器 IP 地址执行网络连接测试。
- aws:changeInstanceState - 停止用于连接测试的 Amazon EC2 实例。
- aws:deleteStack - 删除 AWS CloudFormation 堆栈。
- aws:executeScript - 输出有关在自动化无法删除 AWS CloudFormation 堆栈时如何手动删除堆栈的说明。

AWSSupport-TroubleshootDirectoryTrust

描述

AWSSupport-TroubleshootDirectoryTrust 运行手册诊断 AWS Managed Microsoft AD 与 Microsoft Active Directory 之间的信任创建问题。自动化可确保目录类型支持信任关系，然后检查关联的安全组规则、网络访问控制列表（网络 ACL）和路由表是否存在潜在的连接问题。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- DirectoryId

  类型：字符串

  允许的模式：^d-[a-z0-9]{10}$

  说明：（必需）要排查问题的 AWS Managed Microsoft AD 的 ID。

- RemoteDomainCidrs

  类型：StringList

  允许的模式：^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])(\/(3[0-2]|[1-2][0-9]|[1-9]))$

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

- RemoteDomainName

  类型：字符串

  说明：（必需）将与之建立信任关系的远程域的完全限定域名。

- RequiredTrafficACL

  类型：字符串

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

默认值：{"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- RequiredTrafficSG

  类型：字符串

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

  默认值：{"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- TrustId

  类型：字符串

  说明：（可选）要排查问题的信任关系的 ID。

所需的 IAM 权限

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

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

文档步骤

- aws:assertAwsResourceProperty - 确认目录类型为 AWS Managed Microsoft AD。
- aws:executeAwsApi - 获取有关 AWS Managed Microsoft AD 的信息。
- aws:branch - 在为 TrustId 输入参数提供了值时对自动化进行分支。

- aws:executeAwsApi - 获取有关信任关系的信息。
- aws:executeAwsApi - 获取 RemoteDomainName 的条件转发服务器 DNS IP 地址。
- aws:executeAwsApi - 获取有关已添加到 AWS Managed Microsoft AD 的 IP 路由的信息。
- aws:executeAwsApi - 获取 AWS Managed Microsoft AD 子网的 CIDR。
- aws:executeAwsApi - 获取有关与 AWS Managed Microsoft AD 关联的安全组的信息。
- aws:executeAwsApi - 获取有关与AWS Managed Microsoft AD 关联的网络 ACL 的信息。
- aws:executeScript - 确认 RemoteDomainCidrs 为有效值。确认 AWS Managed Microsoft AD 具有 RemoteDomainCidrs 的条件转发服务器，并且必需的 IP 路由已添加到 AWS Managed Microsoft AD（如果 RemoteDomainCidrs 为非 RFC 1918 IP 地址）。
- aws:executeScript - 评估安全组规则。
- aws:executeScript - 评估网络 ACL。

输出

evalDirectorySecurityGroup.output - 针对与 AWS Managed Microsoft AD 关联的安全组是否允许信任关系建立的必需流量的评估结果。

evalAclEntries.output - 针对与 AWS Managed Microsoft AD 关联的网络 ACL 是否允许信任关系建立的必需流量的评估结果。

evaluateRemoteDomainCidr.output - 针对 RemoteDomainCidrs 是否为有效值的评估结果。确认 AWS Managed Microsoft AD 具有 RemoteDomainCidrs 的条件转发服务器，并且必需的 IP 路由已添加到 AWS Managed Microsoft AD（如果 RemoteDomainCidrs 为非 RFC 1918 IP 地址）。

AWS AppSync

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

主题

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）您要为其启用日志记录功能的 API 的 ID。
- FieldLogLevel

  类型：字符串

  有效值：错误 | 全部

  描述：（必填）字段记录级别。
- CloudWatchLogsRoleArn

  类型：字符串

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

- ExcludeVerboseContent

  类型：布尔值

  默认值：False

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

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- appsync:GetGraphqlApi
- appsync:UpdateGraphqlApi
- iam:PassRole

文档步骤

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

输出

- EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse: 来UpdateGraphqlApi电的回应。
- EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse: 来UpdateGraphqlApi电的回应。
- EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse: 来UpdateGraphqlApi电的回应。

- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`：来`UpdateGraphqlApi`电的回应。

Amazon Athena

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

主题

- AWS-EnableAthenaWorkGroupEncryptionAtRest

`AWS-EnableAthenaWorkGroupEncryptionAtRest`

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- WorkGroup

  类型：字符串

  描述：（必填）要为其启用静态加密的工作组。

- EncryptionOption

  类型：字符串

  有效值：SSE_S3 | SSE_KMS | CSE_KMS

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

- KmsKeyId

  类型：字符串

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

- EnableMinimumEncryptionConfiguration

  类型：布尔值

  默认值：True

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

- EnforceWorkGroupConfiguration

  类型：布尔值

  默认值：True

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

所需的 IAM 权限

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

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

文档步骤

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

DynamoDB

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

主题

- AWS-ChangeDDBRWCapacityMode
- AWS-CreateDynamoDBBackup
- AWS-DeleteDynamoDbBackup
- AWSConfigRemediation-DeleteDynamoDbTable
- AWS-DeleteDynamoDbTableBackups
- AWSConfigRemediation-EnableEncryptionOnDynamoDbTable
- AWSConfigRemediation-EnablePITRForDynamoDbTable
- AWS-EnableDynamoDbAutoscaling
- AWS-RestoreDynamoDBTable

AWS-ChangeDDBRWCapacityMode

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  有效值：已配置 | 按请求付费

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

  类型：整数

  默认：0

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

- TableNames

  类型：字符串

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

  类型：整数

  默认：0

  描述：（可选）DynamoDB 返回限制异常之前每秒消耗的最大写入次数。

所需的 IAM 权限

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

- `dynamodb:DescribeTable`
- `dynamodb:UpdateTable`

文档步骤

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

输出

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

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

AWS-CreateDynamoDBBackup

描述

创建 Amazon DynamoDB 表的备份。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要创建的备份的名称。
- LambdaAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）DynamoDB 表的名称。

AWS-DeleteDynamoDbBackup

描述

删除 Amazon DynamoDB 表的备份。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要删除的 DynamoDB 表备份的 ARN。

AWSConfigRemediation-DeleteDynamoDbTable

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要删除的 DynamoDB 表的名称。

所需的 IAM 权限

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

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

文档步骤

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

AWS-DeleteDynamoDbTableBackups

描述

根据保留天数或计数删除 DynamoDB 表的备份。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

  默认值：10

  说明：（可选）要为表保留的备份数。如果存在超过指定数量的备份，则删除超过该数量的最旧备份。可以使用 RetentionCount 或 RetentionDays，但不能同时使用两者。
- RetentionDays

  类型：字符串

说明：（可选）保留表备份的天数。将删除超过指定天数的备份。可以使用 RetentionCount 或 RetentionDays，但不能同时使用两者。

- TableName

  类型：字符串

  说明：（必需）DynamoDB 表的名称。

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

- KMS KeyId

  类型：字符串

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

- TableName

  类型：字符串

  说明：（必需）您要加密的 DynamoDB 表的名称。

所需的 IAM 权限

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

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

文档步骤

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

AWSConfigRemediation-EnablePITRForDynamoDbTable

描述

AWSConfigRemediation-EnablePITRForDynamoDbTable 运行手册对您指定的 Amazon DynamoDB 表启用时间点故障恢复（PITR）。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）对其启用时间点故障恢复的 DynamoDB 表的名称。

所需的 IAM 权限

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

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

文档步骤

- `aws:executeAwsApi` - 对您在 `TableName` 参数中指定的 DynamoDB 表启用时间点故障恢复。
- `aws:assertAwsResourceProperty` - 确认对 DynamoDB 表启用时间点故障恢复。

AWS-EnableDynamoDbAutoscaling

描述

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

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：整数

  描述：（必填）DynamoDB 表的最小预配置吞吐量读取容量单位数。
- MaxReadCapacity

  类型：整数

  描述：（必填）DynamoDB 表的最大预配置吞吐量读取容量单位数。

- TargetReadCapacityUtilization

  类型：整数

  描述：（必填）所需的目标读取容量利用率。目标利用率是某一时间点消耗的预配置吞吐量的百分比。您可以将 auto scaling 目标利用率值设置在 20% 到 90% 之间。

- ReadScaleOutCooldown

  类型：整数

  描述：（必填）等待上一次读取容量扩展活动生效所需的时间（以秒为单位）。

- ReadScaleInCooldown

  类型：整数

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

- MinWriteCapacity

  类型：整数

  描述：（必填）DynamoDB 表的最小预配置吞吐量写入单位数。

- MaxWriteCapacity

  类型：整数

  描述：（必填）DynamoDB 表的最大预配置吞吐量写入单位数。

- TargetWriteCapacityUtilization

  类型：整数

  描述：（必填）所需的目标写入容量利用率。目标利用率是某一时间点消耗的预配置吞吐量的百分比。您可以将 auto scaling 目标利用率值设置在 20% 到 90% 之间。

- WriteScaleOutCooldown

  类型：整数

  描述：（必填）等待上一次写入容量扩展活动生效所需的时间（以秒为单位）。

- WriteScaleInCooldown

  类型：整数

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

所需的 IAM 权限

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

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- application-autoscaling:DescribeScalableTargets
- application-autoscaling:DescribeScalingPolicies
- application-autoscaling:PutScalingPolicy
- application-autoscaling:RegisterScalableTarget

- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi)-在你指定的 DynamoDB 表上配置 Application Auto Scaling。
- RegisterAppAutoscalingTargetWriteDelay (aws: sleep)-休眠以避免 API 限制。
- PutScalingPolicyWrite (aws:executeAwsApi)-配置 DynamoDB 表的目标写入容量利用率。
- PutScalingPolicyWriteDelay (aws: sleep)-休眠以避免 API 限制。
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi)-为 DynamoDB 表配置最小和最大读取容量单位。
- RegisterAppAutoscalingTargetReadDelay (aws: sleep)-休眠以避免 API 限制。
- PutScalingPolicyRead (aws:executeAwsApi)-配置 DynamoDB 表的目标读取容量利用率。
- VerifyDynamoDbAutoscalingEnabled (aws: ExecuteScript)-根据你指定的值验证 DynamoDB 表是否启用了 Application Auto Scaling。

输出

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

AWS-RestoreDynamoDBTable

描述

该AWS-RestoreDynamoDBTable运行手册使用时间点故障恢复 (PITR) 来恢复您指定的Amazon DynamoDB 表。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
- 根据需要启用时间点故障恢复

  类型：布尔值

  默认值：True

  描述：（可选）确定自动化是否根据需要启用恢复表的时间点故障恢复。
- GlobalSecondaryIndexOverride

  类型：字符串

  描述：（可选）新的全局二级索引，用于替换新表的现有二级索引。

- LocalSecondaryIndexOverride

  类型：字符串

  描述：（可选）新的本地二级索引，用于替换新表的现有二级索引。

- RestoreDateTime

  类型：字符串

  描述：（必需）最近 35 天中要将该表还原到的时间点故障恢复。采用以下格式的指定日期和时间：DD/MM/YYYY HH:MM:SS

- SourceTableArn

  类型：字符串

  说明：（必需）要复原的表的 ARN。

- SseSpecificationOverride

  类型：字符串

  描述：（可选）用于新表的服务器端加密设置。

- TargetTableName

  类型：字符串

  描述：（必需）要恢复的表的名称。

所需的 IAM 权限

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

- dynamodb:BatchWriteItem
- dynamodb:DeleteItem
- dynamodb:DescribeTable
- dynamodb:GetItem
- dynamodb:PutItem
- dynamodb:Query
- dynamodb:RestoreTableToPointInTime

- dynamodb:Scan
- dynamodb:UpdateItem

文档步骤

- aws:executeScript - 使用时间点故障恢复功能恢复您在参数中指定的 DynamoDB 表TargetTableName。

Amazon EBS

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

主题

- AWSSupport-AnalyzeEBSResourceUsage
- AWS-ArchiveEBSSnapshots
- AWS-AttachEBSVolume
- AWSSupport-CalculateEBSPerformanceMetrics
- AWS-CopySnapshot
- AWS-CreateSnapshot
- AWS-DeleteSnapshot
- AWSConfigRemediation-DeleteUnusedEBSVolume
- AWS-DeregisterAMIs
- AWS-DetachEBSVolume
- AWSConfigRemediation-EnableEbsEncryptionByDefault
- AWS-ExtendEbsVolume
- AWSSupport-ModifyEBSSnapshotPermission
- AWSConfigRemediation-ModifyEBSVolumeType

AWSSupport-AnalyzeEBSResourceUsage

描述

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

如何工作？

运行手册执行以下四项任务：

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

运行手册生成 CSV 报告并将其存储在用户提供的 Amazon S3 存储桶中。所提供的存储桶应按照最后概述 AWS 的安全最佳实践进行保护。如果账户中不存在用户提供的 Amazon S3 存储桶，则运行手册会创建一个名称格式的新 Amazon S3 存储桶<User-provided-name>-awssupport-YYYY-MM-DD，使用自定义 AWS Key Management Service (AWS KMS) 密钥加密，启用对象版本控制，禁止公开访问，并要求请求使用 SSL/TLS。

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

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

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

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- S3 BucketName

  类型：`AWS::S3::Bucket::Name`

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

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

- CustomerManagedKmsKeyArn

  类型：字符串

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

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

所需的 IAM 权限

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

- `ec2:DescribeImages`

- ec2:DescribeInstances
- ec2:DescribeSnapshots
- ec2:DescribeVolumes
- kms:Decrypt
- kms:GenerateDataKey
- s3:CreateBucket
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:ListBucket
- s3:ListAllMyBuckets
- s3:PutObject
- s3:PutBucketLogging
- s3:PutBucketPolicy
- s3:PutBucketPublicAccessBlock
- s3:PutBucketTagging
- s3:PutBucketVersioning
- s3:PutEncryptionConfiguration
- ssm:DescribeAutomationExecutions

具有运行此运行手册所需的最低 IAM 权限的策略示例：

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

说明

按照这些步骤对自动化进行配置：

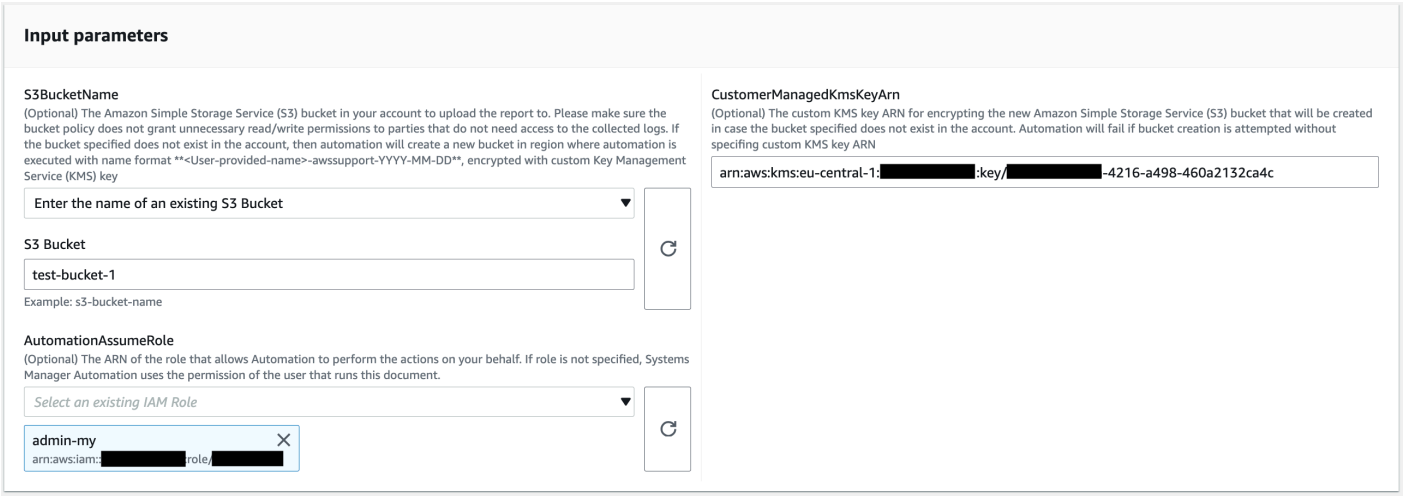
1. 在控制台中导航到 AWSSupport-analyzeEBS ResourceUsage。 AWS Systems Manager

2. 要输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

     允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
   - S3BucketName （必填）：

     您账户中用于将报告上传到的 Amazon S3 存储桶。
   - CustomerManagedKmsKeyArn （可选）：

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



3. 选择执行。
4. 自动化启动。
5. 自动化运行手册执行以下步骤：
   - 检查并发性：

     确保该地区只有一个启动该运行手册。如果 runbook 发现另一个正在执行的执行，则会返回错误并结束。
   - 验证 OrCreate s3Bucket：

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

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

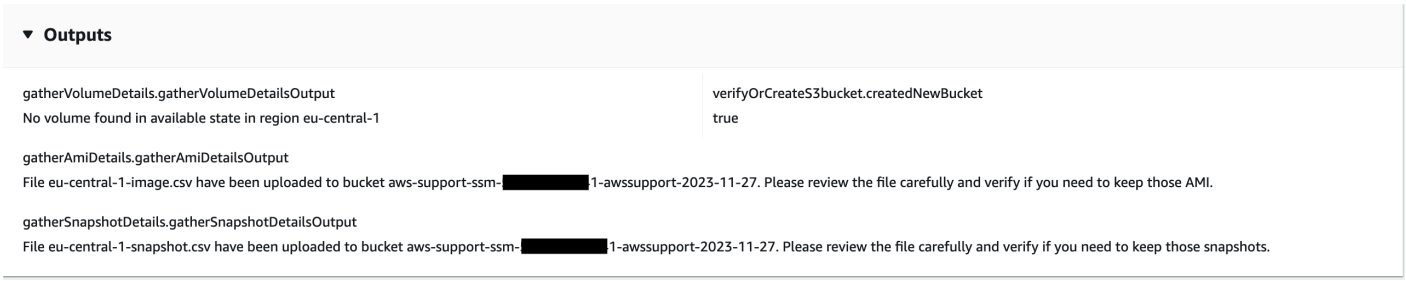
- 收集VolumeDetails：

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

- 收集SnapshotDetails：

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

6. 完成后，查看“输出”部分以了解执行的详细结果。



参考

Systems Manager Automation

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

AWS-ArchiveEBSSnapshots

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- 描述

  类型：字符串

  描述：（可选）对 Amazon EBS 快照的说明。

- DryRun

  类型：字符串

  有效值：是 | 否

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

- RetentionCount

  类型：字符串

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

- RetentionDays

  类型：字符串

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

- SnapshotWith标签

  类型：字符串

  有效值：是 | 否

  描述：（必需）指定要归档的快照是否已添加标签。

- TagKey

  类型：字符串

  描述：（可选）分配给要归档快照的标签的键。

- TagValue

  类型：字符串

  描述：（可选）分配给要归档快照的标签的值。

- VolumeId

  类型：字符串

  描述：（可选）要归档快照的卷 ID。如果快照未添加标签，请使用此参数。

所需的 IAM 权限

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

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

文档步骤

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

AWS-AttachEBSVolume

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）设备名称（例如，/dev/sdh 或 xvdh）。
- InstanceId

  类型：字符串

  描述：（必需）要附加卷的实例的 ID。
- VolumeId

类型：字符串

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

AWSSupport-CalculateEBSPerformanceMetrics

描述

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

如何工作？

运行手册执行以下步骤：

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

> **Note**
>
> 对于可突发卷（gp2、sc2 和 st1），在达到突发平衡之前，应考虑最大的 IOPS/吞吐量。在完全利用突发平衡（即突发平衡变为零）之后，请考虑基准 IOPS/吞吐量指标。

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

运行此自动化（控制台）

所需的 IAM 权限

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

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

政策示例

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

```
            ]
        }
```

说明

按照这些步骤对自动化进行配置：

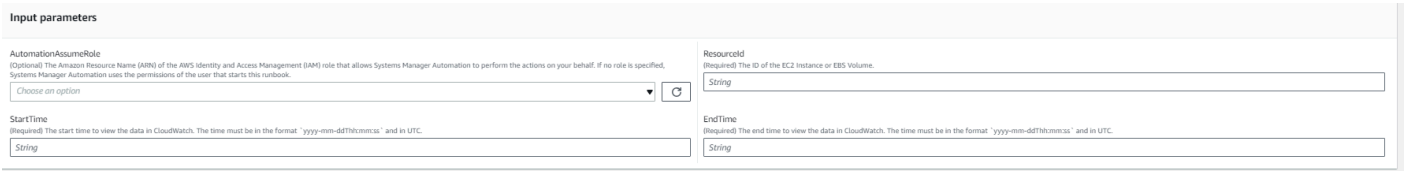
1. AWSSupport-CalculateEBSPerformanceMetrics在 Systems Manager 的 “文档” 下导航至。
2. 选择 Execute automation（执行自动化）。
3. 对于输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

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

     亚马逊 EC2 实例或亚马逊 EBS 卷的 ID。
   - 开始时间（必填）：

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

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



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
   - CheckResourceIdAndTimeStamps:

     检查结束时间是否比开始时间大于开始时间至少一分钟，以及所提供的资源是否存在。
   - CreateCloudWatchDashboard:

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

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

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

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

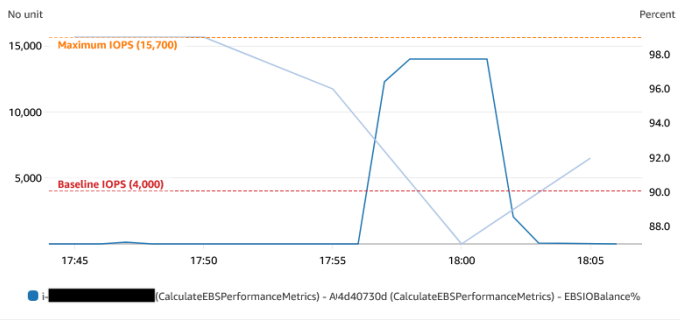
More details on EBS Optimized instances | More details on EBS Volume Types

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

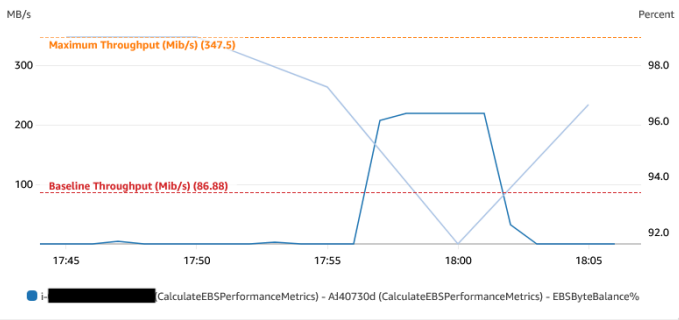
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

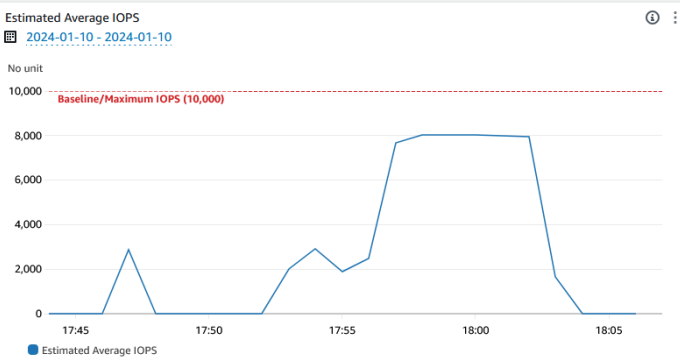
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

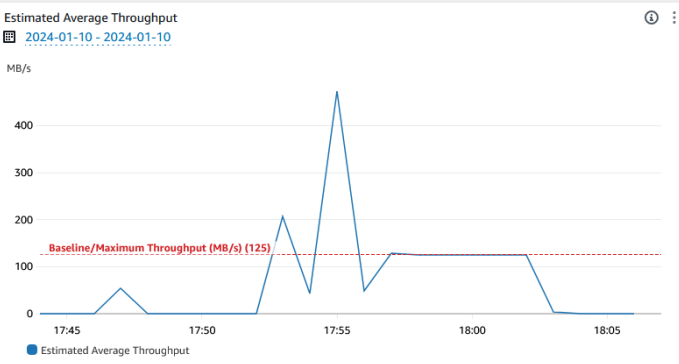
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

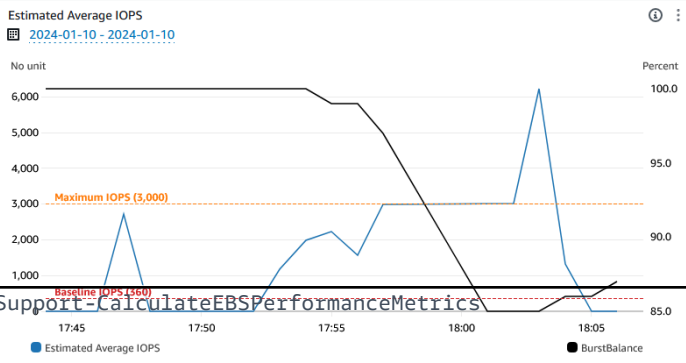


Estimated Average Throughput
2024-01-10 - 2024-01-10

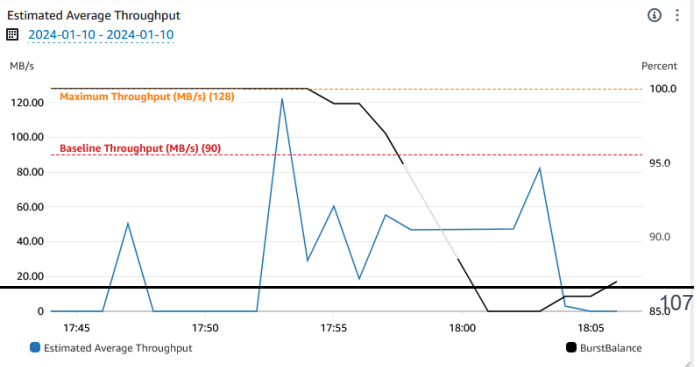


Volume: vol[redacted] | Type: gp2

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



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

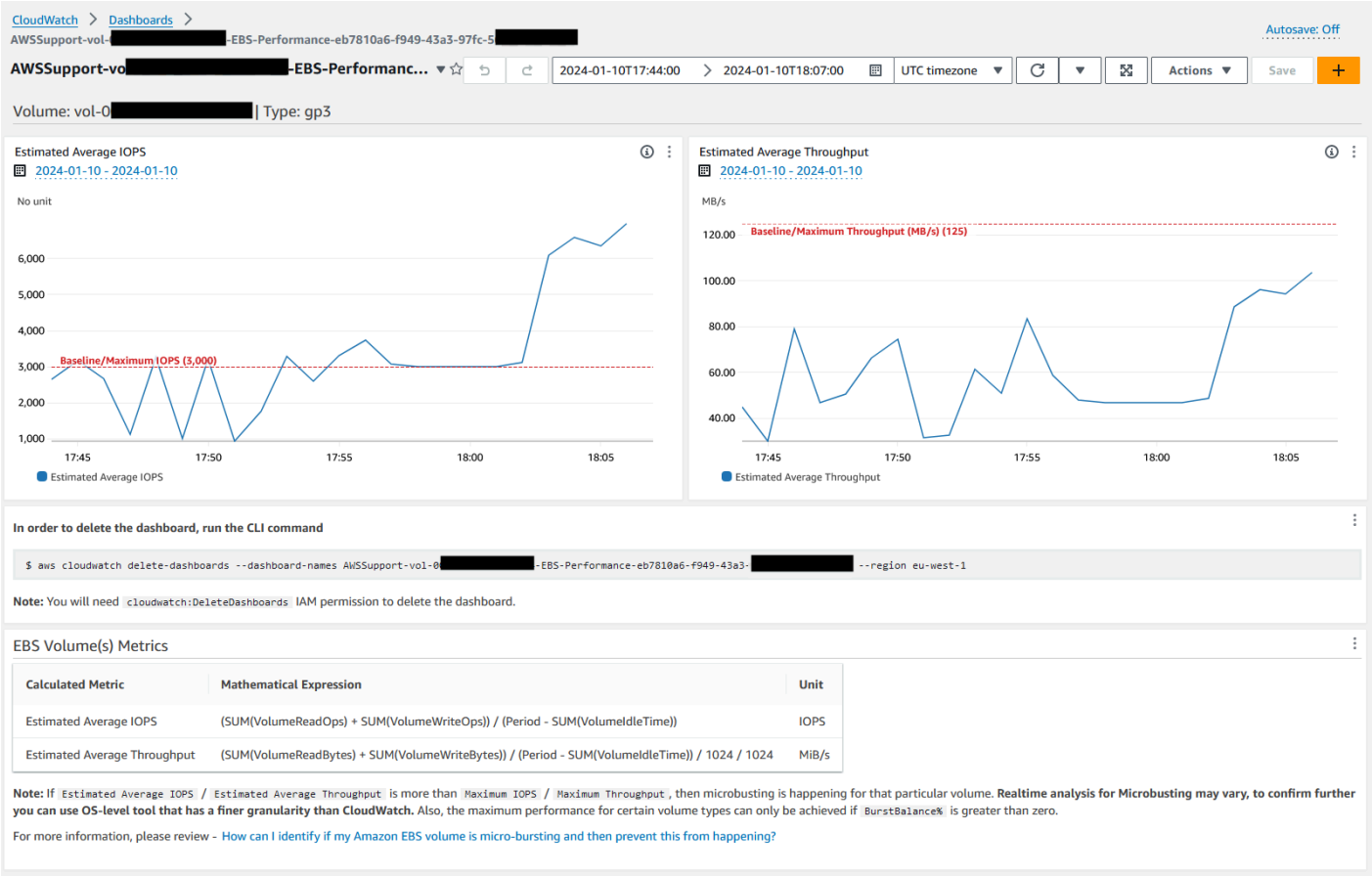


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

资源标识为 Amazon EBS 卷 ID 的示例 CloudWatch 控制面板



参考

Systems Manager Automation

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

AWS 服务文档

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

AWS-CopySnapshot

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（可选）对 Amazon EBS 快照的说明。
- SnapshotId

  类型：字符串

  描述：（必需）要复制的 Amazon EBS 快照的 ID。

- SourceRegion

  类型：字符串

  描述：（必需）源快照当前所在的区域。

文档步骤

copySnapshot - 复制 Amazon EBS 卷的快照。

输出

CopySnapshot。 SnapshotId -新快照的 ID。

AWS-CreateSnapshot

描述

创建 Amazon EBS 卷的快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- 描述

  类型：字符串

  描述：（可选）对快照的说明
- VolumeId

  类型：字符串

  描述：（必需）卷的 ID。

AWS-DeleteSnapshot

描述

删除 Amazon EBS 卷快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

类型：字符串

描述：（必需）EBS 快照的 ID。

AWSConfigRemediation-DeleteUnusedEBSVolume

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：布尔值

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

  类型：字符串

描述：（必需）要删除的 Amazon EBS 卷的 ID。

所需的 IAM 权限

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

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

文档步骤

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

AWS-DeregisterAMIs

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- DryRun

  类型：字符串

  有效值：是 | 否

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

- RetainNumber

  类型：字符串

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

- 天数

  类型：字符串

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

- TagKey

  类型：字符串

  描述：（必需）分配给要取消注册 AMIs 的标签的键。

- TagValue

  类型：字符串

  描述：（必需）分配给要取消注册 AMIs 的标签的值。

所需的 IAM 权限

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

- ec2:DeregisterImage
- ec2:DescribeImages

文档步骤

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

AWS-DetachEBSVolume

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

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

- LambdaAssume角色

  类型：字符串

  描述：（可选）Lambda担任的角色的 ARN。

- VolumeId

  类型：字符串

  描述：（必需）EBS 卷的 ID。卷和实例必须位于同一可用区内

AWSConfigRemediation-EnableEbsEncryptionByDefault

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

类型：字符串

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

所需的 IAM 权限

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

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

文档步骤

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

AWS-ExtendEbsVolume

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

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

  类型：布尔值

  默认：True

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

  类型：字符串

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

  类型：字符串

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

  类型：字符串

描述：（必需）要扩展的 EBS 卷 的 ID。

所需的 IAM 权限

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

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

文档步骤

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

AWSSupport-ModifyEBSSnapshotPermission

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型: StringList

  默认：无

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

  类型：字符串

  有效值：添加 | 移除

  默认：无

  描述：（可选）要执行的操作类型。
- 专属

  类型：字符串

  有效值：是 | 否

  描述：（必需）如果要与特定账户共享快照，则为该值输入 No。
- SnapshotIds

  类型: StringList

  描述：（必需）要修改其权限的 Amazon EBS 快照的 ID。

所需的 IAM 权限

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

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

文档步骤

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

输出

ValidateSnapshots.EncryptedSnapshots

SharewithOther账户. 结果

MakePrivate.Result

MakePrivate. 命令

AWSConfigRemediation-ModifyEBSVolumeType

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要修改的 Amazon EBS 卷的 ID。
- EbsVolume类型

  类型：字符串

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

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

所需的 IAM 权限

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

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

文档步骤

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

Amazon EC2

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

主题

- AWS-ASGEnterStandby
- AWS-ASGExitStandby
- AWS-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

描述

更改 Auto Scaling 组中Amazon Elastic Compute Cloud (Amazon EC2) 实例的备用状态。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  说明：（必需）要更改自动扩缩组中备用状态的 Amazon EC2 实例的 ID。

- LambdaRoleArn

  类型：字符串

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

AWS-ASGExitStandby

描述

更改 Auto Scaling 组中Amazon Elastic Compute Cloud (Amazon EC2) 实例的备用状态。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要更改自动扩缩组中备用状态的 EC2 实例的 ID。
- LambdaRoleArn

  类型：字符串

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

AWS-CreateImage

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）EC2 实例的 ID。
- NoReboot

  类型：布尔值

说明：（可选）创建映像前，不要重启实例。

所需的 IAM 权限

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

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

AWS-DeleteImage

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ImageId

  类型：字符串

  说明：（必需）AMI 的 ID。

所需的 IAM 权限

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

```
{
    "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

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：字符串

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

  类型：字符串

  默认值：PT2M

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

- WaitForReboot

  类型：字符串

  默认值：PT5M

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

所需的 IAM 权限

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

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

- `lambda:InvokeFunction`

AWS-PatchInstanceWithRollback

描述

使 EC2 实例符合适用的补丁基准。失败时对根卷进行回滚。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）patch-baseline 所应用的 EC2 InstanceId。
- LambdaAssumeRole

  类型：字符串

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

- ReportS3Bucket

  类型：字符串

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

文档步骤

步骤编号	步骤名称	自动化操作
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand
5	SleepThruInstallation	aws:invokeLambdaFunction
6	CheckCompliance	aws:invokeLambdaFunction
7	SaveComplianceReportToS3	aws:invokeLambdaFunction
8	ReportSuccessOrFailure	aws:invokeLambdaFunction
9	RestoreFromSnapshot	aws:invokeLambdaFunction
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationTemplate	aws:deleteStack

输出

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

AWS-QuarantineEC2Instance

描述

使用 AWS-QuarantineEC2Instance 运行手册，您可以为不允许任何入站或出站流量的 Amazon Elastic Compute Cloud (Amazon EC2) 实例分配一个安全组。

> **Important**
> 在运行此运行手册前，应仔细检查对 RDP 设置的更改。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  说明：（必需）要管理其 RDP 设置的托管实例的 ID。

- IsolationSecurityGroup

  类型：字符串

  描述：（必需）您要分配给实例以防止入站或出站流量的安全组的名称。

所需的 IAM 权限

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

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

文档步骤

- aws:executeAwsApi - 收集有关该实例的详细信息。
- aws:executeScript - 验证该实例是否为自动扩缩组的一部分。
- aws:executeAwsApi - 创建附加到该实例的根卷的一个快照。
- aws:waitForAwsResourceProperty - 等待快照状态处于 completed。

- aws:executeAwsApi - 将 IsolationSecurityGroup 参数中指定的安全组分配给您的实例。

输出

GetEC2InstanceResources.RevokedSecurityGroupsIds

GetEC2InstanceResources.RevokedSecurityGroupsNames

createSnapshot.SnapId

AWS-ResizeInstance

描述

更改 Amazon Elastic Compute Cloud (Amazon EC2) 实例的实例类型。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）实例的 ID。

- InstanceType

  类型：字符串

  说明：（必需）实例类型。
- LambdaAssumeRole

  类型：字符串

  说明：（可选）Lambda 担任的角色的 ARN。

AWS-RestartEC2Instance

描述

重启一个或多个 Amazon Elastic Compute Cloud（Amazon EC2）实例

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  说明：（可选）允许 AWS Identity and Access Management Systems Manager Automation 代表您执行操作的 (IAM) 角色的 Amazon 资源名称 (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户权限。
- InstanceId

  类型：StringList

说明：（必需）Amazon EC2 实例的 ID 以重新启动。

AWS-SetupJupyter

描述

AWS-SetupJupyter 运行手册可帮助您在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上设置 Jupyter Notebook。您可以指定一个现有实例，也可以为自动化提供一个 Amazon Machine Image (AMI) ID 以启动和设置新实例。开始之前，您必须先在 Parameter Store 中创建一个 SecureString 参数，用作 Jupyter Notebook 的密码。Parameter Store 是 AWS Systems Manager 的一项功能。有关创建参数的更多信息，请参阅 AWS Systems Manager 用户指南 中的 创建参数。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

  说明：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。

- AmiId

  类型：字符串

  描述：（可选）您要用于启动新实例和设置 Jupyter Notebook 的 AMI ID。

- InstanceId

  类型：字符串

  说明：（必需）您想要设置 Jupyter Notebook 的实例的 ID。
- InstanceType

  类型：字符串

  默认：t3.medium

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

  类型：字符串

  描述：（必填）Parameter Store 中要用作 Jupyter Notebook 密码的 `SecureString` 参数的名称。
- KeyPairName

  类型：字符串

  描述：（可选）要与新启动实例关联的密钥对。
- RemoteAccessCidr

  类型：字符串

  默认值：0.0.0.0/0

  描述：（可选）您希望允许 SSH 流量来自的 CIDR 范围。
- RoleName

  类型：字符串

  默认值：SSMManagedInstanceProfileRole

  描述：（可选）新启动实例的实例配置文件的名称。
- StackName

  类型：字符串

  默认值：CreateManagedInstanceStack{{automation:EXECUTION_ID}}

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

- SubnetId

  类型：字符串

  默认值：Default

  描述：（可选）您希望启动新实例以便使用的子网。

- VpcId

  类型：字符串

  默认值：Default

  描述：（可选）要将新实例启动到的虚拟私有云（VPC）的 ID。

所需的 IAM 权限

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

- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ssm:GetParameter
- ssm:SendCommand
- ssm:StartAutomationExecution
- cloudformation:CreateStack
- cloudformation:DeleteStack
- cloudformation:DescribeStacks
- ec2:DescribeInstances
- ec2:DescribeKeyPairs
- ec2:RunInstances
- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePolicy

- iam:DetachRolePolicy
- iam:GetRole
- iam:PassRole
- iam:PutRolePolicy
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction

文档步骤

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

AWS-StartEC2Instance

描述

启动一个或多个 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

说明：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。

- InstanceId

  类型：StringList

  说明：（必需）要启动的 EC2 实例。

AWS-StopEC2Instance

描述

存储一个或多个 Amazon Elastic Compute Cloud（Amazon EC2）实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：StringList

说明：（必需）要停止的 EC2 实例。

AWS-TerminateEC2Instance

描述

终止一个或多个 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：StringList

  说明：（必需）要终止的一个或多个 EC2 实例的 ID。

AWS-UpdateLinuxAmi

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  默认：无

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

  类型：字符串

  默认： ManagedInstanceProfile

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

  类型：字符串

  默认：all

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

- InstanceType

  类型：字符串

  默认：t2.micro

  说明：（可选）启动作为工作区主机的实例的类型。实例类型因区域而异。

- MetadataOptions

  类型: StringMap

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

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

- PostUpdateScript

  类型：字符串

  默认：无

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

- PreUpdateScript

  类型：字符串

  默认：无

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

- SecurityGroupIds

  类型：字符串

  描述：（必填）要应用到的安全组的 ID 列表，以逗号分隔。AMI

- SourceAmiId

  类型：字符串

  说明：（必需）源 Amazon 系统映像 ID。

- SubnetId

类型：字符串

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

- TargetAmiName

  类型：字符串

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

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

AWS-UpdateWindowsAmi

描述

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

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- 类别

  类型：字符串

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

- ExcludeKbs

  类型：字符串

  说明：（可选）指定一个或多个要排除的 Microsoft 知识库 (KB) 文章 ID。可以使用逗号分隔值排除多个 ID。有效格式：KB9876543 或 9876543。

- IamInstanceProfileName

  类型：字符串

  默认： ManagedInstanceProfile

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

- IncludeKbs

  类型：字符串

  说明：（可选）指定一个或多个要包含的 Microsoft 知识库 (KB) 文章 ID。可以使用逗号分隔值安装多个 ID。有效格式：KB9876543 或 9876543。

- InstanceType

  类型：字符串

默认：t2.medium

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

- MetadataOptions

  类型: StringMap

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

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

- PostUpdateScript

  类型：字符串

  说明：（可选）以字符串形式提供的脚本。它将在安装操作系统更新后运行。

- PreUpdateScript

  类型：字符串

  说明：（可选）以字符串形式提供的脚本。它将在安装操作系统更新前运行。

- PublishedDateAfter

  类型：字符串

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

- PublishedDateBefore

  类型：字符串

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

- PublishedDaysOld

  类型：字符串

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

- SecurityGroupIds

类型：字符串

描述：（必填）要应用到的安全组的 ID 列表，以逗号分隔。AMI

- SeverityLevels

  类型：字符串

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

- SourceAmiId

  类型：字符串

  描述：（必填）来源 AMI ID。

- SubnetId

  类型：字符串

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

- TargetAmiName

  类型：字符串

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

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

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

描述

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

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

  类型：整数

  默认值：300

  说明：（可选）自动扩缩在检查已投入使用的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的运行状况之前等待的时间（以秒为单位）。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeAutoScalingGroups`

- ec2:UpdateAutoScalingGroup

文档步骤

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

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

描述

AWSConfigRemediation-EnforceEC2InstanceIMDSv2 运行手册需要您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例才能使用实例元数据服务版本 2 (IMDSv2)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- InstanceId

  类型：字符串

  描述：（必需）您想要请求使用 IMDSv2 的 Amazon EC2 实例的 ID。
- AutomationAssumeRole

  类型：字符串

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

- HttpPutResponseHopLimit

  类型：整数

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

  允许的模式：^([1-5]?\d|6[0-4])$

  默认：0

所需的 IAM 权限

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

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

文档步骤

- aws:executeScript - 在 InstanceId 参数中指定的 Amazon EC2 实例上，将 HttpTokens 选项设置为 required。
- aws:assertAwsResourceProperty - 验证 Amazon EC2 实例上是否需要 imdsvv2。

AWSEC2-CloneInstanceAndUpgradeSQLServer

描述

从适用于 Windows Server 运行 SQL Server 2008（或更高版本）的 EC2 实例创建一个 AMI，然后将此 AMI 升级到 SQL Server 更新版本。

支持的升级路径如下所示：

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

- SQL Server 2014 到 SQL Server 2019、2017 或 2016
- SQL Server 2016 到 SQL Server 2019 或 2017
- SQL Server 2017 到 SQL Server 2019

如果您使用的是与 SQL Server 2019 不兼容的早期版本 Windows Server，则自动化文档必须将你的 Windows Server 版本升级到 2016。

升级是一个多步骤过程，可能需要 2 个小时才能完成。Automation 从实例创建一个 AMI，然后从新创建的 AMI 在您指定的 `SubnetID` 中启动一个临时实例。与您的原始实例关联的安全组将应用于临时实例。Automation 在临时实例上执行到 `TargetSQLVersion` 的就地升级。升级后，自动化会从临时实例创建新 AMI，然后终止临时实例。

您可以通过在 VPC 中启动此新 AMI i来测试应用程序功能。完成测试后，在执行下一次升级之前，请先计划应用程序停机时间，然后再完全切换到升级后的实例。

> **Note**
>
> 如果您想要修改从新 AMI 启动的 EC2 实例的计算机名称，请参阅 重命名托管独立的 SQL Server 实例的计算机。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

先决条件

- TLS 版本 1.2。

- EC2 实例使用的 Windows Server 版本必须为 Windows Server 2008 R2（或更高版本）和 SQL Server 2008（或更高版本）。
- 验证实例上是否安装了 SSM Agent。有关更多信息，请参阅在 EC2 实例中为 Windows Server 安装和配置 SSM Agent。
- 配置实例以使用 AWS Identity and Access Management (IAM) 实例配置文件角色。有关更多信息，请参阅为 Systems Manager 创建 IAM 实例配置文件。
- 验证实例的实例启动盘具有 20 GB 的可用磁盘空间。
- 对于使用自带许可 (BYOL) SQL Server 版本的实例，以下额外的先决条件适用：
  - 提供包含目标 SQL Server 安装介质的 EBS 快照 ID。要实现此目的，应按照以下步骤进行：

    1. 验证 EC2 实例运行的是否是 Windows Server 2008 R2 或更高版本。
    2. 在运行实例的同一可用区中创建一个 6 GB 的 EBS 卷。将卷附加到实例。例如，将其附加为驱动器 D。
    3. 例如，右键单击 ISO 并将其挂载为实例的驱动器 E。
    4. 将 ISO 的内容从驱动器 E:\ 复制到驱动器 D:\
    5. 创建在步骤 2 中创建的 6 GB 卷的 EBS 快照。

限制

- 只能在使用 Windows 身份验证的 SQL Server 上执行升级。
- 验证实例上没有待处理的安全补丁更新。打开控制面板，然后选择检查更新。
- 不支持 HA 和镜像模式下的 SQL Server 部署。

参数

- IamInstanceProfile

  类型：字符串

  说明：（必需）IAM 实例配置文件。
- InstanceId

  类型：字符串

  说明：（必需）运行 Windows Server 2008 R2（或更高版本）和 SQL Server 2008（或更高版本）的实例。

- KeepPreUpgradeImageBackUp

  类型：字符串

  说明：（可选）如果设置为 `true`，则自动化不会删除在升级之前从实例中创建的 AMI。如果设置为 `true`，则必须由您删除此 AMI。默认情况下，将删除此 AMI。

- SubnetId

  类型：字符串

  说明：（必需）为升级过程提供子网。验证子网是否具有到 AWS 服务、Amazon S3 和 Microsoft（用于下载补丁）的出站连接性。

- SQLServerSnapshotId

  类型：字符串

  说明：（视情况而定）SQL Server 安装介质的快照 ID。对于使用 BYOL SQL Server 版本的实例，该参数是必需的。对于包含 SQL Server 许可证的实例（使用 AWS 提供的带有 Microsoft SQL Server 的 Windows Server Amazon 系统映像启动的实例），该参数是可选的。

- RebootInstanceBeforeTakingImage

  类型：字符串

  说明：（可选）如果设置为 `true`，则自动化在创建预升级 AMI 之前重新引导实例。默认情况下，自动化在升级前不重启。

- TargetSQLVersion

  类型：字符串

  描述：（可选）选择目标 SQL Server 版本。

  可能的目标：

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

  默认目标：SQL Server 2016

输出

AMIId：从升级到 SQL Server 更新版本的的实例创建的 AMI 的 ID。

AWSEC2-CloneInstanceAndUpgradeWindows

描述

从 Windows Server 2008 年 R2、2012 年 R2、2016 年或 2019 年的实例创建 Amazon Machine Image (AMI)，然后将其升级AMI到 Windows Server 2016 年、2019 年或 2022 年。支持的升级路径如下所示。

- Windows Server2008 年 R2 到 Windows Server 2016 年。
- Windows Server 2012 R2 到 Windows Server 2016。
- Windows Server 2012 R2 到 Windows Server 2019。
- Windows Server 2012 R2 到 Windows Server 2022。
- Windows Server 2016 到 Windows Server 2019。
- Windows Server 2016 到 Windows Server 2022。
- Windows Server 2019 到 Windows Server 2022。

升级操作是一个多步骤过程，可能需要 2 个小时才能完成。我们建议在具有至少 2 个 vCPU 和 4GB RAM 的实例上执行操作系统升级。自动化从实例创建一个 AMI，然后从新创建的 AMI，在您指定的 `SubnetId` 中启动一个临时实例。与您的原始实例关联的安全组将应用于临时实例。Automation 在临时实例上执行到 `TargetWindowsVersion` 的就地升级。要将 Windows Server 2008 R2 实例升级到 Windows Server 2016、2019 或 2022，请执行就地升级两次，因为不支持直接将 Windows Server 2008 R2 升级到 Windows Server 2016、2019 或 2022。自动化还会更新或安装临时实例所需的 AWS 驱动程序。升级后，自动化会从临时实例创建新 AMI，然后终止临时实例。

您可以通过在 Amazon Virtual Private Cloud (Amazon VPC)中从升级后的 AMI 启动测试实例来测试应用程序的功能。完成测试后，在执行下一次升级之前，请先计划应用程序停机时间，然后再完全切换到升级后的 AMI。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows Server 2008 R2、2012 R2、2016 和2019 标准版和数据中心版

先决条件

- TLS 版本 1.2。
- 验证实例上是否安装了 SSM Agent。有关更多信息，请参阅在 EC2 实例中为 Windows Server 安装和配置 SSM Agent。
- 必须在您的实例上安装 Windows PowerShell 3.0 或更高版本。
- 对于加入到某个 Microsoft Active Directory 域的实例，建议指定一个没有连接到您的域控制器的 `SubnetId`，以帮助避免主机名冲突。
- 实例子网必须具有与互联网的出站连接，这样可以访问 AWS 服务 诸如 Amazon S3 之类的网络，也可以访问从 Microsoft 下载补丁。如果子网是公有子网且实例具有公有 IP 地址，或者子网是私有子网并使用路由将互联网流量发送到公有 NAT 设备，即满足此要求。
- 此自动化工作仅适用于 Windows Server 2008 R2、2012 R2、2016 和 2019 实例。
- 使用为 Windows Server Systems Manager 提供必要权限的 AWS Identity and Access Management (IAM) 实例配置文件配置实例。有关更多信息，请参阅为 Systems Manager 创建 IAM 实例配置文件。
- 验证实例的启动盘具有 20 GB 的可用磁盘空间。
- 如果实例不使用 AWS提供的 Windows 许可证，请指定包含 Windows Server 2012 R2 安装媒体的 Amazon EBS 快照 ID。要实现此目的，应按照以下步骤进行：
  - 确认 EC2 实例运行 Windows Server 2012 或更高版本。
  - 在运行实例的同一可用区中创建一个 6 GB 的 EBS 卷。将卷附加到实例。例如，将其附加为驱动器 D。
  - 例如，右键单击 ISO 并将其挂载为实例的驱动器 E。
  - 将 ISO 的内容从驱动器 E:\ 复制到驱动器 D:\
  - 为上面步骤 2 中创建的 6 GB 卷创建 EBS 快照。

限制

此 Automation 不支持升级 Windows 域控制器、集群或 Windows 桌面操作系统。该 Automation 也不支持安装了以下角色的 Windows Server EC2 实例。

- 远程桌面会话主机 (RDSH)
- 远程桌面连接代理 (RDCB)
- 远程桌面虚拟化主机 (RDVH)
- 远程桌面 Web 访问 (RDWA)

参数

- AlternativeKeyPairName

  类型：字符串

  描述：（可选）升级过程中要使用的备用密钥对的名称。这在分配给初始实例的密钥对不可用的情况下很有用。如果没有为初始实例分配密钥对，则必须为此参数指定一个值。

- BYOL WindowsMediaSnapshotId

  类型：字符串

  描述：（可选）复制包括 Windows Server 2012R2 安装介质的 Amazon EBS 快照 的 ID。只有在升级 BYOL 实例时才需要。

- IamInstanceProfile

  类型：字符串

  描述：（必需）启用 Systems Manager 以管理实例的 IAM 实例配置文件的名称。

- InstanceId

  类型：字符串

  描述：（必需）运行 Windows Server 2008 R2、2012 R2、2016 或 2019 的EC2 实例。

- KeepPreUpgradeImageBackUp

  类型：字符串

  描述：（可选）如果设置为 True，则 Automation 不会删除在升级之前从 EC2 实例创建的 AMI。如果设置为 True，则必须由您删除此 AMI。默认情况下，将删除此 AMI。

- SubnetId

  类型：字符串

描述：（必需）这是执行升级过程的子网以及源 EC2 实例所在的位置。验证子网是否具有与 AWS 服务、Amazon S3 和 Microsoft 的出站连接（用于下载补丁）。

- TargetWindowsVersion

  类型：字符串

  描述：（必需）选择目标 Windows 版本。

  默认：2022

- RebootInstanceBeforeTakingImage

  类型：字符串

  描述：（可选）如果设置为 True，则 Automation 会重启实例，然后再创建升级前 AMI。默认情况下，Automation 在升级前不重启。

AWSEC2-ConfigureSTIG

安全技术实施指南 (STIG) 是 Defense Information Systems Agency (DISA) 创建的配置强化标准，用于保护信息系统和软件。为使您的系统符合 STIG 标准，您必须安装、配置和测试多种安全设置。

Amazon EC2 提供了 Systems Manager 运行手册 AWSEC2-ConfigureSTIG，您可以用它将 STIG 设置应用于实例。本文档可帮助您快速构建符合 STIG 标准的映像。STIG Systems Manager 文档会扫描是否存在配置错误并运行补救脚本。它还可以 InstallRoot 从国防部 (DoD) 在 Windows AMI 上安装，用于安装和更新 DoD 证书，并删除不必要的证书以维持 STIG 合规性。使用 STIG Systems Manager 文档无需额外付费。

> **Important**
>
> 除少数例外情况外，Systems Manager 文档下载的 STIG 加固组件不会安装第三方软件包。如果实例上已经安装了第三方软件包，且 Amazon EC2 支持该软件包的相关 STIG，则会应用这些 STIG。

本页列出了 Amazon EC2 支持的、STIG 加固组件适用于您的 EC2 实例的所有 STIG。

您可以选择要应用的 STIG 合规类别。

法规遵从性级别

- 高（第一类）

  最严重的风险。包括可能导致机密性、可用性或完整性丢失的任何漏洞。
- 中等（第二类）

  包括可能导致机密性、可用性或完整性丢失的任何漏洞，但可以减轻风险。
- 低（第三类）

  包括任何会降级用于防止机密性、可用性或完整性丢失的措施的漏洞。

主题

STIG 加固组件下载

Amazon 将 STIG 加固组件组合成适合每个版本的操作系统相关捆绑包。捆绑包是适用于其下载和运行的目标操作系统的归档文件。Linux 组件包存储为 TAR 文件（文件扩展名为 .tgz）。Windows 组件包存储为 ZIP 文件（文件扩展名为 .zip）。

Amazon 将组件包存储在每个 AWS 区域的 Image Builder S3 STIG 存储桶中。使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。

组件存储路径和包文件名的模式和示例如下所示：

组件存储路径

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

组件路径变量

region

AWS 区域（每个区域都有自己的组件存储桶。）

bundle file name

格式为 *<os bundle name>*_*<YYYY>*_Q*<quarter>*[_*<release>*].*<file extension>*。请注意，名称的节点之间有下划线，而不是句点。

os bundle name

操作系统捆绑包的标准名称前缀为 `LinuxAWSConfigureSTIG` 或 `AWSConfigureSTIG`。为了保持向后兼容性，Windows 版的下载不包含平台前缀。

YYYY

四位数的发布年份。

quarter

识别一年中的季度：1、2、3 或 4。

release

从 1 开始的增量数字，每个新版本都以 1 为增量。该版本不包含在一个季度的第一个版本中，仅在后续版本中添加。

file extension

压缩文件格式 `tgz` (Linux) 或 `zip` (Windows)。

捆绑包文件名示例

- `LinuxAWSConfigureSTIG_2023_Q1_2.tgz`
- `AWSConfigureSTIG_2022_Q4.zip`

Windows STIG 设置

Amazon EC2 Windows STIG AMI 和强化组件是为单独服务器设计的，并应用本地组策略。符合 STIG 标准的组件可 InstallRoot 从国防部 (DoD) 安装在 Windows AMI 上，用于下载、安装和更新 DoD 证书。它们还会删除不必要的证书，以维持 STIG 合规性。目前，Amazon EC2 支持以下版本 Windows Server 的 STIG 基准：2012 R2、2016、2019 和 2022。

本节列出了 Amazon EC2 支持的、适合您的 Windows 基础架构当前 STIG 设置，以及版本历史记录日志。

您可以应用低、中或高 STIG 设置。

Windows STIG 低（第三类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关当前 Windows STIG 的完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

- Windows Server 2022 STIG 版本 1 发行版 1

  V-254335、V-254336、V-254337、V-254338、V-254351、V-254357、V-254363 和 V-254481
- Windows Server 2019 STIG 版本 2 发行版 5

  V-205691、V-205819、V-205858、V-205859、V-205860、V-205870、V-205871 和 V-205923
- Windows Server 2016 STIG 版本 2 发行版 5

  V-224916、V-224917、V-224918、V-224919、V-224931、V-224942 和 V-225060
- Windows Server 2012 R2 MS STIG 版本 3 发行版 5

  V-225537、V-225536、V-225526、V-225525、V-225514、V-225511、V-225490、V-225489、V-225488 和 V-225250
- Microsoft .NET Framework 4.0 STIG 版本 2 发行版 2

  STIG 设置未应用于第三类漏洞的 Microsoft .NET Framework。
- Windows Firewall STIG 版本 2 发行版 1

  V-241994、V-241995、V-241996、V-241999、V-242000、V-242001、V-242006、V-242007 和 V-242008
- Internet Explorer 11 STIG 版本 2 发行版 3

  V-46477、V-46629 和 V-97527
- Microsoft Edge STIG 版本 1 发行版 6（仅限 Windows Server 2022）

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

Windows STIG 中等（第二类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关当前 Windows STIG 的完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

> **Note**
>
> Windows STIG 中等类别包括所有列出的适用于 Windows STIG Low（第三类）的 STIG 强化设置，此外还包括 Amazon EC2 支持的针对第二类漏洞的 STIG 强化设置。

- Windows Server 2022 STIG 版本 1 发行版 1

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-254247、V-254265、V-254269、V-254270、V-254271、V-254272、V-254273、V-254274、V-254276 和 V-254512
- Windows Server 2019 STIG 版本 2 发行版 5

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-205625、V-205626、V-205627、V-205629、V-205630、V-205633、V-205634、V-205635、V-205636 和 V-236001
- Windows Server 2016 STIG 版本 2 发行版 5

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-224850、V-224852、V-224853、V-224854、V-224855、V-224856、V-224857、V-224858、V-224859 和 V-236000
- Windows Server 2012 R2 MS STIG 版本 3 发行版 5

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-225574、V-225573、V-225572、V-225571、V-225570、V-225569、V-225568、V-225567、V-225566 和 V-225239
- Microsoft .NET Framework STIG 4.0 版本 2 发行版 2

包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

V-225238

- Windows Firewall STIG 版本 2 发行版 1

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-241989、V-241990、V-241991、V-241993、V-241998 和 V-242003
- Internet Explorer 11 STIG 版本 2 发行版 3

  包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

  V-46473、V-46475、V-46481、V-46483、V-46501、V-46507、V-46509、V-46511、V-46513、V-46515、和 V-75171
- Microsoft Edge STIG 版本 1 发行版 6（仅限 Windows Server 2022)

  V-235720、V-235721、V-235723、V-235724、V-235725、V-235726、V-235728、V-235729、V-235730 和 V-246736
- Defender STIG 版本 2 发行版 4（仅限 Windows Server 2022）

  V-213427、V-213429、V-213430、V-213431、V-213432、V-213433、V-213434、V-213435、V-213436 和 V-213466

Windows STIG 高（第一类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关当前 Windows STIG 的完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

> **Note**
>
> Windows STIG 高类别包括所有列出的适用于 Windows STIG 中低类别的 STIG 强化设置，此外还包括 Amazon EC2 支持的针对第一类漏洞的 STIG 强化设置。

- Windows Server 2022 STIG 版本 1 发行版 1

V-254293、V-254352、V-254353、V-254354、V-254374、V-254378、V-254381、V-254446、V-254465 和 V-254500

- Windows Server 2019 STIG 版本 2 发行版 5

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

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

- Windows Server 2016 STIG 版本 2 发行版 5

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

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

- Windows Server 2012 R2 MS STIG 版本 3 发行版 5

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

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

- Microsoft .NET Framework STIG 4.0 版本 2 发行版 2

  包括 Amazon EC2 支持的针对 Microsoft .NET Framework 第二类和第三类（中等和低）漏洞的所有 STIG 强化设置。第一类漏洞未应用额外 STIG 设置。

- Windows Firewall STIG 版本 2 发行版 1

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

  V-241992、V-241997 和 V-242002

- Internet Explorer 11 STIG 版本 2 发行版 3

  包括 Amazon EC2 支持的针对 Internet Explorer 11 第二类和第三类（中等和低）漏洞的所有 STIG 强化设置。第一类漏洞未应用额外 STIG 设置。

- Microsoft Edge STIG 版本 1 发行版 6（仅限 Windows Server 2022)

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

  V-235758 和 V-235759

- Defender STIG 版本 2 发行版 4（仅限 Windows Server 2022）

  包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

  V-213426、V-213452 和 V-213453

Windows STIG 版本历史

本节记录 STIG 季度更新的 Windows 组件版本历史记录。要查看一个季度的变化和发布的版本，请选择其标题以展开信息。

2024 年第一季度变化——2024 年 2 月 23 日（没有变化）：

在2024年第一季度版本中，Windows组件STIGS没有变化。

2023 年第四季度变化——2023 年 7 月 12 日（没有变化）：

在2023年第四季度版本中，Windows组件STIGS没有变化。

2023 年第三季度变化 — 2023 年 4 月 10 日（无变化）：

2023 年第三季度发行版的 Windows 组件 STIGS 无变化。

2023 年第二季度变化 — 2023 年 5 月 3 日（无变化）：

在 2023 年第二季度发布版中，Windows 组件 STIGS 无变化。

2023 年第一季度变化 — 2023 年 3 月 27 日（无变化）：

在 2023 年第一季度发布版中，Windows 组件 STIGS 无变化。

2022 年第四季度变化 — 2023 年 2 月 1 日：

更新了 STIG 版本并对 2022 年第四季度发行版应用了 STIG，如下所示：

STIG-Build-Windows-Low 版本 2022.4.0

- Windows Server 2022 STIG 版本 1 发行版 1
- Windows Server 2019 STIG 版本 2 发行版 5
- Windows Server 2016 STIG 版本 2 发行版 5
- Windows Server 2012 R2 MS STIG 版本 3 发行版 5
- Microsoft .NET Framework 4.0 STIG 版本 2 发行版 2
- Windows Firewall STIG 版本 2 发行版 1

- Internet Explorer 11 STIG 版本 2 发行版 3
- Microsoft Edge STIG 版本 1 发行版 6（仅限 Windows Server 2022）

STIG-Build-Windows-Medium 版本 2022.4.0

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

STIG-Build-Windows-High 版本 2022.4.0

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

2022 年第三季度变化 — 2022 年 9 月 30 日（无变化）：

在 2022 年第三季度发布版中，Windows 组件 STIGS 无变化。

2022 年第二季度变化 — 2022 年 8 月 2 日：

更新了 STIG 版本，并对 2022 年第二季度发行版应用了 STIG。

STIG-Build-Windows-Low 版本 1.5.0

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

STIG-Build-Windows-Medium 版本 1.5.0

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

STIG-Build-Windows-High 版本 1.5.0

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

2022 年第一季度变化 — 2022 年 8 月 2 日（无变化）：

2022 年第一季度发行版的 Windows 组件 STIGS 无变化。

2021 年第四季度变化 — 2021 年 12 月 20 日：

更新了 STIG 版本，并对 2021 年第四季度发行版应用了 STIG。

STIG-Build-Windows-Low 版本 1.5.0

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

STIG-Build-Windows-Medium 版本 1.5.0

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

STIG-Build-Windows-High 版本 1.5.0

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

2021 年第三季度变化 — 2021 年 9 月 30 日：

更新了 STIG 版本，并对 2021 年第三季度发行版应用了 STIG。

STIG-Build-Windows-Low 版本 1.4.0

- Windows Server 2019 STIG 版本 2 发行版 2
- Windows Server 2016 STIG 版本 2 发行版 2

- Windows Server 2012 R2 MS STIG 版本 3 发行版 2
- Microsoft .NET Framework 4.0 STIG 版本 2 发行版 1
- Windows Firewall STIG 版本 1 发行版 7
- Internet Explorer 11 STIG 版本 1 发行版 19

STIG-Build-Windows-Medium 版本 1.4.0

- Windows Server 2019 STIG 版本 2 发行版 2
- Windows Server 2016 STIG 版本 2 发行版 2
- Windows Server 2012 R2 MS STIG 版本 3 发行版 2
- Microsoft .NET Framework 4.0 STIG 版本 2 发行版 1
- Windows Firewall STIG 版本 1 发行版 7
- Internet Explorer 11 STIG 版本 1 发行版 19

STIG-Build-Windows-High 版本 1.4.0

- Windows Server 2019 STIG 版本 2 发行版 2
- Windows Server 2016 STIG 版本 2 发行版 2
- Windows Server 2012 R2 MS STIG 版本 3 发行版 2
- Microsoft .NET Framework 4.0 STIG 版本 2 发行版 1
- Windows Firewall STIG 版本 1 发行版 7
- Internet Explorer 11 STIG 版本 1 发行版 19

Linux STIG 设置

本节包含有关 Amazon EC2 支持的 Linux STIG 强化设置的信息，以及版本历史记录日志。如果 Linux 发行版没有自己的 STIG 强化设置，Amazon EC2 将使用 RHEL 设置。支持的 STIG 强化设置适用于基于 Linux 发行版的 Amazon EC2 Linux AMI 和组件，如下所示：

- Red Hat Enterprise Linux (RHEL) 7 设置
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)

- RHEL 8 STIG 设置
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)

Linux STIG 低（第三类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

RHEL 7 STIG 第 3 版 14

- RHEL 7/CentOS 7

  V-204452、V-204576 和 V-204605
- AL2

  V-204452、V-204576 和 V-204605

RHEL 8 STIG 第 1 版 13

- RHEL 8/CentOS 8/AL 2023

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

Ubuntu 18.04 STIG 版本 2 版本 13

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

Ubuntu 20.04 STIG 版本 1 版本 11

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

Linux STIG 中等（第二类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

> **Note**
>
> Linux STIG 中等类别包括所有列出的适用于 Linux STIG 低（第三类）的 STIG 强化设置，此外还包括Amazon EC2 支持的针对第二类漏洞的 STIG 强化设置。

RHEL 7 STIG 第 3 版 14

包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

- RHEL 7/CentOS 7

  V-204585、V-204490、V-204491、V-255928、V-204405、V-204406、V-204407、V-204408、V-204440 和 V-256970

- AL2:

  V-204585、V-204490、V-204491、V-255928、V-204405、V-204406、V-204407、V-204408、V-204440 和 V-256970

RHEL 8 STIG 第 1 版 13

包括 Amazon EC2 支持的针对第 III 类（低）漏洞的所有 STIG 强化设置，以及：

- RHEL 8/CentOS 8/AL 2023

  V-230257、V-230258、V-230259、V-230550、V-230248、V-230249、V-230250、V-230245、V-230246、30311、V-230312、V-230502、V-230532、V-230536、V-230536、V-230537、V-230538、V-230539、V-30377、V-244524、V-244533、V-251713、V-251717、V-251714、V-251715、V-251716、V-230332、V-30337、V-230339、V-230341、V-230343、V-230345、V-230240、V-230282、V-250315、V-250316、V-V-230447、V-230448、V-230449、V-230455、V-230456、V-230462、V-230463、V-230464、V-230466、480、V-230483、V-244542、V-230503、V-230244、V-230286、V-230287、V-230288、V-230288、V-2

V-244526 V-244528 V-237642 V-237643 V-251711 V-230238 V-230239 V-230273 V-230275 V-230478 V-230488 V-230489 V-230559

Ubuntu 18.04 STIG 版本 2 版本 13

V-219188、V-219190、V-219191、V-219198、V-219199、V-219200、V-219201、V-219202、V-219203、242，V-219243，V-219244，V-219250、V-219254、V-219257、V-219263、V-219264、V-219265、V-219 V-219267 V-219268 V-219269 V-219270 V-219271
V-219272、、、fl-219287、V-219291、V-219297、V-219297、V-219298、V-219298、V-219299、V-21929 149、V-219166、V-219176、V-219339、V-219331、V-219337 和 V-219335 V-219273 V-219274 V-219275 V-219276 V-219277 V-219279 V-219281

Ubuntu 20.04 STIG 版本 1 版本 11

V-238205、V-238207、V-238329、V-238337、V-238339、V-238340、V-238344、V-238346、V-238347、V-238285 V-238286 V-238287 V-238288 V-238289 V-238290 V-238291 V-238292
V-238293、、、、B-238301、V-238302、V-238304、V-238304、V-238309、V-238309、V-238310、V-238 和 V-238334 V-238294 V-238295 V-238297 V-238300

Linux STIG 高（第一类）

以下列表包含 Amazon EC2 支持的适合您的基础架构的 STIG 设置。如果支持的设置不适用于您的基础架构，Amazon EC2 会跳过该设置并继续。例如，某些 STIG 强化设置可能不适用于独立服务器。特定于组织的策略也有可能影响哪些设置适用，如针对管理员查看文档设置的要求。

有关完整列表，请参阅 STIG 文档库。有关如何查看完整列表的信息，请参阅 STIG 查看工具。

> **Note**
>
> Linux STIG High 类别包括所有列出的适用于 Linux STIG 中低类别的 STIG 强化设置，以及 Amazon EC2 支持的 I 类漏洞的 STIG 强化设置。

RHEL 7 STIG 第 3 版 14

包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

- RHEL 7/CentOS 7

  V-204425、V-204594、V-204455、V-204424、V-204442、V-204443、V-204447 V-204448 V-204502 V-204620 V-204621

- AL2:

  V-204425、V-204594、V-204455、V-204424、V-204442、V-204443、V-204447 V-204448 V-204502 V-204620 V-204621

RHEL 8 STIG 第 1 版 13

包括 Amazon EC2 支持的针对第一类和第三类（中等和低）漏洞的所有 STIG 强化设置，以及：

- RHEL 8/CentOS 8/AL 2023

  V-230265、V-230529、V-230531、V-230264、V-230487、V-230492、V-230533 和 V-230558

Ubuntu 18.04 STIG 版本 2 版本 13

V-219157、V-219158、V-219177、V-219212 V-219308、V-219314、V-219316 和 V-251507

Ubuntu 20.04 STIG 版本 1 版本 11

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

Linux STIG 版本历史记录

本节记录 STIG 季度更新的 Linux 组件版本历史记录。要查看一个季度的变化和发布的版本，请选择其标题以展开信息。

2024 年第一季度变化——2024 年 6 月 2 日：

更新了STIG版本并应用了2024年第一季度版本的STIGS，如下所示：

stig-build-Linux-Low 版本 2024.1.x

- RHEL 7 STIG 第 3 版 14
- RHEL 8 STIG 第 1 版 13
- Ubuntu 18.04 STIG 版本 2 版本 13
- Ubuntu 20.04 STIG 版本 1 版本 11

stig-build-Linux-medium 版本 2024.1.x

- RHEL 7 STIG 第 3 版 14

- RHEL 8 STIG 第 1 版 13
- Ubuntu 18.04 STIG 版本 2 版本 13
- Ubuntu 20.04 STIG 版本 1 版本 11

stig-build-Linux-High 版本 2024.1.x

- RHEL 7 STIG 第 3 版 14
- RHEL 8 STIG 第 1 版 13
- Ubuntu 18.04 STIG 版本 2 版本 13
- Ubuntu 20.04 STIG 版本 1 版本 11

2023 年第四季度变化——2023 年 7 月 12 日：

更新了 STIG 版本并应用了 2023 年第四季度的 STIG 版本，如下所示：

stig-build-Linux-Low 版本 2023.4.x

- RHEL 7 STIG 版本 3 版本 13
- RHEL 8 STIG 第 1 版 12
- Ubuntu 18.04 STIG 版本 2 版本 12
- Ubuntu 20.04 STIG 版本 1 版本 10

stig-build-Linux-Medium 版本 2023.4.x

- RHEL 7 STIG 版本 3 版本 13
- RHEL 8 STIG 第 1 版 12
- Ubuntu 18.04 STIG 版本 2 版本 12
- Ubuntu 20.04 STIG 版本 1 版本 10

stig-build-Linux-High 版本 2023.4.x

- RHEL 7 STIG 版本 3 版本 13
- RHEL 8 STIG 第 1 版 12
- Ubuntu 18.04 STIG 版本 2 版本 12
- Ubuntu 20.04 STIG 版本 1 版本 10

2023 年第三季度变化 — 2023 年 10 月 4 日：

更新了 STIG 版本，并对 2023 年第三季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 12
- RHEL 8 STIG 版本 1 发行版 11
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 9

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 12
- RHEL 8 STIG 版本 1 发行版 11
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 9

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 12
- RHEL 8 STIG 版本 1 发行版 11
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 9

2023 年第二季度变化 — 2023 年 5 月 3 日：

更新了 STIG 版本，并对 2023 年第二季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 11
- RHEL 8 STIG 版本 1 发行版 10
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 8

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 11
- RHEL 8 STIG 版本 1 发行版 10
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 8

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 11
- RHEL 8 STIG 版本 1 发行版 10
- Ubuntu 18.04 STIG 版本 2 发行版 11
- Ubuntu 20.04 STIG 版本 1 发行版 8

2023 年第一季度更改 — 2023 年 3 月 27 日：

更新了 STIG 版本，并对 2023 年第一季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 10
- RHEL 8 STIG 版本 1 发行版 9
- Ubuntu 18.04 STIG 版本 2 发行版 10
- Ubuntu 20.04 STIG 版本 1 发行版 7

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 10
- RHEL 8 STIG 版本 1 发行版 9
- Ubuntu 18.04 STIG 版本 2 发行版 10
- Ubuntu 20.04 STIG 版本 1 发行版 7

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 10

- RHEL 8 STIG 版本 1 发行版 9
- Ubuntu 18.04 STIG 版本 2 发行版 10
- Ubuntu 20.04 STIG 版本 1 发行版 7

2022 年第四季度变化 — 2023 年 2 月 1 日：

更新了 STIG 版本，并对 2022 年第四季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 9
- RHEL 8 STIG 版本 1 发行版 8
- Ubuntu 18.04 STIG 版本 2 发行版 9
- Ubuntu 20.04 STIG 版本 1 发行版 6

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 9
- RHEL 8 STIG 版本 1 发行版 8
- Ubuntu 18.04 STIG 版本 2 发行版 9
- Ubuntu 20.04 STIG 版本 1 发行版 6

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 9
- RHEL 8 STIG 版本 1 发行版 8
- Ubuntu 18.04 STIG 版本 2 发行版 9
- Ubuntu 20.04 STIG 版本 1 发行版 6

2022 年第三季度变化 — 2022 年 9 月 30 日（无变化）：

2022 年第三季度发行版的 Linux 组件 STIGS 无变化。

2022 年第二季度变化 — 2022 年 8 月 2 日：

引入了 Ubuntu 支持，更新了 STIG 版本，并对 2022 年第二季度发行版应用了 STIGS，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 7
- RHEL 8 STIG 版本 1 发行版 6
- Ubuntu 18.04 STIG 版本 2 发行版 6（全新）
- Ubuntu 20.04 STIG 版本 1 发行版 4（全新）

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 7
- RHEL 8 STIG 版本 1 发行版 6
- Ubuntu 18.04 STIG 版本 2 发行版 6（全新）
- Ubuntu 20.04 STIG 版本 1 发行版 4（全新）

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 7
- RHEL 8 STIG 版本 1 发行版 6
- Ubuntu 18.04 STIG 版本 2 发行版 6（全新）
- Ubuntu 20.04 STIG 版本 1 发行版 4（全新）

2022 年第一季度变化 — 2022 年 4 月 26 日：

已重构以包括对容器更好的支持。将之前的 AL2 脚本与 RHEL 7 结合起来。更新了 STIG 版本，并对 2022 年第一季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 6
- RHEL 8 STIG 版本 1 发行版 5

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 6
- RHEL 8 STIG 版本 1 发行版 5

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 6
- RHEL 8 STIG 版本 1 发行版 5

2021 年第四季度变化 — 2021 年 12 月 20 日：

更新了 STIG 版本，并对 2021 年第四季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 5
- RHEL 8 STIG 版本 1 发行版 4

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 5
- RHEL 8 STIG 版本 1 发行版 4

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 5
- RHEL 8 STIG 版本 1 发行版 4

2021 年第三季度变化 — 2021 年 9 月 30 日：

更新了 STIG 版本，并对 2021 年第三季度发行版应用了 STIG，如下所示：

Linux STIG 低（第三类）

- RHEL 7 STIG 版本 3 发行版 4
- RHEL 8 STIG 版本 1 发行版 3

Linux STIG 中等（第二类）

- RHEL 7 STIG 版本 3 发行版 4
- RHEL 8 STIG 版本 1 发行版 3

Linux STIG 高（第一类）

- RHEL 7 STIG 版本 3 发行版 4
- RHEL 8 STIG 版本 1 发行版 3

AWSEC2-PatchLoadBalancerInstance

描述

升级并修补附加到任何负载均衡器（经典、ALB 或 NLB）的 Amazon EC2 实例（Windows 或 Linux）的次要版本。在修补该实例之前，会应用默认的连接耗尽时间。您可以为 ConnectionDrainTime 参数输入以分钟 (1-59) 为单位的自定义耗尽时间，从而覆盖等待时间。

自动化工作流程如下所示：

1. 确定实例所附加的负载均衡器或目标组，并验证该实例是否运行正常。
2. 该实例已从负载均衡器或目标组移除。
3. 此自动化将等待为连接耗尽时间指定的时间段。
4. 调用 AWS-RunPatchBaseline 自动化以修补该实例。
5. 该实例已从负载均衡器或目标组重新附加。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

先决条件

- 验证实例上是否安装了 SSM Agent。有关更多信息，请参阅在适用于 Windows Server 的 EC2 实例上使用 SSM Agent。

参数

- InstanceId

类型：字符串

描述：（必需）与负载均衡器（经典、ALB 或 NLB）关联的要修补的实例的 ID。

- ConnectionDrainTime

  类型：字符串

  描述：（可选）负载均衡器的连接耗尽时间，以分钟 (1-59) 为单位。

AWSEC2-SQLServerDBRestore

描述

AWSEC2-SQLServerDBRestore 运行手册将存储在 Amazon S3 中的 Microsoft SQL Server 数据库备份还原到在 Amazon Elastic Compute Cloud (EC2) Linux 实例上运行的 SQL Server 2017。您可以提供自己的运行 SQL Server 2017 Linux 的 EC2 实例。如果未提供 EC2 实例，自动化将启动，并使用 SQL Server 2017 配置新的 Ubuntu 16.04 EC2 实例。自动化支持还原完整、差异和事务日志备份。此自动化将接收多个数据库备份并自动还原所提供的文件中每个数据库的最近的有效备份。

要自动执行备份并将本地 SQL Server 数据库还原到运行 SQL Server 2017 Linux 的 EC2 实例，您可以使用 AWS 签名的 PowerShell 脚本 MigrateSQLServerToEC2Linux。

> **Important**
>
> 自动化每次运行时，此运行手册将重置 SQL Server 服务器管理员 (SA) 用户密码。自动化完成后，在连接到 SQL Server 实例之前，您必须重新设置您自己的 SA 用户密码。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

先决条件

要运行此自动化，您必须满足以下先决条件：

- 运行此自动化的 IAM 用户或角色必须拥有内联策略，并附有 所需的 IAM 权限 中概述的权限。
- 如果您提供自己的 EC2 实例：
  - 您提供的 EC2 实例必须是运行微软 SQL Server 2017 的 Linux 实例。
  - 附加了 `AmazonSSMManagedInstanceCore` 托管策略的 AWS Identity and Access Management (IAM) 实例配置文件配置必须您提供的 EC2 实例。有关更多信息，请参阅为 Systems Manager 创建 IAM 实例配置文件。
  - EC2 实例上必须安装 SSM 代理。有关更多信息，请参阅在 Linux 的 EC2 实例上安装和配置 SSM 代理。
  - EC2 实例必须具有足够的可用磁盘空间来下载和还原 SQL Server 备份。

限制

此自动化不支持还原到在 Windows Server 的 EC2 实例上运行的 SQL Server。此自动化仅还原与 SQL Server Linux 2017 兼容的数据库备份。有关更多信息，请参阅 Linux 上的 SQL Server 2017 的版本和支持功能。

参数

此自动化具有以下参数：

- DatabaseNames

  类型：字符串

  说明：（可选）要还原的数据库的名称的逗号分隔列表。
- DataDirectorySize

  类型：字符串

  说明：（可选）所需的新 EC2 实例的 SQL Server 数据目录的卷大小 (GiB)。

  默认值：100
- KeyPair

  类型：字符串

说明：（可选）要在创建新 EC2 实例时使用的密钥对。

- IamInstanceProfileName

  类型：字符串

  说明：（可选）要附加到新 EC2 实例的 IAM 实例配置文件。IAM 实例配置文件必须附加了 `AmazonSSMManagedInstanceCore` 托管策略。

- InstanceId

  类型：字符串

  说明：（可选）Linux 上的运行 SQL Server 2017 的实例。如果未提供 InstanceId，自动化将使用提供的 InstanceType 和 SQLServerEdition 自动化启动新 EC2 实例。

- InstanceType

  类型：字符串

  说明：（可选）要启动的 EC2 实例的实例类型。

- IsS3PresignedUrl

  类型：字符串

  说明：（可选）如果 S3Input 是预签名 S3 URL，则表示 `yes`。

  默认值：No

  有效值：是 | 否

- LogDirectorySize

  类型：字符串

  说明：（可选）所需的新 EC2 实例的 SQL Server 日志目录的卷大小 (GiB)。

  默认值：100

- S3Input

  类型：字符串

  说明：（必需）包含要还原的 SQL 备份文件的 S3 存储桶名称、S3 对象键的逗号分隔列表或预签名的 S3 URL 的逗号分隔列表。

- SQLServerEdition

  类型：字符串

  说明：（可选）要安装在新创建的 EC2 实例上的 SQL Server 2017 版本。

  有效值：Standard | Enterprise | Web | Express

- SubnetId

  类型：字符串

  说明：（可选）要在其中启动新 EC2 实例的子网。子网必须具有与 AWS 服务的出站连接。如果未提供 SubnetId 值，自动化将使用默认子网。

- TempDbDirectorySize

  类型：字符串

  说明：（可选）所需的新 EC2 实例的 SQL Server TempDB 目录的卷大小 (GiB)。

  默认值：100

所需的 IAM 权限

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

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

文档步骤

要使用此自动化，请按照适用于实例类型的步骤进行操作：

对于新 EC2 实例：

1. aws:executeAwsApi - 在 Ubuntu 16.04 上检索 SQL Server 2017 的 AMI ID。
2. aws:runInstances - 启动适用于 Linux 的一个新 EC2 实例。
3. aws:waitForAwsResourceProperty - 等待新创建的 EC2 实例准备就绪。
4. aws:executeAwsApi - 如果实例未准备就绪，将重启实例。
5. aws:assertAwsResourceProperty - 验证安装了 SSM 代理。
6. aws:runCommand - 在 Powershell 中运行 SQL Server 还原脚本。

对于现有 EC2 实例：

1. aws:waitForAwsResourceProperty - 验证EC2 实例是否就绪。
2. aws:executeAwsApi - 如果实例未准备就绪，将重启实例。
3. aws:assertAwsResourceProperty - 验证安装了 SSM 代理。
4. aws:runCommand - 在 Powershell 中运行 SQL Server 还原脚本。

输出

getInstance.InstanceId

restoreToNewInstance.Output

restoreToExistingInstance.Output

AWSSupport-ActivateWindowsWithAmazonLicense

描述

AWSSupport-ActivateWindowsWithAmazonLicense 运行手册使用 Amazon 提供的许可证为 Windows Server 激活一个 Amazon Elastic Compute Cloud (Amazon EC2) 实例。Automation 验证和配置所需的密钥管理服务操作系统设置并尝试激活。这包括通往 Amazon 的密钥管理服务器的操作系统路由以及密钥管理服务操作系统设置。将 AllowOffline 参数设置为 true 将允许 Automation 成功定位到并非由 AWS Systems Manager 管理但需要停止并启动实例的实例。

> **Note**
>
> 此运行手册不能用于自带许可（BYOL）Windows Server 实例。有关使用自己的许可证的信息，请参阅 AWS 上的 Microsoft 许可。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AllowOffline

  类型：字符串

  有效值：true | false

  原定设置值：false

  说明：（可选）当在线故障排除失败或提供的实例不是托管实例时，如果允许进行离线 Windows 激活修复，请将其设置为 true。

> **Important**
>
> 离线方法要求停止提供的 EC2 实例然后启动。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- AutomationAssumeRole

  类型：字符串

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

- ForceActivation

  类型：字符串

  有效值：true | false

  原定设置值：false

  说明：（可选）若要在 Windows 已激活的情况下继续，请将其设置为 `true`。

- InstanceId

  类型：字符串

  说明：（必需）Windows Server 的托管 EC2 实例的 ID。

- SubnetId

  类型：字符串

  默认值：CreateNewVPC

  说明：（可选）仅离线 - 用于执行离线故障排除的 EC2Rescue 实例的子网 ID。使用 `SelectedInstanceSubnet` 以使用同一子网作为您的实例，或使用 `CreateNewVPC` 创建一个新 VPC。重要说明：子网必须与 InstanceId 位于同一可用区中，并且必须允许访问 SSM 终端节点。

所需的 IAM 权限

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

建议接收命令的 EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。您必须至少具有 ssm:StartAutomationExecution 和 ssm:SendCommand 才能运行此 Automation 并将命令发送到实例，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。对于离线修复息，请参阅 AWSSupport-StartEC2RescueWorkflow 所需的权限。

文档步骤

1. aws:assertAwsResourceProperty - 检查所提供的实例的平台是否为 Windows。
2. aws:assertAwsResourceProperty - 确认所提供的实例是托管实例：
   a. （在线激活修复）如果输入实例是托管实例，则运行 aws:runCommand 来运行 PowerShell 脚本，以尝试修复 Windows 激活。
   b. （离线激活修复）如果输入实例不是托管实例：
      i. aws:assertAwsResourceProperty - 验证AllowOffline旗帜是否设置为。true如果是，则启动离线修复，否则自动化将会结束。
      ii. aws:executeAutomation - 使用 Windows 激活离线修复脚本调用 AWSSupport-StartEC2RescueWorkflow。此脚本根据操作系统版本使用 EC2Config 或 EC2Launch。
      iii. aws:executeAwsApi - 阅读来自 AWSSupport-StartEC2RescueWorkflow 的结果。

输出

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

描述

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 运行手册将分析从 Amazon Elastic Compute Cloud (Amazon EC2) 实例或弹性网络接口到 AWS 服务 端点的连接。不支持 IPv6。运行手册使用您为 ServiceEndpoint 参数指定的值来分析与端点的连接。如果在您的 VPC 中找不到 AWS PrivateLink 端点，运行手册将使用当前 AWS 区域中的服务的公有 IP 地址。此自动化使用 Amazon Virtual Private Cloud 中的 Reachability Analyzer。有关更多信息，请参阅 Reachability Analyzer 中的什么是 Reachability Analyzer?。

此自动化将检查以下事项：

- 检查您的虚拟私有云（VPC）是否配置为使用 Amazon 提供的 DNS 服务器。

- 检查您指定的 VPC 中是否存在 AWS PrivateLink 终端节点。 AWS 服务 如果找到一个端点，自动化将验证 `privateDns` 属性是否已开启。
- 检查 AWS PrivateLink 终端节点是否使用默认终端节点策略。

注意事项

- 每次在来源和目标之间运行分析时，您需要支付费用。有关更多信息，请参阅 Amazon VPC 定价。
- 在自动化过程中，将创建网络洞察路径和网络洞察分析。如果自动化成功完成，运行手册将删除这些资源。如果清理步骤失败，则运行手册不会删除网络洞察路径，您需要手动将其删除。如果您不手动删除网络洞察路径，则该路径将继续计入您的 AWS 账户配额。有关 Reachability Analyzer 配额的更多信息，请参阅 Reachability Analyzer 中的 Reachability Analyzer 配额。
- 即使 Reachability Analyzer 返回 `PASS`，操作系统级配置（例如使用代理、本地 DNS 解析器或主机文件）也会影响连接。
- 查看对 Reachability Analyzer 执行的所有检查的评估。如果任何检查返回的状态为 `FAIL`，那么，即使整体可达性检查返回的状态为 `PASS`，也可能会影响连接性。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- 来源

  类型：字符串

  描述：（必需）您要分析自其的可达性的 Amazon EC2 实例或网络接口的 ID。

- ServiceEndpoint

  类型：字符串

  描述：（必需）您要分析到其的可达性的服务端点的主机名。

- RetainVpcReachabilityAnalysis

  类型：字符串

  默认：false

  描述：（可选）确定是否保留所创建的网络洞察路径和相关分析。默认情况下，用于分析可达性的资源将在成功分析后删除。如果您选择保留分析，则运行手册不会删除该分析，您可以在 Amazon VPC 控制台将其可视化。自动化输出中提供了控制台链接。

所需的 IAM 权限

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

- ec2:CreateNetworkInsightsPath
- ec2:DeleteNetworkInsightsAnalysis
- ec2:DeleteNetworkInsightsPath
- ec2:DescribeAvailabilityZones
- ec2:DescribeCustomerGateways
- ec2:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeManagedPrefixLists
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInsightsAnalyses

- ec2:DescribeNetworkInsightsPaths
- ec2:DescribeNetworkInterfaces
- ec2:DescribePrefixLists
- ec2:DescribeRegions
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTransitGatewayAttachments
- ec2:DescribeTransitGatewayPeeringAttachments
- ec2:DescribeTransitGatewayConnects
- ec2:DescribeTransitGatewayRouteTables
- ec2:DescribeTransitGateways
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetManagedPrefixListEntries
- ec2:GetTransitGatewayRouteTablePropagations
- ec2:SearchTransitGatewayRoutes
- ec2:StartNetworkInsightsAnalysis
- elasticloadbalancing:DescribeListeners
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeRules
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:DescribeTargetGroups

- elasticloadbalancing:DescribeTargetHealth
- tiros:CreateQuery
- tiros:GetQueryAnswer
- tiros:GetQueryExplanation

文档步骤

1. aws:executeScript：通过尝试解析主机名来验证服务端点。
2. aws:executeScript：收集有关 VPC 和子网的详细信息。
3. aws:executeScript：评估 VPC 的 DNS 配置。
4. aws:executeScript：评估 VPC 端点检查。
5. aws:executeScript：找到要连接到公共服务端点的互联网网关。
6. aws:executeScript：确定要用于可达性分析的目的地。
7. aws:executeScript：使用 Reachability Analyzer 分析从来源到端点的可达性，并在分析成功时清理资源。
8. aws:executeScript：生成可达性评估报告。
9. aws:executeScript：生成 JSON 形式的输出。

输出

- generateReport.EvalReport - 自动化系统所执行检查的结果，采用文本格式。
- generateJsonOutput.Output - 结果的最小版本，采用 JSON 格式。

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

描述

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 运行手册自动执行从英特尔支持的 Amazon Elastic Compute Cloud (Amazon EC2) 实例迁移到 AMD 支持的同等实例类型。此运行手册支持基于 Nitro 系统构建的通用型 (M)、可突发性通用型 (T)、计算优化型 (C) 和内存优化型 (R) 实例。此运行手册可用于不由 Systems Manager 管理的实例。

为了降低数据丢失和停机的潜在风险，运行手册会检查实例的停止行为、实例是否在 Amazon EC2 Auto Scaling 组中、实例的运行状况，以及同一个可用区中是否有 AMD 支持的同等实例类型可

用。默认情况下，如果已附加实例存储卷或实例是 AWS CloudFormation 堆栈的一部分，则此运行手册不会更改实例类型。如果要更改此行为，请为 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 参数中的任意一个指定 `yes`。

> **Important**
>
> 访问 `AWSPremiumSupport-*` 运行手册需要订阅 Enterprise 或 Business Support。有关更多信息，请参阅比较 AWS Support 计划。

注意事项

- 我们建议您在使用此运行手册之前先备份您的实例。
- 更改实例类型需要运行手册来停止您的实例。当实例停止时，存储在 RAM 或实例存储卷中的所有数据都将丢失，自动公有 IPv4 地址将释放。有关更多信息，请参阅停止和启动实例。
- 如果您没有为 `TargetInstanceType` 参数指定一个值，则运行手册会尝试根据同一实例族中的虚拟 CPU 和内存来识别等效的 AMD 实例。如果运行手册无法识别等效的 AMD 实例类型，运行手册将结束。
- 使用 `DryRun` 选项，您可以捕获等效的 AMD 实例类型并验证需求，而无需实际更改实例类型。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

说明：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。

- 确认

  类型：字符串

  描述：（必填）输入 `yes` 以确认您的目标实例将停止（如果它正在运行）。

- InstanceId

  类型：字符串

  描述：（必填）要更改其类型的 Amazon EC2 实例的 ID。

- TargetInstanceType

  类型：字符串

  默认：自动

  描述：（可选）要将您的实例更改为的 AMD 实例类型。默认的 `automatic` 值使用在虚拟 CPU 和内存方面等效的实例类型。例如，m5.large 将更改为 m5a.large。

- AllowInstanceStoreInstances

  类型：字符串

  有效值：否 | 是

  默认值：no

  描述：（可选）如果您指定 `yes`，运行手册将在已附加实例存储卷的实例上运行。

- AllowCloudFormationInstances

  类型：字符串

  有效值：否 | 是

  默认值：no

  描述：（可选）如果设置为 `yes`，运行手册将在属于 AWS CloudFormation 堆栈的实例上运行。

- AllowCrossGeneration

类型：字符串

有效值：否 | 是

默认值：no

描述：（可选）如果设置为 yes，运行手册将尝试在同一实例族中查找最新的等效 AMD 实例类型。

- DryRun

  类型：字符串

  有效值：否 | 是

  默认值：no

  描述：（可选）如果设置为 yes，运行手册将返回等效的 AMD 实例类型并验证迁移要求，而无需更改实例类型。

- SleepWait

  类型：字符串

  默认：PT3S

  描述：（可选）运行手册在开始新的自动化之前应等待的时间。您为此参数提供的值必须符合 ISO 8601 标准。要了解有关创建 ISO 8601 字符串的更多信息，请参阅为 Systems Manager 创建格式化的日期和时间字符串。

所需的 IAM 权限

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

- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ec2:GetInstanceTypesFromInstanceRequirements
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus

- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeTags
- ec2:ModifyInstanceAttribute
- ec2:StartInstances
- ec2:StopInstances

文档步骤

1. aws:assertAwsResourceProperty：确认目标 Amazon EC2 实例的状态为 running、pending、stopped 或 stopping。否则，自动化将结束。
2. aws:executeAwsApi：从 Amazon EC2 目标实例收集属性。
3. aws:branch：根据 Amazon EC2 实例的状态对自动化进行分支。
   a. 如果为 stopped 或 stopping，则自动化会运行 aws:waitForAwsResourceProperty，直到 Amazon EC2 实例完全停止。
   b. 如果为 running 或 pending，则自动化会运行 aws:waitForAwsResourceProperty，直到 Amazon EC2 实例通过状态检查。
4. aws:assertAwsResourceProperty：通过检查 aws:autoscaling:groupName 标签是否已应用，确认 Amazon EC2 实例不是 Auto Scaling 组的一部分。
5. aws:executeAwsApi：收集当前实例类型属性以查找等效的 AMD 实例类型。
6. aws:assertAwsResourceProperty：确认 AWS Marketplace 产品代码未与 Amazon EC2 实例关联。某些产品类型并非在所有实例类型上都可用。
7. aws:branch：根据您是否希望自动化检查 Amazon EC2 实例是否是 AWS CloudFormation 堆栈的一部分，对自动化进行分支
   a. 如果 aws:cloudformation:stack-name 标签应用于实例，则自动化会运行 aws:assertAwsResourceProperty 以确认该实例不是 AWS CloudFormation 堆栈的一部分。
8. aws:branch：根据实例根卷类型是否为 Amazon Elastic Block Store (Amazon EBS) 的实例对自动化进行分支。
9. aws:assertAwsResourceProperty：确认实例关闭行为是 stop 且不是 terminate。
10. aws:executeScript：确认此运行手册中只有一个针对当前实例的自动化。如果针对同一实例的另一个自动化已经在进行，则它会返回错误并结束。
11. aws:executeAwsApi：返回具有相同内存和 vCPU 量的 AMD 实例类型的列表。

12. aws:executeScript：检查当前实例类型是否受支持并返回其等效的 AMD 实例类型。如果没有等效类型，自动化将结束。
13. aws:executeScript：确认 AMD 实例类型在同一可用区中可用，并验证所提供的 IAM 权限。
14. aws:branch：根据 DryRun 参数值是否为 yes 对自动化进行分支。
15. aws:branch：检查原始和目标实例类型是否相同。如果它们相同，自动化将结束。
16. aws:executeAwsApi：获取当前实例状态。
17. aws:changeInstanceState：停止 Amazon EC2 实例。
18. aws:changeInstanceState: 如果实例卡在了停止状态，则强制其停止。
19. aws:executeAwsApi：将实例类型更改为目标 AMD 实例类型。
20. aws:sleep：更改实例类型后等待 3 秒钟以确保最终一致性。
21. aws:branch：根据前实例的状态对自动化进行分支。如果是 running，则实例已启动。
    a. aws:changeInstanceState：如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
    b. aws:waitForAwsResourceProperty：等待 Amazon EC2 实例通过状态检查。如果实例未通过状态检查，实例将变回其原始的实例类型。
       i. aws:changeInstanceState：停止 Amazon EC2 实例，然后将其更改为原始实例类型。
       ii. aws:changeInstanceState：强制 Amazon EC2 实例停止，然后再将其更改为原始实例类型，以防它卡在停止状态。
       iii. aws:executeAwsApi：将 Amazon EC2 实例更改为其原始类型。
       iv. aws:sleep：更改实例类型后等待 3 秒钟以确保最终一致性。
       v. aws:changeInstanceState：如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
       vi. aws:waitForAwsResourceProperty：等待 Amazon EC2 实例通过状态检查。
22. aws:sleep: 等待，然后结束运行手册。

AWSSupport-CheckXenToNitroMigrationRequirements

描述

AWSSupport-CheckXenToNitroMigrationRequirements 运行手册将验证 Amazon Elastic Compute Cloud (Amazon EC2) 实例是否满足成功将实例类型从 Xen 类型实例变为基于 Nitro 的实例类型的先决条件。此自动化将检查以下事项：

- 根设备是一个 Amazon Elastic Block Store (Amazon EBS) 卷。
- `enaSupport` 属性已启用。
- ENA 模块安装在实例上。
- NVMe 模块安装在实例上。如果是，则模块安装完毕，脚本将验证该模块是否加载到 `initramfs` 镜像中。
- 分析 `/etc/fstab` 并使用设备名称查找正在挂载的块设备。
- 确定操作系统 (OS) 是否默认使用可预测的网络接口名称。

此运行手册支持以下操作系统：

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian 服务器
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

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

- InstanceId

  类型：字符串

  原定设置值：false

  描述：（必需）在迁移到基于 Nitro 的实例类型之前，您要检查其先决条件的 Amazon EC2 实例的 ID。

所需的 IAM 权限

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

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm: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

文档步骤

- aws:executeAwsApi - 收集有关该实例的详细信息。
- aws:executeAwsApi - 收集有关该实例虚拟机管理程序的信息。
- aws:branch - 根据目标实例是否已经在运行基于 Nitro 的实例类型进行分支。
- aws:branch - 检查基于 Nitro 的实例是否支持该实例的操作系统。
- aws:assertAwsResourceProperty - 验证您指定的实例是否由 Systems Manager 管理以及其状态是否为 Online。
- aws:branch - 根据实例的根设备是否是 Amazon EBS 卷进行分支。
- aws:branch - 根据是否为实例启用了 ENA 属性进行分支。
- aws:runCommand - 检查实例上是否有 ENA 驱动程序。
- aws:runCommand - 检查实例上是否有 NVMe 驱动程序。
- aws:runCommand - 检查 fstab 文件是否存在无法识别的格式。
- aws:runCommand - 检查实例上是否有可预测的接口名称配置。
- aws:executeScript - 根据上述步骤生成输出。

输出

finalOutput.output - 自动化执行的检查的结果。

AWSSupport-ConfigureEC2Metadata

描述

此运行手册可帮助您为 Amazon Elastic Compute Cloud (Amazon EC2) 实例配置实例元数据服务（IMDS）选项。使用此运行手册，您可以执行以下配置：

- 强制将 IMDSv2 用于实例元数据。
- 配置 HttpPutResponseHopLimit 值。
- 允许或拒绝访问实例元数据。

有关实例元数据的更多信息，请参阅 Amazon EC2 用户指南中的配置实例元数据服务。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- EnforceIMDSv2

  类型：字符串

  有效值：必需 | 可选

  默认：可选

  描述：（可选）强制执行 IMDSv2。如果您选择 `required`，则 Amazon EC2 实例将仅使用 IMDSv2。如果您选择 `optional`，则可以在 IMDSv1 和 IMDSv2 之间选择以获得元数据访问权限。

  > **Important**
  >
  > 如果您强制执行 IMDSv2，则使用 IMDSv1 的应用程序可能无法正常运行。在强制执行 IMDSv2 之前，请确保使用 IMDS 的应用程序已升级到支持 IMDSv2 的版本。有关实例元数据服务版本 2 (imdsv2) 的信息，请参阅 Amazon EC 2 用户指南中的配置实例元数据服务。

- HttpPutResponseHop极限

  类型：整数

  有效值：0-64

默认：0

描述：（可选）实例元数据请求的所需 HTTP PUT 响应跃点限制值 (1-64)。此值控制 PUT 响应可以遍历的跳点数。为防止响应在实例之外传播，请为参数值指定 1。

- InstanceId

  类型：字符串

  描述：（必需）您要配置其元数据设置 Amazon EC2 实例的 ID。

- MetadataAccess

  类型：字符串

  有效值：启用 | 禁用

  默认值：启用

  描述：（可选）允许或拒绝访问 Amazon EC2 实例中的实例元数据。如果您指定 `disabled`，则所有其他参数将被忽略，且实例的元数据访问将被拒绝。

所需的 IAM 权限

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

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

文档步骤

1. branch OnMetadataAccess -基于`MetadataAccess`参数值的分支自动化。
2. disableMetadataAccess -调用 ModifyInstanceMetadataOptions API 操作以禁用元数据端点访问权限。
3. branch OnHttpPutResponseHopLimit -基于`HttpPutResponseHopLimit`参数值的分支自动化。
4. 维护 HopLimitAndConfigureImdsVersion -如果`HttpPutResponseHopLimit`为 0，则保持当前跳数限制并更改其他元数据选项。

5. 等待 BeforeAsserting imdsv2State-等待 30 秒后再断言 imdsv2 状态。
6. set HopLimitAndConfigureImdsVersion -如果大HttpPutResponseHopLimit于 0，则使用给定的输入参数配置元数据选项。
7. 等待 BeforeAssertingHopLimit -在断言元数据选项之前等待 30 秒。
8. assertHopLimit -断言该HttpPutResponseHopLimit属性已设置为您指定的值。
9. branch VerificationOn imdsv2Option-基于参数值进行分支验证。EnforceIMDSv2
10. assertimdsV IsOptional 2-将值设置为HttpTokens。optional
11. assertimdsV IsEnforced 2-将值设置为HttpTokens。required
12. 等待 BeforeAssertingMetadataState -在断言元数据状态已禁用之前等待 30 秒。
13. 断言 MetadataIsDisabled -断言元数据是。disabled
14. describeMetadataOptions -在应用您指定的更改后获取元数据选项。

输出

描述 MetadataOptions .State

描述MetadataOptions。 MetadataAccess

描述 MetadataOptions .imdsv2

描述MetadataOptions。 HttpPutResponseHop极限

AWSSupport-CopyEC2Instance

描述

AWSSupport-CopyEC2Instance 运行手册为知识中心文章如何将我的 EC2 实例移动到另一个子网、可用区或 VPC？中概述的过程提供了自动化的解决方案 自动化的分支取决于您为 Region 和 SubnetId 参数指定的值。

如果您为 SubnetId 参数指定一个值但未为 Region 参数指定值，自动化将创建目标实例的 Amazon Machine Image (AMI)，并从您指定的子网 AMI 启动一个新实例。

如果您为 SubnetId 参数和 Region 参数指定一个值，自动化将创建目标实例的 AMI，将 AMI 复制到您指定的 AWS 区域，并从您指定的子网中的 AMI 启动一个新实例。

如果您为 Region 参数指定一个值但未为 SubnetId 参数指定值，自动化将创建目标实例的 AMI，将 AMI 复制到您指定的区域，并从您指定的区域中的虚拟私有云（VPC）的默认子网中的 AMI 启动一个新实例。

如果没有为 Region 或 SubnetId 参数指定任何值，自动化将创建目标实例的 AMI，并从 VPC 的默认子网中的 AMI启动一个新实例。

要将 AMI 复制到其他区域，您必须为 AutomationAssumeRole 参数提供一个值。如果在 waitForAvailableDestinationAmi 步骤期间自动化超时，则 AMI 可能仍在复制。在这种情况下，您可以等待复制完成，然后手动启动该实例。

在运行此自动化之前，请注意以下事项：

- AMI 是基于Amazon Elastic Block Store (Amazon EBS) 快照。对于之前没有快照的大型文件系统，创建 AMI 可能需要几个小时。要缩短 AMI 创建时间，请在创建 AMI 之前先创建一个 Amazon EBS 快照。
- 创建 AMI 不会为实例上的实例存储卷创建快照。有关将实例存储卷备份到 Amazon EBS 的信息，请参阅如何将 Amazon EC2 实例上的实例存储卷备份到 Amazon EBS？
- 新的 Amazon EC2 实例具有不同的私有 IPv4 或公有 IPv6 IP 地址。您必须使用分配给新实例的新 IP 地址，更新对旧 IP 地址的所有引用（例如，在 DNS 条目中）。如果您在源实例上使用弹性 IP 地址，请务必将其附加到新实例。
- 当副本启动并尝试联系域时，可能会出现域安全标识符 (SID) 冲突问题。在捕获 AMI 之前，请使用 Sysprep 或从域中移除已加入域的实例，以防止出现冲突问题。有关更多信息，请参阅如何使用 Sysprep 创建和安装自定义的可重复使用的 Windows AMI？

运行此自动化（控制台）

> **Important**
>
> 我们不建议使用此运行手册来复制 Microsoft Active Directory Domain Controller 实例。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  描述：（必需）要复制的实例的 ID。

- KeyPair

  类型：字符串

  描述：（可选）要与新复制的实例关联的密钥对。如果您要将实例复制到其他区域，请确保指定的区域存在密钥。

- 区域

  类型：字符串

  描述：（可选）要将实例复制到的区域。如果您为此参数指定一个值，但未为 `SubnetId` 和 `SecurityGroupIds` 参数指定值，自动化将尝试使用默认安全组在默认的 VPC 中启动实例。如果在目的地区域启用了 EC2-Classic，启动将失败。

- SubnetId

  类型：字符串

  描述：（可选）要将实例复制到的子网的 ID。如果在目的地区域启用了 EC2-Classic，则必须为此参数提供一个值。

- InstanceType

  类型：字符串

  描述：（可选）复制的实例应当启动的目标实例类型。如果您没有为此参数指定一个值，则使用源实例类型。如果要将实例复制到的区域不支持源实例类型，自动化将失败。

- SecurityGroupIds

类型：字符串

描述：（可选）要与已复制实例关联的安全组 ID 的逗号分隔列表。如果您未为此参数指定一个值，且该实例未被复制到其他区域，则使用与源实例关联的安全组。如果您要将实例复制到其他区域，则使用目的地区域中默认 VPC 的默认安全组。

- KeepImageSourceRegion

  类型：布尔值

  有效值：true | false

  默认值：True

  描述：（可选）如果您为此参数指定 `true`，则自动化不会删除源实例的 AMI。如果您为此参数指定 `false`，则自动化会取消注册 AMI 并删除关联的快照。

- KeepImageDestinationRegion

  类型：布尔值

  有效值：true | false

  默认值：True

  描述：（可选）如果您为此参数指定 `true`，则自动化不会删除将复制到的您指定目标区域的 AMI。如果您为此参数指定 `false`，则自动化会取消注册 AMI 并删除关联的快照。

- NoRebootInstanceBeforeTakingImage

  类型：布尔值

  有效值：true | false

  原定设置值：false

  描述：（可选）如果您为此参数指定 `true`，则在创建 AMI 之前源实例不会重新启动。如果使用此选项，则无法保证所创建映像上的文件系统的完整性。

所需的 IAM 权限

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

- ec2:CreateImage
- ec2:DeleteSnapshot
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeImages
- ec2:RunInstances

如果您要将实例复制到其他区域，则还需要具有以下权限。

- ec2:CopyImage

文档步骤

- describeOriginalInstanceDetails - 从要复制的实例收集详细信息。
- assertrootVolumeiSebs - 检查根卷设备类型是否为，如果不是ebs，则结束自动化。
- evalInputParameters - 评估为输入参数提供的值。
- createLocalAmi - 创建源实例的 AMI。
- tagLocalAmi - 标记在上一步创建的 AMI。
- branchassertRegionisSame - 根据将实例复制到相同区域内还是不同区域中进行分支。
- branchAssertSameRegionWithKeyPair - 根据是否为在同一区域内要复制的实例的 KeyPair 参数提供了值进行分支。
- sameRegionLaunchInstanceWithKeyPair - 使用您指定的密钥对从位于您指定的同一子网或子网中的源实例的 AMI 启动一个 Amazon EC2 实例。
- sameRegionLaunchInstanceWithoutKeyPair - 无需密钥对，从位于同一子网或您指定的子网中的源实例的 AMI 启动一个 Amazon EC2 实例。
- copyAmiToRegion - 将 AMI 复制到目标区域。
- waitForAvailableDestinationAmi - 等待复制的 AMI 状态变为 available。
- destinationRegionLaunchInstance - 使用复制的 AMI 实例启动一个 Amazon EC2 实例。
- branchassertDestinationAmitoDelete - 根据你为参数提供的值进行分支。KeepImageDestinationRegion
- deregisterDestinationAmiAndDeleteSnapshots - 取消注册复制的 AMI 并删除关联的快照。
- branchassertSourceAmitoDelete - 根据你为参数提供的值进行分支。KeepImageSourceRegion

- deregisterSourceAmiAndDeleteSnapshots - 取消注册 AMI 从源实例创建的快照并删除关联的快照。
- sleep - 使自动化休眠 2 秒钟。这是最终步骤。

输出

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstance.DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

描述

该运行手册AWSSupport-EnableWindowsEC2SerialConsole可帮助您在亚马逊 EC2 Windows 实例上启用亚马逊 EC2 串行控制台、特殊管理控制台 (SAC) 和启动菜单。借助 Amazon Elastic Compute Cloud (Amazon EC2) 串行控制台功能，您可以访问亚马逊 EC2 实例的串行端口，以解决启动、网络配置和其他问题。运行手册自动执行在处于运行状态并由管理的实例以及处于停止状态或未由AWS Systems Manager管理的实例上启用该功能所需的步骤。 AWS Systems Manager

如何工作？

AWSSupport-EnableWindowsEC2SerialConsole自动化运行手册有助于在运行微软 Windows Server 的亚马逊 EC2 实例上启用 SAC 和启动菜单。对于处于运行状态且由管理的实例 AWS Systems Manager，运行手册会运行 R AWS Systems Manager un Command PowerShell 脚本来启用 SAC 和启动菜单。对于处于停止状态或未由管理的实例 AWS Systems Manager，运行手册使用 AWSSupport-Startec2 创建一个临时 Amazon EC2 RescueWorkflow 实例，以离线执行所需的更改。

有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 串行控制台。

Important

- 如果您在实例上启用 SAC，则依赖密码检索的 Amazon EC2 服务将无法在 Amazon EC2 控制台上运行。有关更多信息，请参阅使用 SAC 排查 Windows 实例的问题。
- 要配置对串行控制台的访问权限，您必须在账户级别授予串行控制台访问权限，然后配置 AWS Identity and Access Management (IAM) 策略以向您的用户授予访问权限。您还必须在每个实例上配置基于密码的用户，以使您的用户能够使用串行控制台进行故障排查。有关更多信息，请参阅配置对 Amazon EC2 串行控制台的访问权限。

- 要查看您的账户是否启用了串行控制台，请参阅查看串行控制台的账户访问状态。
- 只有在 Nitro 系统上构建的虚拟化实例才支持串行控制台访问。

有关更多信息，请参阅 Amazon EC2 串行控制台先决条件。

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

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

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

说明

按照这些步骤对自动化进行配置：

1. 导航到 AWS Systems Manager 控制台AWSSupport-EnableWindowsEC2SerialConsole中的。
2. 选择 Execute automation（执行自动化）。
3. 对于输入参数，请输入以下内容：
   - InstanceId:（必填）

     您要启用亚马逊 EC2 串行控制台、(SAC) 和启动菜单的 Amazon EC2 实例的 ID。
   - AutomationAssumeRole:（可选）

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

     运行手册预配置的 Amazon EC2 实例的类型，用于为离线实例配置 Amazon EC2 串行控制台。
   - HelperInstanceProfileName:（视情况而定）

     帮助程序实例的现有 IAM 实例配置文件的名称。如果您在处于停止状态或不由管理的实例上启用 SAC 和启动菜单 AWS Systems Manager，则这是必需的。如果未指定 IAM 实例配置文件，则自动化会代表您创建一个。
   - SubnetId:（视情况而定）

帮助程序实例的子网 ID。默认情况下，它使用的子网与所提供的实例所在的子网相同。

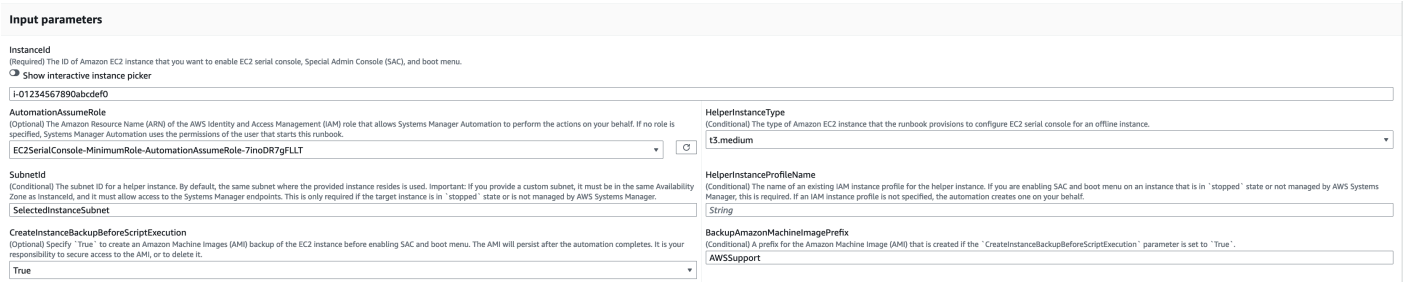
> **Important**
>
> 如果您提供自定义子网，则该子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 Systems Manager 端点。只有当目标实例处于停止状态或不是由管理时，才需要这样做 AWS Systems Manager。

- CreateInstanceBackupBeforeScriptExecution:（可选）

  指定 True 可在启用 SAC 和启动菜单之前创建 Amazon EC2 实例的亚马逊系统映像 (AMI) 备份。Automation 完成后，AMI 仍将存在。您有责任保护对 AMI 的访问权限或将其删除。

- BackupAmazonMachineImagePrefix:（视情况而定）

  如果将`CreateInstanceBackupBeforeScriptExecution`参数设置为 ，则创建的 Amazon 系统映像 (AMI) 的前缀`True`。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

   - CheckIfEc2SerialConsoleAccessEnabled:

     检查是否在账户级别启用了 Amazon EC2 串行控制台访问权限。注意：默认情况下，无法访问串行控制台。有关更多信息，请参阅配置对 Amazon EC2 串行控制台的访问权限。

   - CheckIfEc2InstanceIsWindows:

     断言目标实例平台是否是 Windows。

   - GetInstanceType:

     检索目标实例的实例类型。

   - CheckIfInstanceTypeIsNitro:

检查实例类型虚拟机管理程序是否基于 Nitro。仅在 Nitro 系统上构建的虚拟化实例支持串行控制台访问。

- CheckIfInstanceIsInAutoScaling群组:

  通过调用 `DescribeAutoScalingInstances` API 来检查 Amazon EC2 实例是否属于 Amazon EC2 Auto Scaling 组。如果该实例是 Amazon EC2 Auto Scaling 组的一部分，则它可以确保.NET 实例的移植助手处于待机生命周期状态。

- WaitForEc2InstanceStateStablized:

  等待实例进入运行或停止状态。

- GetEc2InstanceState:

  获取实例的当前状态。

- BranchOnEc2InstanceState:

  基于上一步中检索到的实例状态进行分支。如果该实例状态正在运行，则进入`CheckIfEc2InstanceIsManagedBySSM`步骤，如果没有，则进入该`CheckIfHelperInstanceProfileIsProvided`步骤。

- CheckIfEc2 InstanceIsManagedBy SSM：

  检查实例是否由管理 AWS Systems Manager。如果是托管的，则运行手册使用 PowerShell 运行命令启用 SAC 和启动菜单。

- BranchOnPreEC2RescueBackup：

  基于`CreateInstanceBackupBeforeScriptExecution`输入参数进行分支。

- CreateAmazonMachineImageBackup:

  创建实例的 AMI 备份。

- 启用 S AndBootMenu AC：

  通过 PowerShell 运行命令脚本启用 SAC 和启动菜单。

- RebootInstance:

  重新启动 Amazon EC2 实例以应用配置。如果实例处于联机状态并且由管理，则这是最后一步 AWS Systems Manager。

- CheckIfHelperInstanceProfileIsProvided:

在使用临时 Amazon EC2 实例离线启用 SAC 和启动菜单之前，请检查`HelperInstanceProfileName`指定的是否存在。

- RunAutomationToInjectOfflineScriptFor启用 SACAndBootMenu：

  当实例处于停止状态或未由 AWS Systems Manager管理时，运行启用 SAC 和启动菜单。`AWSSupport-StartEC2RescueWorkflow`

- GetExecutionDetails:

  检索备份和脱机脚本输出的图像 ID。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

   - 启用 SAC。输出AndBootMenu：

     `EnableSACAndBootMenu`步骤中执行命令的输出。

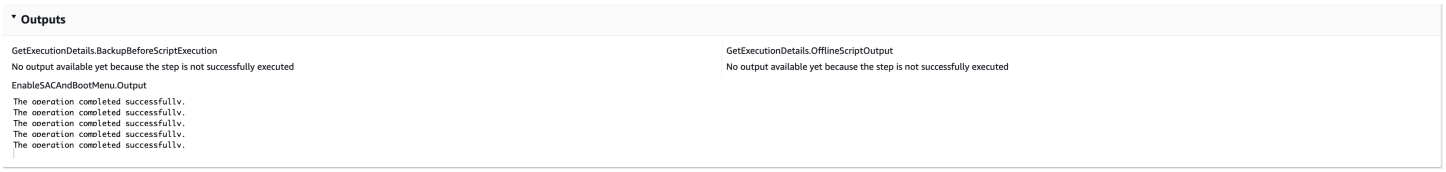
   - GetExecutionDetails.OfflineScriptOutput:

     `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`步骤中执行的离线脚本的输出。

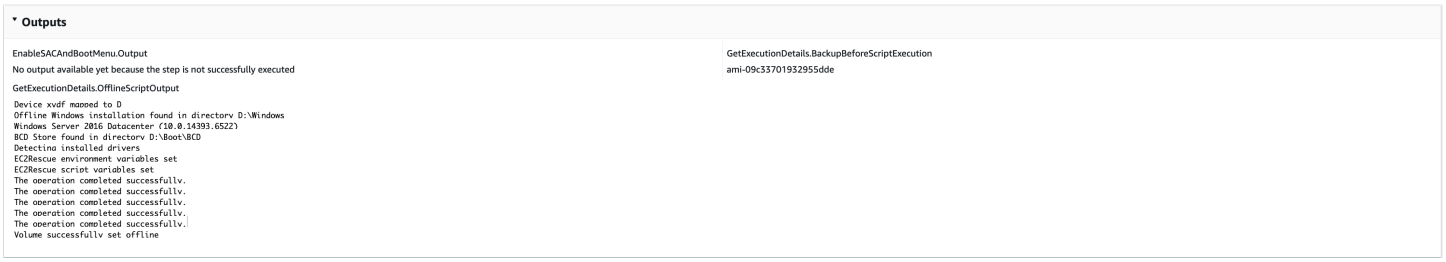
   - GetExecutionDetails.BackupBeforeScriptExecution:

     如果`CreateInstanceBackupBeforeScriptExecution`输入参数为 True，则拍摄的 AMI 备份的映像 ID。

在运行和管理的实例上执行的输出 AWS Systems Manager



在已停止或未由管理的实例上执行的输出 AWS Systems Manager



参考

Systems Manager Automation

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

AWSSupport-ExecuteEC2Rescue

描述

此运行手册使用 EC2Rescue 工具进行故障排除，并尽可能通过指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例为 Linux 或 Windows Server 修复常见的连接问题。不支持带有加密根卷的实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
- EC2RescueInstanceType

  类型：字符串

有效值：t2.small | t2.medium | t2.large

默认值：t2.small

描述：（必需）适用于 EC2Rescue 实例的 EC2 实例类型。推荐大小：`t2.small`

- LogDestination

  类型：字符串

  描述：（可选）您账户中用于上传故障排除日志的 Amazon S3 存储桶的名称。请确保存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

  类型：字符串

  默认值：CreateNewVPC

  描述：（可选）适用于 EC2Rescue 实例的子网 ID。默认情况下，AWS Systems Manager Automation 会创建一个新 VPC。或者，您也可以使用 `SelectedInstanceSubnet` 来使用与您的实例相同的子网，或指定一个自定义的子网 ID。

  > **Important**
  >
  > 子网必须与 `UnreachableInstanceId` 位于同一可用区中，并且必须允许访问 SSM 端点。

- UnreachableInstanceId

  类型：字符串

  描述：（必需）您的无法访问的 EC2 实例的 ID。

  > **Important**
  >
  > Systems Manager Automation 会停止此实例，并在尝试任何操作前创建一个 AMI。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP 地址，则公有 IP 地址将发生更改。

所需的 IAM 权限

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

您必须至少拥有 ssm:StartAutomationExecution 和 ssm:GetAutomationExecution 才能读取自动化输出。有关所需权限的更多信息，请参阅AWSSupport-StartEC2RescueWorkflow。

文档步骤

1. aws:assertAwsResourceProperty - 断言提供的实例是否为 Windows Server：
   a. (EC2Rescue 对于 Windows Server) 如果提供的实例是 Windows Server 实例：
      i. aws:executeAutomation - 使用 Windows Server 离线脚本的 EC2Rescue 调用 AWSSupport-StartEC2RescueWorkflow。
      ii. aws:executeAwsApi - 从嵌套的 Automation 检索备份 AMI ID。
      iii. aws:executeAwsApi - 从嵌套的 Automation 检索 EC2Rescue 摘要。
   b. (EC2Rescue 对于 Linux) 如果提供的实例是 Linux 实例：
      i. aws:executeAutomation - 使用 Linux 离线脚本的 EC2Rescue 调用 AWSSupport-StartEC2RescueWorkflow
      ii. aws:executeAwsApi - 从嵌套的 Automation 检索备份 AMI ID。
      iii. aws:executeAwsApi - 从嵌套的 Automation 检索 EC2Rescue 摘要。

输出

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

AWSSupport-ListEC2Resources

描述

AWSSupport-ListEC2Resources运行手册返回有关Amazon EC2 实例和相关资源的信息，Amazon Elastic Block Store (Amazon EBS) 卷、弹性 IP 地址和Amazon EC2 Auto Scaling 您指定的 AWS 区域 组。默认情况下，信息从所有区域收集，并在在自动化的输出中显示。或者，您可以指定要将信息以逗号分隔值 (.csv) 文件形式上传到的 Amazon Simple Storage Service (Amazon S3) 存储桶。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（可选）要将所收集的信息上传到的 S3 存储桶的名称。
- DisplayResourceDeletionDocumentation

  类型：字符串

  默认值：True

  描述：（可选）如果设置为 `true`，此自动化会在输出中创建指向与删除资源相关的文档的链接。
- RegionsToQuery

  类型：字符串

  默认值：全部

  描述：（可选）您要从中收集 Amazon EC2 相关信息的区域。

所需的 IAM 权限

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

- autoscaling:DescribeAutoScalingGroups
- ec2:DescribeAddresses
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeVolumes
- ec2:DescribeSnapshots
- elasticloadbalancing:DescribeLoadBalancers

此外，要成功将收集到的信息上传到您指定的 S3 存储桶，AutomationAssumeRole 需要执行以下操作：

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

文档步骤

- aws:executeAwsApi - 收集为该账户启用的区域。
- aws:executeScript - 确认为账户启用的区域支持RegionsToQuery参数中指定的区域。
- aws:branch - 如果未对账户启用任何区域，自动化将结束。
- aws:executeScript - 列出您指定的账户和区域的所有 EC2 实例。
- aws:executeScript - 列出您指定的账户和区域的所有亚马逊机器映像（AMI）。
- aws:executeScript - 列出您指定的账户和区域的所有 EBS 卷。
- aws:executeScript - 列出您指定的账户和区域的所有弹性 IP 地址。
- aws:executeScript - 列出您指定的账户和区域的所有弹性网络接口。
- aws:executeScript - 列出您指定的账户和区域的所有自动扩缩组。
- aws:executeScript - 列出您指定的账户和区域的所有负载均衡器。

- aws:executeScript - 在您为 Bucket 参数提供值时将收集到的信息上传到指定的 S3 存储桶。

AWSSupport-ManageRDPSettings

描述

AWSSupport-ManageRDPSettings 运行手册能够让用户管理常见的远程桌面协议 (RDP) 设置，例如 RDP 端口和网络层身份验证 (NLA)。默认情况下，此运行手册读取和输出这些设置的值。

> **Important**
>
> 在运行此运行手册前，应仔细检查对 RDP 设置的更改。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

说明：（必需）要管理其 RDP 设置的托管实例的 ID。

- NLASettingAction

  类型：字符串

  有效值：Check | 启用 | 禁用

  默认值：Check

  说明：（必需）要对 NLA 设置执行的操作：Check、Enable、Disable。

- RDPPort

  类型：字符串

  默认值：3389

  说明：（可选）指定新的 RDP 端口。仅在操作设置为 Modify 时使用。端口号必须介于 1025-65535 之间。注意：更改端口后，将重启 RDP 服务。

- RDPPortAction

  类型：字符串

  有效值：Check | 修改

  默认值：Check

  说明：（必需）要应用于 RDP 端口的操作。

- RemoteConnections

  类型：字符串

  有效值：Check | 启用 | 禁用

  默认值：Check

  说明：（必需）要对 fDenyTSConnections 设置执行的操作。

所需的 IAM 权限

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

接收命令的 EC2 实例必须具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。用户必须至少具有 ssm:SendCommand 才能将命令发送到实例，并且需要具有 ssm:GetCommandInvocation 才能读取命令输出。

文档步骤

aws:runCommand - 运行 PowerShell 脚本来更改或检查目标实例上的 RDP 设置。

输出

manageRDPSettings.Output

AWSSupport-ManageWindowsService

描述

AWSSupport-ManageWindowsService 运行手册允许您在目标实例上停止、启动、重启、暂停或禁用任何 Windows 服务。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

  类型：字符串

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

类型：字符串

描述：（必需）要管理其服务的托管实例的 ID。

- ServiceAction

  类型：字符串

  有效值：Check | 重启 | 强制重启 | 启动 | 停止 | 前置停止 | 暂停

  默认值：Check

  描述：（必填）要应用于 Windows 服务的操作。注意：`Force-Restart` 和 `Force-Stop` 可用于重启和停止具有从属服务的服务。

- StartupType

  类型：字符串

  有效值：Check | 自动 | 要求 | 禁用 | 延迟自动启动

  默认值：Check

  描述：（必填）要应用于 Windows 服务的启动类型。

- WindowsServiceName

  类型：字符串

  描述：（必需）有效的 Windows 服务名称。

所需的 IAM 权限

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

建议接收命令的 EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。用户必须至少具有 ssm:StartAutomationExecution 和 ssm:SendCommand 才能运行此 Automation 并将命令发送到实例，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。

文档步骤

`aws:runCommand` - 运行 PowerShell 脚本来将所需配置应用到目标实例上的 Windows 服务。

输出

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

描述

AWSSupport-MigrateEC2ClassicToVPC 运行手册将 Amazon Elastic Compute Cloud (Amazon EC2) 实例从 EC2-Classic 迁移到虚拟私有云（VPC）。此运行手册支持使用 Amazon Elastic Block Store (Amazon EBS) 根卷迁移硬件虚拟机 (HVM) 虚拟化类型的 Amazon EC2 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：StringList

  描述：（可选）可以批准或拒绝操作的 IAM 用户的 Amazon 资源名称 (ARN)。如果您为 MigrationType 参数指定 CutOver 值，则此参数才应用。
- DestinationSecurityGroupId

类型：StringList

描述：（可选）要与在 VPC 中启动的 Amazon EC2 实例关联的安全组的 ID。如果您没有为此参数指定一个值，则自动化会在您的 VPC 中创建一个安全组，并从 EC2-Classic 中的安全组复制规则。如果规则无法复制到该新安全组，则 VPC 的默认安全组将与 Amazon EC2 实例关联。

- DestinationSubnetId

  类型：字符串

  描述：（可选）要将 Amazon EC2 实例迁移到的子网的 ID。如果您没有为此参数指定一个值，则自动化将从 VPC 中随机选择一个子网。

- InstanceId

  类型：字符串

  说明：（必需）要迁移的 Amazon EC2 实例的 ID。

- MigrationType

  类型：字符串

  有效值：割接 | 测试

  描述：（必需）要执行的迁移的类型。

  `CutOver` 选项需要获得批准才能停止在 EC2-Classic 中运行的 Amazon EC2 实例。此操作获得批准后，Amazon EC2 实例将停止，自动化将创建一个 Amazon Machine Image (AMI)。当 AMI 状态为 `available` 时，将在指定的 `DestinationSubnetId` VPC 中的 AMI 启动一个新的 Amazon EC2 实例。如果在 EC2-Classic 中运行的 Amazon EC2 实例附加了弹性 IP 地址，该实例将被移至您 VPC 中新创建的 Amazon EC2 实例。如果在 VPC 中启动的 Amazon EC2 实例由于任何原因未能创建，该实例将被终止，并请求获得批准以在 EC2-Classic 中启动 Amazon EC2 实例。

  `Test` 选项创建 Amazon EC2 实例的 AMI，该实例无需重启即可在 EC2-Classic 中运行。由于 Amazon EC2 实例不会重启，因此我们无法保证所创建映像的文件系统完整性。当 AMI 状态为 `available` 时，将在 VPC 中指定的 `DestinationSubnetId` 中的 AMI 启动一个新的 Amazon EC2 实例。如果在 EC2-Classic 中运行的 Amazon EC2 实例附加了弹性 IP 地址，自动化将验证您指定的 `DestinationSubnetId` 是否公有。如果在 VPC 中启动的 Amazon EC2 实例由于任何原因未能创建，该实例将被终止且自动化结束。

- SNSNotificationARNforApproval

类型：字符串

描述：（必需）要向其发送批准通知的 Amazon Simple Notification Service (Amazon SNS) 主题的 ARN。如果您为 MigrationType 参数指定 CutOver 值，则此参数才应用。

- TargetInstanceType

  类型：字符串

  默认：t2.2xlarge

  描述：（可选）您要在 VPC 中启动的 Amazon EC2 实例的类型。仅支持基于 Xen 的实例类型，例如 T2、M4 或 C4。

所需的 IAM 权限

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

- ssm:GetDocument
- ssm:ListDocumentVersions
- ssm:ListDocuments
- ssm:StartAutomationExecution
- sns:GetTopicAttributes
- sns:ListSubscriptions
- sns:ListTopics
- sns:Publish
- ec2:AssociateAddress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateImage
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:MoveAddressToVpc
- ec2:RunInstances
- ec2:StopInstances
- ec2:CreateTags

- ec2:DescribeAddresses
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroupReferences
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTags
- ec2:DescribeVpcs
- ec2:DescribeInstanceTypes
- ec2:DescribeImages

文档步骤

- aws:executeAwsApi - 收集有关您在 InstanceId 参数中指定的 Amazon EC2 实例的详细信息。
- aws:assertAwsResourceProperty - 确认您在 TargetInstanceType 参数中指定的实例类型是基于 XEN。
- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例属于硬件虚拟机虚拟化类型。
- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例具有 Amazon EBS 根卷。
- aws:executeScript - 根据您为 DestinationSecurityGroupId 参数指定的值视需要创建一个安全组。
- aws:branch - 根据您在 DestinationSubnetId 参数中指定的值进行分支。
- aws:executeAwsApi - 标识您运行此自动化所在 AWS 区域 的默认 VPC。
- aws:executeAwsApi - 随机选择位于默认 VPC 中的子网的 ID。
- aws:createImage - 创建一个 AMI 而不重启 Amazon EC2 实例。
- aws:branch - 根据您为 MigrationType 参数指定的值进行分支。
- aws:branch - 根据您为 DestinationSubnetId 参数指定的值进行分支。

- aws:runInstances - 从创建 AMI 的启动一个新实例，而不重启 EC2 Classic 中的 Amazon EC2 实例。
- aws:changeInstanceState - 在上一步因任何原因而失败时终止新启动的 Amazon EC2 实例。
- aws:runInstances - 从创建的 AMI 启动一个新实例，而不重启 DestinationSubnetId （如果提供）中的 Amazon EC2 实例。
- aws:changeInstanceState - 在上一步因任何原因而失败时终止新启动的 Amazon EC2 实例。
- aws:assertAwsResourceProperty - 确认在 EC2-Classic 中运行的 Amazon EC2 实例的停止行为。
- aws:approve - 等待批准以停止 Amazon EC2 实例。
- aws:changeInstanceState - 停止在 EC2-Classic 中运行的 Amazon EC2 实例。
- aws:changeInstanceState - 必要时强制停止在 EC2-Classic 中运行的 Amazon EC2 实例。
- aws:createImage - 在 Amazon EC2 实例的 AMI 停止后创建一个。
- aws:branch - 根据为 DestinationSubnetId 参数指定的值进行分支。
- aws:runInstances - 从 EC2 Classic 中的停止的 Amazon EC2 实例创建的 AMI 启动一个新实例。
- aws:approve - 等待批准以终止新启动的实例，并在上一步因任何原因而失败时在 EC2-Classic 中启动 Amazon EC2 实例。
- aws:changeInstanceState - 终止新启动的 Amazon EC2 实例。
- aws:runInstances - 从 AMI 启动一个新实例，该实例根据 DestinationSubnetId 参数为在 EC2 Classic 中已停止的 Amazon EC2 实例创建。
- aws:approve - 等待批准以终止新启动的实例，并在上一步因任何原因而失败时在 EC2-Classic 中启动 Amazon EC2 实例。
- aws:changeInstanceState - 终止新启动的 Amazon EC2 实例。
- aws:changeInstanceState - 启动 EC2-Classic 中已停止的 Amazon EC2 实例。
- aws:branch - 根据 Amazon EC2 实例是否具有公有 IP 地址进行分支。
- aws:executeAwsApi - 验证公有 IP 地址是否为弹性 IP 地址。
- aws:branch - 根据您在 MigrationType 参数中指定的值进行分支。
- aws:executeAwsApi - 将弹性 IP 地址移至您的 VPC。
- aws:executeAwsApi - 收集已移至 VPC 的弹性 IP 地址的分配 ID。
- aws:branch - 根据在您的 VPC 中运行的 Amazon EC2 实例启动所在的子网进行分支。
- aws:executeAwsApi - 将弹性 IP 地址附加到 VPC 中新启动的实例。

- aws:executeScript - 确认您在您的 VPC 中运行的新启动的 Amazon EC2 实例的子网是公有的。

输出

g etInstanceProperties.virtualizationType - 在 EC2-Classic 中运行的 Amazon EC2 实例的虚拟化类型。

getInstanceProperties.rootDeviceType - 在 EC2-Classic 中运行的 Amazon EC2 实例的根设备类型。

createAMIWithoutReboot.ImageId - 在未重启在 EC2-Classic 中运行的 Amazon EC2 实例的情况下创建的 AMI 的 ID。

getDefaultVPC.VpcId - 启动新 Amazon EC2 实例所在的默认 VPC 的 ID（如果未提供 DestinationSubnetId 参数的值）。

getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc - 启动新 Amazon EC2 实例所在的默认 VPC 的子网的 ID（如果未提供 DestinationSubnetId 参数的值）。

launchTestInstanceDefaultVPC.InstanceIds - 在 Test 迁移类型期间在默认 VPC 中新启动的 Amazon EC2 实例的 ID。

launchTestInstanceProvidedSubnet.InstanceIds - 在 Test 迁移类型期间在您指定的 DestinationSubnetId 中新启动的 Amazon EC2 实例的 ID。

createAMIAfterStoppingInstance.ImageId - 在 EC2-Classic 中运行的 Amazon EC2 实例停止后创建的 AMI 的 ID。

launchCutOverInstanceProvidedSubnet.InstanceIds - 在 CutOver 迁移类型期间在您指定的 DestinationSubnetId 中新启动的 Amazon EC2 实例的 ID。

launchCutOverInstanceDefaultVPC.InstanceIds - 在 CutOver 迁移类型期间在默认 VPC 中新启动的 Amazon EC2 实例的 ID。

verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic - 在默认 VPC 中由自动化选择的子网是否为公有子网。

verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic - 您在 DestinationSubnetId 中指定的子网是否为公有子网。

AWSSupport-MigrateXenToNitroLinux

描述

AWSSupport-MigrateXenToNitroLinux 运行手册将克隆、准备一个 Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen 实例并将其迁移到 Nitro实例类型。此运行手册为操作类型提供了两个选项：

- Clone&Migrate – 此选项的工作流程包括初步检查、测试和Clone&Migrate阶段。工作流程使用 AWSSupport-CloneXenEC2InstanceAndMigrateToNitro 运行手册运行。
- FullMigration – 此选项运行 Clone&Migrate 工作流程，然后执行 替换 Amazon EBS 根卷的额外步骤。

> **Important**
>
> 使用此运行手册会让您的账户产生运行 Amazon EC2 实例、创建 Amazon Elastic Block Store (Amazon EBS) 卷和 AMIs 的费用。有关更多信息，请参见Amazon EC2 定价 和 Amazon EBS 定价。

初步检查

在继续迁移之前，自动化会执行以下初步检查。如果任何检查失败，自动化将结束。此阶段只是 Clone&Migrate 工作流程的一部分。

- 检查目标实例是否已经是 Nitro 实例类型。
- 检查竞价型实例购买选项是否用于目标实例。
- 检查实例存储卷是否附加到目标实例。
- 验证目标实例操作系统 (OS) 是否为 Linux。
- 检查目标实例是否是 Amazon EC2 Auto Scaling 自动扩缩组的一部分。如果它是自动扩缩组的一部分，自动化操作将验证该实例是否处于 standby 状态。
- 验证实例是否由 AWS Systems Manager 管理。

测试

自动化将从目标实例创建 Amazon Machine Image (AMI)，并从新创建的 AMI 启动一个测试实例。此阶段只是 Clone&Migrate 工作流程的一部分。

如果测试实例通过了所有状态检查，则自动化将暂停，并通过 Amazon Simple Notification Service (Amazon SNS) 通知请求指定委托人批准。如果提供了批准，则自动化会终止测试实例，停止目标实例，然后继续迁移，而新创建 AMI 的实例将在 `Clone&Migrate` 工作流程结束时取消注册。

> **Note**
>
> 在提供批准之前，我们建议您确认目标实例上运行的所有应用程序均已正常关闭。

克隆和迁移

此自动化将从目标实例创建另一个 AMI，然后启动一个新实例以变为 Nitro 实例类型。在继续迁移之前，自动化会完成以下先决条件。如果任何检查失败，自动化将结束。此阶段也只是 `Clone&Migrate` 工作流程的一部分。

- 开启增强联网 (ENA) 属性。
- 安装最新版本的 ENA 驱动程序（如果尚未安装），或者将 ENA 驱动程序版本更新至最新版本。为确保最大联网性能，如果 Nitro 实例类型为第 6 代，则需要更新到最新的 ENA 驱动程序版本。
- 验证是否已安装 NVMe 模块。如果模块安装完毕，自动化将验证该模块是否加载到 `initramfs` 中。
- 分析 `/etc/fstab` 并将带有区块设备名称（`/dev/sd*` 或 `/dev/xvd*`）的条目替换为相应的 UUID。在修改配置之前，自动化会在路径 `/etc/fstab*` 上创建文件的备份。
- 关闭可预测的接口命名，方法是将 `net.ifnames=0` 选项添加到 `/etc/default/grub` 文件（如果存在）中的 `GRUB_CMDLINE_LINUX` 行，或添加到 `/boot/grub/menu.lst` 中的内核。
- 如果 `/etc/udev/rules.d/70-persistent-net.rules` 文件存在，则将其移除。在移除文件之前，自动化会在路径 `/etc/udev/rules.d/` 上创建文件的备份。

验证所有要求后，实例类型将更改为您指定的 Nitro 实例类型。在作为 Nitro 实例类型启动后，自动化会等待新创建的实例通过所有状态检查。然后，自动化将等待指定主体的批准以创建成功启动 Nitro 的实例的 AMI。如果批准被拒绝，自动化将结束，从而让新创建的实例保持运行状态，目标实例将保持停止状态。

替换根 Amazon EBS 卷

如果您选择 `FullMigration` 作为 `OperationType`，则自动化会将目标 Amazon EC2 实例迁移到您指定的 Nitro 实例类型。自动化会请求获得指定主体的批准，以将目标 Amazon EC2 实例的 Amazon EBS 根卷替换为克隆的 Amazon EC2 实例的根卷。成功迁移后，克隆的 Amazon EC2 实例将终止。

如果自动化失败，初始 Amazon EBS 根卷将附加到目标 Amazon EC2 实例。如果附加到目标 Amazon EC2 实例的 Amazon EBS 根卷具有应用了 `aws:` 前缀的标签，则不支持 `FullMigration` 操作。

开始前的准备工作

目标实例必须具有出站互联网访问权限。这是为了访问存储库以获取驱动程序和依赖项，例如kernel-devel、gcc、patch、rpm-build、wget、dracut、make、linux-headers 和 unzip。如果需要，可以使用程序包管理器。

需要使用 Amazon SNS 主题才能发送批准和更新的通知。有关如何创建 Amazon SNS 主题的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的创建 Amazon SNS 主题。

此运行手册支持以下操作系统：

- RHEL 7.x - 8.5
- Amazon Linux (2018.03)、Amazon Linux 2
- Debian 服务器
- Ubuntu Server 18.04 LTS、20.04 LTS 和 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

- 确认

  类型：字符串

  描述：（必需）阅读此自动化运行手册所执行操作的完整详细信息，然后输入**Yes, I understand and acknowledge**以继续使用运行手册。

- ApproverIAM

  类型：字符串

  描述：（必需）可以批准自动化的 IAM 角色、用户或用户名的 ARN。您可以指定最多 10 个 批准者。

- DeleteResourcesOnFailure

  类型：布尔值

  描述：（可选）确定在自动化失败时是否删除新创建的实例和迁移的 AMI。

  有效值：True | False

  默认值：True

- MinimumRequiredApprovals

  类型：字符串

  描述：（可选）在请求批准时继续运行自动化所需的最低批准数。

  有效值：1-10

  默认值：1

- NitroInstanceType

  类型：字符串

  描述：（必需）您要将Nitro实例更改为的实例类型。支持的实例类型包括 M5、M6、C5、C6、R5、R6 和 T3。

默认：m5.xlarge

- OperationType

  类型：字符串

  描述：（必需）希望执行的操作。FullMigration 选项执行的任务与 Clone&Migrate 的相同，还会替换目标实例的根卷。迁移过程结束后，目标实例的根卷将替换为来自新创建实例的根卷。FullMigration 操作不支持逻辑卷管理器 (LVM) 定义的根卷。

  有效值：Clone&Migrate | FullMigration

- SNSTopicArn

  类型：字符串

  说明：（必需）用于批准通知的 Amazon SNS 主题的 ARN。Amazon SNS 主题用于在自动化期间发送所需的批准通知。

- TargetInstanceId

  类型：字符串

  说明：（必需）要迁移的 Amazon EC2 实例的 ID。

Clone&Migrate 工作流

所需的 IAM 权限

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

- ssm:DescribeAutomationExecutions
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:DescribeAutomationStepExecutions
- ssm:SendCommand
- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations

- ec2:DescribeInstances
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeImages
- ec2:CreateImage
- ec2:RunInstances
- ec2:DescribeInstanceStatus
- ec2:DeregisterImage
- ec2:DeleteSnapshot
- ec2:TerminateInstances
- ec2:StartInstances
- ec2:DescribeKeyPairs
- ec2:StopInstances
- kms:CreateGrant*
- kms:ReEncrypt
- ec2:ModifyInstanceAttribute
- autoscaling:DescribeAutoScalingInstances
- iam:passRole
- iam:ListRoles

文档步骤

- startOfPreliminaryChecksBranch - 分支到初步检查工作流程。
- getTargetInstanceProperties - 从目标实例收集详细信息。
- checkIfNitroInstanceTypeIsSupportedInAZ - 确定在与目标实例相同的可用区是否支持目标 Amazon EC2 实例类型。
- getXenInstanceTypeDetails - 收集有关源实例类型的详细信息。
- checkIfInstanceHypervisorIsNitroAlready - 检查目标实例是否已作为Nitro实例类型运行。
- checkIfTargetInstanceLifecycleIsSpot - 检查目标实例的购买选项是否为 Spot。

- checkIfOperatingSystemIsLinux - 检查目标实例操作系统是否为 Linux。
- verifySSMConnectivityForTargetInstance - 验证目标实例是否由 Systems Manager 管理。
- checkIfEphemeralVolumeAreSupported - 检查目标实例的当前实例类型是否支持实例存储卷。
- verifyIfTargetInstanceHasEphemeralVolumesAttached - 检查目标实例是否包含附加的实例存储卷。
- checkIfRootVolumeIsEBS - 检查目标实例的根卷类型是否为 EBS。
- checkIfTargetInstanceIsInASG - 检查目标实例是否是自动扩缩组的一部分。
- endOfPreliminaryChecksBranch - 初步检查分支结束。
- startOfTestBranch - 分支到测试工作流程。
- createTestImage - 创建目标实例AMI的测试。
- launchTestInstanceInSameSubnet - 使用与目标实例相同的配置，从测试 AMI 启动一个测试实例。
- cleanupTestInstance - 终止测试实例。
- endOfTestBranch - 测试分支结束。
- checkIfTestingBranchSucceeded - 检查测试分支的状态。
- approvalToStopTargetInstance - 等待指定委托人的批准才能停止目标实例。
- stopTargetEC2Instance - 停止目标实例。
- forceStopTargetEC2Instance - 只有在上一步未能停止目标实例时才强制停止该实例。
- startOfCloneAndMigrateBranch - 分支到 Clone&Migrate 工作流程。
- createBackupImage - 创建目标实例中的一个作为备份。AMI
- launchInstanceInSameSubnet - 使用与源实例相同的配置，从备份 AMI 启动一个新实例。
- waitForClonedInstanceToPassStatusChecks - 等待新创建的实例通过所有状态检查。
- verifySSMConnectivityForClonedInstance - 验证新创建的实例是否由 Systems Manager 管理。
- checkAndInstallENADrivers - 检查新创建的实例上是否安装了 ENA 驱动程序，并在需要时安装驱动程序。
- checkAndAddNVMEDrivers - 检查新创建的实例上是否安装了 NVMe 驱动程序，并在需要时安装驱动程序。

- checkAndModifyFSTABEntries - 检查中是否使用了设备名称，/etc/fstab并在需要时将其替换为 UUID。
- stopClonedInstance - 停止新创建的实例。
- forceStopClonedInstance - 只有在上一步未能停止实例时才强制停止新创建的实例。
- checkENAAttributeForClonedInstance - 检查是否为新创建的实例启用了增强联网属性。
- setNitroInstanceTypeForClonedInstance - 将新创建实例的实例类型更改为您指定的 Nitro 实例类型。
- startClonedInstance - 启动您已更改其实例类型的新创建实例。
- approvalForCreatingImageAfterDriversInstallation - 如果实例作为 Nitro 实例类型成功启动，自动化将等待所需主体的批准。如果获得批准，将会创建用作 Golden AMI 的 AMI。
- createImageAfterDriversInstallation - 创建一个AMI用作金币AMI。
- endOfCloneAndMigrateBranch - Clone&Migrate 分支结束。
- cleanupTestImage - 取消注册为测试而创建的 AMI。
- failureHandling - 检查您是否选择在出现故障时终止资源。
- onFailureTerminateClonedInstance - 在自动化失败时终止新创建的实例。
- onFailurecleanupTestImage - 取消注册为测试而创建的 AMI。
- onFailureApprovalToStartTargetInstance - 在自动化失败时等待指定主体的批准以启动目标实例。
- onFailureStartTargetInstance - 在自动化失败时启动目标实例。

FullMigration 工作流

所需的 IAM 权限

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

- ssm:DescribeAutomationExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeAutomationStepExecutions
- ssm:SendCommand
- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations

- ec2:DescribeInstances
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeImages
- ec2:CreateImage
- ec2:RunInstances
- ec2:DescribeInstanceStatus
- ec2:DeregisterImage
- ec2:DeleteSnapshot
- ec2:TerminateInstances
- ec2:StartInstances
- ec2:DescribeKeyPairs
- ec2:StopInstances
- kms:CreateGrant*
- kms:ReEncrypt
- ec2:ModifyInstanceAttribute
- ec2:DetachVolume
- ec2:AttachVolume
- ec2:DescribeVolumes
- autoscaling:DescribeAutoScalingInstances
- iam:PassRole
- ec2:CreateTags
- cloudformation:DescribeStackResources

文档步骤

FullMigration 工作流程运行的步骤与 Clone&Migrate 工作流运行的相同，另外还执行以下步骤：

- checkConcurrency - 验证此运行手册中是否只有一个针对您指定的 Amazon EC2 实例的自动化。如果运行手册发现另一个针对同一实例的自动化正在进行，自动化将结束。

- getTargetInstanceProperties - 从目标实例收集详细信息。
- checkRootVolumeTags - 确定目标 Amazon EC2 实例的根卷是否包含任何 AWS 预留标签。
- cloneTargetInstanceAndMigrateToNitro - 使用AWS-CloneXenInstanceToNitro运行手册启动儿童自动化。
- branchOnTheOperationType - 根据您为 OperationType 参数指定的值进行分支。
- getClonedInstanceId - 从子自动化中检索新启动的实例的 ID。
- checkIfRootVolumeIsBasedOnLVM - 确定根分区是否由 LVM 管理。
- branchOnTheRootVolumeLVMStatus - 如果从主体收到了要求的最低限度批准，自动化将继续执行根卷替换。
- manualInstructionsInCaseOfLVM - 如果根卷由 LVM 管理，自动化将发送包含如何手动替换根卷说明的输出。
- startOfReplaceRootEBSVolumeBranch - 启动“替换根 EBS 卷”分支工作流。
- checkIfTargetInstanceIsManagedByCFN - 确定目标实例是否由 AWS CloudFormation 堆栈管理。
- branchOnCFNStackStatus - 根据 CloudFormation 堆栈的状态进行分支。
- approvalForRootVolumesReplacement(WithCFN) - 如果目标实例由 CloudFormation 启动，则在新启动的实例作为 Nitro 实例类型成功启动后，自动化将等待批准。获得批准后，目标实例的 Amazon EBS 卷将替换为新启动实例的根卷。
- approvalForRootVolumesReplacement - 在新启动的实例作为 Nitro 实例类型成功启动后等待批准。获得批准后，目标实例的 Amazon EBS 卷将替换为新启动实例的根卷。
- assertIfTargetEC2InstanceIsStillStopped - 在更换根卷之前，验证目标实例是否处于 stopped 状态。
- stopTargetInstanceForRootVolumeReplacement - 如果目标实例正在运行，则自动化会在替换根卷之前停止该实例。
- forceStopTargetInstanceForRootVolumeReplacement - 在上一步失败时强制停止目标实例。
- stopClonedInstanceForRootVolumeReplacement - 停止新创建的实例后再替换 Amazon EBS 卷。
- forceStopClonedInstanceForRootVolumeReplacement - 在上一步失败时强制停止新创建的实例。
- getBlockDeviceMappings - 检索目标实例和新创建实例的块设备映射。
- replaceRootEbsVolumes - 将目标实例的根卷替换为新创建实例的根卷。

- EndOfReplaceRootEBSVolumeBranch - 结束“替换根 EBS 卷”分支工作流。
- checkENAAttributeForTargetInstance - 检查目标 Amazon EC2 实例的增强联网 (ENA) 属性是否已开启。
- enableENAAttributeForTargetInstance - 必要时为目标 Amazon EC2 实例开启 ENA 属性。
- setNitroInstanceTypeForTargetInstance - 将目标实例更改为您指定的 Nitro 实例类型。
- replicateRootVolumeTags - 从目标 Amazon EC2 实例复制根 Amazon EBS 卷上的标签。
- startTargetInstance - 更改实例类型后启动目标 Amazon EC2 实例。
- onFailureStopTargetEC2Instance - 在目标 Amazon EC2 实例未能作为 Nitro 实例类型启动时将其停止。
- onFailureForceStopTargetEC2Instance - 在上一步失败时强制停止目标 Amazon EC2 实例。
- OnFailureRevertOriginalInstanceType - 在目标实例未能作为 Nitro 实例类型启动时将目标 Amazon EC2 实例恢复为初始实例类型。
- onFailureRollbackRootVolumeReplacement - 必要时还原 replaceRootEbsVolumes 步骤所做的所有更改。
- onFailureApprovalToStartTargetInstance - 在回滚之前的更改后，等待指定主体的批准以启动目标 Amazon EC2 实例。
- onFailureStartTargetInstance - 启动目标 Amazon EC2 实例。
- terminateClonedEC2Instance - 在替换根 Amazon EBS 卷后，终止克隆的 Amazon EC2 实例。

AWSSupport-ResetAccess

描述

此运行手册在指定的 EC2 实例上使用 EC2Rescue 工具，通过 EC2 控制台 (Windows) 或生成并添加新 SSH 密钥对 (Linux) 的方式重新启用密码解密。如果丢失了密钥对，则此 Automation 将创建一个启用了密码的 AMI，您可以使用此 AMI 启动具有您拥有的密钥对的新 EC2 实例 (Windows)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
- EC2RescueInstanceType

  类型：字符串

  有效值：t2.small | t2.medium | t2.large

  默认值：t2.small

  说明：（必需）EC2Rescue 实例的 EC2 实例类型。建议大小：t2.small。
- InstanceId

  类型：字符串

  说明：（必需）要重置其访问权限的 EC2 实例的 ID。

  > **Important**
  >
  > Systems Manager Automation 会停止此实例，并在尝试任何操作前创建一个 AMI。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。
- SubnetId

  类型：字符串

  默认值：CreateNewVPC

说明：（可选）EC2Rescue 实例的子网 ID。默认情况下，Systems Manager Automation 会创建一个新 VPC。或者，您也可以使用 SelectedInstanceSubnet 来使用实例所在的子网，或指定一个自定义的子网 ID。

> **Important**
>
> 子网必须与 InstanceId 位于同一可用区中，并且必须允许访问 SSM 终端节点。

所需的 IAM 权限

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

您必须至少具有 ssm:StartAutomationExecution 和 ssm:GetParameter 才能检索 SSH 密钥参数名称，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。有关所需权限的更多信息，请参阅[AWSSupport-StartEC2RescueWorkflow]。

文档步骤

1. `aws:assertAwsResourceProperty` - 断言 提供的实例是否是 Windows。
   a. (EC2Rescue for Windows) 如果提供的实例是 Windows：
      i. `aws:executeAutomation` - 使用适用于 Window `AWSSupport-StartEC2RescueWorkflow` s 的 ec2Rescue 离线密码重置脚本进行调用
      ii. `aws:executeAwsApi` - 从嵌套的 Automation 检索备份 AMI ID
      iii. `aws:executeAwsApi` - 从嵌套的 Automation 检索启用了密码的 AMI ID
      iv. `aws:executeAwsApi` - 从嵌套的 Automation 检索 EC2Rescue 摘要
   b. (EC2Rescue for Linux) 如果提供的实例是 Linux：
      i. `aws:executeAutomation` - 使用 EC2Rescue for Linux 离线 SSH 密钥注入脚本调用 `AWSSupport-StartEC2RescueWorkflow`
      ii. `aws:executeAwsApi` - 从嵌套的 Automation 检索备份 AMI ID
      iii. `aws:executeAwsApi` - 检索注入的 SSH 密钥的 SSM 参数名称
      iv. `aws:executeAwsApi` - 从嵌套的 Automation 检索 EC2Rescue 摘要

输出

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getWindowsPasswordEnabledAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

getLinuxSSHKeyParameter.Name

AWSSupport-ResetLinuxUserPassword

描述

AWSSupport-ResetLinuxUserPassword 运行手册可帮助您重置本地操作系统 (OS) 用户的密码。对于需要使用串行控制台访问其 Amazon Elastic Compute Cloud (Amazon EC2) 实例的用户，此运行手册尤其有用。运行手册在您的账户中创建了一个临时 Amazon EC2 实例 AWS 账户 和一个 AWS Identity and Access Management (IAM) 角色，该角色有权检索包含密码的 AWS Secrets Manager 私有值。

运行手册可停止您的目标 Amazon EC2 实例，分离 Amazon Elastic Block Store (Amazon EBS) 根卷，并将其附加到临时 Amazon EC2 实例。利用运行命令，可以在临时实例上运行脚本，以设置您指定的操作系统用户的密码。然后，Amazon EBS 根卷会重新附加到您的目标实例。此运行手册还提供了在自动化开始时创建根卷快照的选项。

开始之前

使用您要分配给操作系统用户的密码的值创建一个 Secrets Manager 密钥。该值必须为纯文本形式。有关更多信息，请参阅《AWS Secrets Manager 用户指南》中的创建 AWS Secrets Manager 密钥。

注意事项

- 我们建议您在使用此运行手册之前先备份您的实例。考虑将 CreateSnapshot 参数的值设置为 **Yes**。
- 更改本地用户密码需要运行手册停止您的实例。停止实例后，存储在内存或实例存储卷上的数据将丢失。此外，所有自动分配的公有 IPv4 地址都会被释放。有关停止实例时会发生什么情况的更多信息，请参阅 Amazon EC2 用户指南中的停止和启动实例。
- 如果连接到您的目标 Amazon EC2 实例的 Amazon EBS 卷使用客户托管 AWS Key Management Service (AWS KMS) 密钥进行加密，请确保 AWS KMS 密钥未加密，deleteddisabled否则您的实例将无法启动。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）包含您要重置的操作系统用户密码的 Amazon EC2 Linux 实例的 ID。
- LinuxUser姓名

  类型：字符串

  默认：ec2-user

  描述：（可选）要重置其密码的操作系统用户账户。
- SecretArn

  类型：字符串

  描述：（必需）包含新密码的 Secrets Manager 密钥的 ARN。
- SecurityGroup我是

类型：字符串

描述：（可选）要附加到临时 Amazon EC2 实例的安全组的 ID。如果您没有为此参数提供一个值，将使用默认的 Amazon Virtual Private Cloud (Amazon VPC) 安全组。

- SubnetId

  类型：字符串

  描述：（可选）要将 Amazon EC2 临时实例启动到的子网的 ID。默认情况下，自动化会选择与您的目标实例相同的子网。如果您选择提供不同的子网，则它必须与目标实例位于同一可用区，并且可以访问 Systems Manager 端点。

- CreateSnapshot

  类型：字符串

  有效值：是 | 否

  默认：是

  描述：（可选）确定是否在自动化运行之前创建目标 Amazon EC2 实例根卷的快照。

- StopConsent

  类型：字符串

  有效值：是 | 否

  默认：否

  描述：输入 **Yes** 以确认目标 Amazon EC2 实例将在此自动化期间停止。当 Amazon EC2 实例停止时，存储在内存或实例存储卷中的所有数据都将丢失，自动公有 IPv4 地址将释放。有关更多信息，请参阅 Amazon EC2 用户指南中的停止和启动您的实例。

所需的 IAM 权限

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

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

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

文档步骤

1. aws:branch – 根据您是否同意停止目标 Amazon EC2 实例进行分支。
2. aws:assertAwsResourceProperty 确保 Amazon EC2 实例的状态为 running 或 stopped 状态。否则，自动化将结束。
3. aws:executeAwsApi 获取 Amazon EC2 实例的属性。
4. aws:executeAwsApi 获取根卷的属性。
5. aws:branch 根据是否提供了临时 Amazon EC2 实例的子网 ID 对自动化进行分支。
6. aws:assertAwsResourceProperty 确保在您 SubnetId 参数中指定的子网与目标 Amazon EC2 实例位于同一可用区。
7. aws:assertAwsResourceProperty 确保目标 Amazon EC2 实例根卷为 Amazon EBS 卷。
8. aws:assertAwsResourceProperty 确保 Amazon EC2 实例架构为 arm64 或 x86_64。
9. aws:assertAwsResourceProperty 确保 Amazon EC2 实例的关闭行为是 stop 且不是 terminate。
10. aws:branch: 确保 Amazon EC2 实例不是竞价型实例。否则，自动化将结束。
11. aws:executeScript 确保 Amazon EC2 实例不是自动扩缩组的一部分。如果该实例是自动扩缩组的一部分，则自动化会确认 Amazon EC2 实例是否处于 Standby 生命周期状态。
12. aws:createStack 创建临时 Amazon EC2 实例，用于重置您指定的操作系统用户的密码。
13. aws:waitForAwsResourceProperty 等到新启动的临时 Amazon EC2 实例开始运行。
14. aws:executeAwsApi 获取临时 Amazon EC2 实例的 ID。
15. aws:waitForAwsResourceProperty 等待临时 Amazon EC2 实例报告为由 Systems Manager 管理。
16. aws:changeInstanceState 停止目标 Amazon EC2 实例。
17. aws:changeInstanceState 强制目标 Amazon EC2 实例停止，以防它卡在停止状态。
18. aws:branch 根据是否请求了目标 Amazon EC2 实例的根卷快照对自动化进行分支。
19. aws:executeAwsApi 创建目标 Amazon EC2 实例根卷的快照。
20. aws:waitForAwsResourceProperty 等待快照变为 completed 状态。
21. aws:executeAwsApi 将 Amazon EBS 根卷与目标 Amazon EC2 实例分离。
22. aws:waitForAwsResourceProperty 等待 Amazon EBS 根卷与目标 Amazon EC2 实例分离。
23. aws:executeAwsApi 将根 Amazon EBS 卷附加到临时 Amazon EC2 实例。
24. aws:waitForAwsResourceProperty 等待 Amazon EBS 根卷附加到临时 Amazon EC2 实例。

25. aws:runCommand 通过在临时 Amazon EC2 实例上使用运行命令运行 Shell 脚本来重置目标用户密码。
26. aws:executeAwsApi 将 Amazon EBS 根卷与临时 Amazon EC2 实例分离。
27. aws:waitForAwsResourceProperty 等待 Amazon EBS 根卷与临时 Amazon EC2 实例分离。
28. aws:executeAwsApi 出现错误后，将 Amazon EBS 根卷与临时 Amazon EC2 实例分离。
29. aws:waitForAwsResourceProperty 出现错误后，等待 Amazon EBS 根卷与临时 Amazon EC2 实例分离。
30. aws:branch 根据是否请求根卷的快照来确定出现错误时的恢复路径对自动化进行分支。
31. aws:executeAwsApi 将根 Amazon EC2 卷重新附加到目标 Amazon EC2 实例。
32. aws:waitForAwsResourceProperty 等待 Amazon EBS 根卷附加到 Amazon EC2 实例。
33. aws:executeAwsApi 从目标 Amazon EC2 实例根卷的快照创建新 Amazon EBS 卷。
34. aws:waitForAwsResourceProperty 等到新的 Amazon EBS 卷处于 available 状态。
35. aws:executeAwsApi 将新的 Amazon EBS 卷作为根卷附加到目标实例。
36. aws:waitForAwsResourceProperty 等待 Amazon EBS 卷处于 attached 状态。
37. aws:executeAwsApi描述运行手册无法创建或更新 AWS CloudFormation 堆栈时的 AWS CloudFormation 堆栈事件。
38. aws:branch 根据前一个 Amazon EC2 实例状态对自动化进行分支。如果状态为 running，则实例已启动。如果处于 stopped 状态，则自动化会继续。
39. aws:changeInstanceState 根据需要启动 Amazon EC2 实例。
40. aws:waitForAwsResourceProperty等到 AWS CloudFormation 堆栈处于终端状态后再删除。
41. aws:executeAwsApi删除包含临时 Amazon EC2 实例的 AWS CloudFormation 堆栈。

AWSPremiumSupport-ResizeNitroInstance

描述

AWSPremiumSupport-ResizeNitroInstance 运行手册提供了一种自动化的解决方案，用于调整基于 Nitro 系统构建的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的大小。

为了降低数据丢失和停机的潜在风险，运行手册对以下事项进行验证：

- 实例停止行为。
- 实例是否是 Amazon EC2 Auto Scaling 组的一部分且处于 standby 模式。
- 实例状态和租赁。

- 您要更改成的实例类型支持当前附加到您实例的网络接口的数量。
- 当前实例类型和目标实例类型的处理器架构和虚拟化类型相同。
- 如果实例正在运行，则表明它正在通过所有状态检查。
- 您要更改的实例类型在相同可用区中是可用的。

如果 Amazon EC2 在更改实例类型后未通过状态检查，运行手册将自动回退到以前的实例类型。

默认情况下，如果实例正在运行以及已附加实例存储卷，则此运行手册不会更改实例类型。如果实例是 AWS CloudFormation 堆栈的一部分，运行手册也不会更改实例类型。如果要更改这些行为中的任意一个，请为 `AllowInstanceStoreInstances` 和 `AllowCloudFormationInstances` 参数指定 `yes`。

运行手册提供了两种不同的方法来指定要更改为的实例类型：

- 对于针对单个实例的简单自动化，请使用 `TargetInstanceTypeFromParameter` 参数指定要更改为的实例类型。
- 要大规模运行自动化以更改多个实例的实例类型，请使用 `TargetInstanceTypeFromTagValue` 参数指定实例类型。有关大规模运行自动化的信息，请参阅大规模运行自动化。

如果您没有为任一参数指定一个值，自动化将失败。

> **Important**
>
> 访问 `AWSPremiumSupport-*` 运行手册需要订阅 Enterprise 或 Business Support。有关更多信息，请参阅比较 AWS Support 计划。

注意事项

- 我们建议您在使用此运行手册之前先备份您的实例。
- 有关更改实例类型的兼容性的信息，请参阅更改实例类型的兼容性。
- 如果自动化失败并回退到初始实例类型，请参阅更改实例类型疑难解答。
- 更改实例类型需要运行手册来停止您的实例。停止实例后，存储在内存或实例存储卷上的数据将丢失。此外，所有自动分配的公有 IPv4 地址都会被释放。有关停止实例时会发生什么的更多信息，请参阅停止和启动您的实例。
- 使用 `SkipInstancesWithTagKey` 参数，您可以跳过应用了特定 Amazon EC2 标签键的实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- AutomationAssumeRole

  类型：字符串

  说明：（可选）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon Resource Name (ARN)。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
- 确认

  类型：字符串

  描述：（必需）输入**yes**以确认如果您的实例当前正在运行，则该实例将停止。
- AllowInstanceStoreInstances

  类型：字符串

  有效值：否 | 是

  默认值：no

  描述：（可选）如果您指定 yes，您将允许运行手册在已附加实例存储卷的实例上运行。
- AllowCloudFormationInstances

  类型：字符串

  有效值：否 | 是

默认值：no

描述：（可选）如果您指定 yes，运行手册将在属于 AWS CloudFormation 堆栈一部分的实例上运行。

- DryRun

  类型：字符串

  有效值：否 | 是

  默认值：no

  描述：（可选）如果您指定 yes，运行手册将验证大小调整要求，而不会更改实例类型。

- InstanceId

  类型：字符串

  描述：（必填）要更改其类型的 Amazon EC2 实例的 ID。

- SkipInstancesWithTagKey

  类型：字符串

  描述：（可选）如果您指定的标签键应用于目标实例，自动化将跳过该实例。

- SleepTime

  类型：字符串

  原定设置值：3

  描述：（可选）此运行手册在完成后应处于休眠状态的秒数。

- TagInstance

  类型：字符串

  描述：（可选）使用您选择的键和值按以下格式为标记该实例：*Key=ChangingType,Value=True*。此选项允许您跟踪此运行手册所针对的实例。标签键和值区分大小写。

- TargetInstanceTypeFromParameter

  类型：字符串

描述：（可选）要将您的实例更改为的实例类型。如果您要使用 TargetInstanceTypeFromTagValue 参数中提供的标签键的值，请将此参数留空。

- TargetInstanceTypeFromTagValue

  类型：字符串

  描述：（可选）应用于目标实例的标签键，其值包含您要更改为的实例类型。如果您为 TargetInstanceTypeFromParameter 参数指定值，那么它将替换您为此参数指定的任何值。

所需的 IAM 权限

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

- autoscaling:DescribeAutoScalingInstances
- cloudformation:DescribeStackResources
- ssm:GetAutomationExecution
- ssm:DescribeAutomationExecutions
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeTags
- ec2:ModifyInstanceAttribute
- ec2:StartInstances
- ec2:StopInstances

文档步骤

1. aws:assertAwsResourceProperty：确保 Amazon EC2 实例未使用 SkipInstancesWithTagKey 参数中指定的资源标签键进行标记。如果发现标签键应用于该实例，该步骤将失败，自动化将结束。
2. aws:assertAwsResourceProperty：确认目标 Amazon EC2 实例的状态为 running、pending、stopped 或 stopping。否则，自动化将结束。

3. aws:executeAwsApi：从 Amazon EC2 实例收集属性。
4. aws:executeAwsApi：收集有关当前 Amazon EC2 实例类型的详细信息。
5. aws:branch：检查当前实例类型和 TargetInstanceTypeFromParameter 参数中指定的实例类型是否相同。如果相同，自动化将结束。
6. aws:assertAwsResourceProperty：确保实例在 Nitro 系统上运行。
7. aws:branch：确保 Amazon EC2 实例根卷类型为 Amazon Elastic Block Store (Amazon EBS) 卷。
8. aws:assertAwsResourceProperty：确认实例关闭行为是 stop 且不是 terminate。
9. aws:branch: 确保 Amazon EC2 实例不是竞价型实例。
10. aws:branch：确保 Amazon EC2 实例的租赁是默认的，而不是专属主机或专用实例。
11. aws:executeScript：确认此运行手册中只有一个针对当前实例 ID 的自动化。如果针对同一实例的另一个自动化已经在进行，则它会返回错误并结束。
12. aws:branch：根据 Amazon EC2 实例的状态对自动化进行分支。
    a. 如果为 stopped 或 stopping，则自动化会运行 aws:waitForAwsResourceProperty，直到 Amazon EC2 实例完全停止。
    b. 如果为 running 或 pending，则自动化会运行 aws:waitForAwsResourceProperty，直到 Amazon EC2 实例通过状态检查。
13. aws:assertAwsResourceProperty：通过调用 DescribeAutoScalingInstances API 操作，确认 Amazon EC2 实例不是自动扩缩组的一部分。如果实例是自动扩缩组的一部分，确保 Amazon EC2 实例处于 standby 模式。
14. aws:branch：根据您是否希望自动化检查 Amazon EC2 实例是否属于 AWS CloudFormation 堆栈的一部分，对自动化进行分支：
    a. aws:executeScript 通过调用 DescribeStackResources API 操作确保 Amazon EC2 实例不是 AWS CloudFormation 堆栈的一部分。
15. aws:executeAwsApi：返回具有相同处理器架构类型、虚拟化类型且支持当前附加到目标实例的网络接口数量的实例类型列表。
16. aws:executeAwsApi：从 TargetInstanceTypeFromTagValue 参数中指定的标签键获取目标实例类型值。
17. aws:executeScript：确认当前实例类型和目标实例类型兼容。确保目标实例类型在同一个子网中可用。验证已启动运行手册的主体是否拥有更改实例类型的权限，以及是否拥有当实例正在运行时停止和启动该实例的权限。
18. aws:branch：根据 DryRun 参数值是否设置为 yes，对自动化进行分支。如果是 yes，自动化将结束。

19aws:branch：检查原始和目标实例类型是否相同。如果它们相同，自动化将结束。

20aws:executeAwsApi：获取当前实例状态。

21aws:changeInstanceState：停止 Amazon EC2 实例。

22aws:changeInstanceState: 如果实例卡在了 stopping 停止状态，则强制其停止。

23aws:executeAwsApi：将实例类型更改为目标实例类型。

24aws:sleep：更改实例类型后等待 3 秒钟以确保最终一致性。

25aws:branch：根据前实例的状态对自动化进行分支。如果是 running，则实例已启动。

a. aws:changeInstanceState：如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
b. aws:waitForAwsResourceProperty：等待 Amazon EC2 实例通过状态检查。如果实例未通过状态检查，实例将变回其原始的实例类型。
   i. aws:changeInstanceState：停止 Amazon EC2 实例，然后将其更改为原始实例类型。
   ii. aws:changeInstanceState：强制 Amazon EC2 实例停止，然后再将其更改为原始实例类型，以防它卡在停止状态。
   iii. aws:executeAwsApi：将 Amazon EC2 实例更改为其原始类型。
   iv. aws:sleep：更改实例类型后等待 3 秒钟以确保最终一致性。
   v. aws:changeInstanceState：如果 Amazon EC2 实例在更改实例类型之前正在运行，则启动该实例。
   vi. aws:waitForAwsResourceProperty：等待 Amazon EC2 实例通过状态检查。

26aws:sleep: 等待，然后结束运行手册。

AWSSupport-RestoreEC2InstanceFromSnapshot

描述

AWSSupport-RestoreEC2InstanceFromSnapshot 运行手册可帮助您识别 Amazon Elastic Compute Cloud (Amazon EC2) 实例，并将其从根卷的有效Amazon Elastic Block Store (Amazon EBS) 快照中恢复。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（可选）要自动化查看快照的最后日期。
- InplaceSwap

  类型：布尔值

  有效值：true | false

  描述：（可选）如果此参数的值设置为 `true`，则从快照中新创建的卷将替换附加到您的实例的现有根卷。
- InstanceId

  类型：字符串

  说明：（必需）要从快照复原的实例的 ID。
- LookForInstanceStatusCheck

  类型：布尔值

  有效值：true | false

  默认值：True

描述：（可选）如果此参数的值设置为 true，则自动化将检查从快照启动的测试实例的实例状态检查是否失败。

- SkipSnapshotsBy

  类型：字符串

  描述：（可选）搜索快照以恢复实例时跳过快照的时间间隔。例如，如果有 100 个快照可用，且您为此参数指定的值为 2，则每三张快照就会被审查一次。

  原定设置值：0

- SnapshotId

  类型：字符串

  描述：（可选）要从中复原实例的快照的 ID。

- StartDate

  类型：字符串

  描述：（可选）要自动化查看快照的最早日期。

- TotalSnapshotsToLook

  类型：字符串

  描述：（可选）自动化审查的快照数。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation
- ec2:AttachVolume
- ec2:CreateImage
- ec2:CreateTags
- ec2:CreateVolume

- ec2:DeleteTags
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeImages
- ec2:DescribeSnapshots
- ec2:DescribeVolumes
- ec2:DetachVolume
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudwatch:GetMetricData

文档步骤

1. aws:executeAwsApi - 收集有关目标实例的详细信息。
2. aws:assertAwsResourceProperty - 验证目标实例是否存在。
3. aws:assertAwsResourceProperty - 验证根卷是否为 Amazon EBS 卷。
4. aws:assertAwsResourceProperty - 验证另一个针对此实例的自动化是否尚未运行。
5. aws:executeAwsApi - 标记目标实例。
6. aws:executeAwsApi - 创建实例的 AMI。
7. aws:executeAwsApi - 收集有关在上一步创建的 AMI 的详细信息。
8. aws:waitForAwsResourceProperty - 等待 AMI 状态变为 available 后再继续。
9. aws:executeScript - 从新创建的实例 AMI 启动一个新实例。
10. aws:assertAwsResourceProperty - 验证实例状态为 available。
11. aws:executeAwsApi - 收集有关新启动实例的详细信息。
12. aws:branch - 根据您是否为 SnapshotId 参数提供了值进行分支。
13. aws:executeScript - 返回指定时间段内快照的列表。
14. aws:executeAwsApi - 停止实例。
15. aws:waitForAwsResourceProperty - 等待卷状态处于 available。

16. aws:waitForAwsResourceProperty - 等待实例状态处于 stopped。
17. aws:executeAwsApi - 分离根卷。
18. aws:waitForAwsResourceProperty - 等待根卷被分离。
19. aws:executeAwsApi - 附加新的根卷。
20. aws:waitForAwsResourceProperty - 等待新卷被附加。
21. aws:executeAwsApi - 启动实例。
22. aws:waitForAwsResourceProperty - 等待实例状态处于 available。
23. aws:waitForAwsResourceProperty - 等待通过实例的系统和实例状态检查。
24. aws:executeScript - 运行脚本以查找可用于成功创建卷的快照。
25. aws:executeScript - 运行脚本，以使用根据自动化识别的快照新创建的卷，或使用根据您在 SnapshotId 参数中指定的快照创建的卷来恢复实例。
26. aws:executeScript - 删除此自动化创建的资源。

输出

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

描述

AWSSupport-SendLogBundleToS3Bucket 运行手册将 EC2Rescue 工具生成的日志包从目标实例上传到指定的 S3 存储桶。运行手册基于目标实例的平台安装 EC2Rescue 的平台特定版本。然后使用 EC2Rescue 收集所有可用的操作系统 (OS) 日志。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  说明：（必需）要从其收集日志的 Windows 或 Linux 托管实例的 ID。
- S3BucketName

  类型：字符串

  说明：（必需）要将日志上传到的 S3 存储桶。
- S3Path

  类型：字符串

  默认：`AWSSupport-SendLogBundleToS3Bucket/`

  说明：（可选）收集的日志的 S3 路径。

所需的 IAM 权限

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

建议接收命令的 EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。用户必须至少具有 ssm:StartAutomationExecution 和 ssm:SendCommand 才能运行此

Automation 并将命令发送到实例，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。

文档步骤

1. aws:runCommand - 通过 AWS-ConfigureAWSPackage 安装 EC2Rescue。
2. aws:runCommand - 运行 PowerShell 脚本以使用 EC2Rescue 收集 Windows 故障排除日志。
3. aws:runCommand - 运行 bash 脚本以使用 EC2Rescue 收集 Linux 故障排除日志。

输出

collectAndUploadWindowsLogBundle.Output

collectAndUploadLinuxLogBundle.Output

AWSSupport-StartEC2RescueWorkflow

描述

AWSSupport-StartEC2RescueWorkflow 运行手册在创建的帮助程序实例上运行提供 base64 编码脚本（Bash 或 Powershell）以修复实例。实例的根卷已附加并挂载到帮助程序实例（也称为 EC2Rescue 实例）。如果实例是 Windows，请提供 Powershell 脚本。否则，请使用 Bash。运行手册会设置一些可供脚本使用的环境变量。环境变量包含有关您提供的输入的信息，以及有关离线根卷的信息。离线卷已挂载，可供使用。例如，您可以将 Desired State Configuration 文件保存到离线 Windows 根卷，或 chroot 到一个离线 Linux 根卷并执行离线修复。

运行此自动化（控制台）

> **Important**
> 此自动化不支持从 Marketplace 亚马逊机器映像（AMI）创建的 Amazon EC2 实例。

附加信息

要对脚本进行 base64 编码，可以使用 Powershell 或 Bash。Powershell：

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::Rea
```

Bash：

```
base64 PATH_TO_FILE
```

下面是您可以在离线脚本中使用的环境变量列表，具体视目标操作系统而定

Windows:

变量	描述	示例值
$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	EC2Rescue for Windows 安装路径	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EC2RW_DIR	EC2Rescue for Windows 安装路径	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	离线 Windows 目前控制设置路径	`HKLM:\AWSTempSystem\ControlSet001`
$env:EC2RESCUE_OFFLINE_DRIVE	离线 Windows 驱动器号	D:\
$env:EC2RESCUE_OFFLINE_EBS_DEVICE	离线根卷 EBS 设备	xvdf
$env:EC2RESCUE_OFFLINE_KERNEL_VER	离线 Windows 内核版本	6.1.7601.24214
$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	离线 Windows 架构	AMD64

变量	描述	示例值
$env:EC2RESCUE_OFFLINE_OS_CAPTION	离线 Windows 标题	Windows Server 2008 R2（数据中心版）
$env:EC2RESCUE_OFFLINE_OS_TYPE	离线 Windows 操作系统类型	服务器
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	离线 Windows 程序文件目录路径	D:\Program Files
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	离线 Windows 程序文件 x86 目录路径	D:\Program Files (x86)
$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	离线 Windows 注册表目录路径	D:\Windows\System32\config
$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT	离线 Windows 系统根目录路径	D:\Windows
$env:EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket
$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	离线 Windows 安装元数据	客户 Powershell 对象

Linux：

变量	描述	示例值
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	EC2Rescue for Linux 安装路径	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	离线设备名称	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	离线根卷 EBS 设备	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	离线根卷挂载点	/mnt/mount
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

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AMIPrefix

  类型：字符串

  默认值：`AWSSupport-EC2Rescue`

  描述：（可选）备份 AMI 名称的前缀。
- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
- CreatePostEC2RescueBackup

  类型：字符串

  有效值：true | false

  原定设置值：false

  描述：（可选）将其设置为 `true` 可在运行脚本后、启动其前创建 InstanceId 的 AMI。Automation 完成后，AMI 仍将存在。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。
- CreatePreEC2RescueBackup

  类型：字符串

  有效值：true | false

  原定设置值：false

  描述：（可选）将其设置为 `true` 可在运行脚本前创建 InstanceId 的 AMI。Automation 完成后，AMI 仍将存在。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。
- EC2RescueInstanceType

类型：字符串

有效值：t2.small | t2.medium | t2.large

默认值：t2.small

描述：（可选）EC2Rescue 实例的 EC2 实例类型。

- InstanceId

  类型：字符串

  描述：（必需）您的 EC2 实例的 ID。重要信息：AWS Systems Manager Automation 会停止此实例。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- OfflineScript

  类型：字符串

  描述：（必需）将对帮助程序实例运行的 Base64 编码的脚本。如果源实例为 Linux，使用 Bash；如果为 Windows，则使用 PowerShell。

- S3BucketName

  类型：字符串

  描述：（可选）您账户中用于上传故障排除日志的 S3 存储桶的名称。请确保存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- S3Prefix

  类型：字符串

  默认值：`AWSSupport-EC2Rescue`

  描述：（可选）S3 日志的前缀。

- SubnetId

  类型：字符串

  默认值：SelectedInstanceSubnet

描述：（可选）EC2Rescue 实例的子网 ID。默认情况下，使用提供的实例所在的同一子网。重要描述：如果提供了自定义子网，则其必须与 InstanceId 位于同一可用区中，并且必须允许访问 SSM 终端节点。

- UniqueId

  类型：字符串

  默认值：{{ automation:EXECUTION_ID }}

  描述：（可选）用于自动化的唯一标识符。

所需的 IAM 权限

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

建议为运行 Automation 的用户附加 AmazonSSMAutomationRole IAM 托管策略。除了此策略以外，用户还必须：

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

文档步骤

1. aws:executeAwsApi - 描述提供的实例
2. aws:executeAwsApi - 描述提供的实例的根卷
3. aws:assertAwsResourceProperty - 检查根卷设备类型是否为 EBS
4. aws:assertAwsResourceProperty - 检查根卷是否未加密
5. aws:assertAwsResourceProperty - 检查提供的子网 ID
   a. （使用当前实例子网）- 如果 *SubnetId = SelectedInstanceSubnet*，则运行 aws:createStack 来部署 EC2Rescue CloudFormation 堆栈
   b. （创建新的 VPC）- 如果 *SubnetId = CreateNewVPC*，然后运行 aws:createStack 来部署 EC2Rescue CloudFormation 堆栈
   c. （使用自定义子网）- 在所有其他情况下：

      aws:assertAwsResourceProperty - 检查提供的子网是否与提供的实例位于同一可用区中

      aws:createStack - 部署 EC2Rescue CloudFormation 堆栈
6. aws:invokeLambdaFunction - 执行额外输入验证
7. aws:executeAwsApi - 更新 EC2Rescue CloudFormation 堆栈来创建 EC2Rescue 帮助程序实例
8. aws:waitForAwsResourceProperty - 等待 EC2Rescue CloudFormation 堆栈完成更新
9. aws:executeAwsApi - 描述 EC2Rescue CloudFormation 堆栈输出来获取 EC2Rescue 帮助程序实例 ID
10. aws:waitForAwsResourceProperty - 等待 EC2Rescue 帮助程序实例变为托管实例
11. aws:changeInstanceState - 停止提供的实例
12. aws:changeInstanceState - 停止提供的实例
13. aws:changeInstanceState - 强制停止提供的实例
14. aws:assertAwsResourceProperty - 检查 createPreec2RescueBackup 输入值

a. （创建前 EC2Rescue 备份）- 如果 *CreatePreEC2RescueBackup = true*

b. aws:executeAwsApi - 创建提供的实例的 AMI 备份

c. aws:createTags - 标记 AMI 备份

15. aws:runCommand - 在 EC2Rescue 帮助程序实例上安装 EC2Rescue

16. aws:executeAwsApi - 从提供的实例分离根卷

17. aws:assertAwsResourceProperty - 检查提供的实例平台

a. （实例为 Windows）：

aws:executeAwsApi - 将根卷作为 *xvdf* 附加到 EC2Rescue 帮助程序实例

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Powershell 中运行提供的离线脚本

b. （实例为 Linux）：

aws:executeAwsApi - 将根卷作为 */dev/sdf* 附加到 EC2Rescue 帮助程序实例

aws:sleep - 休眠 10 秒

aws:runCommand - 在 Bash 中运行提供的离线脚本

18. aws:changeInstanceState - 停止 EC2Rescue 帮助程序实例

19. aws:changeInstanceState - 强制停止 EC2Rescue 帮助程序实例

20. aws:executeAwsApi - 从 EC2Rescue 帮助程序实例中分离根卷

21. aws:executeAwsApi - 将根卷附加回提供的实例

22. aws:assertAwsResourceProperty - 检查 createPostec2RescueBackup 输入值

a. （在运行 EC2Rescue 后创建备份）- 如果 *CreatePostEC2RescueBackup = True*

b. aws:executeAwsApi - 创建提供的实例的 AMI 备份

c. aws:createTags - 标记 AMI 备份

23. aws:executeAwsApi - 为提供的实例的根卷恢复初始的终止时删除状态

24. aws:changeInstanceState - 将提供的实例恢复为初始状态（运行/停止）

25. aws:deleteStack - 删除 EC2Rescue CloudFormation 堆栈

输出

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

描述

AWSPremiumSupport-TroubleshootEC2DiskUsage 运行手册可帮助您调查并有可能纠正 Amazon Elastic Compute Cloud (Amazon EC2) 实例根磁盘和非根磁盘使用方面的问题。如果可能，运行手册会尝试通过扩展卷及其文件系统来纠正问题。为执行这些任务，此运行手册会根据受影响实例的操作系统协调执行多个运行手册。

第一个运行手册（AWSPremiumSupport-DiagnoseDiskUsageOnWindows或AWSPremiumSupport-DiagnoseDiskUsageOnLinux）确定是否可以通过扩展卷来缓解磁盘问题。

第二个运行手册（AWSPremiumSupport-ExtendVolumesOnWindows或AWSPremiumSupport-ExtendVolumesOnLinux）使用第一个运行手册的输出来运行可修改卷的 Python 代码。修改卷后，运行手册会扩展受影响卷的分区和文件系统。

> **Important**
>
> 访问 AWSPremiumSupport-* 运行手册需要订阅 Enterprise 或 Business Support。有关更多信息，请参阅比较 AWS Support 计划。

本文档与 AWS Managed Services (AMS) 合作编写。AMS 可帮助您更高效、更安全地管理AWS基础架构。AMS 还提供操作灵活性、增强的安全性和合规性、容量优化和成本节约识别功能。有关更多信息，请参阅AWS Managed Services。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- InstanceId

  类型：字符串

  允许的值：^i-[a-z0-9]{8,17}$

  说明：（必需）您的 Amazon EC2 实例的 ID。
- VolumeExpansionEnabled

  类型：布尔值

  描述：（可选）用于控制文档是否扩展受影响的卷和分区的标志。

  默认值：True
- VolumeExpansionUsageTrigger

  类型：字符串

  描述：（可选）触发扩展所需的分区空间的最小使用量（以百分比表示）。

  允许的值：^[0-9]{1,2}$

  默认：85
- VolumeExpansionCapSize

  类型：字符串

  （可选）：（可选）可以将 Amazon Elastic Block Store (Amazon EBS) 卷增加到的最大大小（以 GiB 为单位）。

  允许的值：^[0-9]{1,4}$

  默认：2048
- VolumeExpansionGibIncrease

  类型：字符串

Description (描述)：（可选）卷容量增加，以 GiB 为单位。将使用介于 VolumeExpansionGibIncrease 和 VolumeExpansionPercentageIncrease 之间的最大净增加量。

允许的值：^[0-9]{1,4}$

原定设置值：20

- VolumeExpansionPercentageIncrease

  类型：字符串

  描述：（可选）卷的百分比增大。将使用介于 VolumeExpansionGibIncrease 和 VolumeExpansionPercentageIncrease 之间的最大净增加量。

  允许的值：^[0-9]{1,2}$

  原定设置值：20

- AutomationAssumeRole

  类型：字符串

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

所需的 IAM 权限

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

- ec2:DescribeVolumes
- ec2:DescribeVolumesModifications
- ec2:ModifyVolume
- ec2:DescribeInstances
- ec2:CreateImage
- ec2:DescribeImages
- ec2:DescribeTags
- ec2:CreateTags
- ec2:DeleteTags

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationExecutions
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations

文档步骤

1. aws:assertAwsResourceProperty - 检查实例是否由 Systems Manager 管理
2. aws:executeAwsApi - 描述要获取平台的实例。
3. aws:branch - 根据实例平台对自动化进行分支。
   a. 如果实例是 Windows：
      i. aws:executeAutomation - 运行 AWSPremiumSupport-DiagnoseDiskUsageOnWindows 运行手册以诊断实例上的磁盘使用问题。
      ii. aws:executeAwsApi - 获取上一个自动化的输出。
      iii. aws:branch - 根据诊断结果进行分支，以及是否存在可以扩展以缓解警报的音量。
         A. 没有需要扩展的卷：结束自动化。
         B. 以下是需要扩展的卷：
            I. aws:executeAwsApi - 创建实例的 Amazon Machine Image (AMI)。
            II. aws:waitForAwsResourceProperty - 等待 AMI 状态变为 available。
            III. aws:executeAutomation - 运行 AWSPremiumSupport-ExtendVolumesOnWindows 运行手册以执行卷修改以及在操作系统 (OS) 中执行使新空间可用的所需步骤。
   b. （平台不是窗口）如果输入实例不是 Windows：
      i. aws:executeAutomation - 运行 AWSPremiumSupport-DiagnoseDiskUsageOnLinux 运行手册以诊断实例上的磁盘使用问题。
      ii. aws:executeAwsApi - 获取上一个自动化的输出。
      iii. aws:branch - 根据诊断结果进行分支，以及是否存在可以扩展以缓解警报的音量。
         A. 没有需要扩展的卷：结束自动化。

B. 以下是需要扩展的卷：

I. `aws:executeAwsApi` - 创建实例的 AMI。

II. `aws:waitForAwsResourceProperty` - 等待 AMI 状态变为 `available`。

III. `aws:executeAutomation` -运行 `AWSPremiumSupport-ExtendVolumesOnLinux` 运行手册以执行卷修改以及在操作系统中执行使新空间可用所需的步骤。

输出

diagnoseDiskUsageAlertOnWindows.Output

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Output

extendVolumesOnLinux.Output

BackupAMILinux.ImageId

BackupAMIWindows.ImageId

AWSSupport-TroubleshootEC2InstanceConnect

描述

`AWSSupport-TroubleshootEC2InstanceConnect`自动化有助于分析和检测阻止使用 Amazon EC2 Instance Connect 连接到亚马逊弹性计算云 (Amaz on EC 2) 实例的错误。它可以识别由不支持的亚马逊系统映像 (AMI)、缺少操作系统级软件包安装或配置、缺少 AWS Identity and Access Management (IAM) 权限或网络配置问题导致的问题。

如何工作？

该运行手册采用 IAM 角色或在 Amazon EC2 Instance Connect 中遇到问题的用户的 Amazon EC2 实例 ID、用户名、连接模式、源 IP CIDR、SSH 端口和亚马逊资源名称 (ARN)。然后，它会检查使用 Amazon EC2 Instance Connect 连接到 Amazon EC2 实例的先决条件：

- 该实例正在运行且处于正常状态。
- 该实例位于 Amazon EC2 Instance Connect 支持的AWS区域。
- Amazon EC2 Instance Connect 支持该实例的 AMI。
- 该实例可以访问实例元数据服务 (imdsv2)。
- Amazon EC2 Instance Connect 软件包已在操作系统级别正确安装和配置。

- 网络配置（安全组、网络 ACL 和路由表规则）允许通过 Amazon EC2 Instance Connect 连接到实例。
- 用于利用 Amazon EC2 Instance Connect 的 IAM 角色或用户有权将密钥推送到 Amazon EC2 实例。

Important

- 要检查实例 AMI、imdsv2 的可访问性和 Amazon EC2 Instance Connect 软件包的安装，该实例必须由 SSM 托管。否则，它会跳过这些步骤。有关更多信息，请参阅为什么我的 Amazon EC2 实例没有显示为托管节点。
- 只有将 SourceIp CIDR 作为输入参数提供时，网络检查才会检测安全组和网络 ACL 规则是否会阻止流量。否则，它将仅显示与 SSH 相关的规则。
- 本运行手册中未验证使用 Amazon EC2 Instance Connect 终端节点的连接。
- 对于私有连接，自动化不会检查源计算机上是否安装了 SSH 客户端，以及它是否可以访问实例的私有 IP 地址。

文档类型

自动化

所有者

Amazon

平台

Linux

参数

所需的 IAM 权限

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

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand

说明

按照这些步骤对自动化进行配置：

1. 导航到AWS Systems Manager控制台AWSSupport-TroubleshootEC2InstanceConnect中的。
2. 选择 Execute automation（执行自动化）。
3. 对于输入参数，请输入以下内容：
   - InstanceId （必填）：

     您无法使用 Amazon EC2 Instance Connect 连接到的目标 Amazon EC2 实例的 ID。
   - AutomationAssumeRole （可选）：

     允许 Systems Manager Automation 代表你执行操作的 IAM 角色的 ARN。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
   - 用户名（必填）：

     用于使用 Amazon EC2 Instance Connect 连接到亚马逊 EC2 实例的用户名。它用于评估是否向该特定用户授予 IAM 访问权限。
   - EC2InstanceConnectRoleOrUser （必填）：

     利用 Amazon EC2 Instance Connect 向实例推送密钥的 IAM 角色或用户的 ARN。
   - sshPort（可选）：

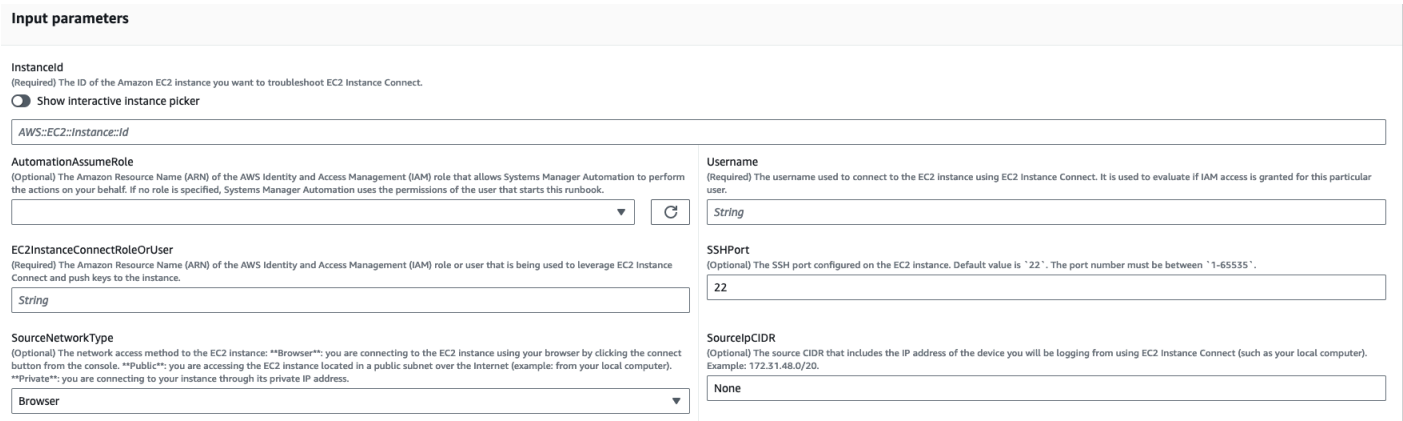
     在 Amazon EC2 实例上配置的 SSH 端口。默认值为 22。端口号必须介于两者之间1-65535。
   - SourceNetworkType （可选）：

     Amazon EC2 实例的网络访问方法：

- 浏览器：您可以从AWS管理控制台进行连接。
- 公用：您通过 Internet 连接到位于公有子网中的实例（例如，您的本地计算机）。
- 私有：您通过实例的私有 IP 地址进行连接。

- SourceIpCIDR（可选）：

  源 CIDR，包括您将使用 Amazon EC2 Instance Connect 登录的设备（例如您的本地计算机）的 IP 地址。示例：172.31.48.6/32。如果公有或私有访问模式未提供任何值，则运行手册将不会评估 Amazon EC2 实例安全组和网络 ACL 规则是否允许 SSH 流量。它将改为显示与 SSH 相关的规则。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- AssertInitialState:

  确保 Amazon EC2 实例的状态处于运行状态。否则，自动化将结束。

- GetInstanceProperties:

  获取当前 Amazon EC2 实例的属性（PlatformDetails PublicIpAddress VpcId、、 SubnetId 和 MetadataHttpEndpoint）。

- GatherInstanceInformationFromSSM：

  如果该实例由 SSM 托管，则获取 Systems Manager 实例的 ping 状态和操作系统详细信息。

- CheckIfAWSRegionSupported:

  检查 Amazon EC2 实例是否位于 Amazon EC2 Instance Connect 支持的AWS区域。

- BranchOnIfAWSRegionSupported:

如果 Amazon EC2 Inst AWS ance Connect 支持该区域，则继续执行。否则，它会创建输出并退出自动化。

- CheckIfInstanceAMIIsSupported：

  检查 Amazon EC2 Instance Connect 是否支持与该实例关联的 AMI。

- BranchOnIfInstanceAMIIsSupported：

  如果支持实例 AMI，它将执行操作系统级别的检查，例如元数据可访问性以及 Amazon EC2 Instance Connect 软件包的安装和配置。否则，它会使用 AWS API 检查是否启用了 HTTP 元数据，然后进入网络检查步骤。

- checkIMDReachabilityFromOs：

  在目标 Amazon EC2 Linux 实例上运行 Bash 脚本以检查它是否能够访问 imdsv2。

- checke PackageInstallation IC：

  在目标 Amazon EC2 Linux 实例上运行 Bash 脚本，以检查 Amazon EC2 Instance Connect 软件包是否已正确安装和配置。

- checkSSHConfigFromOs：

  在目标 Amazon EC2 Linux 实例上运行 Bash 脚本，以检查配置的 SSH 端口是否与输入参数 “sshPort” 相匹配。`

- CheckMetadataHTTPEndpointIsEnabled:

  检查实例元数据服务 HTTP 端点是否已启用。

- checke NetworkAccess IC：

  检查网络配置（安全组、网络 ACL 和路由表规则）是否允许通过 Amazon EC2 Instance Connect 连接到实例。

- checki RoleOrUserPermissions AM：

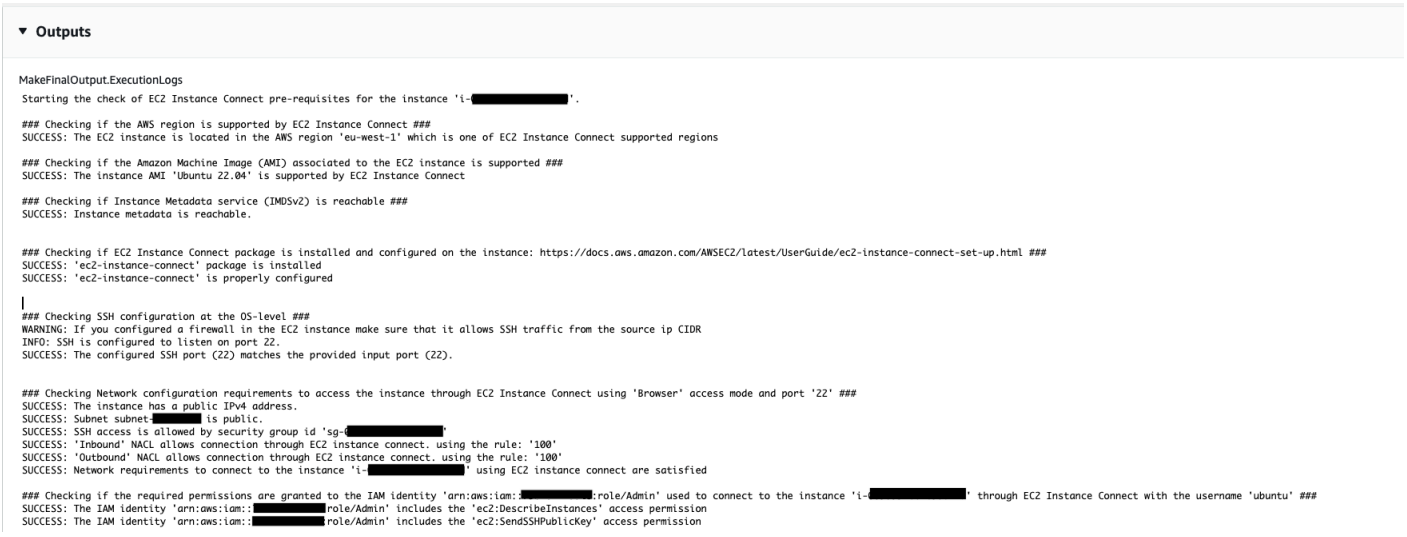
  检查用于利用 Amazon EC2 Instance Connect 的 IAM 角色或用户是否有权使用提供的用户名将密钥推送到 Amazon EC2 实例。

- MakeFinalOutput:

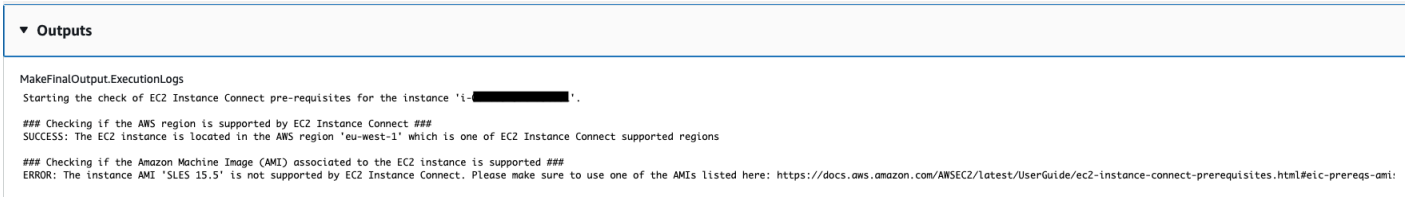
  合并所有先前步骤的输出。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

目标实例具有所有必需先决条件的执行：



在不支持目标实例的 AMI 的情况下执行：



参考

Systems Manager Automation

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

AWS 服务文档

- 如何解决使用 Amazon EC2 Instance Connect 连接到我的 Amazon EC2 实例的问题？

AWSSupport-TroubleshootRDP

描述

AWSSupport-TroubleshootRDP 运行手册允许用户检查或修改目标实例上可能影响远程桌面协议 (RDP) 连接的常规设置，如 RDP 端口、网络层身份验证 (NLA) 和 Windows 防火墙配置文件。（可选）如果用户明确允许进行离线修复，则可以通过停止和启动实例来离线应用更改。默认情况下，此运行手册读取和输出这些设置的值。

> **Important**
>
> 在使用此运行手册之前，应仔细检查对 RDP 设置、RDP 服务和 Windows 防火墙配置文件的更改。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- 操作

  类型：字符串

  有效值：CheckAll | FixAll | Custom

  默认值：Custom

  描述：（可选）[自定义] 使用 Firewall、RDPServiceStartupType、RDPServiceAction、RDPPortAction、NLASettingAction 和 RemoteConnections 中的值来管理设置。[CheckAll] 在不更改设置的值的情况下读取这些值。[FixAll] 恢复 RDP 默认设置并禁用 Windows 防火墙。

- AllowOffline

  类型：字符串

有效值：true | false

原定设置值：false

说明：（可选）仅修复 - 如果当在线故障排除失败或提供的实例不是托管实例时允许进行离线 RDP 修复，请将其设置为 true。注意：对于离线修复，SSM Automation 会停止实例，并在尝试任何操作前创建一个 AMI。

- AutomationAssumeRole

  类型：字符串

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

- 防火墙

  类型：字符串

  有效值：Check | 禁用

  默认值：Check

  说明：（可选）检查或禁用 Windows 防火墙（所有配置文件）。

- InstanceId

  类型：字符串

  说明：（必需）要对其 RDP 设置进行故障排除的实例的 ID。

- NLASettingAction

  类型：字符串

  有效值：Check | 禁用

  默认值：Check

  说明：（可选）检查或禁用网络层身份验证 (NLA)。

- RDPPortAction

  类型：字符串

有效值：Check | 修改

默认值：Check

说明：（可选）检查用于 RDP 连接的当前端口，或将 RDP 端口修改回 3389 并重启服务。

- RDPServiceAction

  类型：字符串

  有效值：Check | 启动 | 重启 | 强制重启

  默认值：Check

  说明：（可选）检查、启动、重启或强制重启 RDP 服务 (TermService)。

- RDPServiceStartupType

  类型：字符串

  有效值：Check | 自动

  默认值：Check

  说明：（可选）检查或设置 RDP 服务在 Windows 启动时自动启动。

- RemoteConnections

  类型：字符串

  有效值：Check | 启用

  默认值：Check

  说明：（可选）要对 fDenyTSConnections 设置执行的操作：Check、Enable。

- S3BucketName

  类型：字符串

  说明：（可选）仅离线 - 您账户中用于上传故障排除日志的 S3 存储桶的名称。请确保存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

类型：字符串

默认值：SelectedInstanceSubnet

说明：（可选）仅离线 - 用于执行离线故障排除的 EC2Rescue 实例的子网 ID。如果未指定子网 ID，AWS Systems Manager Automation 将创建一个新 VPC。重要说明：子网必须与 InstanceId 位于同一可用区中，并且必须允许访问 SSM 终端节点。

所需的 IAM 权限

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

建议接收命令的 EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。对于在线修复，用户必须至少具有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution 和 ssm:SendCommand 才能运行此 Automation 并将命令发送到实例，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。对于离线修复，用户必须至少具有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution、ec2:DescribeInstances 以及 ssm:GetAutomationExecution 才能读取自动化输出。AWSSupport-TroubleshootRDP 调用 AWSSupport-ExecuteEC2Rescue 以执行离线修复 — 请查看 AWSSupport-ExecuteEC2Rescue 的权限以确保您可以成功运行自动化。

文档步骤

1. aws:assertAwsResourceProperty - 检查实例是否为 Windows Server 实例
2. aws:assertAwsResourceProperty - 检查实例是否为托管实例
3. （在线故障排除）如果实例为托管实例，则：
   a. aws:assertAwsResourceProperty - 检查提供的操作值
   b. （在线检查）如果 Action = CheckAll，则：

      aws:runPowerShellScript - 运行 PowerShell 脚本来获取 Windows 防火墙配置文件状态。

      aws:executeAutomation - 调用 AWSSupport-ManageWindowsService 以获取 RDP 服务状态。

      aws:executeAutomation - 调用 AWSSupport-ManageRDPSettings 以获取 RDP 设置。
   c. （在线修复）如果 Action = FixAll，则：

aws:runPowerShellScript - 运行 PowerShell 脚本来禁用所有 Windows 防火墙配置文件。

aws:executeAutomation - 调用 AWSSupport-ManageWindowsService 以启动 RDP 服务。

aws:executeAutomation - 调用 AWSSupport-ManageRDPSettings 以启用远程连接并禁用 NLA。

d. （在线管理）如果 Action = Custom，则：

aws:runPowerShellScript - 运行 PowerShell 脚本来管理 Windows 防火墙配置文件。

aws:executeAutomation - 调用 AWSSupport-ManageWindowsService 以管理 RDP 服务。

aws:executeAutomation - 调用 AWSSupport-ManageRDPSettings 以管理 RDP 设置。

4. （离线修复）如果实例并非托管实例，则：

a. aws:assertAwsResourceProperty - 断言AllowOffline = true

b. aws:assertAwsResourceProperty - 断言 Action = FixAll

c. aws:assertAwsResourceProperty - 断言 SubnetId 的值

（使用提供的实例的子网）如果 SubnetId 为 SELECTED_INSTANCE_SUBNET

aws:executeAwsApi - 检索当前实例的子网。

aws:executeAutomation - 使用提供的实例的子网运行 AWSSupport-ExecuteEC2Rescue。

d. （使用提供的自定义子网）如果 SubnetId 不为 SELECTED_INSTANCE_SUBNET

aws:executeAutomation - 使用提供的 SubnetId 值运行 AWSSupport-ExecuteEC2Rescue。

输出

manageFirewallProfiles.Output

manageRDPServiceSettings.Output

manageRDPSettings.Output

checkFirewallProfiles.Output

checkRDPServiceSettings.Output

checkRDPSettings.Output

disableFirewallProfiles.Output

restoreDefaultRDPServiceSettings.Output

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

描述

AWSSupport-TroubleshootSSH 运行手册安装适用于 Linux 的 Amazon EC2Rescue工具，使用该工具检查或尝试修复阻止通过 SSH 远程连接到 Linux 计算机的常见问题。（可选）如果用户明确允许进行离线修复，则可以通过停止和启动实例来离线应用更改。默认情况下，运行手册以只读模式运行。

运行此自动化（控制台）

有关使用 AWSSupport-TroubleshootSSH 运行手册的信息，请参阅来自 AWS Premium Support 的此 AWSSupport-TroubleshootSSH故障排除主题。

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- 操作

类型：字符串

有效值：CheckAll | FixAll

默认值：CheckAll

说明：（必需）指定只检查而不修复问题还是检查并自动修复任何发现的问题。

- AllowOffline

  类型：字符串

  有效值：true | false

  原定设置值：false

  说明：（可选）仅修复 - 如果当在线故障排除失败或提供的实例不是托管实例时允许进行离线 SSH 修复，请将其设置为 true。注意：对于离线修复，SSM Automation 会停止实例，并在尝试任何操作前创建一个 AMI。

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  说明：（必需）您的 Linux EC2 实例的 ID。

- S3BucketName

  类型：字符串

  说明：（可选）仅离线 - 您账户中用于上传故障排除日志的 S3 存储桶的名称。请确保存储桶策略不会向不需要访问收集的日志的各方授予不必要的读/写权限。

- SubnetId

  类型：字符串

默认值：SelectedInstanceSubnet

说明：（可选）仅离线 - 用于执行离线故障排除的 EC2Rescue 实例的子网 ID。如果未指定子网 ID，AWS Systems Manager Automation 将创建一个新 VPC。

> **Important**
>
> 子网必须与 InstanceId 位于同一可用区中，并且必须允许访问 SSM 终端节点。

所需的 IAM 权限

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

建议接收命令的 EC2 实例具有一个附加了 AmazonSSMManagedInstanceCore Amazon 托管策略的 IAM 角色。对于在线修复，用户必须至少具有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution 和 ssm:SendCommand 才能运行此 Automation 并将命令发送到实例，并且需要具有 ssm:GetAutomationExecution 才能读取 Automation 输出。对于离线修复，用户必须至少具有 ssm:DescribeInstanceInformation、ssm:StartAutomationExecution、ec2:DescribeInstances 以及 ssm:GetAutomationExecution 才能读取自动化输出。`AWSSupport-TroubleshootSSH` 调用 `AWSSupport-ExecuteEC2Rescue` 以执行离线修复 — 请查看 `AWSSupport-ExecuteEC2Rescue` 的权限以确保您可以成功运行自动化。

文档步骤

1. `aws:assertAwsResourceProperty` - 检查实例是否为托管实例
   a. （在线修复）如果实例为托管实例，则：
      i. `aws:configurePackage` - 通过 `AWS-ConfigureAWSPackage` 安装适用于 Linux 的 EC2Rescue。
      ii. `aws:runCommand` - 运行 bash 脚本来运行适用于 Linux 的 EC2Rescue。
   b. （离线修复）如果实例并非托管实例，则：
      i. `aws:assertAwsResourceProperty` - 断言AllowOffline = true
      ii. `aws:assertAwsResourceProperty` - 断言 Action = FixAll
      iii. `aws:assertAwsResourceProperty` - 断言 SubnetId 的值

iv. （使用提供的实例的子网）如果 SubnetId 为 SelectedInstanceSubnet，则使用 `aws:executeAutomation` 通过提供的实例的子网运行 `AWSSupport-ExecuteEC2Rescue`。

v. （使用提供的自定义子网）如果 SubnetId 不是 SelectedInstanceSubnet，则使用 `aws:executeAutomation` 通过提供的子网值运行 `AWSSupport-ExecuteEC2Rescue`。

输出

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSSupport-TroubleshootSUSERegistration

描述

`AWSSupport-TroubleshootSUSERegistration` 运行手册可帮助您查明向 SUSE Update Infrastructure 注册 Amazon Elastic Compute Cloud (Amazon EC2) SUSE Linux Enterprise Server 实例失败的原因。此自动化输出提供了解决问题或帮助您排查问题的步骤。如果实例在自动化期间通过了所有检查，该实例将注册到 SUSE Update Infrastructure。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  描述：（必需）需要排除故障的 Amazon EC2 实例 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:DescribeInstanceProperties
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:ListCommands

文档步骤

- aws:assertAwsResourceProperty - 检查 Amazon EC2 实例是否由 AWS Systems Manager 管理。
- aws:runCommand - 检查 Amazon EC2 实例平台是否由 SLES 管理。
- aws:runCommand - 检查软件包 cloud-regionsrv-client 版本是否高于或等于所需的版本 9.0.10。
- aws:runCommand - 检查基础产品的符号链接是否损坏，并在链接损坏时修复链接。
- aws:runCommand - 检查主机文件 (/etc/hosts) 是否包含 smt-ec2-suscloud.net 的记录。自动化将删除所有重复的条目。
- aws:runCommand - 检查 curl 命令是否已安装。
- aws:runCommand - 检查 Amazon EC2 实例是否能访问实例元数据服务（IMDS）地址 169.254.169.254。
- aws:runCommand - 检查 Amazon EC2 实例是否有账单代码或 AWS Marketplace 产品代码。

- aws:runCommand - 检查 Amazon EC2 实例是否可以通过 HTTPS 到达至少 1 个区域服务器。
- aws:runCommand - 检查 Amazon EC2 实例是否可以通过 HTTP 到达订阅管理工具 (SMT) 服务器。
- aws:runCommand - 检查 Amazon EC2 实例是否可以通过 HTTPS 到达订阅管理工具 (SMT) 服务器。
- aws:runCommand - 检查 Amazon EC2 实例是否可以通过 HTTPS 到达 smt-ec2.susecloud.net 地址。
- aws:runCommand - 向 SUSE Update Infrastructure 注册 Amazon EC2 实例。
- aws:executeScript - 收集并输出所有先前步骤的输出。

AWSSupport-TroubleshootWindowsPerformance

描述

该运行手册AWSSupport-TroubleshootWindowsPerformance有助于解决亚马逊弹性计算云 (Amazon EC2) Windows 实例上持续存在的性能问题。运行手册从目标实例捕获日志，并分析 CPU、内存、磁盘和网络性能指标。或者，自动化可以捕获进程转储，以帮助您确定性能下降的潜在原因。如果您允许安装此运行手册，则自动化还会使用最新的EC2Rescue工具捕获事件和系统日志。

如何工作？

运行手册执行以下步骤：

- 检查 Amazon EC2 实例的先决条件。
- 在 Amazon EC2 Windows 实例的根磁盘中生成性能日志
- 将捕获的日志存储在文件夹中 C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance
- 如果提供了亚马逊简单存储服务 (Amazon S3) Service 存储桶，并且自动代入角色具有所需的权限，则捕获的日志将上传到 Amazon S3 存储桶。
- 将最新EC2Rescue工具安装到 Amazon EC2 Windows 实例，用于捕获事件和系统日志（如果您选择安装），但它不会分析所捕获的进程转储和日志EC2Rescue。

Important

- 要执行本运行手册，Amazon EC2 Windows 实例必须由 AWS Systems Manager管理。有关更多信息，请参阅为什么我的 Amazon EC2 实例没有显示为托管节点。
- 要执行本运行手册，Amazon EC2 Windows 实例必须在 Windows 8.1/ Windows Server 2012 R2 (6.3) 或更高版本上运行 PowerShell 4.0 或更高版本。有关更多信息，请参阅 Windows 操作系统版本。
- 要生成性能日志，根设备上至少需要 10 GB 的可用空间。如果根磁盘大于 100 GB，则可用空间必须大于磁盘大小的 10%。如果您在执行过程中转储进程，则可用空间必须大于 10 GB，再加上该进程消耗的内存总量（当该进程消耗的内存超过 10 GB 时）。
- 根设备上生成的日志不会自动删除。
- 运行手册不会卸载该EC2Rescue工具。有关更多信息，请参阅用EC2Rescue于 Windows 服务器。
- 最佳做法是在性能影响期间运行此自动化。您也可以使用 AWS Systems Manager 状态管理器关联或通过安排 AWS Systems Manager 维护窗口来定期运行它。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

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

- `ec2:DescribeInstances`
- `ssm:DescribeAutomationExecutions`

- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand
- s3:ListBucket
- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:PutObject
- s3:GetBucketAcl
- s3:GetAccountPublicAccessBlock

（可选）在实例配置文件上附加的 IAM 角色或在实例上配置的 IAM 用户需要执行以下操作才能将日志上传到为参数指定的 Amazon S3 存储桶*LogUploadBucketName*：

- s3:PutObject
- s3:GetObject
- s3:ListBucket

说明

按照这些步骤对自动化进行配置：

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

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

您要在其中运行自动化的目标 Amazon EC2 Windows 实例的 ID。该实例必须由 Systems Manager 管理才能执行自动化。

- CaptureProcessDump （可选）：

  要捕获的进程转储类型。自动化可以为可能在自动化开始时造成性能影响的流程捕获一个进程转储。实例根卷需要至少 10 GB 的可用空间（当根卷大小大于 100 GB 时，需要大于磁盘大小的 10%；如果进程消耗的内存超过 10 GB，则需要加上 10 GB 加上进程消耗的总内存大小）。

- LogCaptureDuration （可选）：

  问题出现时，此自动化将捕获日志的分钟数，介于1和15之间。默认值为 5。

- LogUploadBucketName （可选）：

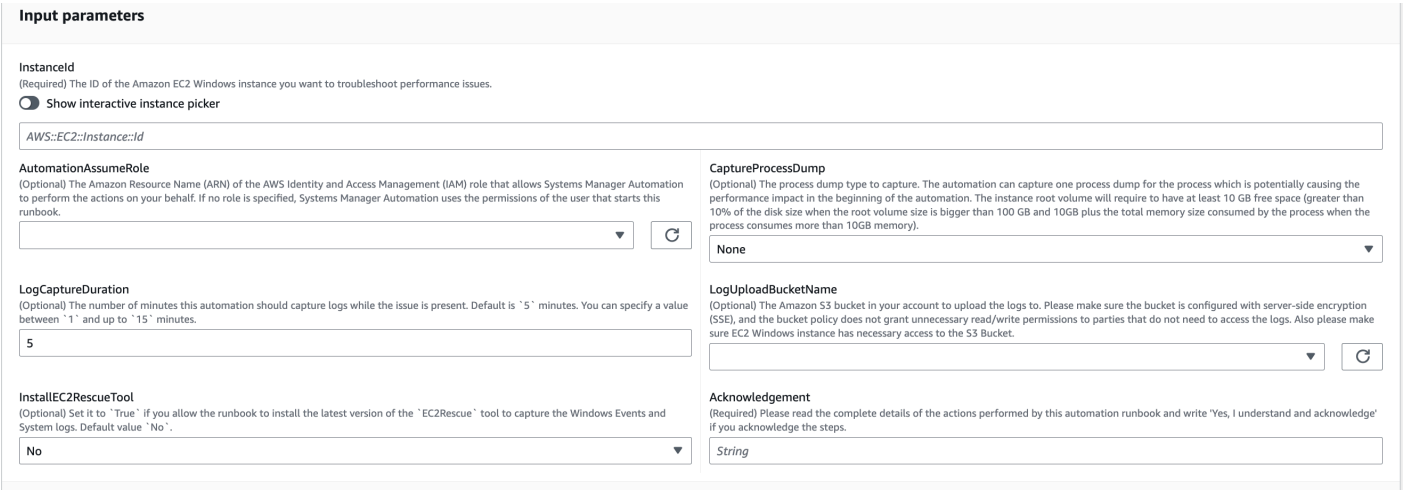
  您账户中您要上传日志的 Amazon S3 存储桶。存储桶必须配置服务器端加密 (SSE)，并且存储桶策略不得向不需要访问捕获日志的各方授予不必要的读/写权限。亚马逊 EC2 Windows 实例必须有权访问亚马逊 S3 存储桶。

- 安装 EC2RescueTool （可选）：

  设置为Yes允许运行手册安装该EC2Rescue工具的最新版本以捕获 Windows 事件和系统日志。默认值为 No。

- 致谢（必填）：

  阅读本自动化操作手册所执行操作的完整详细信息，如果您同意，请键入Yes, I understand and acknowledge。



4. 选择执行。
5. 自动化启动。

6. 文档将执行以下步骤：

- **CheckConcurrency:**

  确保只有一次针对该实例执行此运行手册。如果运行手册发现另一个针对同一实例的执行，它将返回错误并结束。

- **AssertInstanceIsWindows:**

  断言 Amazon EC2 实例在 Windows 操作系统上运行。否则，自动化将结束。

- **AssertInstanceIsManagedInstance:**

  断言 Amazon EC2 实例由管理。 AWS Systems Manager否则，自动化将结束。

- **VerifyPrerequisites:**

  验证实例操作系统上的 PowerShell 版本，并确保可以通过 Systems Manager 连接实例以运行 PowerShell 命令。此自动化支持在 Windows 8.1 /Server 2012 R2 (6.3) 或更高版本上运行 PowerShell 4.0 及更高版本。如果版本较旧，则自动化将失败。当您选择将日志上传到 Amazon S3 存储桶时，此自动操作会检查 “ AWS 工具” PowerShell 模块是否可用。否则，自动化将结束。

- **BranchOnProcessDump:**

  分支取决于您是否将其设置为捕获影响性能的进程的转储。

- **CaptureProcessDump:**

  检查实例是否有足够的空间来运行此自动化（当您选择最高 CPU /内存时）。

- **CapturePerformanceLogs:**

  再次检查磁盘空间并在实例上运行 PowerShell 脚本以创建 perfmon 计数器并启动性能监视器和 Windows 性能记录器日志记录。脚本在满足定义`LogCaptureDuration`后停止。

- **SummarizePerformanceLogs:**

  汇总上一步生成的 XML 报告`CapturePerformanceLogs`，找出自动化输出中显示的消耗最多 WorkingSet 64（内存）和处理器时间 (CPU) 百分比的负责进程。它会生成类似的网络接口、内存 LogicalDisk、TCPv4、IPv4 和 UDPv4 的使用信息，并将其保存到`analysis_output.log`输出文件夹中。

- **BranchOnInstallEC2Rescue:**

  分支（如果您将其设置为在 Amazon EC2 实例中安装最新`EC2Rescue`工具）。

- **InstallEC2RescueTool:**

  在实例操作系统中安装该EC2Rescue工具以使用捕获EC2Rescue日志AWS-ConfigureAWSPackage。

- **RunEC2RescueTool:**

  在实例操作系统中运行该EC2Rescue工具以捕获所需的所有日志。 EC2Rescue仅捕获所需的日志以节省空间。

- **BranchOnIfS3BucketProvided:**

  根据用户的输入进行分支LogUploadBucketName，以查看是否有可用于上传日志的存储桶名称。

- **GetS3BucketPublicStatus:**

  确定是否提供了 Amazon S3 存储桶，如果提供了，则确认该 Amazon S3 存储桶不是公有的，并且配置了 SSE。

- **UploadLogResult:**

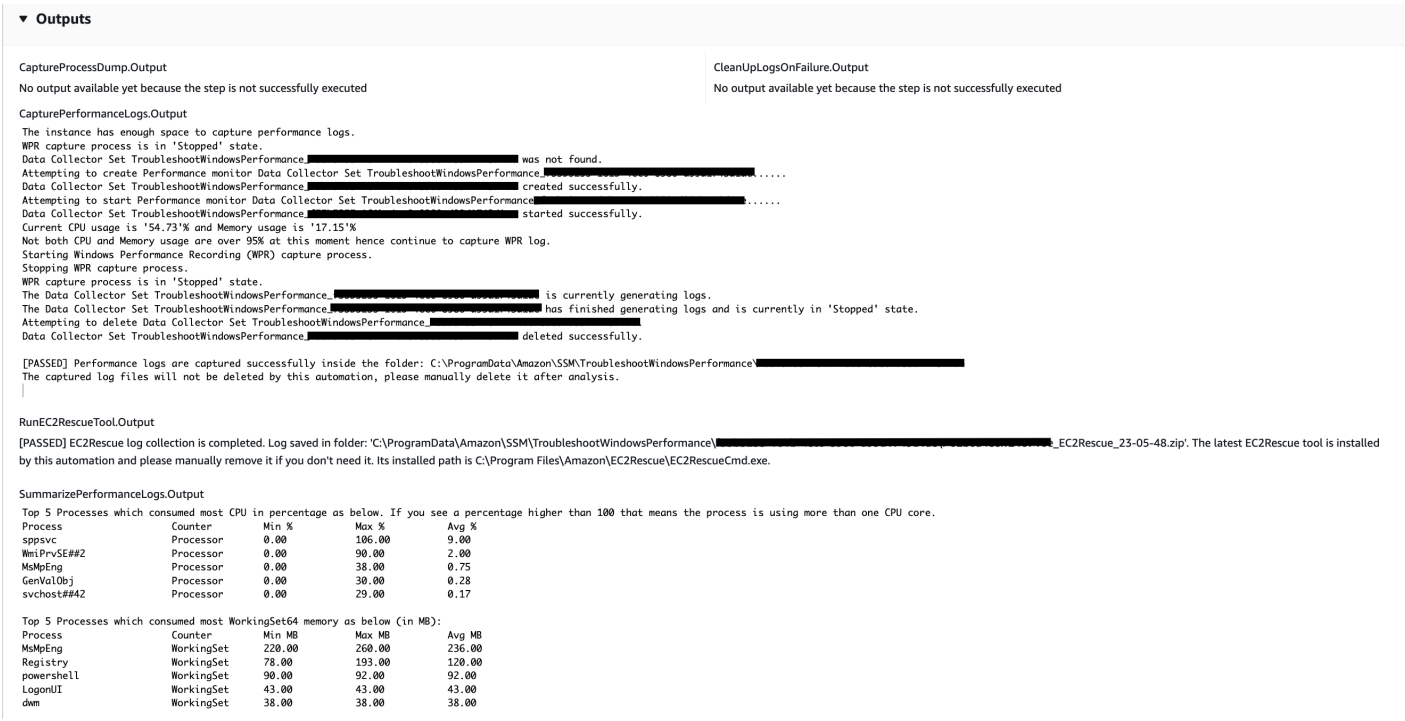
  将日志上传到提供的 Amazon S3 存储桶。如果 PowerShell 版本为 5.0 或更高版本，它会将日志压缩为 ZIP 存档并上传。它会在上传完成后删除 ZIP 文件。如果 PowerShell 版本低于 5.0，则会将文件直接上传到文件夹。

- **CleanUpLogsOnFailure:**

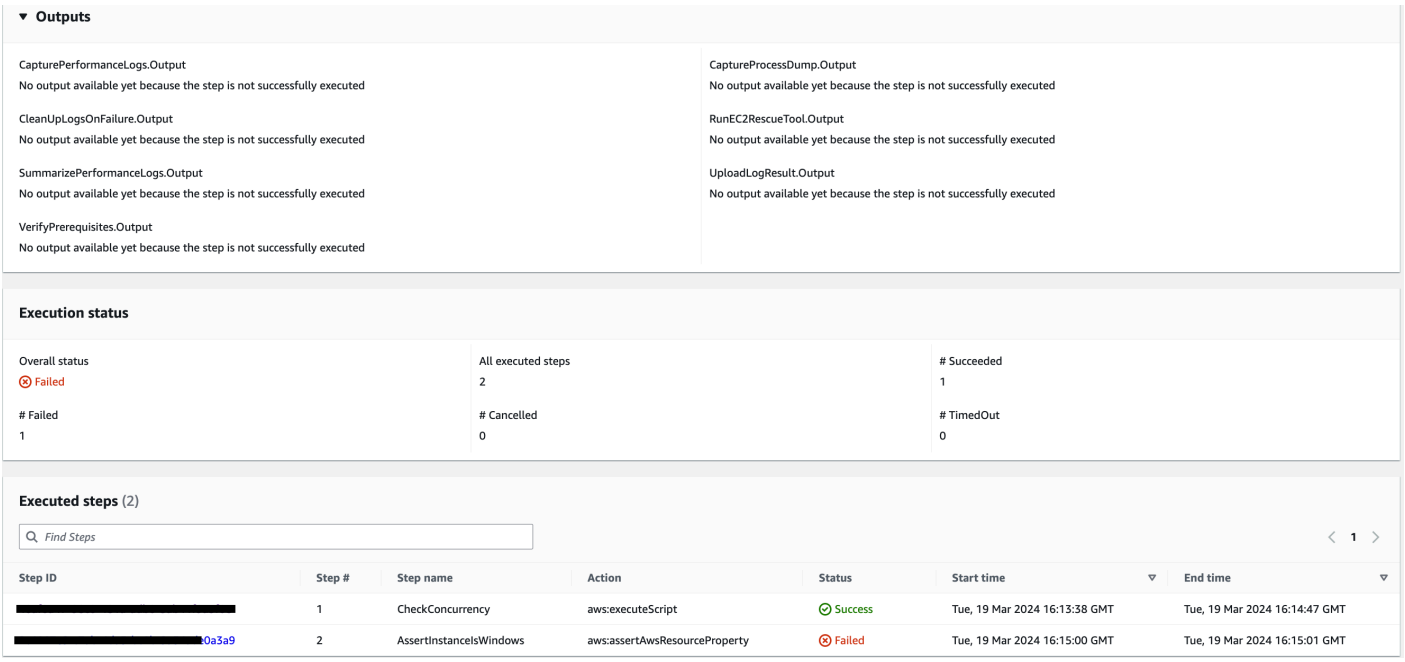
  当步骤失败时，清除该CapturePerformanceLogs步骤生成的所有日志。如果 SSM 代理无法正常工作或 Windows 系统没有响应，则该CleanUpLogsOnFailure步骤可能会失败或超时。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

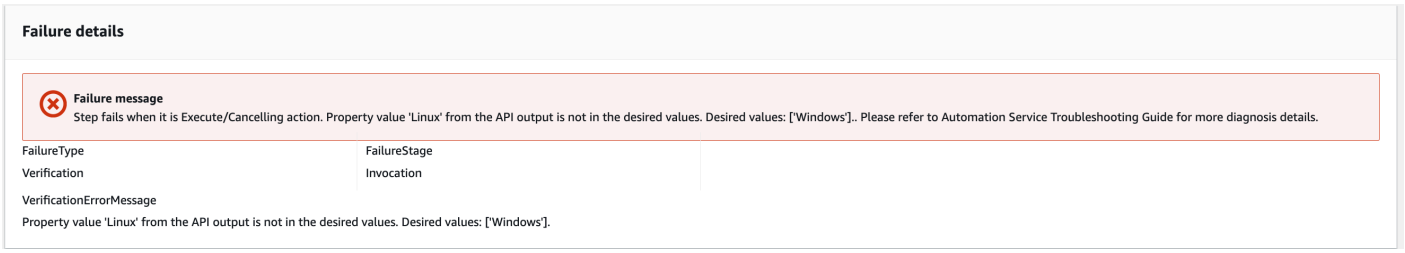
在目标实例具有所有必需先决条件的情况下执行。



目标实例在 Linux 平台上执行且执行失败。您可以选择步骤 ID 以查看失败详情。



步骤的失败详情AssertInstanceIsWindows。



参考

Systems Manager Automation

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

AWSSupport-TroubleshootWindowsUpdate

描述

该AWSSupport-TroubleshootWindowsUpdate运行手册用于识别可能导致亚马逊弹性计算云 (Amazon EC2) Windows 实例的 Windows 更新失败的问题。

如何工作？

运行手册执行以下步骤：

- 检查目标 Amazon EC2 实例是否由管理 AWS Systems Manager。
- 检查 Systems Manager 的修补操作是否支持代 AWS Systems Manager 理（SSM 代理）和 Windows Server 版本。
- 检查为 Windows 更新推荐的可用磁盘空间以及是否正在等待重启。待重启通常表示更新处于待处理状态，并且在执行其他更新之前需要重新启动。
- 在操作系统级别配置代理设置，这有助于解决连接问题。
- 执行亚马逊简单存储服务 (Amazon S3) Semple Service 终端节点连接测试，并调用 GetDeployablePatchSnapshotForInstanceAPI 操作来检索托管节点使用的补丁基准的当前快照。
- 如果连接失败，则提供AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2运行手册的选项，以分析实例与 Amazon S3 终端节点的连接。

- 验证 Windows 更新配置并测试 Windows 服务器更新服务 (WSUS)（如果适用）。

> **Important**
>
> - 不支持活动目录域控制器。
> - 不支持 Windows Server 版本 2008 R2 或之前的版本。
> - 不支持 SSM Agent 1.2.371 或之前的版本。
> - AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2运行手册VPC Reachability Analyzer用于分析源端点和服务端点之间的网络连接。每次在来源和目标之间运行分析时，您需要支付费用。有关详细信息，请参阅 Amazon VPC 定价。
> - 并非所有支持 Systems Manager 的地区都提供该操作手AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2册。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation

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

> **Note**
>
> 要运行子运行手册AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2，请添加本文档中列出的权限。

说明

按照这些步骤对自动化进行配置：

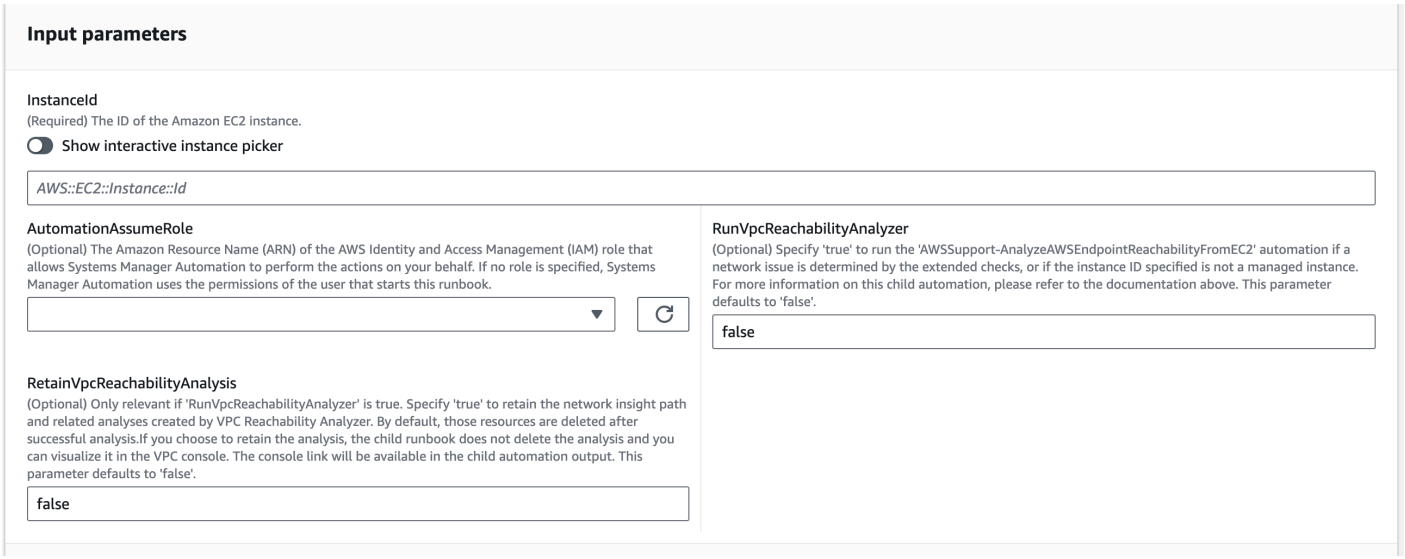
1. AWSSupport-TroubleshootWindowsUpdate在 Systems Manager 的 “文档” 下导航至。
2. 选择 Execute automation（执行自动化）。
3. 对于输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

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

     输入 Windows 更新失败的亚马逊 EC2 实例的 ID。
   - RunVpcReachabilityAnalyzer（可选）：

     如果网络问题是由扩展检查确定的，或者指定的true实例 ID 不是托管实例，则指定运行AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2自动化。有关此子自动化的更多信息，请参阅文档。默认值为 false。
   - RetainVpcReachabilityAnalysis（可选）：

     只有在RunVpcReachabilityAnalyzer是的情况下才相关true。指定true保留由创建的网络洞察路径和相关分析Reachability Analyzer。默认情况下，这些资源将在成功分析后删除。如果您选择保留分析，则子运行手册不会删除该分析，您可以在 Amazon VPC 控制台中将其可视化。控制台链接将在儿童自动化输出中可用。默认值false。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

- **`getWindowsServerAndSSMAgentVersion:`**

  验证目标实例是否由管理， AWS Systems Manager 并获取有关 SSM 代理版本和 Windows 版本的详细信息。

- **`assertifInstanceIsSsmManaged:`**

  确保 Amazon EC2 实例由 AWS Systems Manager (SSM) 管理，否则自动化将结束。

- **`CheckProxy:`**

  检查 Windows 实例的所有代理类型。

- **`CheckPrerequisites:`**

  获取 SSM 代理版本和 Windows 版本，并确定它是否是 Active Directory 域控制器 (DC)。如果实例是 DC 或者不支持 SSM 代理或 Windows 版本，则运行手册将停止。

- **`CheckDiskSpace:`**

  获取并验证 Windows 实例上的可用磁盘空间是否足以执行 Windows 更新。

- **`CheckPendingReboot:`**

  在 Windows 实例上检查是否有任何待重启的任务。

- **`CheckS3Connectivity:`**

检查实例是否可以访问的 Amazon S3 终端节点Patchbaseline。

- **branchOnRunVpcReachabilityAnalyzer:**

  如果RunVpcReachabilityAnalyzer为 true，则它会分支自动化以对调试 Amazon S3 连接进行更深入的分析。

- **GenerateEndpoints:**

  生成一个终端节点，以便对 Amazon S3 终端节点进行扩展连接检查。

- **analyzeAwsEndpointReachabilityFromEC2:**

  调用自动化 runbook，AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2. 以检查所选实例与所需终端节点的可访问性。

- **CheckWindowsUpdateServices:**

  检查 Windows 更新服务状态和启动类型。

- **CheckWindowsUpdateSettings:**

  检查是否在 Windows 实例上配置了 Windows 更新策略。

- **CheckWSUSSettings:**

  检查 Windows 更新是使用 WSUS 还是使用 Microsoft 更新目录配置的，并验证连接。

- **CheckWUGlobalSettings:**

  检查通过 Windows 实例配置的 Windows 更新全局设置。

- **GenerateLogs:**

  将 Windows 更新日志和 CBS 日志下载到实例桌面，并检查 Windows 事件日志是否出现故障。

- **FinalReport:**

  生成所有步骤的完整报告。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

```
FinalReport.Results
"
==================================================Prerequisites Check==================================================
Result: ✅ [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

====================================================Disk Space Check====================================================
Result: ✅ [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

==================================================Pending Reboot Check==================================================
Result: ✅ [PASSED]
INFO: There is no pending reboot.

================================================Amazon S3 Connectivity Check================================================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

==============================AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2==============================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

============================================Windows Update Services Status============================================
Result: ✅ [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

============================================Windows Proxy Settings============================================
Result: ✅ [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.


============================================Windows Update Settings============================================
Result: ✅ [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\\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
"
```

参考

Systems Manager Automation

- 运行此自动化（控制台）
- 运行自动化

- 设置自动化
- 支持自动化工作流登录页面

与 AWS 服务相关的文档

- 有关更多信息，请参阅文章《TroubleShoot Windows 更新》。

AWSSupport-UpgradeWindowsAWSDrivers

描述

AWSSupport-UpgradeWindowsAWSDrivers 运行手册在指定的 EC2 实例上升级或修复存储及网络 AWS 驱动程序。运行手册尝试通过调用 SSM 代理，在线安装最新版本的 AWS 驱动程序。如果无法与 SSM Agent 通信，则在明确要求时，运行手册可以执行 AWS 驱动程序的离线安装。

> **Note**
>
> 注意：在线和离线升级都将在尝试任何操作前创建一个 AMI，此 AMI 在 Automation 完成后予以保留。对此 AMI 的安全访问由您负责；或者，您也可以将其删除。在线方法在升级过程中会重启实例，而离线方法则需要停止然后启动提供的 EC2 实例。

> **Important**
>
> 如果您的实例使用 VPC 端点连接到 AWS Systems Manager，除非在 us-east-1 区域中使用，否则此运行手册将失败。此运行手册也将在域控制器上失败。要更新域控制器上的 AWS 半虚拟化驱动程序，请参阅升级域控制器（AWS 半虚拟化升级）。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AllowOffline

  类型：字符串

  有效值：true | false

  默认值：false

  说明：（可选）如果允许在无法执行在线安装时进行离线驱动程序升级，请将其设置为 true。注意：离线方法需要停止提供的 EC2 实例然后启动。存储在实例存储卷中的数据将丢失。如果不使用弹性 IP，则公有 IP 地址将发生更改。

- AutomationAssumeRole

  类型：字符串

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

- ForceUpgrade

  类型：字符串

  有效值：true | false

  默认值：false

  说明：（可选）仅离线 - 如果允许离线驱动程序升级在实例已安装最新驱动程序的情况下继续，请将其设置为 true。

- InstanceId

  类型：字符串

  说明：（必需）您的 Windows Server EC2 实例的 ID。

- SubnetId

类型：字符串

默认： SelectedInstanceSubnet

说明：（可选）仅离线 - 用于执行离线驱动程序升级的 EC2Rescue 实例的子网 ID。如果未指定子网 ID，Systems Manager Automation 将创建一个新 VPC。

> **Important**
> 子网必须与位于同一个可用区中 InstanceId，并且必须允许访问 SSM 端点。

所需的 IAM 权限

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

接收命令的 EC2 实例必须至少具有一个 IAM 角色，该角色包括 ssm: StartAutomationExecution 和 ssm: SendCommand 的权限，用于运行自动化并将命令发送到实例，以及 ssm: GetAutomationExecution 才能读取自动化输出。您可以将 `AmazonSSMManagedInstanceCore` Amazon 托管策略附加到 IAM 角色以提供这些权限。不过，我们建议使用 Automation IAM 角色 `AmazonSSMAutomationRole` 以实现该目的。有关更多信息，请参阅 使用 IAM 为自动化配置角色。

如果要执行离线升级，请参阅 `AWSSupport-StartEC2RescueWorkflow` 所需的权限。

文档步骤

1. `aws:assertAwsResourceProperty` - 验证输入实例是否为 Windows。
2. `aws:assertAwsResourceProperty` - 验证输入实例是否为托管实例。如果是托管实例，则启动在线升级，否则将评估离线升级。
   a. （在线升级）如果输入实例为托管实例：
      i. `aws:createImage` - 创建 AMI 备份。
      ii. `aws:createTags` - 标记 AMI 备份。
      iii. `aws:runCommand` - 通过 `AWS-ConfigureAWSPackage` 安装 ENA 网络驱动程序。
      iv. `aws:runCommand` - 通过 `AWS-ConfigureAWSPackage` 安装 NVMe 驱动程序。
      v. `aws:runCommand` - 通过 `AWS-ConfigureAWSPackage` 安装 AWS PV 驱动程序。
   b. （离线升级）如果输入实例不为托管实例：

i. `aws:assertAwsResourceProperty` - 验证AllowOffline 旗帜是否设置为。`true`如果是，则启动离线升级，否则自动化流程结束。

ii. `aws:changeInstanceState` - 停止源实例。

iii. `aws:changeInstanceState` - 强制停止源实例。

iv. `aws:createImage` - 创建源实例的 AMI 备份。

v. `aws:createTags` - 标记源实例的 AMI 备份。

vi. `aws:executeAwsApi` - 为实例启用 ENA

vii.`aws:assertAwsResourceProperty`-宣称ForceUpgrade 旗帜。

viii强制离线升级）如果ForceUpgrade 为 true`aws:executeAutomation`，则`AWSSupport-StartEC2RescueWorkflow`使用驱动程序强制升级脚本运行调用。不管当前安装的是何种版本，都将安装驱动程序

ix.（离线升级）如果ForceUpgrade 为 false`aws:executeAutomation`，则`AWSSupport-StartEC2RescueWorkflow`使用驱动程序升级脚本运行调用。

输出

preUpgradeBackup.ImageId

preOfflineUpgradeBackup。 ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline。输出

forceUpgradeDrivers离线。输出

Amazon ECS

AWS Systems Manager Automation 为 Amazon 弹性容器服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWSSupport-CollectECSInstanceLogs

- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

描述

AWSSupport-CollectECSInstanceLogs 运行手册从 Amazon Elastic Compute Cloud (Amazon EC2) 实例收集操作系统和 Amazon Elastic Container Service (Amazon ECS) 相关日志文件，以帮助解决常见的 Amazon ECS 问题。当自动化收集关联的日志文件时，会对文件系统进行更改。这些更改包括创建临时目录和日志目录、将日志文件复制到这些目录，以及将日志文件压缩到档案中。

如果您为 LogDestination 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 Amazon EC2 实例收集的日志的安全，如果策略状态 isPublic 设置为 true，或者如果访问控制列表（ACL）向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，日志将不会上传。此外，如果提供的存储桶在您的账户中不可用，日志将不会上传。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 预定义组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ECS InstanceId

  类型：字符串

  描述：（必需）需要收集日志的实例 ID。指定的实例必须由 Systems Manager 托管。

- LogDestination

  类型：字符串

  描述：（可选）您中 AWS 账户 用于上传存档日志的 Amazon S3 存储桶。

所需的 IAM 权限

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

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

建议您在 `ECSInstanceId` 参数中指定的 Amazon EC2 实例具有一个附加了 `AmazonSSMManagedInstanceCore` Amazon 托管策略的 IAM 角色。要将日志档案上传到您在 `LogDestination` 参数中指定的 Amazon S3 存储桶，您必须添加以下权限：

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

文档步骤

- `assertInstanceIsManaged` - 验证您在 `ECSInstanceId` 参数中指定的实例是否由 Systems Manager 管理。

- getInstancePlatform - 获取您在 ECSInstanceId 参数中指定的实例的操作系统 (OS) 平台的相关信息。
- verifyInstancePlatform - 根据 OS 平台对自动化进行分支。
- runLogCollectionScriptOnLinux - 在 Linux 实例上收集操作系统和 Amazon ECS 相关日志文件，并在 /var/log/collectECSlogs 目录中创建一个归档文件。
- runLogCollectionScriptOnWindows - 在 Windows 实例上收集操作系统和 Amazon ECS 相关日志文件，并在 C:\ProgramData\collectECSlogs 目录中创建一个归档文件。
- verifyIfS3BucketProvided - 验证是否为 LogDestination 参数指定了一个值。
- runUploadScript - 基于操作系统平台对自动化步骤进行分支。
- runUploadScriptOnLinux - 将日志档案上传到 LogDestination 参数中指定的 Amazon S3 存储桶，并从操作系统中删除归档的日志文件。
- runUploadScriptOnWindows - 将日志档案上传到 LogDestination 参数中指定的 Amazon S3 存储桶，并从操作系统中删除归档的日志文件。

AWS-InstallAmazonECSAgent

描述

AWS-InstallAmazonECSAgent 运行手册将 Amazon Elastic Container Service (Amazon ECS) 代理安装在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例上。此运行手册仅支持 Amazon Linux 和 Amazon Linux 2 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

类型：字符串

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

- InstanceIds

  类型: StringList

  描述：（必需）要在其上安装 Amazon ECS 代理的 Amazon EC2 实例的 ID。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

文档步骤

`aws:executeScript` - 将 Amazon ECS 代理安装到您在 `InstanceIds` 参数中指定的 Amazon EC2 实例上。

输出

InstallAmazonecsAgent。 SuccessfulInstances -成功安装 Amazon ECS 代理的实例的 ID。

InstallAmazonecsAgent。 FailedInstances -安装 Amazon ECS 代理失败的实例的 ID。

InstallAmazonecsAgent。 InProgressInstances -正在安装 Amazon ECS 代理的实例的 ID。

AWS-ECSRunTask

描述

运行AWS-ECSRunTask手册运行您指定的亚马逊弹性容器服务 (Amazon ECS) 任务。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（可选）用于任务的容量提供者策略。
- cluster

  类型：字符串

  描述：（可选）用于运行任务的集群的短名称或 ARN。如果未指定集群，则使用默认集群。
- count

  类型：字符串

  描述：（可选）要在集群上放置的指定任务的实例化次数。您最多可以为每个请求指定 10 个任务。
- 启用 ECS ManagedTags

类型：布尔值

描述：（可选）指定是否对任务使用 Amazon ECS 托管标签。有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的标记 Amazon ECS 资源。

- 启用 ExecuteCommand

  类型：布尔值

  描述：（可选）确定是否激活此任务中容器的执行命令功能。如果为 true，则将在任务中的所有容器上激活执行命令功能。

- 组

  类型：字符串

  描述：（可选）要与任务关联的任务组的名称。默认值为任务定义的姓氏。例如，`family:my-family-name`。

- 启动类型

  类型：字符串

  有效值：EC2 | FARGATE | EXTERNAL

  描述：（可选）运行独立任务的基础架构。

- networkConfiguration

  类型：字符串

  描述：（可选）任务的网络配置。使用`awsvpc`网络模式接收自己的 elastic network interface 的任务定义必须使用此参数，其他网络模式则不支持此参数。

- 覆盖

  类型：字符串

  描述：（可选）JSON 格式的容器覆盖列表，用于指定任务定义中指定容器的名称以及容器应接收的替代项。您可以使用命令替换在任务定义或 Docker 镜像中指定的容器的默认命令。您还可以覆盖任务定义或容器上的 Docker 镜像中指定的现有环境变量。此外，您还可以使用环境覆盖来添加新的环境变量。

- 放置限制

类型：字符串

描述：（可选）用于任务的放置约束对象数组。您最多可以为每项任务指定 10 个约束条件，包括任务定义中的约束条件和运行时指定的约束条件。

- 放置策略

  类型：字符串

  描述：（可选）用于任务的放置策略对象。您最多可以为每个任务指定 5 条策略规则。

- platformVersion

  类型：字符串

  描述：（可选）任务使用的平台版本。仅为 Fargate 上托管的任务指定平台版本。如果未指定任何版本，将使用 LATEST 平台版本。

- propagateTags

  类型：字符串

  描述：（可选）确定标签是否从任务定义传播到任务。如果未指定任何值，则不会传播标签。只能在任务创建过程中将标签传播到任务。

- referenceId

  类型：字符串

  描述：（可选）用于任务的参考 ID。参考 ID 的最大长度可以为 1024 个字符。

- 开始者

  类型：字符串

  描述：（可选）任务启动时指定的可选标签。这有助于您通过筛选 ListTasks API 操作的结果来确定哪些任务属于特定作业。最多允许 36 个字母（大写和小写）、数字、连字符 (-) 和下划线 (_)。

- 标签

  类型：字符串

  描述：（可选）要应用于任务的元数据，以帮助您对任务进行分类和组织。每个标签都由用户定义的键和值组成。

- 任务定义

类型：字符串

描述：（可选）要family运行的任务定义的和 revision (family:revision) 或完整 ARN。如果未指定修订版，则使用最新的ACTIVE修订版。

所需的 IAM 权限

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

- ecs:RunTask

文档步骤

aws:executeScript-根据您为运行手册输入参数指定的值运行 Amazon ECS 任务。

AWSSupport-TroubleshootECSContainerInstance

描述

AWSSupport-TroubleshootECSContainerInstance 运行手册可帮助排除无法向 Amazon ECS 集群注册的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的问题。此自动化会检查实例的用户数据是否包含正确的集群信息、实例配置文件是否包含所需的权限，还会检查网络配置问题。

> **Important**
>
> 要成功运行此自动化，Amazon EC2 实例的状态必须为 running，Amazon ECS 集群的状态必须为 ACTIVE。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）实例未能向其注册的 Amazon ECS 集群的名称。
- InstanceId

  类型：字符串

  描述：（必需）需要排除故障的 Amazon EC2 实例 ID。

所需的 IAM 权限

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

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

- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy

文档步骤

aws:executeScript：审查 Amazon EC2 实例是否满足向 Amazon ECS 集群注册所需的先决条件。

AWSSupport-TroubleshootECSTaskFailedToStart

描述

AWSSupport-TroubleshootECSTaskFailedToStart 运行手册可帮助解决 Amazon ECS 集群中的 Amazon Elastic Container Service (Amazon ECS) 任务无法启动的问题。您必须以与未能启动的任务 AWS 区域 相同的方式运行此运行手册。运行手册分析了以下可能导致任务无法启动的常见问题：

- 与已配置的容器注册表的网络连接
- 缺少任务执行角色所需的 IAM 权限
- VPC 端点连接
- 安全组规则配置
- AWS Secrets Manager 秘密参考
- 日志记录配置

> **Note**
>
> 如果分析确定需要对网络连接进行测试，则会在您的账户中创建 Lambda 函数和必要的 IAM 角色。这些资源用于模拟失败任务的网络连接。当这些资源不再需要时，此自动化会将其删除。但是，如果此自动化无法删除这些资源，则必须手动将其删除。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）任务启动失败的 Amazon ECS 集群的名称。
- CloudwatchRetention时期

  类型：整数

  描述：（可选）要存储在 Ama CloudWatch zon Logs 中的 Lambda 函数日志的保留期，以天为单位。只有在分析确定需要测试网络连通性时，才需要这样做。

  有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  默认：30
- TaskId

  类型：字符串

  描述：（必需）失败任务的 ID。使用最近失败的任务。

所需的 IAM 权限

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

- `cloudtrail:LookupEvents`

- ec2:DeleteNetworkInterface
- ec2: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

文档步骤

- aws:executeScript - 验证启动此自动化的用户或角色是否具有所需的 IAM 权限。如果您没有足够的权限来使用此运行手册，则缺少的必需权限将包含在此自动化的输出中。
- aws:branch - 根据您是否对运行手册的所有必要操作拥有权限进行分支。
- aws:executeScript - 如果分析确定需要测试网络连通性，则会在 VPC 中创建 Lambda 函数。
- aws:branch - 根据上一步的结果进行分支。
- aws:executeScript - 分析启动任务失败的可能原因。
- aws:executeScript - 删除此自动化创建的资源。
- aws:executeScript - 格式化此自动化的输出，将分析结果返回到控制台。在此步骤之后，您可以在自动化完成前查看分析。
- aws:branch - 根据 Lambda 函数和关联资源是否已创建以及是否需要删除进行分支。
- aws:sleep - 休眠 30 分钟，使得可以删除 Lambda 函数的弹性网络接口。
- aws:executeScript - 删除 Lambda 函数网络接口。
- aws:executeScript - 格式化 Lambda 函数网络接口删除步骤的输出。

AWS-UpdateAmazonECSAgent

描述

AWS-UpdateAmazonECSAgent 运行手册更新了您指定的Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Container Service (Amazon ECS) 代理。此运行手册仅支持 Amazon Linux 和 Amazon Linux 2 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型: StringList

  描述：（必需）容器实例所注册的 Amazon ECS 集群的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

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

- ec2:DescribeInstanceAttribute
- ecs:DescribeContainerInstances
- ecs:DescribeClusters
- ecs:ListContainerInstances
- ecs:UpdateContainerAgent

文档步骤

aws:executeScript - 更新您在 ClusterARN 参数中指定的 Amazon ECS 集群上的 Amazon ECS 代理。

输出

UpdateAmazonecsAgent。 UpdatedContainers -成功更新 Amazon ECS 代理的实例的 ID。

UpdateAmazonecsAgent。 FailedContainers -Amazon ECS 代理更新失败的实例的 ID。

UpdateAmazonecsAgent。 InProgressContainers -正在更新 Amazon ECS 代理的实例的 ID。

Amazon EFS

AWS Systems Manager Automation 为亚马逊 Elastic File System 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWSSupport-CheckAndMountEFS

AWSSupport-CheckAndMountEFS

描述

AWSSupport-CheckAndMountEFS 运行手册验证挂载 Amazon Elastic File System (Amazon EFS) 文件系统并在您指定的 Amazon Elastic Compute Cloud (Amazon EC2) 实例上挂载文件系统的先决条件。此运行手册支持使用 DNS 名称或使用挂载目标的 IP 地址来挂载 Amazon EFS 文件系统。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  有效值：选中 | CheckAndMount

  描述：（必需）确定运行手册是验证先决条件，还是验证先决条件并装载文件系统。
- EfsId

  类型：字符串

  描述：（必选）要挂载的文件系统的 ID。
- InstanceId

  类型：字符串

  描述：（必需）要在其上挂载文件系统的 Amazon EC2 实例的 ID。
- MountOptions

  类型：字符串

描述：（可选）要在挂载文件系统时使用的 Amazon EFS 挂载帮助程序支持的选项。如果您指定 `tls` 选项，则验证目标实例上的 stunnel 是否已升级。

- MountPoint

  类型：字符串

  描述：（可选）要挂载文件系统的目录。如果为 `Action` 参数指定了 `Check` 值，则不应指定此参数。

- MountTargetIP

  类型：字符串

  描述：（可选）挂载目标的 IP 地址。通过 IP 地址挂载适用于 DNS 被禁用的环境，例如禁用 DNS 主机名的虚拟私有云（VPC）。此外，如果您的环境使用 Amazon Route 53 (Route 53) 以外的 DNS 提供商，则可以使用此选项。

- 区域

  类型：字符串

  描述：（必填）Amazon EC2 实例和文件系统所在的位置。 AWS 区域

所需的 IAM 权限

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

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

- ssm:StartAutomationExecution
- iam:ListRoles
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- elasticfilesystem:DescribeFileSystemPolicy
- elasticfilesystem:DescribeMountTargets
- elasticfilesystem:DescribeMountTargetSecurityGroups
- resource-groups:*

文档步骤

- aws:executeScript - 收集有关您在 InstanceId 参数中指定的 Amazon EC2 实例的详细信息。
- aws:executeScript - 收集有关您在 EfsId 参数中指定的文件系统的详细信息。
- aws:executeScript - 验证与文件系统关联的安全组是否允许来自您在 InstanceId 参数中指定的 Amazon EC2 实例的端口 2049 上的流量。
- aws:assertAwsResourceProperty - 验证您在 InstanceId 参数中指定的 Amazon EC2 实例是否由 Systems Manager 管理以及其状态是否为 Online。
- aws:branch - 根据您为 Action 参数指定的值进行分支。
- aws:runCommand - 验证挂载您在 EfsId 参数中指定的文件系统的先决条件。
- aws:runCommand - 验证挂载您在 EfsId 参数中指定的文件系统的先决条件，并将文件系统挂载到您在 InstanceId 参数中指定的 Amazon EC2 实例上。

Amazon EKS

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

主题

- AWSSupport-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup

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

AWSSupport-CollectEKSInstanceLogs

描述

AWSSupport-CollectEKSInstanceLogs 运行手册从 Amazon Elastic Compute Cloud (Amazon EC2) 实例收集操作系统和 Amazon Elastic Kubernetes Service (Amazon EKS) 相关日志文件，以帮助解决常见问题。在此自动化收集关联的日志文件时，会对文件系统结构进行更改，包括创建临时目录、将日志文件复制到临时目录以及将日志文件压缩到档案中。此活动可能会导致 EC2 实例上的 CPUUtilization 增加。有关更多信息CPUUtilization，请参阅 Amazon CloudWatch 用户指南中的实例指标。

如果您为 LogDestination 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 EC2 实例收集的日志的安全性，如果策略状态 isPublic 设置为 true，或者访问控制列表（ACL）向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，则不会上传日志。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 预定义组。

> **Note**
>
> 此自动化要求附加到 EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 根卷上至少有 10% 的可用磁盘空间。如果根卷上没有足够的可用磁盘空间，此自动化将停止。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

- EKS InstanceId

  类型：字符串

  描述：（必需）需要收集日志的 Amazon EKS EC2 实例的 ID。

- LogDestination

  类型：字符串

  描述：（可选）账户中用于将归档日志上传到的 S3 存储桶。

所需的 IAM 权限

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

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

我们建议接收命令的 EC2 实例具有附加 A mazonSSM Core Amaz ManagedInstance on 托管策略的 IAM 角色。要将日志档案上传到您在 `LogDestination` 参数中指定的 S3 存储桶，您必须添加 `s3:PutObject` 权限。

文档步骤

- aws:assertAwsResourceProperty - 确认您在 EKSInstanceId 参数中指定的值的操作系统为 Linux。
- aws:runCommand - 收集操作系统和 Amazon EKS 相关日志文件，从而将其压缩到 /var/log 目录中的档案中。
- aws:branch - 确认是否为 LogDestination 参数指定了一个值。
- aws:runCommand - 将日志档案上传到您在 LogDestination 参数中指定的 S3 存储桶。

AWS-CreateEKSClusterWithFargateProfile

描述

AWS-CreateEKSClusterWithFargateProfile运行手册使用创建了亚马逊 Elastic Kubernetes Service（亚马逊 EKS）集群。 AWS Fargate

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

描述：（必填）集群的唯一名称。

- ClusterRoleArn

  类型：字符串

  描述：（必填）IAM 角色的 ARN，该角色为 Kubernetes 控制平面提供代表您调用 AWS API 操作的权限。

- FargateProfile姓名

  类型：字符串

  描述：（必填）Fargate 配置文件的名称。

- FargateProfileRoleArn

  类型：字符串

  描述：（必填）亚马逊 EKS Pod 执行 IAM 角色的 ARN。

- FargateProfile选择器

  类型：字符串

  描述：（必填）用于将吊舱与 Fargate 配置文件进行匹配的选择器。

- SubnetIds

  类型: StringList

  描述：（必填）您要用于 Amazon EKS 集群的子网的 ID。Amazon EKS 在这些子网中创建弹性网络接口，用于您的节点与 Kubernetes 控制平面之间的通信。您必须指定至少两个子网 ID。

- EKS EndpointPrivate 访问权限

  类型：布尔值

  默认值：True

  描述：（可选）将此值设置为，`True`以允许对集群的 Kubernetes API 服务器终端节点进行私有访问。如果启用私有访问，集群的 VPC 内的 Kubernetes API 请求将使用私有 VPC 端点。如果您禁用私有访问并且集群中有节点或 AWS Fargate Pod，请确保`publicAccessCidrs`其中包含与节点或 Fargate Pod 通信所必需的 CIDR 块。

- EKS EndpointPublic 访问权限

类型：布尔值

默认值：False

描述：（可选）将此值设置为，False以禁用对集群的 Kubernetes API 服务器端点的公共访问权限。如果您禁用公共访问，则集群的 Kubernetes API 服务器只能接收来自其启动的 VPC 内部的请求。

- PublicAccessCIDR

  类型: StringList

  描述：（可选）允许访问集群的公共 Kubernetes API 服务器端点的 CIDR 块。拒绝从您指定的 CIDR 块之外的地址与端点的通信。如果您已禁用私有终端节点访问并且集群中有节点或 Fargate pod，请确保指定必要的 CIDR 块。
- SecurityGroup身份证

  类型: StringList

  描述：（可选）指定一个或多个安全组以与 Amazon EKS 在您的账户中创建的弹性网络接口相关联。

所需的 IAM 权限

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

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- eks:CreateCluster
- eks:CreateFargateProfile
- eks:DescribeCluster
- eks:DescribeFargateProfile
- iam:CreateServiceLinkedRole
- iam:GetRole

- iam:ListAttachedRolePolicies
- iam:PassRole

文档步骤

- createeksCluster (aws: execute) AwsApi-创建亚马逊 EKS 集群。
- verifyEKS ClusterIsActive (await: wait ForAwsResourceProperty)-验证集群状态为。ACTIVE
- CreateFargateProfile (aws: executeAwsApi)-为集群创建 Fargate。
- VerifyFargateProfileIsActive (aws: wait ForAwsResourceProperty)-验证 Fargate 配置文件状态为。ACTIVE

输出

CreateEKSCluster.CreateClusterResponse

描述：从 CreateCluster API 调用中收到的响应。

CreateFargateProfile.CreateFargateProfileResponse

描述：从 CreateFargateProfile API 调用中收到的响应。

AWS-CreateEKSClusterWithNodegroup

描述

该AWS-CreateEKSClusterWithNodegroup运行手册使用容量节点组创建了亚马逊 Elastic Kubernetes Service（Amazon EKS）集群。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ClusterName

  类型：字符串

  描述：（必填）集群的唯一名称。

- ClusterRoleArn

  类型：字符串

  描述：（必填）IAM 角色的 ARN，该角色为 Kubernetes 控制平面提供代表您调用 AWS API 操作的权限。

- NodegroupName

  类型：字符串

  描述：（必填）节点组的唯一名称。

- NodegroupRoleArn

  类型：字符串

  描述：（必填）要与您的节点组关联的 IAM 角色的 ARN。Amazon EKS 工作节点 kubelet 守护程序代表你调用 AWS API。节点通过 IAM 实例配置文件和关联的策略获得这些 API 调用的权限。您必须先为节点创建 IAM 角色以在启动它们时使用，然后才能启动这些节点并在集群中注册它们。

- SubnetIds

  类型: StringList

  描述：（必填）您要用于 Amazon EKS 集群的子网的 ID。Amazon EKS 在这些子网中创建弹性网络接口，用于您的节点与 Kubernetes 控制平面之间的通信。您必须指定至少两个子网 ID。

- EKS EndpointPrivate 访问权限

  类型：布尔值

  默认值：True

  描述：（可选）将此值设置为，True以允许对集群的 Kubernetes API 服务器终端节点进行私有访问。如果启用私有访问，集群的 VPC 内的 Kubernetes API 请求将使用私有 VPC 端点。如果您禁用私有访问并且集群中有节点或 AWS Fargate Pod，请确保publicAccessCidrs其中包含与节点或 Fargate Pod 通信所必需的 CIDR 块。

- EKS EndpointPublic 访问权限

  类型：布尔值

  默认值：False

  描述：（可选）将此值设置为，False以禁用对集群的 Kubernetes API 服务器端点的公共访问权限。如果您禁用公共访问，则集群的 Kubernetes API 服务器只能接收来自其启动的 VPC 内部的请求。

- PublicAccessCIDR

  类型: StringList

  描述：（可选）允许访问集群的公共 Kubernetes API 服务器端点的 CIDR 块。拒绝从您指定的 CIDR 块之外的地址与端点的通信。如果您已禁用私有终端节点访问并且集群中有节点或 Fargate pod，请确保指定必要的 CIDR 块。

- SecurityGroup身份证

  类型: StringList

  描述：（可选）指定一个或多个安全组以与 Amazon EKS 在您的账户中创建的弹性网络接口相关联。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- ec2:DescribeSubnets
- eks:CreateCluster
- eks:CreateNodegroup
- eks:DescribeCluster
- eks:DescribeNodegroup
- iam:CreateServiceLinkedRole
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:PassRole

文档步骤

- createeksCluster (aws: execute) AwsApi-创建亚马逊 EKS 集群。
- verifyEKS ClusterIsActive (await: wait ForAwsResourceProperty)-验证集群状态为。ACTIVE
- CreateNodegroup (aws: executeAwsApi)-为群集创建节点组。
- VerifyNodegroupIsActive (aws: wait ForAwsResourceProperty)-验证节点组的状态为。ACTIVE

输出

- CreateEKSCluster.CreateClusterResponse: 从 CreateCluster API 调用中收到的响应。
- CreateNodegroup.CreateNodegroupResponse: 从 CreateNodegroup API 调用中收到的响应。

AWS-DeleteEKSCluster

描述

此运行手册将删除与 Amazon EKS 集群关联的资源，包括节点组和 Fargate 配置文件。或者，您可以选择删除所有自管理节点、用于创建节点的 AWS CloudFormation 堆栈以及集群的 VPC CloudFormation 堆栈。有关删除集群的更多信息，请参阅《Amazon EKS 用户指南》中的删除集群。

> **Note**
>
> 如果集群中具有与负载均衡器关联的有效服务，则必须先删除这些服务，然后再删除集群。否则，系统将无法删除负载均衡器。在运行 AWS-DeleteEKSCluster 运行手册之前，请通过以下过程查找和删除服务。

查找和删除集群中的服务

1. 安装 Kubernetes 命令行实用程序 kubectl。有关更多信息，请参阅《Amazon EKS 用户指南》中的安装 kubectl。
2. 运行以下命令列出集群中运行的所有服务。

```
kubectl get svc --all-namespaces
```

3. 运行以下命令以删除所有具有关联 EXTERNAL-IP 值的服务。这些服务的前面配置了一个负载均衡器，您必须从 Kubernetes 中将其删除才能释放负载均衡器和关联资源。

```
kubectl delete svc
service-name
```

现在您可以运行 AWS-DeleteEKSCluster 运行手册了。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- EKS ClusterName

  类型：字符串

  描述：（必需）要删除的 Amazon EKS 集群的名称。

- VPC CloudFormation 堆栈

  类型：字符串

  描述：（可选）要删除的 EKS 集群的 VPC AWS CloudFormation 堆栈名称。这将删除 VPC 的 AWS CloudFormation 堆栈以及该堆栈创建的所有资源。

- VPC CloudFormation StackRole

  类型：字符串

  描述：（可选） AWS CloudFormation 假定删除 VPC CloudFormation 堆栈的 IAM 角色的 ARN。 AWS CloudFormation 使用该角色的凭据代表您拨打电话。

- SelfManagedNodeStacks

  类型：字符串

  描述：（可选）以逗号分隔的自管理节点 AWS CloudFormation 堆栈名称列表，这将删除自管理节点的 AWS CloudFormation 堆栈。

- SelfManagedNodeStacks角色

  类型：字符串

  描述：（可选） AWS CloudFormation 假定删除自管理节点堆栈的 IAM 角色的 ARN。 AWS CloudFormation 使用该角色的凭据代表您拨打电话。

所需的 IAM 权限

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

- sts:AssumeRole
- eks:ListNodegroups
- eks:DeleteNodegroup
- eks:ListFargateProfiles
- eks:DeleteFargateProfile
- eks:DeleteCluster
- cfn:DescribeStacks
- cfn:DeleteStack

文档步骤

- aws:executeScript- DeleteNodeGroups：查找并删除 EKS 集群中的所有节点组。
- aws:executeScript- DeleteFargateProfiles：在 EKS 集群中查找并删除所有 Fargate 配置文件。
- aws:executeScript- DeleteSelfManagedNodes：删除所有自行管理的节点和用于创建节点的 CloudFormation 堆栈。
- aws:executeScript - DeleteEKSCluster：删除 EKS 集群。
- aws:executeScript-删除 VPC CloudFormation 堆栈：删除 VPC CloudFormation 堆栈。

AWS-MigrateToNewEKSSelfManagedNodeGroup

描述

该AWS-MigrateToNewEKSSelfManagedNodeGroup运行手册可帮助您创建一个新的亚马逊 Elastic Kubernetes Service（Amazon EKS）Linux 节点组，以将现有应用程序迁移到该节点组。有关更多信息，请参阅 Amazon EKS 用户指南中的迁移到新节点组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

- OldStack姓名

  类型：字符串

  描述：（必填）现有堆栈的名称或 AWS CloudFormation 堆栈 ID。

- NewStack姓名

  类型：字符串

  描述：（可选）为您的新节点组创建的新 AWS CloudFormation 堆栈的名称。如果您未为此参数指定值，则使用以下格式创建堆栈名称：NewNodeGroup-*ClusterName*-*AutomationExecutionID*。

- ClusterControlPlaneSecurity组

  类型：字符串

  描述：（可选）您希望节点用于与 Amazon EKS 控制平面通信的安全组的 ID。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的安全组。

- NodeInstance类型

  类型：字符串

  描述：（可选）您要用于新节点组的实例类型。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的实例类型。

- NodeGroup姓名

类型：字符串

描述：（可选）您的新节点组的名称。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的节点组名称。

- NodeAutoScalingGroupDesiredCapacity

  类型：字符串

  描述：（可选）创建新堆栈时要扩展到的所需节点数量。此数字必须大于或等于该NodeAutoScalingGroupMinSize值且小于或等于NodeAutoScalingGroupMaxSize。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的节点组所需容量。

- NodeAutoScalingGroupMaxSize

  类型：字符串

  描述：（可选）您的节点组可以扩展到的最大节点数。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的节点组最大大小。

- NodeAutoScalingGroupMinSize

  类型：字符串

  描述：（可选）您的节点组可以扩展到的最小节点数。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的节点组最小大小。

- NodeImage我是

  类型：字符串

  描述：（可选）希望节点组使用的 Amazon Machine Image (AMI) 的 ID。

- NodeImageidssmParam

  类型：字符串

  描述：（可选）希望节点组使用的 AMI 的公共 Systems Manager 参数。

- NodeVolume大小

  类型：字符串

  描述：（可选）节点的根卷大小（以 GiB 为单位）。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的节点卷大小。

- NodeVolume类型

  类型：字符串

  描述：（可选）您要用于节点根卷的 Amazon EBS 卷的类型。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的卷类型。

- KeyName

  类型：字符串

  描述：（可选）您要分配给节点的 key pair。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的密钥对。

- 子网

  类型: StringList

  描述：（可选）要用于新节点组的子网 ID 的逗号分隔列表。如果您未为此参数指定值，则使用现有 AWS CloudFormation 堆栈中指定的子网。

- DisableIMDSv1

  类型：布尔值

  描述：（可选）指定禁`true`用实例元数据服务版本 1 (imdsv1)。默认情况下，节点支持 imdsv1 和 imdsv2。

- BootstrapArguments

  类型：字符串

  描述：（可选）要传递给节点引导脚本的其他参数。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `autoscaling:CreateAutoScalingGroup`
- `autoscaling:CreateOrUpdateTags`

- autoscaling:DeleteTags
- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeScalingActivities
- autoscaling:DescribeScheduledActions
- autoscaling:SetDesiredCapacity
- autoscaling:TerminateInstanceInAutoScalingGroup
- autoscaling:UpdateAutoScalingGroup
- cloudformation:CreateStack
- cloudformation:DescribeStackResource
- cloudformation:DescribeStacks
- cloudformation:UpdateStack
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateLaunchTemplateVersion
- ec2:CreateLaunchTemplate
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteLaunchTemplate
- ec2:DeleteSecurityGroup
- ec2:DescribeAvailabilityZones
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2: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

文档步骤

- DetermineParameterValuesForNewNodeGroup (aws: ExecuteScript)-收集用于新节点组的参数值。
- CreateStack (aws: CreateStack)-为新节点组创建 AWS CloudFormation 堆栈。
- GetNewStackNodeInstanceRole (aws: executeAwsApi)-获取节点实例角色。
- GetNewStackSecurityGroup (aws: executeAwsApi)-该步骤获取节点安全组。
- AddIngressRulesToNewNodeSecurityGroup (aws: executeAwsApi)-向新创建的安全组添加入口规则，使其可以接受来自分配给您先前节点组的安全组的流量。
- AddIngressRulesToOldNodeSecurityGroup (aws: executeAwsApi)-向先前的安全组添加入口规则，使其可以接受来自分配给您新创建的节点组的流量。
- VerifyStackComplete (aws: assert AwsResource 属性)-验证新的堆栈状态为。CREATE_COMPLETE

输出

DetermineParameterValuesForNewNode组。 NewStackParameters -用于创建新堆栈的参数。

GetNewStackNodeInstanceRole。 NewNodeInstanceRole -新节点组的节点实例角色。

GetNewStackSecurity组。 NewNodeSecurityGroup -新节点组的安全组的 ID。

DetermineParameterValuesForNewNode组。 NewStackName -新节点组的 AWS CloudFormation 堆栈名称。

CreateStack。 StackId -新节点组的 AWS CloudFormation 堆栈 ID。

AWSPremiumSupport-TroubleshootEKSCluster

描述

AWSPremiumSupport-TroubleshootEKSCluster 运行手册诊断 Amazon Elastic Kubernetes Service (Amazon EKS) 集群和底层基础架构的常见问题，并提供建议的修复步骤。

> **Important**
>
> 访问 AWSPremiumSupport-* 运行手册需要订阅 Enterprise 或 Business Support。有关更多信息，请参阅比较 Supp AWS ort 计划。

如果您为 S3BucketName 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 EC2 实例收集的日志的安全性，如果策略状态 isPublic 设置为 true，或者访问控制列表（ACL）向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，则不会上传日志。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 预定义组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ClusterName

  类型：字符串

  描述：（必需）要排除问题的 Amazon EKS 集群的名称。

- S3 BucketName

  类型：字符串

  描述：（可选）运行手册生成的报告应当上传到的私有 Amazon S3 存储桶的名称。

所需的 IAM 权限

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

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

- autoscaling:DescribeAutoScalingGroups

此外，附加到启动自动化的用户或角色的 AWS Identity and Access Management (IAM) 策略必须允许对以下公共 AWS Systems Manager 参数进行ssm:GetParameter操作，才能为工作节点获取最新推荐的 Amazon EKS Amazon Machine Image (AMI)。

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

要将运行手册生成的报告上传到 Amazon S3 存储桶，需要对指定的指定 Amazon S3 存储桶拥有以下权限。

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

文档步骤

- aws:executeAwsApi - 收集指定 Amazon EKS 集群的详细信息。
- aws:executeScript - 收集 Amazon Elastic Compute Cloud (Amazon EC2) 实例、Auto Scaling 组、AMI 和 Amazon EC2 GPU 图形实例类型的详细信息。
- aws:executeScript - 收集 Amazon EKS 集群的虚拟私有云（VPC）、子网、网络地址转换 (NAT) 网关、子网路由、安全组和网络访问控制列表 (ACL) 的详细信息。
- aws:executeScript - 收集附加的 IAM 实例配置文件和角色策略的详细信息。
- aws:executeScript - 收集您在 S3BucketName 参数中指定的 Amazon S3 存储桶的详细信息。
- aws:executeScript - 将 Amazon VPC 子网分类为公共或私有子网。

- aws:executeScript - 检查 Amazon VPC 子网中是否有需要作为 Amazon EKS 集群一部分的标签。
- aws:executeScript - 检查 Amazon VPC 子网中是否有 Elastic Load Balancing 子网所需的标签。
- aws:executeScript - 检查 Worker 节点 Amazon EC2 实例是否使用最新的 Amazon EKS 优化的 AMI
- aws:executeScript - 检查 Amazon VPC 安全组是否已附加到所需标签的 Worker 节点。
- aws:executeScript - 检查 Amazon EKS 集群和 Worker 节点 Amazon VPC 安全组规则中是否有建议的 Amazon EKS 集群入口规则。
- aws:executeScript - 检查 Amazon EKS 集群和 Worker 节点 Amazon VPC 安全组规则中是否有建议的 Amazon EKS 集群出口规则。
- aws:executeScript - 检查 Amazon VPC 子网的网络 ACL 配置。
- aws:executeScript - 检查 Worker 节点 Amazon EC2 实例是否具有所需的托管策略。
- aws:executeScript - 检查 Auto Scaling 组是否具有集群自动扩展所需的标签。
- aws:executeScript - 检查 Worker 节点 Amazon EC2 实例是否已连接到互联网。
- aws:executeScript - 根据前面步骤的输出生成报告。如果为 S3BucketName 参数指定了一个值，则生成的报告将上传到 Amazon S3 存储桶。

AWSSupport-TroubleshootEKSWorkerNode

描述

AWSSupport-TroubleshootEKSWorkerNode 运行手册分析 Amazon Elastic Compute Cloud (Amazon EC2) Worker 节点和 Amazon Elastic Kubernetes Service (Amazon EKS)集群，以帮助识别和解决阻碍 Worker 节点加入集群的常见原因。运行手册会输出指南，以帮助解决已发现的任何问题。

> **Important**
>
> 要成功运行此自动化，Amazon EC2 Worker 节点的状态必须为 running，Amazon EKS 集群的状态必须为 ACTIVE。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）Amazon EKS 集群的名称。
- WorkerID

  类型：字符串

  描述：（必需）未能加入集群的 Amazon EC2 Worker 节点的 ID。

所需的 IAM 权限

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

- `ec2:DescribeDhcpOptions`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeNatGateways`

- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- eks:DescribeCluster
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand

文档步骤

- aws:assertAwsResourceProperty - 确认您在 ClusterName 参数中指定的 Amazon EKS 集群存在且处于 ACTIVE 状态。
- aws:assertAwsResourceProperty - 确认您在 WorkerID 参数中指定的 Amazon EC2 Worker 节点存在且处于 running 状态。
- aws:executeScript - 运行 Python 脚本以帮助确定 Worker 节点未能加入集群的可能原因。

AWS-UpdateEKSCluster

描述

AWS-UpdateEKSCluster运行手册可帮助你将亚马逊 Elastic Kubernetes Service（亚马逊 EKS）集群更新到你要使用的 Kubernetes 版本。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）您的 Amazon EKS 集群的名称。
- 版本

  类型：字符串

  描述：（必填）你要将集群更新到的 Kubernetes 版本。

所需的 IAM 权限

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

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

文档步骤

- `aws:executeAwsApi`-更新您的亚马逊 EKS 集群使用的 Kubernetes 版本。
- `aws:waitForAwsResourceProperty`-等待更新状态变为。`Successful`

AWS-UpdateEKSManagedNodeGroup

描述

`AWS-UpdateEKSManagedNodeGroup` 运行手册可帮助您更新 Amazon Elastic Kubernetes Service (Amazon EKS) 托管节点组。您可以选择 `Version` 或 `Configuration` 更新。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要更新其节点组的集群的名称。
- NodeGroup姓名

  类型：字符串

描述：（必选）要更新的节点组的名称。

- UpdateType

  类型：字符串

  有效值：更新节点组版本 | 更新节点组配置

  默认：更新节点组版本

  描述：（必需）要对节点组执行的更新的类型。

以下参数仅适用于 `Version` 更新类型：

- AMI ReleaseVersion

  类型：字符串

  描述：（可选）要使用的 Amazon EKS 优化 AMI 的版本。默认情况下会使用最新版本。
- ForceUpgrade

  类型：布尔值

  描述：（可选）如果为真，则更新不会因容器组中断预算违规而失败。
- KubernetesVersion

  类型：字符串

  描述：（可选）要将节点组更新到的 Kubernetes 版本。
- LaunchTemplate我是

  类型：字符串

  描述：（可选）启动模板的 ID。
- LaunchTemplate姓名

  类型：字符串

  描述：（可选）启动模板的名称。
- LaunchTemplate版本

类型：字符串

描述：（可选）Amazon Elastic Compute Cloud (Amazon EC2) 启动模板版本。此参数仅在节点组是根据启动模板创建时才有效。

以下参数仅适用于 `Configuration` 更新类型：

- AddOrUpdateNodeGroupLabels

  类型: StringMap

  描述：（可选）要添加或更新的 Kubernetes 标签。
- AddOrUpdateKubernetesTaintsEffect

  类型: StringList

  描述：（可选）要添加或更新的 Kubernetes 污点。
- MaxUnavailableNodeGroups

  类型：整数

  默认：0

  描述：（可选）版本更新期间一次不可用的最大节点数量。
- MaxUnavailablePercentageNode组

  类型：整数

  默认值：0

  描述：（可选）版本更新期间不可用的节点的最大百分比。
- NodeGroupDesiredSize

  类型：整数

  默认值：0

  描述：（可选）托管节点组应保留的当前节点数。
- NodeGroupMaxSize

类型：整数

默认值：0

描述：（可选）托管节点组可以扩展到的最大节点数。

- NodeGroupMinSize

  类型：整数

  默认值：0

  描述：（可选）托管节点组可以缩减到的最小节点数。

- RemoveKubernetesTaintsEffect

  类型: StringList

  描述：（可选）要删除的 Kubernetes 污点。

- RemoveNodeGroupLabels

  类型: StringList

  描述：（可选）要删除的以逗号分隔的标签列表。

所需的 IAM 权限

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

- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

文档步骤

- aws:executeScript - 根据您为运行手册输入参数指定的值更新 Amazon EKS 集群节点组。
- aws:waitForAwsResourceProperty - 等待集群更新状态变为 Successful。

AWS-UpdateEKSSelfManagedLinuxNodeGroups

描述

AWS-UpdateEKSSelfManagedLinuxNodeGroups 运行手册使用 AWS CloudFormation 堆栈更新 Amazon Elastic Kubernetes Service (Amazon EKS) 集群中的自托管节点组。

如果您的集群使用自动扩缩，则我们建议在使用此运行手册之前将部署缩小到两个副本。

将部署扩展到两个副本

1. 安装 Kubernetes 命令行实用程序 kubectl。有关更多信息，请参阅 Amazon EKS 用户指南 中的安装 kubectl。
2. 运行以下命令。

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

3. 运行 AWS-UpdateEKSSelfManagedLinuxNodeGroups 运行手册。
4. 运行以下命令，将部署缩回到所需的副本数。

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

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ClusterName

  类型：字符串

  描述：（必需）Amazon EKS 集群的名称。

- NodeGroup姓名

  类型：字符串

  描述：（必需）托管节点组的名称。

- ClusterControlPlaneSecurity组

  类型：字符串

  描述：（必需）控制面板安全组的 ID。

- DisableIMDSv1

  类型：布尔值

  描述：（可选）确定您是否要允许实例元数据服务版本 1 (IMDSv1) 和 IMDSv2。

- KeyName

  类型：字符串

  描述：（可选）实例的秘钥名称。

- NodeAutoScalingGroupDesiredCapacity

  类型：字符串

  描述：（可选）节点组应保留的节点数。

- NodeAutoScalingGroupMaxSize

  类型：字符串

  描述：（可选）节点组可以扩展到的最大节点数。

- NodeAutoScalingGroupMinSize

  类型：字符串

  描述：（可选）节点组可以缩减到的最小节点数。

- NodeInstance类型

  类型：字符串

  默认：t3.large

  描述：（可选）要用于节点组的实例类型。
- NodeImage我是

  类型：字符串

  描述：（可选）希望节点组使用的 Amazon Machine Image (AMI) 的 ID。
- NodeImageidssmParam

  类型：字符串

  默认：/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  描述：（可选）希望节点组使用的 AMI 的公共 Systems Manager 参数。
- StackName

  类型：字符串

  描述：（必填）用于更新节点组的 AWS CloudFormation 堆栈的名称。
- 子网

  类型：字符串

  描述：（必需）要集群使用的子网的逗号分隔列表。
- VpcId

  类型：字符串

  默认：Default

  描述：（必需）部署集群的虚拟私有云（VPC）。

所需的 IAM 权限

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

- eks:CreateCluster
- eks:CreateNodegroup
- eks:DeleteNodegroup
- eks:DeleteCluster
- eks:DescribeCluster
- eks:DescribeNodegroup
- eks:ListClusters
- eks:ListNodegroups
- eks:UpdateClusterConfig
- eks:UpdateNodegroupConfig

文档步骤

- aws:executeScript - 根据您为运行手册输入参数指定的值更新 Amazon EKS 集群节点组。
- aws:waitForAwsResourceProperty-等待 AWS CloudFormation 堆栈更新状态返回。

Elastic Beanstalk

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

主题

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

AWSSupport-CollectElasticBeanstalkLogs

描述

AWSSupport-CollectElasticBeanstalkLogs 运行手册从 Elastic Beanstalk 启动的 Amazon Elastic Compute Cloud (Amazon EC2) Windows Server 实例收集 AWS Elastic Beanstalk 相关日

志文件，以帮助解决常见问题。在此自动化收集关联的日志文件时，会对文件系统结构进行更改，包括创建临时目录、将日志文件复制到临时目录以及将日志文件压缩到档案中。此活动可能会导致 Amazon EC2 实例上的 CPUUtilization 增加。有关更多信息CPUUtilization，请参阅 Amazon CloudWatch 用户指南中的实例指标。

如果您为 S3BucketName 参数指定一个值，此自动化会评估您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶的策略状态。为了帮助保护从 Amazon EC2 实例收集的日志的安全，如果策略状态 isPublic 设置为 true，或者如果访问控制列表（ACL）向 All Users Amazon S3 预定义组授予 READ|WRITE 权限，日志将不会上传。有关 Amazon S3 预定义组的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 预定义组。

如果您没有为 S3BucketName 参数指定一个值，此自动化会将日志捆绑包上传到您运行自动化所在 AWS 区域 的默认 Elastic Beanstalk Amazon S3 存储桶。该目录根据以下结构 elasticbeanstalk- *region* - *accountID* 命名。*region* 和 *accountID* 值将因您运行自动化所在的区域和 AWS 账户 不同而有所不同。日志捆绑包将保存到 resources/environments/logs/bundle/ *environmentID* / *instanceID* 目录。根据您的 Elastic Beanstalk 环境和您从中收集日志的 Amazon EC2 实例，*environmentID* 和 *instanceID* 的值会有所不同。

默认情况下，附加到 Elastic Beanstalk 环境的 Amazon EC2 实例的 AWS Identity and Access Management (IAM) 实例配置文件具有将捆绑包上传到您的环境的默认 Elastic Beanstalk Amazon S3 存储桶所需的权限。如果您为 S3BucketName 参数指定一个值，则附加到 Amazon EC2 实例的实例配置文件必须允许对指定的 Amazon S3 存储桶和路径执行 s3:GetBucketAcl、s3:GetBucketPolicy、s3:GetBucketPolicyStatus 和 s3:PutObject 操作。

> **Note**
>
> 此自动化要求附加到 Amazon EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 根卷上至少有 500 MB 的可用磁盘空间。如果根卷上没有足够的可用磁盘空间，此自动化将停止。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- EnvironmentId

  类型：字符串

  描述：（必需）要从中收集日志捆绑包的 Elastic Beanstalk 环境的 ID。

- InstanceId

  类型：字符串

  （必需）要从中收集日志捆绑包的 Amazon Beanstalk 环境中的 Amazon EC2 实例的 ID。

- S3 BucketName

  类型：字符串

  （可选）要将归档的日志上传到的 Amazon S3 存储桶。

- S3 BucketPath

  类型：字符串

  （可选）要将日志捆绑包上传到的 Amazon S3 存储桶路径。如果您没有为 S3BucketName 参数指定一个值，则忽略此参数。

所需的 IAM 权限

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

- ssm:StartAutomationExecution

- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

文档步骤

- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例由 AWS Systems Manager管理。
- aws:assertAwsResourceProperty - 确认您在 InstanceId 参数中指定的 Amazon EC2 实例是 Windows Server 实例。
- aws:runCommand - 检查该实例是否属于 Elastic Beanstalk 环境，是否有足够的磁盘空间来捆绑日志，以及要上传到的 Amazon S3 存储桶是否是公开的。
- aws:runCommand - 收集日志文件并将档案上传到 S3BucketName 参数中指定的 Amazon S3 存储桶，如果未指定一个值，则上传到 Elastic Beanstalk 环境的默认存储桶。

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

描述

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming运行手册允许在你指定的 AWS Elastic Beanstalk （ Elastic Beanstalk ）环境中进行登录。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- EnvironmentId

  类型：字符串

  描述：（必需）要对其启用日志记录的 Elastic Beanstalk 环境的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文档步骤

- aws:executeAwsApi - 允许对您在 EnvironmentId 参数中指定的 Elastic Beanstalk 环境启用日志记录。
- aws:waitForAwsResourceProperty - 等待环境状态变为 Ready。
- aws:executeScript - 验证是否对 Elastic Beanstalk 环境启用了日志记录。

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

描述

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications运行手册为你指定的 AWS Elastic Beanstalk （Elastic Beanstalk）环境启用通知。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要为之启用通知的 Elastic Beanstalk 环境的 ID。
- TopicArn

  类型：字符串

  描述：（必需）要向其发送通知的 Amazon Simple Notification Service (Amazon SNS) 主题的 ARN。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`

- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

文档步骤

- aws:executeAwsApi - 为您在 EnvironmentId 参数中指定的 Elastic Beanstalk 环境启用通知。
- aws:waitForAwsResourceProperty - 等待环境状态变为 Ready。
- aws:executeScript - 验证是否已为 Elastic Beanstalk 环境启用通知。

AWSSupport-TroubleshootElasticBeanstalk

描述

该AWSSupport-TroubleshootElasticBeanstalk运行手册可帮助您排除 AWS Elastic Beanstalk 环境处于Degraded或Severe状态的潜在原因。此自动化功能会检查与您的 Elastic Beanstalk 环境关联的以下 AWS 资源：

- 负载均衡器、 AWS CloudFormation 堆栈、Amazon EC2 Auto Scaling 组、亚马逊弹性计算云 (Amazon EC2) 实例和虚拟私有云 (VPC) 的配置详细信息。
- 与子网关联的关联安全组规则、路由表和网络访问控制列表（ACL）存在网络配置问题。
- 验证与 Elastic Beanstalk 端点的连接以及公共互联网接入。
- 验证负载均衡器的状态。
- 验证 Amazon EC2 实例的状态。
- 从 Elastic Beanstalk 环境中检索日志包，并可选择将文件上传到。 AWS Support

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- ApplicationName

  类型：字符串

  描述：（必需）您的 Elastac Beanstalk 应用程序的名称。

- EnvironmentName

  类型：字符串

  描述：（必需）您的 Elastic Beanstalk 环境的名称。

- AWSS3UploaderLink

  类型：字符串

  描述：（可选）向您提供的 AWS Support 网址，用于将日志包从 Elastic Beanstalk 环境上传到。此选项仅适用于已购买 AWS Support 计划并已提出 Support 案例的客户。

所需的 IAM 权限

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

- `autoscaling:Describe*`
- `cloudformation:Describe*`
- `cloudformation:Estimate*`
- `cloudformation:Get*`
- `cloudformation:List*`
- `cloudformation:Validate*`

- cloudwatch:Describe*
- cloudwatch:Get*
- cloudwatch:List*
- ec2:Describe*
- elasticbeanstalk:Check*
- elasticbeanstalk:Describe*
- elasticbeanstalk:List*
- elasticbeanstalk:RetrieveEnvironmentInfo*
- elasticbeanstalk:RequestEnvironmentInfo*
- elasticloadbalancing:Describe*
- rds:Describe*
- s3:Get*
- s3:List*
- sns:Get*
- sns:List*

文档步骤

- aws:executeScript-验证启动自动化的 AWS Identity and Access Management (IAM) 委托人是否具有执行运行手册中定义的所有操作的必要权限。
- aws:branch - 根据上一步的结果对工作流进行分支。
- aws:executeScript-收集有关 Elastic Beanstalk 环境的信息，包括负载均衡器、 AWS CloudFormation 堆栈、Auto Scaling 组、Amazon EC2 实例和 VPC 配置。
- aws:executeScript - 检查与 VPC 中的子网关联的路由表和 ACL 是否存在网络连接问题。
- aws:executeScript - 检查与 Amazon EC2 实例关联的安全组规则是否存在网络连接问题。
- aws:executeScript - 验证 Amazon EC2 实例的状态检查。
- aws:executeScript - 为 Elastic Beanstalk 环境的日志捆绑包生成一个链接。
- aws:executeScript-将日志包上传到。 AWS Support
- aws:executeScript - 输出一份操作项报告，以帮助排除可能会影响 Elastic Beanstalk 环境状态的问题。

Elastic Load Balancing

AWS Systems Manager 自动化为 Elastic Load Balancing 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

AWSConfigRemediation-DropInvalidHeadersForALB

描述

AWSConfigRemediation-DropInvalidHeadersForALB 运行手册能让指定的应用程序负载均衡器移除带无效标头的 HTTP 标头。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要丢弃无效标头的负载均衡器的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `aws:executeAwsApi` - 为您在 `LoadBalancerArn` 参数中指定的负载均衡器启用丢弃无效标头设置。
- `aws:executeScript` - 验证是否已对您在 `LoadBalancerArn` 参数中指定的负载均衡器启用丢弃无效标头设置。

AWS-EnableCLBAccessLogs

描述

`AWS-EnableCLBAccessLogs`运行手册启用 Classic Load Balancer 的访问日志。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：整数

  有效值：5 | 60

  默认值：60

  描述：（可选）发布访问日志的时间间隔（以分钟为单位）。
- LoadBalancer名字

  类型：字符串

  描述：（必填）要为其启用访问日志的经典负载均衡器列表，以逗号分隔。
- S3 BucketName

  类型：字符串

  描述：（必填）存储访问日志的亚马逊简单存储服务 (Amazon S3) 存储桶的名称。
- S3 BucketPrefix

类型：字符串

描述：（可选）例如，您为 Amazon S3 存储桶创建的逻辑层次结构`my-bucket-prefix/prod`。如果未提供前缀，则将日志置于存储桶的根级别。

所需的 IAM 权限

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

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `aws:executeAwsApi`-启用您在`LoadBalancerNames`参数中指定的经典负载均衡器的访问日志。

输出

启用 CLB。AccessLogs SuccessesLoadBalancers -成功启用访问日志的负载均衡器名称列表。

启用 CLB。AccessLogs FailedLoadBalancers -启用访问日志失败 MapList 的负载均衡器名称以及失败的原因。

AWS-EnableCLBConnectionDraining

描述

`AWS-EnableCLBConnectionDraining`运行手册允许将 Classic Load Balancer (CLB) 上的连接耗尽到指定的超时值。连接耗尽使 CLB 能够完成向正在注销注册或运行状况不佳的实例发出的动态请求，指定的超时时间是它在报告实例已注销注册之前保持连接活跃的时间。有关 CLB 上连接耗尽的更多信息，请参阅 Classic Load B alanc er 用户指南中的为 Classic Load Balancer 配置连接耗尽。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）要启用连接耗尽的负载均衡器的名称。
- ConnectionTimeout

  类型：整数

  有效值：1-3600

  默认：300

  描述：（必填）负载均衡器的连接超时值。超时值可以设置在 1 到 3600 秒之间。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- ModifyLoadBalancerConnectionDraining (aws: executeAwsApi)：启用连接耗尽并为您指定的负载均衡器设置指定的超时值。
- VerifyLoadBalancerConnectionDrainingEnabled（aws: assert AwsResource 属性）：验证是否已为负载均衡器启用连接耗尽功能。
- VerifyLoadBalancerConnectionDrainingTimeout(aws: assert AwsResource 属性)：验证负载均衡器的连接超时值是否与您指定的值相匹配。

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

描述

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing 运行手册为指定的经典负载均衡器 (CLB) 启用跨区域负载均衡。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用跨区域负载平衡的 CLB 的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elb:DescribeLoadBalancerAttributes
- elb:ModifyLoadBalancerAttributes

文档步骤

- aws:executeAwsApi - 为您在 LoadBalancerName 参数中指定的 CLB 启用跨区域负载均衡。
- aws:assertAwsResourceProperty - 验证是否已对 CLB 启用跨区域负载均衡。

AWSConfigRemediation-EnableELBDeletionProtection

描述

AWSConfigRemediation-EnableELBDeletionProtection 运行手册为指定的弹性负载均衡器 (ELB) 启用删除保护。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

类型：字符串

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

- LoadBalancerArn

  类型：字符串

  描述：（必需）要为其启用删除保护的 ELB 的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `aws:executeScript` - 对您在 `LoadBalancerArn` 参数中指定的 ELB 启用删除保护。

AWSConfigRemediation-EnableLoggingForALBAndCLB

描述

`AWSConfigRemediation-EnableLoggingForALBAndCLB`运行手册允许对指定的 Application Load Balancer 或 C AWS lassic Load Balancer (CLB) 进行日志记录。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）经典负载均衡器名称或应用程序负载均衡器 ARN。
- S3 BucketName

  类型：字符串

  描述：（必需）Amazon S3 存储桶名称。
- S3 BucketPrefix

  类型：字符串

  描述：（可选）为 Amazon Simple Storage Service (Amazon S3) 存储桶创建的逻辑层次结构，例如 `my-bucket-prefix/prod`。如果未提供前缀，则将日志置于存储桶的根级别。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- aws:executeScript - 对经典负载均衡器或应用程序负载均衡器启用日志记录并验证。

AWSSupport-TroubleshootCLBConnectivity

描述

AWSSupport-TroubleshootCLBConnectivity 运行手册可帮助解决经典负载均衡器 (CLB) 和 Amazon Elastic Compute Cloud (Amazon EC2) 实例之间的连接问题。此外，还会审查客户端与 CLB 之间的连接问题。此运行手册还审查 CLB 的运行状况检查，验证是否遵循了最佳实践，并创建问题排查控制面板。或者，也可以将自动化输出上传到 Amazon Simple Storage Service (Amazon S3) 存储桶。但是，此运行手册不支持将输出上传到可公共访问的 S3 存储桶。我们建议为此自动化创建一个临时 S3 存储桶。

> **Important**
>
> 使用此运行手册可能会对创建的控制面板产生费用。有关更多信息，请参阅 Amazon CloudWatch 定价

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- InvestigationType

  类型：字符串

  有效值：最佳实践 | 连接问题 |问题排除控制面板

  描述：（必需）希望运行手册执行的操作。

- LoadBalancer姓名

  类型：字符串

  描述：（必需）CLB 的名称。

- S3Location

  类型：字符串

  描述：（可选）要将自动化结果发送到的 S3 存储桶的名称。不支持可公共访问的存储桶。如果 S3 存储桶使用服务器端加密，则运行此自动化的用户或角色必须拥有 AWS KMS 键的 `kms:GenerateDataKey` 权限。

- S3 LocationPrefix

  类型：字符串

  描述：（可选）要将自动化输出上传到的 Amazon S3 键前缀（子文件夹）。*############ DOC-EXAMPLE-BUCKET/ S3LocationPrefix/{{}} _ {{automation: EXECUTION_ID InvestigationType}}} .txt#*

所需的 IAM 权限

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

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`

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

文档步骤

- aws:executeScript - 验证您在 LoadBalancerName 参数中指定的 CLB 是否存在。

- aws:branch - 根据为 InvestigationType 参数指定的值进行分支。
- aws:executeScript - 对 CLB 执行连接检查。
- aws:executeScript - 验证 CLB 配置是否符合 Elastic Load Balancing 最佳实践。
- aws:executeScript-为您的 CLB 创建 Amazon CloudWatch 控制面板。
- aws:executeScript - 创建包含自动化结果的文本文件，并将其上传到您在 S3Location 参数中指定的 Amazon S3 存储桶。

输出

RunBest实践。摘要

RunConnectivity支票。摘要

CreateTroubleshooting仪表板 > 输出

UploadOutputtos3. 输出

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

描述

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing 运行手册为指定的网络负载均衡器 (NLB) 启用跨区域负载平衡。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- LoadBalancerArn

  类型：字符串

  描述：（必需）要为之启用跨区域负载均衡的 NLB 的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- `aws:executeAwsApi` - 为您在 `LoadBalancerArn` 参数中指定的 NLB 启用跨区域负载平衡。
- `aws:executeScript` - 验证是否已对 NLB 启用跨区域负载平衡。

AWS-updat DesyncMitigation ealB 模式

描述

`AWS-UpdateALBDesyncMitigationMode`运行手册会将 Application Load Balancer (ALB) 上的不同步缓解模式更新为指定的缓解模式。不同步缓解模式决定了负载均衡器如何处理可能对您的应用程序构成安全风险的请求。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）您要修改其不同步缓解模式的 ALB 的 Amazon 资源名称 (ARN)。
- DesyncMitigation模式

  类型：字符串

  有效值：监控 | 防御 | 最严格

  描述：（必填）您希望 ALB 使用的缓解模式。有关不同步缓解模式的信息，请参阅《应用程序负载均衡器用户指南》中的不同步缓解模式。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`

- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- VerifyLoadBalancerType (aws: assert P AwsResource roperty)-在继续下一步之前，验证为`LoadBalancerArn`输入参数指定的值是否适用于应用程序负载均衡器。
- ModifyLoadBalancerDesyncMode (aws: executeAwsApi)-更新 ALB 以使用指定的。`DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws: executeScript)-验证目标 ALB 的不同步缓解模式是否已更新。

输出

VerifyLoadBalancerDesyncMitigationMode。 ModificationResult -脚本的消息有效负载，用于验证对 ALB 的修改。

AWS-updat DesyncMitigation eCLB 模式

描述

`AWS-UpdateCLBDesyncMitigationMode`运行手册会将 Classic Load Balancer (CLB) 上的不同步缓解模式更新为指定的缓解模式。不同步缓解模式决定了负载均衡器如何处理可能对您的应用程序构成安全风险的请求。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- LoadBalancer姓名

  类型：字符串

  描述：（必填）要修改其不同步缓解模式的 CLB 的名称。

- DesyncMitigation模式

  类型：字符串

  有效值：监控 | 防御 | 最严格

  描述：（必填）您希望 CLB 使用的防护模式。有关不同步缓解模式的信息，请参阅《应用程序负载均衡器用户指南》中的不同步缓解模式。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

文档步骤

- ModifyLoadBalancerDesyncMode (aws: executeAwsApi)-更新负载均衡以使用指定的。`DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws: executeScript)-验证目标 CLB 的不同步缓解模式是否已更新。

输出

VerifyLoadBalancerDesyncMitigationMode。 ModificationResult -脚本的消息有效负载，用于验证对 CLB 的修改。

Amazon EMR

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

主题

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

AWSSupport-AnalyzeEMRLogs

描述

此运行手册可帮助识别在 Amazon EMR 集群上运行任务时出现的错误。运行手册分析文件系统上已定义日志的列表，并查找预定义关键字的列表。这些日志条目用于创建 Amazon Events CloudWatch 事件，因此您可以根据事件采取任何必要的操作。或者，运行手册将日志条目发布到您选择的 Amazon Log CloudWatch s 日志组。此运行手册目前在日志文件中查找以下错误和模式：

- container_out_of_memory – YARN 容器内存不足，运行作业可能会失败。
- yarn_nodemanager_health：CORE 或 TASK 节点在磁盘中的运行空间不足，将无法运行任务。
- node_state_change：MASTER 节点无法访问核心或 TASK 节点。
- step_failure：EMR 步骤已失败。
- no_core_nodes_running：当前没有 CORE 节点在运行，集群运行状况不佳。
- hdfs_missing_blocks：缺少 HDFS 块可能会导致数据丢失。
- hdfs_high_util：HDFS 利用率较高，这可能会影响作业和集群运行状况。
- instance_controller_restart：实例控制器进程已重启。此进程对集群运行状况至关重要。
- instance_controller_restart_legacy：实例控制器进程已重启。此进程对集群运行状况至关重要。
- high_load：检测到平均负载过高，这可能会影响节点运行状况报告或导致超时或减速。
- yarn_node_blacklisted：CORE 或 TASK 节点已被 YARN 列入黑名单，无法运行任务。

- yarn_node_lost：CORE 或 TASK 节点已被 YARN 标记为丢失，这可能是连接问题。

与指定的关联的 `ClusterID` 实例必须由 AWS Systems Manager管理。您可以运行此自动化一次，将此自动化安排为按特定的时间间隔运行，或者删除以前由某个自动化创建的时间安排。此运行手册支持 Amazon EMR 发行版 5.20 至 6.30。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要分析其节点日志的集群的 ID。
- 操作

  类型：字符串

  有效值：运行一次 | 计划 | 移除计划

  描述：（必需）要在集群上执行的操作。

- IntervalTime

  类型：字符串

  有效值：5 分钟 | 10 分钟 | 15 分钟

  描述：（可选）运行自动化的间隔时间。此参数仅在您为 Operation 参数指定 Schedule 时适用。

- LogToCloudWatch日志

  类型：字符串

  有效值：是 | 否

  描述：（可选）如果您指定此参数yes的值，则自动化会使用CloudWatchLogGroup参数中指定的名称创建一个 CloudWatch 日志日志组，以存储任何匹配的日志条目。

- CloudWatchLogGroup

  类型：字符串

  描述：（可选）您要在其中存储任何匹配的 CloudWatch 日志条目的日志组的名称。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

- CreateLogInsightsDashboard

  类型：字符串

  有效值：是 | 否

  描述：（可选）如果指定yes，则创建 CloudWatch 仪表板（如果尚不存在）。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

- CreateMetric过滤器

  类型：字符串

  有效值：是 | 否

  描述：（可选）指定yes是否要为 CloudWatch 日志组创建指标筛选器。此参数仅在您为 LogToCloudWatchLogs 参数指定 yes 时适用。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- iam:CreateRole
- iam:DeleteRole
- iam:GetRolePolicy
- iam:PutRolePolicy
- iam:DeleteRolePolicy
- iam:passrole
- cloudformation:DescribeStacks
- cloudformation:DeleteStack
- cloudformation:CreateStack
- events:DeleteRule
- events:RemoveTargets
- events:PutTargets
- events:PutRule
- events:DescribeRule
- logs:DescribeLogGroups
- logs:CreateLogGroup
- logs:PutMetricFilter

- cloudwatch:PutDashboard
- elasticmapreduce:ListInstances
- elasticmapreduce:DescribeCluster

文档步骤

- aws:executeAwsApi - 收集在 ClusterID 参数中指定的 Amazon EMR 集群的相关信息。
- aws:branch - 根据输入进行分支。
  - 如果提供的操作是 Run Once 或 Schedule：
    - aws:assertAwsResourceProperty - 验证集群是否可用。
    - aws:executeAwsApi - 收集集群中运行的所有实例的 ID。
    - aws:assertAwsResourceProperty - 验证 SSM 代理是否在集群中的所有实例上运行。
    - aws:branch - 根据您指定运行自动化一次还是按计划运行进行分支。
      - 如果提供的操作是 Run Once：
        - aws:branch - 根据在 LogToCloudWatchLogs 参数中指定的值进行分支。
          - 如果 LogToCloudWatchLogs 值为 yes：
            - aws:executeScript-检查参数中指定名称的 CloudWatch 日志组是否CloudWatchLogGroup已经存在。如果不存在，则使用指定的名称创建组。
            - aws:branch - 根据在 CreateMetricFilters 参数中指定的值进行分支。
              - 如果 CreateMetricFilters 值为 yes：
                - aws:executeAwsApi - 为每个指标筛选器运行 12 个步骤
                - aws:branch - 根据在 CreateLogInsightsDashboard 参数中指定的值进行分支。
                  - 如果 CreateLogInsightsDashboard 值为 yes：
                    - aws:executeAwsApi-使用CloudWatchLogGroup参数中指定的相同名称创建 CloudWatch仪表板（如果尚不存在）。
                  - 如果 CreateLogInsightsDashboard 值为 no：
                    - aws:runCommand - 运行 Shell 脚本以查找集群中每个实例的日志模式。
              - 如果 CreateMetricFilters 值为 no：
                - aws:branch - 根据在 CreateLogInsightsDashboard 参数中指定的值进行分支。
                  - 如果 CreateLogInsightsDashboard 值为 yes：

- aws:executeAwsApi-使用CloudWatchLogGroup参数中指定的相同名称创建 CloudWatch仪表板（如果尚不存在）。
- 如果 CreateLogInsightsDashboard 值为 no：
  - aws:runCommand - 运行 Shell 脚本以查找集群中每个实例的日志模式。
- 如果 LogToCloudWatchLogs 值为 no：
  - aws:executeAwsApi - 运行 Shell 脚本以查找集群中每个实例的日志模式。
- 如果提供的操作是 Schedule：
  - aws:createStack-创建针对此运行手册的 Amazon EventBridge 事件。
- 如果提供的操作是 Remove Schedule：
  - aws:executeAwsApi - 验证集群是否存在时间表。
  - aws:deleteStack - 删除时间表。

输出

GetCluster信息。 ClusterName

GetCluster信息。 ClusterState

ListingCluster实例。实例 ID

CreatingScheduleCloudFormation堆栈。 StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroup存在。输出

FindLogPatternOnemrNode。 CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

描述

该AWSSupport-DiagnoseEMRLogsWithAthena运行手册使用与数据目录集成的亚马逊 Athena 帮助诊断亚马逊 EMR 日志。 AWS Glue Amazon Athena 用于查询 Amazon EMR 日志文件中的容器、节点日志或两者兼而有之，可选参数用于特定日期范围或基于关键字的搜索。

运行手册可以自动检索现有集群的 Amazon EMR 日志位置，或者您可以指定 Amazon S3 日志位置。为了分析日志，运行手册：

- 创建 AWS Glue 数据库并在 Amazon EMR Amazon S3 日志位置执行 Amazon Athena 数据定义语言 (DDL) 查询，为集群日志和已知问题列表创建表。
- 执行数据操纵语言 (DML) 查询，在 Amazon EMR 日志中搜索已知问题模式。这些查询会按照 Amazon S3 文件路径返回检测到的问题列表、出现次数以及匹配的关键词数量。
- 结果将上传到您在前缀下指定的 Amazon S3 存储桶`saw_diagnose_EMR_known_issues`。
- 运行手册返回 Amazon Athena 的查询结果，重点介绍来自预定义子集的调查结果、建议以及对亚马逊知识中心 (KC) 文章的引用。
- 完成或失败后，上传到 Amazon S3 存储桶的 AWS Glue 数据库和已知问题文件将被删除。

如何工作？

使用 Amazon Athena 对 Amazon EMR 日志`AWSSupport-DiagnoseEMRLogsWithAthena`进行分析，以检测错误并重点介绍调查结果、建议和相关知识中心文章。

运行手册执行以下步骤：

- 使用集群 ID 获取 Amazon EMR 集群日志位置或输入 Amazon S3 位置以检索日志位置和大小。
- 根据日志位置大小提供 Athena 成本估算。
- 在运行 Athena 查询并继续执行后续步骤之前，请向指定的 IAM 委托人申请批准，即可获得批准。
- 将已知问题上传到指定的 Amazon S3 存储桶，创建 AWS Glue 数据库和表。
- 对亚马逊 EMR 日志数据执行 Athena 查询。查询可以按日期范围、关键字和两个条件进行搜索，也可以根据提供的输入在不带筛选条件的情况下运行。
- 分析结果，重点介绍调查结果、建议和相关的 KC 文章。
- 亚马逊 Athena DML 的输出链接查询结果。
- 通过删除已创建的数据库、表和已上传的已知问题来清理环境。

文档类型

自动化

所有者

Amazon

平台

/

该 AutomationAssumeRole 参数需要以下操作才能成功使用运行手册：

- 雅典娜：处决 GetQuery
- 雅典娜：处决 StartQuery
- 雅典娜：声明 GetPrepared
- 雅典娜：声明 CreatePrepared
- 胶水：GetDatabase
- 胶水：CreateDatabase
- 胶水：DeleteDatabase
- 胶水：CreateTable
- 胶水：GetTable
- 胶水：DeleteTable
- 弹性地图减少：DescribeCluster
- s3：ListBucket
- s3：GetBucket版本控制
- s3：ListBucket版本
- s3：GetBucketPublicAccess阻止
- s3：GetBucketPolicyStatus
- s3：GetObject
- s3：GetBucket位置
- 定价：GetProducts
- 定价：GetAttribute价值
- 定价：DescribeServices
- 定价：ListPrice清单

Important

要限制仅访问此自动化所需的资源，请将以下策略附加到信任 SSM 服务的 IAM 角色。将 “分区”、“区域” 和 “帐户” 替换为执行运行手册的分区、区域和账号的相应值。

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

说明

按照这些步骤对自动化进行配置：

1. 在 “文档” 下方导航 AWSSupport-diagn LogsWith oseMr Athena。 AWS Systems Manager
2. 选择 Execute automation（执行自动化）。
3. 要输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

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

     亚马逊 EMR 集群 ID。
   - S3LogLocation （可选）：

     亚马逊 S3 亚马逊 EMR 日志位置。输入路径样式的 URL Amazon S3 位置，例如：。`s3://mybucket/myfolder/j-1K48XXXXXXHCB/`如果 Amazon EMR 集群已终止超过`30`天数，请提供此参数。
   - S3BucketName （必填）：

     用于上传已知问题列表的 Amazon S3 存储桶名称，以及 Amazon Athena 查询的输出。该存储桶应启用封锁公共访问功能，并且与 Amazon EMR 集群位于同一 AWS 区域和账户。
   - 批准者（必填）：

     能够批准或拒绝操作的 AWS 经过身份验证的委托人列表。您可以使用以下任一格式指定委托人：用户名、用户 ARN、IAM 角色 ARN 或 IAM 代入角色 ARN。最大审批者数量为 10。
   - FetchNodeLogsOnly （可选）：

     如果设置为`true`，则自动化会诊断 Amazon EMR 应用程序容器日志。默认值为 `false`。
   - FetchContainersLogsOnly （可选）：

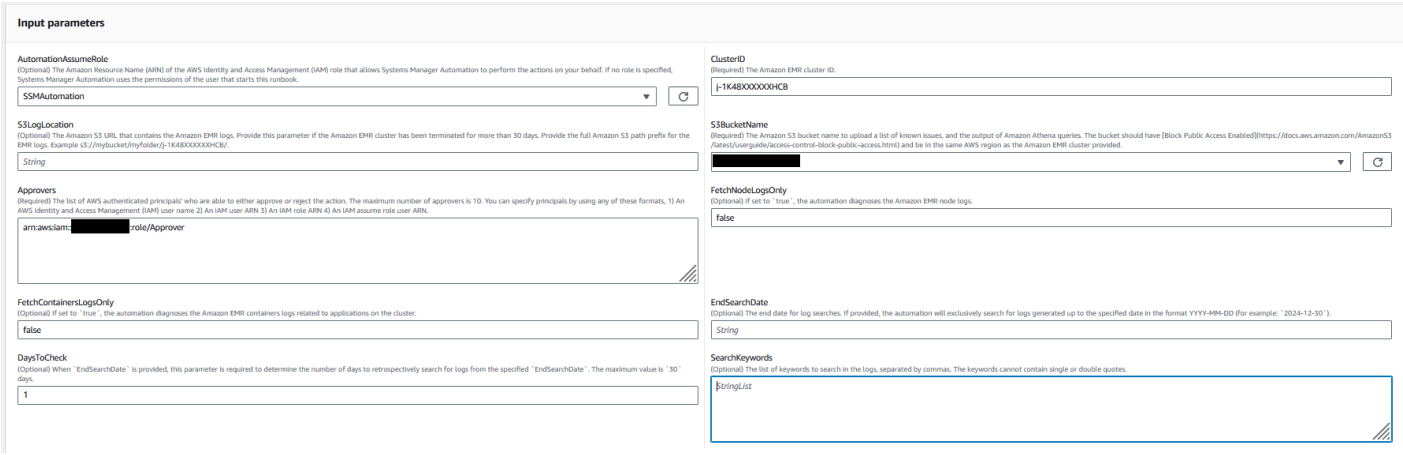
     如果设置为`true`，则自动化会诊断 Amazon EMR 容器日志。默认值为 `false`。
   - EndSearchDate （可选）：

     日志搜索的结束日期。如果提供，则自动化将专门搜索截至指定日期生成的日志，格式为 YYYY-MM-DD（例如：）。`2024-12-30`
   - DaysToCheck （可选）：

如果EndSearchDate提供此参数，则需要使用此参数来确定追溯搜索指定日志的天数。EndSearchDate最大值为30天。默认值为 1。

- SearchKeywords （可选）：

  要在日志中搜索的关键字列表，以逗号分隔。关键字不能包含单引号或双引号。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
   - 得到LogLocation：

     通过查询指定的 Amazon EMR 集群 ID 来检索 Amazon S3 日志位置。如果自动化无法从 Amazon EMR 集群 ID 中查询日志位置，则运行手册将使用输入参数。S3LogLocation
   - 分支OnValid日志：

     验证 Amazon EMR 日志的位置。如果位置有效，则继续估算对亚马逊 EMR 日志执行查询时的 Amazon Athena 潜在成本。
   - 估计AthenaCosts：

     确定 Amazon EMR 日志的大小，并提供对日志数据集执行 Athena 扫描的成本估算。对于非商业区域（非AWS 分区），此步骤仅提供日志大小而不估算成本。可以使用指定区域的 Athena 定价文档计算成本。
   - 批准自动化：

     等待指定的 IAM 委托人批准后继续执行自动化的后续步骤。批准通知包含 Amazon EMR 日志上的 Amazon Athena 扫描的估计费用，以及有关自动配置的资源的详细信息。
   - 上传KnownIssuesExecuteAthena查询：

将预定义的已知问题上传到S3BucketName参数中指定的 Amazon S3 存储桶。创建 AWS Glue 数据库和表。根据输入参数在数据库 AWS Glue 中执行 Amazon Athena 查询。

- 获取QueryExecution状态：

  等待直到 Amazon Athena 查询执行处于状态。SUCCEEDEDAmazon Athena DML 查询在亚马逊 EMR 集群日志中搜索错误和异常。

- 分析AthenaResults：

  分析 Amazon Athena 结果，提供来自一组预定义映射的调查结果、建议和知识中心 (KC) 文章。

- 获取AnalyzeResults查询 1：ExecutionStatus

  等待直到查询执行处于SUCCEEDED状态。Amazon Athena DML 查询分析了之前的 DML 查询的结果。此分析查询将返回匹配的异常以及解决方案和 KC 文章

- 获取 AnalyzeResults Query2：ExecutionStatus

  等待直到查询执行处于SUCCEEDED状态。Amazon Athena DML 查询分析了之前的 DML 查询的结果。此分析查询将返回在每个 Amazon S3 日志路径中检测到的异常/错误的列表。

- 打印AthenaQueries消息：

  打印亚马逊 Athena DML 查询结果的链接。

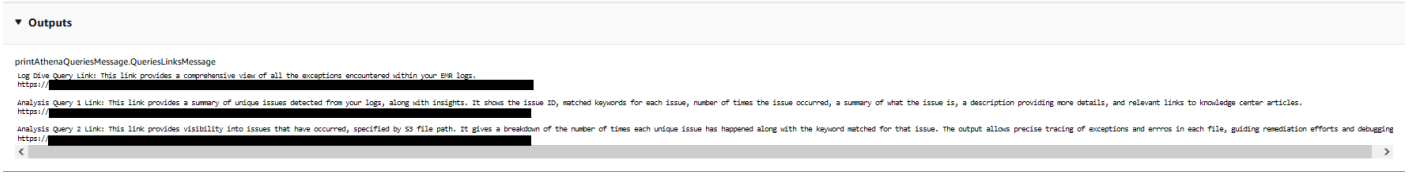
- CleanupResources：

  通过删除已创建的 AWS Glue 数据库来清理资源，并删除在 Amazon EMR 日志存储桶中创建的已知问题文件。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

   输出为 Athena 查询结果提供了三个链接：

   - 列出在 Amazon EMR 集群日志中发现的所有错误和经常发生的异常以及相应的日志位置（Amazon S3 前缀）。
   - Amazon EMR 日志中匹配的唯一已知异常摘要，以及建议的解决方案和 KC 文章，以帮助进行故障排除。
   - 有关特定错误和异常在 Amazon S3 日志路径中出现位置的详细信息，以支持进一步诊断。



参考

Systems Manager Automation

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

AWS 服务文档

- 有关更多信息，请参阅 Amazon EMR 集群故障排除

亚马逊 OpenSearch 服务

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

主题

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

AWSConfigRemediation-DeleteOpenSearchDomain

描述

AWSConfigRemediation-DeleteOpenSearchDomain运行手册使用 DeleteDomainAPI 删除给定的亚马逊 OpenSearch 服务域。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- DomainName

  类型：字符串

  允许的值：(\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  描述：（必填）您要删除的亚马逊 OpenSearch 服务域的名称。
- AutomationAssume角色

  类型：字符串

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

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

文档步骤

- `aws:executeScript`-接受 Amazon Serv OpenSearch ice 域名作为输入，将其删除，然后验证删除。

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

描述

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain运行手册使用 C UpdateDomainonfig API 在给定的亚马逊 OpenSearch 服务域EnforceHTTPS上启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- DomainName

  类型：字符串

  允许的值：(\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  描述：（必填）您要用于强制执行 HTTPS 的亚马逊 OpenSearch 服务域的名称。
- AutomationAssume角色

  类型：字符串

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

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- es:DescribeDomain
- es:UpdateDomainConfig

文档步骤

- aws:executeScript-在DomainName参数中指定的亚马逊 OpenSearch 服务域上启用EnforceHTTPS终端节点选项。

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

描述

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups运行手册使用 C UpdateDomainonfig API 更新给定亚马逊 OpenSearch 服务域上的安全组配置。

> **Note**
>
> AWS 安全组只能应用于为亚马逊虚拟私有云 (VPC) Virtual Private Cloud 访问配置的亚马逊 OpenSearch 服务域，不能应用于配置为公共访问的 OpenSearch 亚马逊服务域。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- DomainName

  类型：字符串

描述：（必填）您要用于更新安全组的 Amazon S OpenSearch ervice 域的名称。

- SecurityGroup名单

  类型: StringList

  描述：（必填）您要分配给 Amazon OpenSearch 服务域的安全组 ID。

- AutomationAssume角色

  类型：字符串

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

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

文档步骤

- `aws:executeScript`-更新您在`DomainName`参数中指定的亚马逊 OpenSearch 服务域上的安全组配置。

AWSSupport-TroubleshootOpenSearchRedYellowCluster

描述

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`automation runbook 用于识别红色或黄色集群运行状况的原因，并指导您将集群更改回绿色。

如何工作？

该运行手册`AWSSupport-TroubleshootOpenSearchRedYellowCluster`可帮助您排除红色或黄色群集的原因，并通过分析群集配置和资源利用率提供了解决此问题的后续步骤。

运行手册执行以下步骤：

- 对目标域调用 DescribeDomainAPI 以获取集群配置。
- 检查 OpenSearch 服务域是基于互联网（公共）还是基于亚马逊虚拟私有云 (VPC) 的。
- 根据集群配置创建公共 AWS Lambda 函数或基于 Amazon VPC 的函数。注意：Lambda 函数包含故障排除代码，用于对集群运行 OpenSearch 服务 API，以确定集群为何处于红色或黄色状态。
- 删除 Lambda 函数。
- 显示已执行的检查以及解决红色或黄色群集问题的后续建议步骤。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

所需的 IAM 权限

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

- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:DeleteStack
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:InvokeFunction
- lambda:GetFunction
- es:DescribeDomain
- es:DescribeDomainConfig

- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:DeleteNetworkInterface
- ec2:DescribeInstances
- ec2:AttachNetworkInterface
- cloudwatch:GetMetricData
- iam:PassRole

该LambdaExecutionRole参数需要以下操作才能成功使用运行手册：

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

LambdaExecutionRole政策概述：

以下是 Lambda 函数的执行角色（AWS Identity and Access Management (IAM) 角色）的示例，该角色向该函数授予访问本运行手册所需的 AWS 服务和资源的权限。有关更多信息，请参阅 Lambda 执行角色。

> **Note**
>
> 只有当ec2:DescribeNetworkInterfaces您的 OpenSearch 服务集群基于 Amazon VPC 时，才需要ec2:CreateNetworkInterface、和ec2:DeleteNetworkInterface，以允许 Lambda 函数创建和管理 Amazon VPC 网络接口。有关更多信息，请参阅将出站联网连接到 Amazon VPC 和 Lambda 执行角色中的资源。

```
{
```

```
            "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"
                }

            ]
        }
```

说明

按照这些步骤对自动化进行配置：

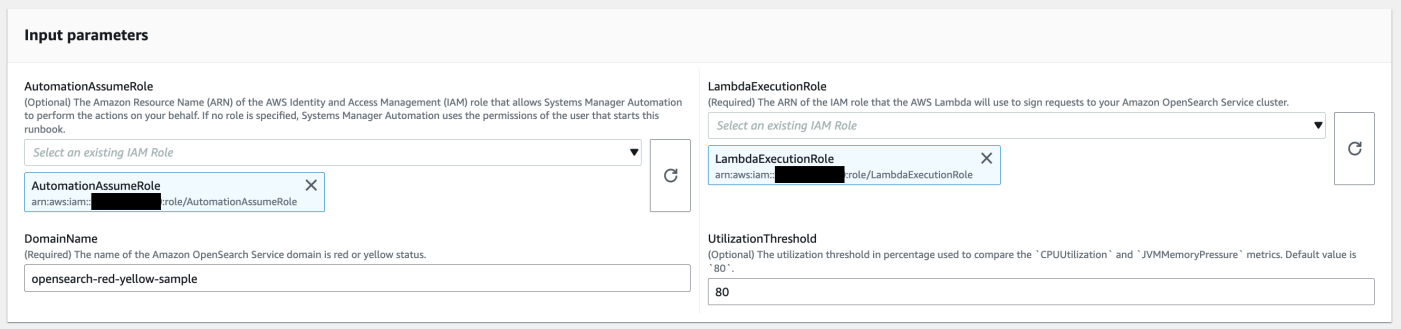
1. 在 AWS Systems Manager 控制台TroubleshootOpenSearchRedYellowCluster中导航到 AWSSupport-。
2. 选择 Execute automation（执行自动化）。
3. 要输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

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

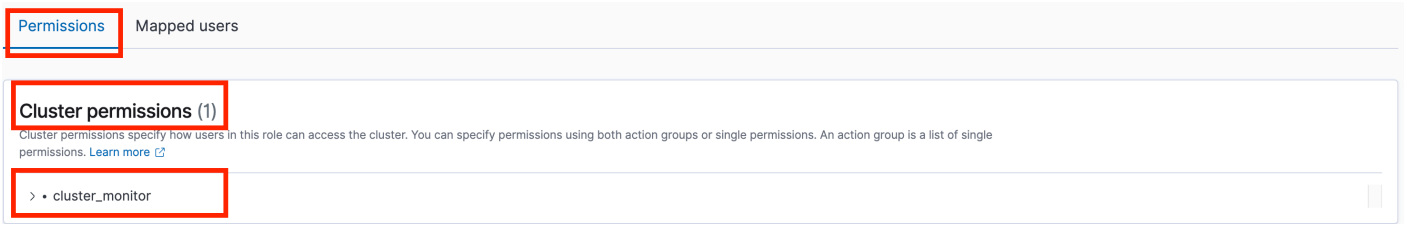
     Lambda 将用于签署对您的亚马逊服务集群的请求的 IAM 角色的 ARN。 OpenSearch
   - DomainName （必填）：

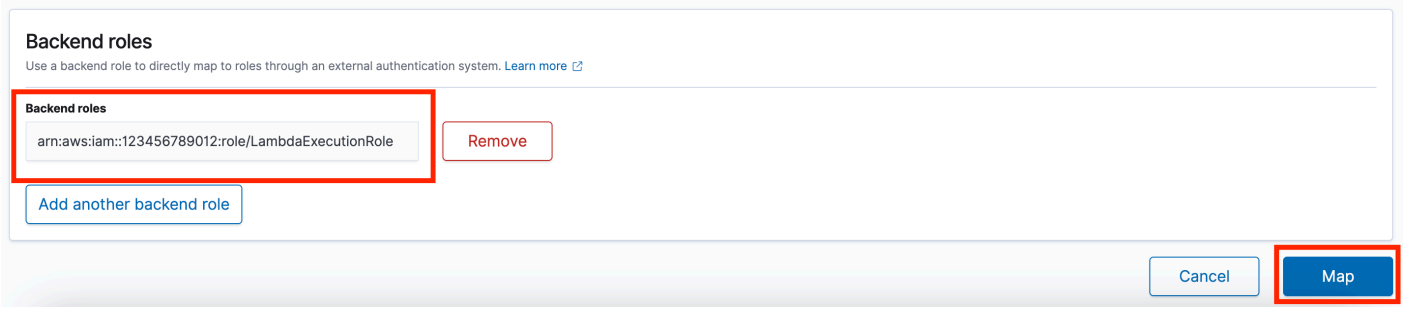
     群集运行状况为红色或黄色的 OpenSearch 服务域的名称。
   - UtilizationThreshold （可选）：

     用于比较 CPU利用率和 J MemoryPressure VM 指标的利用率阈值百分比。默认值为 80。



4. 如果您已在 S OpenSearch ervice 集群上启用了精细访问控制，请确保将LambdaExecutionRole角色 arn 映射到至少具有权限的角色。cluster_monitor





5. 选择执行。
6. 自动化启动。
7. 自动化运行手册执行以下步骤：
   - GetClusterConfiguration:

     获取 OpenSearch 服务集群配置。
   - 创建AWSLambdaFunctionStack：

     使用在您的账户中创建一个临时 Lambda 函数。 AWS CloudFormationLambda 函数用于运行 OpenSearch 服务 API。
   - WaitForAWSLambdaFunctionStack:

     等待 CloudFormation 堆栈完成。
   - GetClusterMetricsFromCloudWatch:

     获取与亚马逊 CloudWatch ClusterStatus、CPU利用率和 JVM MemoryPressure OpenSearch 服务集群相关的指标及其创建日期。
   - RunOpenSearchAPI：

     使用 Lambda 函数调用 OpenSearch 服务 API 并分析集群指标数据，以诊断红色或黄色集群状态的原因。
   - 删除AWSLambdaFunctionStack：

     删除您的账户中由此自动化创建的 Lambda 函数。
8. 完成后，查看“输出”部分以了解执行的详细结果。
   - RootCause:

     概述已确定的集群运行状况处于红色或黄色状态的原因。
   - IssueDescription:

提供有关集群为何处于红色或黄色状态以及使集群恢复到绿色状态的可能步骤的详细信息。

参考

Systems Manager Automation

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

AWS 服务文档

- 有关更多信息，请参阅 Amazon OpenSearch 服务疑难解答

AWSSupport-TroubleshootOpenSearchHighCPU

描述

该AWSSupport-TroubleshootOpenSearchHighCPU运行手册提供了一种自动解决方案，用于从 Amazon S OpenSearch ervice 域收集诊断数据，以解决高 CPU 问题。

如何工作？

该AWSSupport-TroubleshootOpenSearchHighCPU运行手册有助于解决亚马逊 OpenSearch 服务域中 CPU 使用率过高的问题。

运行手册执行以下步骤：

- 对提供的亚马逊 OpenSearch 服务域运行 DescribeDomainAPI 以获取集群元数据。
- 检查亚马逊 OpenSearch 服务域是公共域还是基于 Amazon VPC 的域，并在的帮助下创建公共函数或基于 A mazon V AWS Lambda PC 的 AWS CloudFormation函数。
- Lambda 函数从亚马逊 OpenSearch 服务域中获取诊断数据。
- 使用 AWS Step Functions 状态机协调多个 Lambda 函数执行，以收集更全面的数据。
- 默认情况下，将收集的数据存储在 Amazon CloudWatch 日志组中 24 小时。
- 删除已创建的资源，但 CloudWatch 日志组除外。

所需的 IAM 权限

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

- cloudformation:CreateStack
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:DeleteStack
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:InvokeFunction
- lambda:GetFunction
- lambda:TagResource
- es:DescribeDomain
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:DescribeInstances
- ec2:AttachNetworkInterface
- ec2:DeleteNetworkInterface
- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:TagResource
- states:CreateStateMachine
- states:DeleteStateMachine
- states:StartExecution
- states:TagResource

- states:DescribeStateMachine
- states:DescribeExecution
- iam:PassRole
- iam:CreateRole
- iam:DeleteRole
- iam:GetRole
- iam:PutRolePolicy
- iam:DeleteRolePolicy
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

该LambdaExecutionRole参数需要以下操作才能成功使用运行手册：

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

Lambda 执行角色向该函数授予访问本运行手册所需的 AWS 服务和资源的权限。有关更多信息，请参阅 Lambda 执行角色。

> **Note**
>
> 只有当ec2:DescribeNetworkInterfaces您的 OpenSearch 服务集群基于 Amazon VPC 时，才需要ec2:CreateNetworkInterface、和ec2:DeleteNetworkInterface，以允许 Lambda 函数创建和管理 Amazon VPC 网络接口。有关更多信息，请参阅将出站联网连接到 Amazon VPC 和 Lambda 执行角色中的资源。

说明

按照这些步骤对自动化进行配置：

1. 在 AWS Systems Manager 控制台中导航到 AWSSupport-TroubleshootOpenSearchHigh CPU。
2. 选择 Execute automation（执行自动化）。
3. 要输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

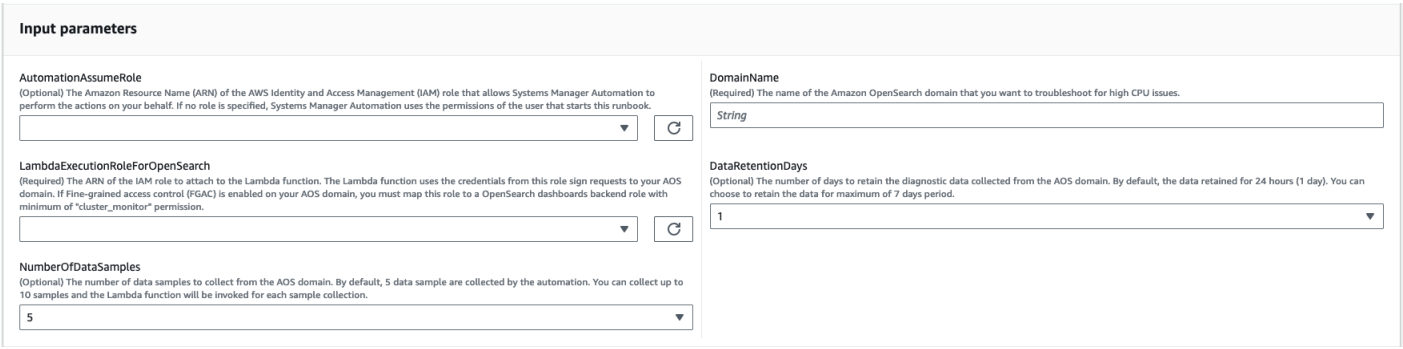
     允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的亚马逊资源名称 (ARN)。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
   - DomainName （必填）：

     您要针对高 CPU 问题进行故障排除的 Amazon OpenSearch 服务域的名称。
   - LambdaExecutionRoleForOpenSearch （必填）：

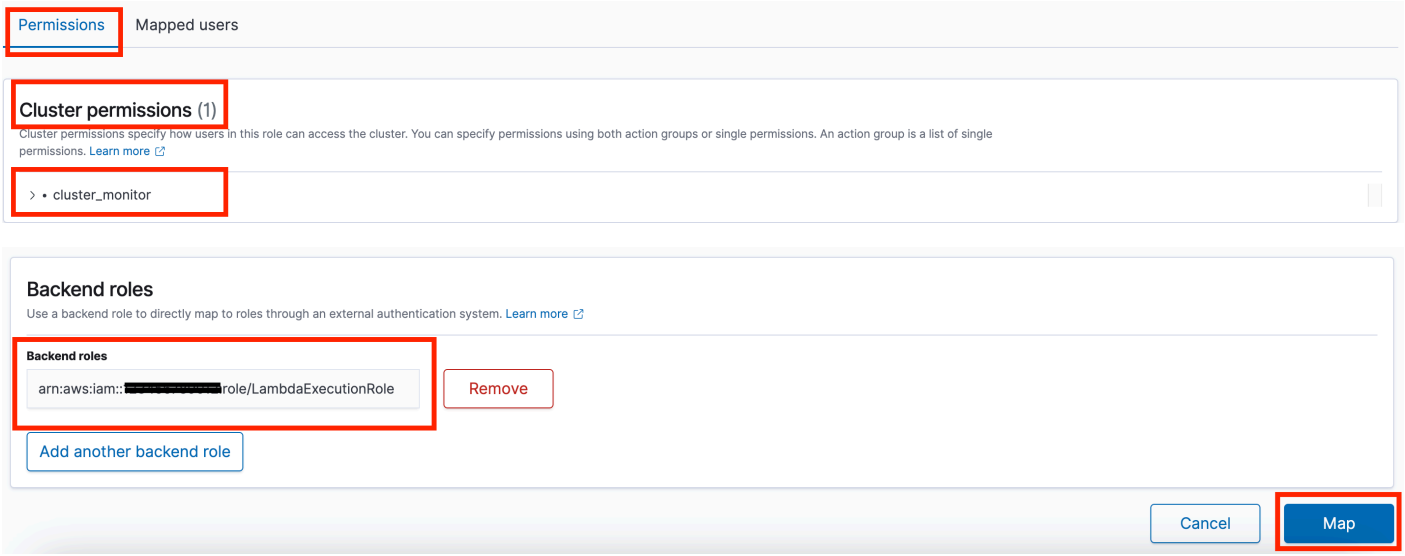
     要附加到 Lambda 函数的 IAM 角色的 ARN。Lambda 函数使用此角色的证书签署对亚马逊 OpenSearch 服务域的请求。如果在 Amazon Ser OpenSearch vice 域上启用了精细访问控制，则必须将此角色映射到至少具有 “cluster_monitor” 权限的 OpenSearch 服务控制面板后端角色。
   - DataRetentionDays （可选）：

     保留从 Amazon OpenSearch 服务域收集的诊断数据的天数。默认情况下，数据保留 24 小时（一天）。您可以选择将数据最多保留 30 天。
   - NumberOfDataSamples （可选）：

     要从 Amazon OpenSearch 服务域中收集的数据样本数量。默认情况下，会收集 5 个数据样本。您最多可以收集 10 个样本，并且将为每个样本集合调用 Lambda 函数。



4. 如果您已在 S OpenSearch ervice 集群上启用了精细访问控制，请确保将`LambdaExecutionRole`角色 arn 映射到至少具有权限的角色。`cluster_monitor`



5. 选择执行。
6. 自动化启动。
7. 自动化运行手册执行以下步骤：
   - 检查并发性：

     确保只有一次针对指定的 Amazon S OpenSearch ervice 域名执行此操作手册。如果 runbook 发现另一次针对相同域名的执行，则会返回错误并结束。
   - getDomainConfig:

     获取目标 OpenSearch 服务域的配置详细信息。
   - 配置资源：

     使用配置用于数据收集的资源 AWS CloudFormation。
   - waitForStack创作：

     等待 AWS CloudFormation 堆栈完成。
   - describeStackResources:

     描述 AWS CloudFormation 堆栈并获取状态机的 ARN。
   - runStateMachine:

     通过运行 Step Functions 状态机来调用数据收集器 Lambda 函数一次或多次。
   - describeErrorsFromStackEvents:

     描述 AWS CloudFormation 堆栈中的错误是否存在错误。

- unstageOpenSearch高 CPU 自动化程度：

  删除AWSSupport-TroubleshootOpenSearchHighCPU AWS CloudFormation 堆栈。

- describeErrorsFromStackDeletion:

  描述删除 AWS CloudFormation 堆栈时遇到的错误。

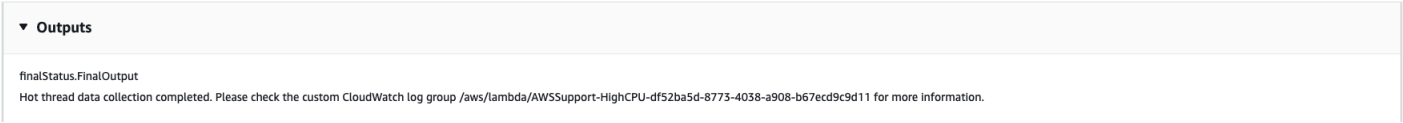
- 最终状态：

  返回AWSSupport-TroubleshootOpenSearchHighCPU运行手册的最终输出。

8. 完成后，查看“输出”部分以了解执行的详细结果。

   - 最终状态。 FinalOutput:

     提供存储诊断数据的 CloudWatch 日志组。



参考

Systems Manager Automation

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

AWS 服务文档

- 有关更多信息，请参阅 Amazon OpenSearch 服务疑难解答

EventBridge

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

主题

- AWS-AddOpsItemDedupStringToEventBridgeRule

- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

描述

该AWS-AddOpsItemDedupStringToEventBridgeRule运行手册为所有 AWS Systems Manager OpsItems 与 Ama EventBridge zon 规则关联的内容添加了重复数据删除字符串。如果已应用重复数据删除字符串，则此运行手册不会添加该字符串至规则中。要了解更多重复数据删除字符串和 OpsItems，请参阅《AWS Systems Manager 用户指南》 OpsItems中的减少重复内容。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- DedupString

  类型：字符串

  描述：（必需）要添加到规则的重复删除字符串。

- RuleName

类型：字符串

描述：（必需）要将重复删除字符串添加到的规则的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:ListTargetsByRule
- events:PutTargets

文档步骤

- aws:executeScript-在RuleName参数中指定的 EventBridge规则中添加重复数据删除字符串。

AWS-DisableEventBridgeRule

描述

AWS-DisableEventBridgeRule运行手册禁用您指定的亚马逊 EventBridge 规则。要了解有关规则的更多信息 EventBridge ，请参阅亚马逊用户指南 EventBridge 中的亚马逊规则。 EventBridge

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- EventBus姓名

  类型：字符串

  默认：default

  描述：（可选）与要禁用的规则关联的事件总线。

- RuleName

  类型：字符串

  描述：（必选）要禁用的规则的名称。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

文档步骤

- `aws:executeAwsApi`-禁用您在`RuleName`参数中指定的 EventBridge 规则。

GuardDuty

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

主题

- AWSConfigRemediation-CreateGuardDutyDetector

AWSConfigRemediation-CreateGuardDutyDetector

描述

AWSConfigRemediation-CreateGuardDutyDetector运行手册会在您运行自动化的 AWS 区域位置创建一个 Amazon GuardDuty (GuardDuty) 检测器。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector

- `guardduty:GetDetector`

文档步骤

- `aws:executeAwsApi`-创建 GuardDuty 探测器。
- `aws:assertAwsResourceProperty` - 验证检测器的 `Status` 是否为 `ENABLED`。

IAM

AWS Systems Manager 自动化为用户提供了预定义的运行手册。 AWS Identity and Access Management有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- 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

描述

将 AWS Identity and Access Management (IAM) 角色附加到托管实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：布尔值

  描述：（可选）指定是否替换现有 IAM 配置文件的标志。

  默认：True
- InstanceId

  类型：字符串

  描述：（必需）要为其分配 IAM 角色的实例 ID。
- RoleName

  类型：字符串

  描述：（必需）要添加到托管实例的 IAM 角色名称。

文档步骤

1. aws:executeAwsApi- DescribeInstanceProfile -查找附加到 EC2 实例的 IAM 实例配置文件。
2. aws:branch- CheckInstanceProfileAssociations -检查附加到 EC2 实例的 IAM 实例配置文件。
   a. 如果附加了 ForceReplace IAM 实例配置文件并将 设置为 true：
      i. aws:executeAwsApi- DisassociateIamInstanceProfile -解除 IAM 实例配置文件与 EC2 实例的关联。
   b. aws:executeAwsApi- ListInstanceProfilesForRole -列出所提供的 IAM 角色的实例配置文件。
   c. aws:branch- CheckInstanceProfileCreated -检查提供的 IAM 角色是否有关联的实例配置文件。
      i. 如果 IAM 角色具有关联的实例配置文件：
         A. aws:executeAwsApi-AttacHiam ProfileToInstance -将 IAM 实例配置文件角色附加到 EC2 实例。
      i. 如果 IAM 角色没有关联的实例配置文件：
         A. aws:executeAwsApi- CreateInstanceProfileForRole -为指定的 IAM 角色创建实例配置文件角色。
         B. aws:executeAwsApi- AddRoleToInstanceProfile -将实例配置文件角色附加到指定的 IAM 角色。
         C. aws:executeAwsApi- GetInstanceProfile-获取指定 IAM 角色的实例配置文件数据。
         D. aws:executeAwsApi-AttacHiam ProfileToInstanceWithRetry -将 IAM 实例配置文件角色附加到 EC2 实例。

输出

AttacHiam ProfileTo InstanceWith 重试。 AssociationId

GetInstance个人资料。 InstanceProfile姓名

GetInstance个人资料。 InstanceProfileArn

AttacHiam 实例ProfileTo。 AssociationId

ListInstanceProfilesFor角色。 InstanceProfile姓名

ListInstanceProfilesFor角色。 InstanceProfileArn

AWS-DeleteIAMInlinePolicy

描述

AWS-DeleteIAMInlinePolicy运行手册会删除附加到您指定的 IAM 身份的所有 AWS Identity and Access Management (IAM) 内联策略。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）要从中删除内联策略的 IAM 身份的 ARN 列表，以逗号分隔。此列表可以包括 IAM 用户、群组或角色。

所需的 IAM 权限

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

- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy

- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

文档步骤

- aws:executeScript-删除附加到目标 IAM 身份的 IAM 内联策略。

AWSConfigRemediation-DeleteIAMRole

描述

AWSConfigRemediation-DeleteIAMRole 运行手册可删除您指定的 AWS Identity and Access Management (IAM) 角色。此自动化并不删除与 IAM 角色或服务相关角色关联的实例配置文件。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

描述：（必选）要删除的 IAM 角色的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfilesForRole
- iam:ListRolePolicies
- iam:ListRoles
- iam:RemoveRoleFromInstanceProfile

文档步骤

- aws:executeScript - 收集您在 IAMRoleID 参数中指定的 IAM 角色的名称。
- aws:executeScript - 收集与 IAM 角色关联的策略和实例配置文件。
- aws:executeScript - 删除附加的策略。
- aws:executeScript - 删除 IAM 角色并验证该角色已被删除。

AWSConfigRemediation-DeleteIAMUser

描述

AWSConfigRemediation-DeleteIAMUser 运行手册可删除您指定的 AWS Identity and Access Management (IAM) 用户。此自动化可删除或分离与 IAM 用户关联的以下资源：

- 访问密钥
- 附加的托管策略

- Git 凭证
- IAM 群组成员资格
- IAM 用户密码
- 内联策略
- 多重身份验证 (MFA) 设备
- 签名证书
- SSH 公约

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必选）要删除的 IAM 用户的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeactivateMFADevice
- iam:DeleteAccessKey
- iam:DeleteLoginProfile
- iam:DeleteServiceSpecificCredential
- iam:DeleteSigningCertificate
- iam:DeleteSSHPublicKey
- iam:DeleteVirtualMFADevice
- iam:DeleteUser
- iam:DeleteUserPolicy
- iam:DetachUserPolicy
- iam:GetUser
- iam:ListAttachedUserPolicies
- iam:ListAccessKeys
- iam:ListGroupsForUser
- iam:ListMFADevices
- iam:ListServiceSpecificCredentials
- iam:ListSigningCertificates
- iam:ListSSHPublicKeys
- iam:ListUserPolicies
- iam:ListUsers
- iam:RemoveUserFromGroup

文档步骤

- aws:executeScript - 收集您在 IAMUserId 参数中指定的 IAM 用户的用户名。
- aws:executeScript - 收集与 IAM 用户关联的访问密钥、证书、凭证、MFA 设备和 SSH 密钥。
- aws:executeScript - 收集 IAM 用户的群组成员资格和策略。
- aws:executeScript - 删除与 IAM 用户关联的访问密钥、证书、凭证、MFA 设备和 SSH 密钥。

- aws:executeScript - 删除 IAM 用户的群组成员资格和策略。
- aws:executeScript - 删除 IAM 用户并验证该用户已被删除。

AWSConfigRemediation-DeleteUnusedIAMGroup

描述

AWSConfigRemediation-DeleteUnusedIAMGroup 运行手册将删除不包含任何用户的 IAM 群组。

AWSConfigRemediation-DeleteUnusedIAMGroup 运行手册将删除不包含任何用户的 IAM 群组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- GroupName

  类型：字符串

  描述：（必需）要删除的 IAM 群组的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteGroup
- iam:DeleteGroupPolicy
- iam:DetachGroupPolicy

文档步骤

- aws:executeScript - 移除附加到目标 IAM 群组的托管和内联 IAM 策略，然后删除该 IAM 组。

AWSConfigRemediation-DeleteUnusedIAMPolicy

描述

AWSConfigRemediation-DeleteUnusedIAMPolicy 运行手册将删除未附加到任何用户、群组或角色的 AWS Identity and Access Management (IAM) 策略。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- IAM ResourceId

  类型：字符串

  描述：（必需）要删除的 IAM policy 的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DeletePolicy
- iam:DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

文档步骤

- aws:executeScript - 删除您在 IAMResourceId 参数中指定的策略，并验证该策略是否已删除。

AWSConfigRemediation-DetachIAMPolicy

描述

AWSConfigRemediation-DetachIAMPolicy 运行手册将分离您指定的 AWS Identity and Access Management (IAM) 策略。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必选）要分离的 IAM policy 的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy
- iam:DetachUserPolicy
- iam:GetPolicy

- iam:ListEntitiesForPolicy

文档步骤

- aws:executeScript - 将 IAM policy 与所有资源分离。

AWSConfigRemediation-EnableAccountAccessAnalyzer

描述

AWSConfigRemediation-EnableAccountAccessAnalyzer运行手册将在您的 AWS 账户中创建一个 AWS Identity and Access Management (IAM) 访问分析器。有关 Access Analyzer 的信息，请参阅《IAM 用户指南》中的使用 AWS IAM Access Analyzer。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AnalyzerName

  类型：字符串

  描述：（必需）要创建的分析器名称。
- AutomationAssume角色

  类型：字符串

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

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- access-analyzer:CreateAnalyzer
- access-analyzer:GetAnalyzer

文档步骤

- aws:executeAwsApi - 为您的账户创建一个访问分析器。
- aws:waitForAwsResourceProperty - 等待访问分析器的状态变为 ACTIVE。
- aws:assertAwsResourceProperty - 确认访问分析器的状态为 ACTIVE。

AWSSupport-GrantPermissionsToIAMUser

描述

此运行手册将指定的权限授予 IAM 组（新建组或现有组），并将现有的 IAM 用户添加到此组。您可以选择的策略：账单或支持。要为 IAM 启用账单访问权限，请注意还需要激活 IAM 用户和联合用户对“账单和成本管理”页面的访问权限。

> **Important**
>
> 如果提供的是现有 IAM 组，则此组中的所有当前 IAM 用户都将收到新权限。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  默认： ExampleSupportAndBillingGroup

  描述：（必需）可以是新组或现有组。必须符合 IAM 实体名称限制。
- IAM UserName

  类型：字符串

  默认： ExampleUser

  描述：（必需）必须是现有用户。
- LambdaAssume角色

  类型：字符串

  描述：（可选）Lambda担任的角色的 ARN。
- 权限

  类型：字符串

  有效值： SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  默认： SupportAndBillingFullAccess

  描述：（必需）选择以下值之一：`SupportFullAccess` 授予支持中心的完全访问权限。`BillingFullAccess` 授予“账单”控制面板的完全访问权

限。SupportAndBillingFullAccess 授予支持中心和“账单”控制面板的完全访问权限。有关策略的更多信息，请参阅文档详细信息。

所需的 IAM 权限

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

所需的权限取决于 AWSSupport-GrantPermissionsToIAMUser 的运行方式。

以当前登录的用户或角色运行

建议附加 AmazonSSMAutomationRole Amazon 托管策略以及以下额外权限，以便创建 Lambda 函数和将 IAM 角色传递给 Lambda：

```
{
                    "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

用户必须对运行手册具有 ssm: StartAutomation 执行权限，对作为AutomationAssume角色和角色传递的 IAM 角色必须具有 iam: PassRole 权限。LambdaAssume以下是每个 IAM 角色所需的权限：

```
AutomationAssumeRole

                    {
                        "Version": "2012-10-17",
                        "Statement": [
                            {
                                "Action": [
                                    "lambda:InvokeFunction",
                                    "lambda:CreateFunction",
                                    "lambda:DeleteFunction",
                                    "lambda:GetFunction"
                                ],
```

```
                                "Resource":
 "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
                                "Effect": "Allow"
                            }
                        ]
                    }
```

LambdaAssumeRole

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

```
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:ListAccountAliases",
                            "iam:GetAccountSummary"
                        ],
                        "Resource" : "*"
                    }
                ]
            }
```

文档步骤

1. aws:createStack-运行 AWS CloudFormation 模板创建 Lambda 函数。
2. aws:invokeLambdaFunction - 运行 Lambda 以设置 IAM 权限。
3. aws:deleteStack-删除 CloudFormation 模板。

输出

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

描述

AWSConfigRemediation-RemoveUserPolicies 运行手册将删除 AWS Identity and Access Management (IAM) 内联策略，并分离附加到指定用户的所有托管策略。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- IAMUserID

  类型：字符串

  描述：（必需）要从其移除策略的用户的 ID。

- PolicyType

  类型：字符串

  有效值：全部 | 内联 | 托管

  默认：全部

  描述：（必需）要从用户移除的 IAM 策略的类型。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteUserPolicy
- iam:DetachUserPolicy
- iam:ListAttachedUserPolicies
- iam:ListUserPolicies
- iam:ListUsers

文档步骤

- aws:executeScript - 删除您在 IAMUserID 参数中指定的用户的 IAM 策略并将其与该用户分离。

AWSConfigRemediation-ReplaceIAMInlinePolicy

描述

该AWSConfigRemediation-ReplaceIAMInlinePolicy运行手册将内联 AWS Identity and Access Management (IAM) 策略替换为复制的托管 IAM 策略。对于附加到用户、群组或角色的内联策略，内联策略权限会克隆到托管 IAM policy。托管 IAM 策略已添加到资源中，并删除内联策略。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型: StringList

  描述：（必需）要替换的内联 IAM policy。
- ResourceId

  类型：字符串

  描述：（必需）要替换其内联策略的 IAM 用户、群组或角色的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:AttachGroupPolicy
- iam:AttachRolePolicy
- iam:AttachUserPolicy
- iam:CreatePolicy
- iam:CreatePolicyVersion
- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:GetGroupPolicy
- iam:GetRolePolicy
- iam:GetUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

文档步骤

- aws:executeScript - 将内联 IAM policy 替换为指定资源的 AWS 复制策略。

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

描述

AWSConfigRemediation-RevokeUnusedIAMUserCredentials运行手册会撤销未使用的 AWS Identity and Access Management (IAM) 密码和有效的访问密钥。此运行手册还会停用过期的访问密钥，并删除过期的登录配置文件。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要从其撤销未使用的凭证的 IAM 资源的 ID。
- MaxCredentialUsageAge

  类型：字符串

  默认：90

  描述：（必需）凭证必须已使用的天数。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`

- iam:DeleteAccessKey
- iam:DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

文档步骤

- aws:executeScript - 撤销您在 IAMResourceId 参数中指定的用户的 IAM 凭证。过期的访问密钥将被停用，过期的登录配置文件将被删除。

> **Note**
>
> 确保将此修复操作的MaxCredentialUsageAge参数配置为与用于触发此操作的 AWS Config 规则的maxAccessKeyAge参数相匹配：access-keys- rotated。

AWSConfigRemediation-SetIAMPasswordPolicy

描述

AWSConfigRemediation-SetIAMPasswordPolicy运行手册将为您的 AWS 账户设置 AWS Identity and Access Management (IAM) 用户密码策略。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- AllowUsersToChange密码

  类型：布尔值

  默认：false

  描述：（可选）如果设置为`true`，则您的所有 IAM 用户都 AWS 账户 可以使用 AWS Management Console 来更改其密码。

- HardExpiry

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，IAM 用户将无法在密码到期后重置密码。

- MaxPassword年龄

  类型：整数

  默认值：0

  描述：（可选）IAM 用户密码的有效天数。

- MinimumPassword长度

  类型：整数

  默认：6

  描述：（可选）IAM 用户的密码可以包含的最少字符数。

- PasswordReuse预防

类型：整数

默认值：0

描述：（可选）阻止 IAM 用户再次使用的先前密码的数量。

- RequireLowercase人物

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，则 IAM 用户的密码必须包含 ISO 基本拉丁字母（a 到 z）中的小写字符。

- RequireNumbers

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，则 IAM 用户的密码必须包含数字字符 (0-9)。

- RequireSymbols

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，则 IAM 用户的密码必须包含非字母数字字符 (! @ # $ % ^ * ( ) _ + - = [ ] { } | ')。

- RequireUppercase人物

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，则 IAM 用户的密码必须包含 ISO 基本拉丁字母（A 到 Z）中的大写字符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:GetAccountPasswordPolicy
- iam:UpdateAccountPasswordPolicy

文档步骤

- aws:executeScript - 根据您为 AWS 账户的运行手册参数指定的值设置 IAM 用户密码策略。

Amazon Kinesis Data Streams

AWS Systems Manager Automation 为 Amazon Kinesis Data Streams 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-EnableKinesisStreamEncryption

AWS-EnableKinesisStreamEncryption

描述

该AWS-EnableKinesisStreamEncryption运行手册支持对亚马逊 Kinesis Data Streams（Kinesis Data Streams）进行加密。写入加密流的生产者应用程序如果无权访问 AWS Key Management Service (AWS KMS) 密钥，则会遇到错误。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- KinesisStreamName

  类型：字符串

  描述：（必填）要启用加密的直播的名称。

- KeyId

  类型：字符串

  默认：别名/aws/kinesis

  描述：（必填）您要用于加密的客户管理的密AWS KMS钥。此值可以是全局唯一标识符、别名或密钥的 ARN，也可以是以 “alias/” 为前缀的别名。您也可以通过使用参数的默认值来使用AWS托管密钥。

所需的 IAM 权限

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

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

文档步骤

- VerifyKinesisStreamStatus (aws: waitforAwsResource 财产)-检查 Kinesis Data Streams 的状态。
- EnableKinesisStreamEncryption (aws:executeAwsApi)-为 Kinesis Data Streams 启用加密。

- VerifyKinesisStreamUpdateComplete (aws: waitForAwsResourceProperty)-等待 Kinesis Data Streams 状态恢复为。ACTIVE
- VerifyKinesisStreamEncryption (aws: P assertAwsResource roperty)-验证是否已为 Kinesis Data Streams 启用加密。

AWS KMS

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

主题

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

AWSConfigRemediation-CancelKeyDeletion

描述

AWSConfigRemediation-CancelKeyDeletion运行手册取消对您指定的 AWS Key Management Service (AWS KMS) 客户托管密钥的删除。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

类型：字符串

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

- KeyId

  类型：字符串

  描述：（必需）要为其取消删除的客户托管密钥的 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion
- kms:DescribeKey

文档步骤

- aws:executeAwsApi - 取消删除您在 KeyId 参数中指定的客户托管密钥。
- aws:assertAwsResourceProperty - 确认客户托管密钥已被禁用。

AWSConfigRemediation-EnableKeyRotation

描述

该AWSConfigRemediation-EnableKeyRotation运行手册支持对 symmetric AWS Key Management Service (AWS KMS) 客户托管密钥进行自动密钥轮换。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用自动密钥轮换的客户托管密钥的 ID。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

文档步骤

- `aws:executeAwsApi` - 对您在 `KeyId` 参数中指定的客户托管密钥启用自动密钥轮换。
- `aws:assertAwsResourceProperty` - 确认对客户托管密钥启用了自动密钥轮换。

Lambda

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

主题

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

描述

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing运行手册允许对您在FunctionName参数中指定的 AWS Lambda 函数进行 AWS X-Ray 实时跟踪。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

类型：字符串

描述：（必需）要对其启用跟踪的 Lambda 函数的名称或 ARN。

所需的 IAM 权限

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

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

文档步骤

- aws:executeAwsApi - 对您在 FunctionName 参数中指定的 Lambda 函数启用 X-Ray 跟踪。
- aws:assertAwsResourceProperty - 验证是否已对 Lambda 函数启用 X-Ray 跟踪。

输出

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

AWSConfigRemediation-DeleteLambdaFunction

描述

AWSConfigRemediation-DeleteLambdaFunction运行手册将删除您指定的 AWS Lambda 函数。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- LambdaFunction姓名

  类型：字符串

  描述：（必需）要删除的 Lambda 函数的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:DeleteFunction
- lambda:GetFunction

文档步骤

- aws:executeAwsApi - 删除在 LambdaFunctionName 参数中指定的 Lambda 函数。
- aws:executeScript - 验证 Lambda 函数是否已被删除。

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

描述

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK运行手册对您使用 () 客户托管密钥指定的 AWS Key Management Service (AWS Lambda AWS KMS Lambda) 函数的环

境变量进行静态加密。此运行手册应仅用作基准，以确保根据建议的最低安全性最佳实践对 Lambda 函数的环境变量进行加密。我们建议使用不同的客户托管密钥对多个函数进行加密。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要加密其环境变量的 Lambda 函数的名称或 ARN。
- KMS KeyArn

  类型：字符串

  描述：（必填）您要用于加密 Lambda 函数环境变量的 AWS KMS 客户托管密钥的 ARN。

所需的 IAM 权限

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

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

- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文档步骤

- aws:waitForAwsResourceProperty - 等待 LastUpdateStatus 属性变为 Successful。
- aws:executeAwsApi-使用您在参数中指定的客户托管密钥加密您在参数中FunctionName指定的 Lambda 函数 AWS KMS 的环境变量。KMSKeyArn
- aws:assertAwsResourceProperty - 确认对 Lambda 函数的环境变量启用了加密。

AWSConfigRemediation-MoveLambdaToVPC

描述

AWSConfigRemediation-MoveLambdaToVPC 运行手册将 AWS Lambda （Lambda）函数移至 Amazon Virtual Private Cloud (Amazon VPC)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- FunctionName

  类型：字符串

  描述：（必需）要移至 Amazon VPC 的 Lambda 函数的名称。
- SecurityGroup身份证

  类型：字符串

  描述：（必需）要分配给与 Lambda 函数关联的弹性网络接口 (ENI) 的安全组 ID。
- SubnetIds

  类型：字符串

  描述：（必需）要创建与 Lambda 函数关联的弹性网络接口 (ENI) 的子网 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunction
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

文档步骤

- aws:executeAwsApi - 更新您在 FunctionName 参数中指定的 Lambda 函数的 Amazon VPC 配置。
- aws:waitForAwsResourceProperty - 等待 Lambda 函数 LastUpdateStatus 生成 successful。
- aws:executeScript - 验证 Lambda 函数 Amazon VPC 配置是否已成功更新。

AWSSupport-RemediateLambdaS3Event

描述

该AWSSupport-TroubleshootLambdaS3Event运行手册为 AWS 知识中心文章中概述的程序提供了自动解决方案为什么我的 Amazon S3 事件通知没有触发我的 Lambda 函数？ 以及为什么在创建 Amazon S3 事件通知以触发我的 Lambda 函数时会出现 “无法验证以下目标配置” 错误？ 本运行手册可帮助您识别和修复亚马逊简单存储服务 (Amazon S3) Simple Service 事件通知未能触发您指定的功能的原因。 AWS Lambda 如果运行手册的输出建议验证和配置 Lambda 函数并发性，请参阅异步调用和AWS Lambda 函数扩展。

> **Note**
>
> 由于 Amazon Simple Notification Service (Amazon SNS) 和 Amazon Simple Queue Service (Amazon SQS) Amazon S3 事件配置不正确，因此也可能出现“无法验证以下目标配置”错误。此运行手册仅检查 Lambda 函数配置。如果在使用运行手册后仍然收到“无法验证以下目标配置”错误，请查看所有现有的 Amazon SNS 和 Amazon SQS Amazon S3 事件配置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- LambdaFunctionArn

  类型：字符串

描述：（必需）Lambda 函数的 ARN。

- S3 BucketName

  类型：字符串

  描述：（必需）其事件通知会触发 Lambda 函数的 Amazon S3 存储桶的名称。

- 操作

  类型：字符串

  有效值：故障排除 | 纠正

  描述：（必需）要运行手册执行的操作。Troubleshoot 选项可帮助识别任何问题，但不会执行任何变更操作来解决问题。Remediate 选项有助于识别并尝试解决问题。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- lambda:GetPolicy
- lambda:AddPermission
- s3:GetBucketNotification

文档步骤

- aws:branch- 根据为 Action 参数指定的输入进行分支。

  如果指定的值为 Troubleshoot：

  - aws:executeAutomation - 运行 AWSSupport-TroubleshootLambdaS3Event 运行手册。

- aws:executeAwsApi - 检查在上一步运行的 AWSSupport-TroubleshootLambdaS3Event 运行手册的输出。

如果指定的值为 Remediate：

- aws:executeScript - 运行脚本来纠正为什么我的 Amazon S3 事件通知没有触发 Lambda 函数？以及为什么我在创建 Amazon S3 事件通知以触发 Lambda 函数时会出现“无法验证以下目标配置”错误？中概述的问题。知识中心文章。

输出

checkoutput.Output

remediatelambdas3event.Output

AWSSupport-TroubleshootLambdaInternetAccess

描述

该AWSSupport-TroubleshootLambdaInternetAccess运行手册可帮助您解决在亚马逊虚拟私有云（Amazon VPC）中启动的 AWS Lambda 功能的互联网访问问题。对子网路由、安全组规则和网络访问控制列表 (ACL) 规则等资源进行审查，以确认允许出站互联网访问。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- FunctionName

  类型：字符串

  描述：（必需）要为其排除互联网访问问题的 Lambda 函数的名称。

- destinationIp

  类型：字符串

  描述：（必需）要与之建立出站连接的目标 IP 地址。

- destinationPort

  类型：字符串

  默认值：443

  描述：（可选）要在其上建立出站连接的目标端口。

所需的 IAM 权限

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

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

文档步骤

- `aws:executeScript` - 验证启动 Lambda 函数的 VPC 中各种资源的配置。
- `aws:branch` - 根据指定的 Lambda 函数是否在 VPC 中进行分支。
- `aws:executeScript` - 查看其中启动 Lambda 函数的子网的路由表路由，并验证是否存在到网络地址转换 (NAT) 网关和互联网网关的路由。确认 Lambda 函数不在公有子网中。

- aws:executeScript - 根据为 destinationIp 和 destinationPort 参数指定的值，验证与 Lambda 函数关联的安全组是否允许出站互联网访问。
- aws:executeScript - 根据为 destinationIp 和 destinationPort 参数指定的值，验证与 Lambda 函数子网关联的 ACL 规则和 NAT 网关是否允许出站互联网访问。

输出

checkVpc.vpc - Lambda 函数启动所在 VPC 的 ID。

checkVpc.subnet - Lambda 函数启动所在子网的 ID。

checkVpc.securityGroups - 与 Lambda 函数关联的安全组。

checkNACL.NACL - 带有资源名称的分析消息。LambdaIp 指 Lambda 函数的弹性网络接口的私有 IP 地址。LambdaIpRules 对象仅对具有通往 NAT 网关的路由的子网生成。以下内容为输出示例。

```
{
   "subnet-1234567890":{
      "NACL":"acl-1234567890",
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / 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"
   }
}
```

查看 SecurityGroups .secgrps-分析与您的 Lambda 函数关联的安全组。以下内容为输出示例。

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets - 对 VPC 中与 Lambda 函数关联的子网的分析。以下内容为输出示例。

```
{
   "subnet-0c4ee6cdexample15":{
      "Route":{
         "DestinationCidrBlock":"8.8.8.0/26",
         "NatGatewayId":"nat-00f0example69fdec",
         "Origin":"CreateRoute",
         "State":"active"
      },
      "Analysis":"This Route Table has an active NAT gateway path. Also, The NAT
 gateway is launched in public subnet",
      "RouteTable":"rtb-0b1fexample16961b"
   }
}
```

AWSSupport-TroubleshootLambdaS3Event

描述

该AWSSupport-TroubleshootLambdaS3Event运行手册为 AWS 知识中心文章中概述的程序提供了自动解决方案为什么我的 Amazon S3 事件通知没有触发我的 Lambda 函数？ 以及为什么在创建 Amazon S3 事件通知以触发我的 Lambda 函数时会出现 “无法验证以下目标配置” 错误？ 本运行手册可帮助您确定亚马逊简单存储服务 (Amazon S3) Simple Service 事件通知未能触发 AWS Lambda 您指定的功能的原因。如果运行手册的输出建议验证和配置 Lambda 函数并发性，请参阅异步调用和AWS Lambda 函数扩展。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）Amazon S3 事件通知触发的 Lambda 函数的 ARN。
- S3 BucketName

  类型：字符串

  描述：（必需）其事件通知会触发 Lambda 函数的 Amazon S3 存储桶的名称。

所需的 IAM 权限

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

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

文档步骤

- `aws:executeScript` - 运行脚本以验证 Amazon S3 事件通知的配置设置。验证您的 Lambda 函数的基于资源的 IAM 策略，并在策略中缺少所需权限时生成 AWS Command Line Interface (AWS CLI) 命令以添加所需的权限。验证其他 Lambda 函数资源策略，这些策略是同一 S3 存储桶的事件通知的一部分，如果缺少所需权限，则生成命令 AWS CLI 作为输出。

输出

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager Automation 为 Apache Airflow 的亚马逊托管工作流程提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWSSupport-TroubleshootMWAAEnvironmentCreation

AWSSupport-TroubleshootMWAAEnvironmentCreation

描述

该AWSSupport-TroubleshootMWAAEnvironmentCreation运行手册提供了调试适用于 Apache Airflow 的亚马逊托管工作流程 (Amazon MWAA) 环境创建问题的信息，并尽最大努力执行检查和记录在案的原因，以帮助识别故障。

如何工作？

运行手册执行以下步骤：

- 检索 Amazon MWAA 环境的详细信息。
- 验证执行角色权限。
- 检查环境是否有权使用提供的 AWS KMS 密钥进行日志记录，以及所需的 CloudWatch 日志组是否存在。
- 解析提供的日志组中的日志以查找任何错误。
- 检查网络配置以验证 Amazon MWAA 环境是否可以访问所需的终端节点。
- 生成包含调查结果的报告。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

/

所需的 IAM 权限

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

- airflow:GetEnvironment
- cloudtrail:LookupEvents
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:ListAttachedRolePolicies
- iam:ListRolePolicies
- iam:SimulateCustomPolicy
- kms:GetKeyPolicy
- kms:ListAliases
- logs:DescribeLogGroups
- logs:FilterLogEvents
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetPublicAccessBlock

- s3control:GetPublicAccessBlock
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

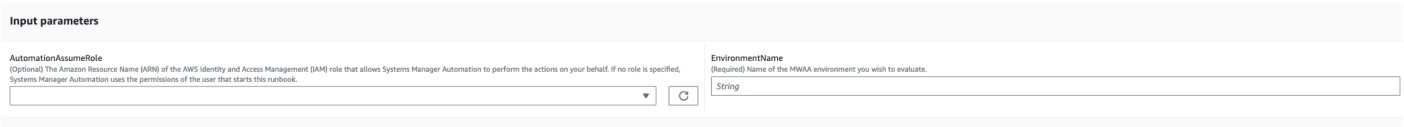
说明

按照这些步骤对自动化进行配置：

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

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

     您要评估的 Amazon MWAA 环境的名称。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
   - **GetMWAAEnvironmentDetails:**

     检索 Amazon MWAA 环境的详细信息。如果此步骤失败，自动化过程将停止并显示为Failed。
   - **CheckIAMPermissionsOnExecutionRole:**

     验证执行角色是否具有使用 Amazon MWAA、Amazon S3 CloudWatch、 CloudWatch 日志和亚马逊 SQS 资源所需的权限。如果它检测到客户托管 AWS Key Management Service (AWS KMS) 密钥，则自动化会验证该密钥的所需权限。此步骤使用 iam:SimulateCustomPolicy API 来确定自动化执行角色是否满足所有必需的权限。
   - **CheckKMSPolicyOnKMSKey:**

检查 AWS KMS 密钥策略是否允许 Amazon MWAA 环境使用该密钥加密 CloudWatch 日志。如果 AWS KMS 密钥是 AWS-managed，则自动化会跳过此检查。

- **CheckIfRequiredLogGroupsExists:**

  检查 Amazon MWAA 环境所需的 CloudWatch 日志组是否存在。如果不是，则自动化会 CloudTrail 检查`CreateLogGroup`和`DeleteLogGroup`事件。此步骤还会检查`CreateLogGroup`事件。

- **BranchOnLogGroupsFindings:**

  基于是否存在与 Amazon MWAA 环境相关的 CloudWatch 日志组进行分支。如果至少存在一个日志组，则自动化会对其进行解析以查找错误。如果不存在任何日志组，则自动化会跳过下一步。

- **CheckForErrorsInLogGroups:**

  解析 CloudWatch 日志组以查找错误。

- **GetRequiredEndPointsDetails:**

  检索 Amazon MWAA 环境使用的服务终端节点。

- **CheckNetworkConfiguration:**

  验证 Amazon MWAA 环境的网络配置是否符合要求，包括检查安全组、网络 ACL、子网和路由表配置。

- **CheckEndpointsConnectivity:**

  调用`AWSSupport-ConnectivityTroubleshooter`子自动化来验证 Amazon MWAA 与所需终端节点的连接。

- **CheckS3BlockPublicAccess:**

  检查亚马逊 MWAA 环境的 Amazon S3 存储桶是否已`Block Public Access`启用，并查看该账户的整体 Amazon S3 阻止公共访问设置。

- **GenerateReport:**

  从自动化中收集信息并打印每个步骤的结果或输出。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

   - 正在检查 Amazon MWAA 环境执行角色权限：

验证执行角色是否具有 Amazon MWAA、Amazon S3 CloudWatch、 CloudWatch 日志和 Amazon SQS 资源所需的权限。如果检测到客户管理的 AWS KMS 密钥，则自动化将验证该密钥的所需权限。

- 查看 Amazon MWAA 环境 AWS KMS 密钥策略：

  验证执行角色是否拥有使用 Amazon MWAA、Amazon S3、 CloudWatch CloudWatch日志和 Amazon SQS 资源的必要权限。此外，如果检测到客户管理的 AWS KMS 密钥，自动化系统会检查该密钥的所需权限。

- 检查 Amazon MWAA 环境 CloudWatch 日志组：

  检查 Amazon MWAA 环境所需的 CloudWatch 日志组是否存在。如果没有，则自动化系统会检查 CloudTrail 定位`CreateLogGroup`和`DeleteLogGroup`事件。

- 检查 Amazon MWAA 环境路由表：

  检查 Amazon MWAA 环境中的 Amazon VPC 路由表配置是否正确。

- 检查 Amazon MWAA 环境安全组：

  检查 Amazon MWAA 环境 Amazon VPC 安全组的配置是否正确。

- 检查 Amazon MWAA 环境网络 ACL：

  检查 Amazon MWAA 环境中的 Amazon VPC 安全组是否配置正确。

- 检查 Amazon MWAA 环境子网：

  验证 Amazon MWAA 环境的子网是否为私有子网。

- 检查 Amazon MWAA 环境所需的终端节点连接：

  验证 Amazon MWAA 环境是否可以访问所需的终端节点。为此，自动化会调用自动化。`AWSSupport-ConnectivityTroubleshooter`

- 检查亚马逊 MWAA 环境亚马逊 S3 存储桶：

  检查亚马逊 MWAA 环境的 Amazon S3 存储桶是否已`Block Public Access`启用，并查看该账户的 Amazon S3 阻止公共访问设置。

- 检查 Amazon MWAA 环境 CloudWatch 日志组错误：

  解析 Amazon MWAA 环境的现有 CloudWatch 日志组以查找错误。

参考

Systems Manager Automation

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

Neptune

AWS Systems Manager Automation 为 Amazon Neptune 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

AWS-EnableNeptuneDbAuditLogsToCloudWatch

描述

该AWS-EnableNeptuneDbAuditLogsToCloudWatch运行手册可帮助您将 Amazon Neptune 数据库集群的审计日志发送到 Amazon Logs。 CloudWatch

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

类型：字符串

描述：（必填）要为其启用审核日志的 Neptune 数据库集群的资源 ID。

所需的 IAM 权限

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

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi)-返回 Neptune 数据库集群的 ID。
- VerifyNeptuneDbEngine (aws: P assertAwsResource roperty)-验证 Neptune 数据库引擎类型为。neptune
- EnableNeptuneDbAuditLogs (aws:executeAwsApi)-允许向 Neptune 数据库集群发送 CloudWatch 审计日志。
- VerifyNeptuneDbStatus (aws: waitAwsResource 属性)-验证 Neptune 数据库集群的状态为。available
- VerifyNeptuneDbAuditLogs (AWS: ExecuteScript)-验证审核日志是否已成功配置为发送到日志。CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

描述

该AWS-EnableNeptuneDbBackupRetentionPeriod运行手册可帮助您为 Amazon Neptune 数据库集群启用自动备份，备份保留期在 7 到 35 天之间。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）要为其启用备份的 Neptune 数据库集群的资源 ID。
- BackupRetentionPeriod

  类型：整数

  有效值：7-35

  描述：（必填）备份的保留天数。
- PreferredBackupWindow

  类型：字符串

  描述：（可选）每天进行备份的时间段至少为 30 分钟。该值必须采用协调世界时 (UTC)，并使用以下格式：hh24:mm-hh24:mm。备份保留期不能与首选维护时段发生冲突。

所需的 IAM 权限

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

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi)-返回 Neptune 数据库集群的 ID。
- VerifyNeptuneDbEngine (aws: P assertAwsResource roperty)-验证 Neptune 数据库引擎类型为。neptune
- VerifyNeptuneDbStatus (aws: waitAwsResource 属性)-验证 Neptune 数据库集群的状态为。available
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi)-设置 Neptune 数据库集群的保留期。
- VerifyNeptuneDbBackupsEnabled (aws: ExecuteScript)-验证是否成功设置了保留期和备份窗口。

AWS-EnableNeptuneClusterDeletionProtection

描述

AWS-EnableNeptuneClusterDeletionProtection运行手册为您指定的 Amazon Neptune 集群启用删除保护。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- DbClusterResourceId

  类型：字符串

  描述：（必填）要启用删除保护的 Neptune 集群的 ID。

所需的 IAM 权限

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

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

文档步骤

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi)-返回 Neptune 数据库集群的 ID。
- VerifyNeptuneDbEngine (aws: P assertAwsResource roperty)-验证指定数据库集群的引擎类型为`neptune`。
- VerifyNeptuneStatus (aws: waitForAwsResourceProperty)-验证集群的状态是否为`available`。
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi)-在 Neptune 数据库集群上启用删除保护。
- VerifyNeptuneDbDeletionProtection (aws: P assertAwsResource roperty)-验证数据库集群上是否启用了删除保护。

输出

- EnableNeptuneDbDeletionProtection。 EnableNeptuneDbDeletionProtectionResponse -API 操作的输出。

Amazon RDS

AWS Systems Manager 自动化为 Amazon Relational Database Service 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-CreateEncryptedRdsSnapshot
- AWS-CreateRdsSnapshot
- AWSConfigRemediation-DeleteRDSCluster
- AWSConfigRemediation-DeleteRDSClusterSnapshot
- AWSConfigRemediation-DeleteRDSInstance
- AWSConfigRemediation-DeleteRDSInstanceSnapshot
- AWSConfigRemediation-DisablePublicAccessToRDSInstance
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance
- AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance
- AWSConfigRemediation-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

描述

AWS-CreateEncryptedRdsSnapshot运行手册从未加密的亚马逊关系数据库服务 (Amazon RDS) 实例创建加密快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

描述：（必填）您要为其创建快照的 Amazon RDS 实例的 ID。

- 数据库 SnapshotIdentifier

  类型：字符串

  描述：（可选）Amazon RDS 快照的名称模板。默认名称模板是 *DB InstanceIdentifier-yyyymmdd* hhmss。

- encryptedDB SnapshotIdentifier

  类型：字符串

  描述：（可选）加密快照的名称。默认名称是您为附加的DBSnapshotIdentifier参数指定的值。-encrypted

- InstanceTags

  类型：字符串

  描述：（可选）要添加到数据库实例的标签。（例如：key=tagKey1，value=tagValue1；key=tagKey2，value=tagValue2）'

- KmsKey我是

  类型：字符串

  默认：alias/aws/rds

  描述：（可选）您要用于加密快照的客户托管密钥的 ARN、密钥 ID 或密钥别名。

- SnapshotTags

  类型：字符串

  描述：（可选）要添加到快照的标签。（例如：key=tagKey1，value=tagValue1；key=tagKey2，value=tagValue2）'

所需的 IAM 权限

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

- rds:AddTagsToResource
- rds:CopyDBSnapshot

- rds:CreateDBSnapshot
- rds:DeleteDBSnapshot
- rds:DescribeDBSnapshots

文档步骤

- aws:executeScript-创建您在DBInstanceIdentifier参数中指定的数据库实例的快照。
- aws:executeScript-验证在上一步中创建的快照是否存在。available
- aws:executeScript-将先前创建的快照复制到加密快照。
- aws:executeScript-验证上一步中创建的加密快照是否存在。

输出

CopyRdsSnapshotToEncryptedRds快照。 EncryptedSnapshotId -加密的 Amazon RDS 快照的 ID。

AWS-CreateRdsSnapshot

描述

为 Amazon RDS 实例创建 Amazon Relational Database Service (Amazon RDS) 快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

- 数据库 InstanceIdentifier

  类型：字符串

  描述：（必填）用于创建快照的 RDS 实例的数据库 InstanceId ID。

- 数据库 SnapshotIdentifier

  类型：字符串

  描述：（可选）要创建的 RDS 快照的数据库 SnapshotIdentifier ID。

- InstanceTags

  类型：字符串

  描述：（可选）要为实例创建的标签。

- SnapshotTags

  类型：字符串

  描述：（可选）要为快照创建的标签。

文档步骤

createRDSSnapshot – 创建 RDS 快照并返回快照 ID。

verifyRDSSnapshot – 检查在上一步中创建的快照是否存在。

输出

CreatersSnapshot。 SnapshotId — 创建的快照的 ID。

AWSConfigRemediation-DeleteRDSCluster

描述

AWSConfigRemediation-DeleteRDSCluster运行手册将删除您指定的亚马逊关系数据库服务 (Amazon RDS) 集群。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用删除保护的数据库集群的资源标识符。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

文档步骤

- aws:executeScript - 删除您在 DBClusterId 参数中指定的数据库集群。

AWSConfigRemediation-DeleteRDSClusterSnapshot

描述

AWSConfigRemediation-DeleteRDSClusterSnapshot 运行手册将删除给定的 Amazon Relational Database Service (Amazon RDS) 集群快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要删除的 Amazon RDS 集群快照标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution

- ssm:GetAutomationExecution
- rds:DeleteDBClusterSnapshot
- rds:DescribeDBClusterSnapshots

文档步骤

- aws:branch - 检查集群快照是否处于 available 状态。如果它不可用，则流程结束。
- aws:executeAwsApi - 使用数据库（DB）集群快照标识符删除给定的 Amazon RDS 集群快照。
- aws:executeScript - 验证给定的 Amazon RDS 集群快照是否已删除。

AWSConfigRemediation-DeleteRDSInstance

描述

AWSConfigRemediation-DeleteRDSInstance运行手册将删除指定的Amazon Relational Database Service (Amazon RDS) 实例。删除数据库 (DB) 实例时，会删除该实例的所有自动备份，且无法恢复。手动数据库快照不会删除。如果要删除的数据库实例处于 failed、incompatible-network 或 incompatible-restore 状态，则必须将 SkipFinalSnapshot 参数设置为 true。

> **Note**
>
> 如果要删除的数据库实例位于 Amazon Aurora 数据库集群中，若该数据库实例是只读副本并且是数据库集群中唯一的实例，则运行手册不会将其删除。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

- DbiResource我是

  类型：字符串

  描述：（必需）要删除的数据库实例的资源标识符。

- SkipFinal快照

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `true`，则在删除数据库实例之前不会创建最终快照。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

文档步骤

- `aws:executeAwsApi` - 从您在 `DbiResourceId` 参数中指定的值收集数据库实例名称。
- `aws:branch` - 根据您在 `SkipFinalSnapshot` 参数中指定的值进行分支。
- `aws:executeAwsApi` - 删除您在 `DbiResourceId` 参数中指定的数据库实例。
- `aws:executeAwsApi` - 创建最终快照后，删除您在 `DbiResourceId` 参数中指定的数据库实例。
- `aws:assertAwsResourceProperty` - 验证数据库实例是否已删除。

AWSConfigRemediation-DeleteRDSInstanceSnapshot

描述

AWSConfigRemediation-DeleteRDSInstanceSnapshot 运行手册将删除指定的 Amazon Relational Database Service (Amazon RDS) 实例快照。只有处于 available 状态的快照才会被删除。此运行手册不支持从 Amazon Aurora 数据库实例中删除快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要删除的快照 ID。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- rds:DeleteDBSnapshot
- rds:DescribeDBSnapshots

文档步骤

- aws:executeAwsApi - 收集在 DbSnapshotId 参数中指定的快照的状态。
- aws:assertAwsResourceProperty - 确认快照的状态为 available。
- aws:executeAwsApi - 删除在 DbSnapshotId 参数中指定的快照。
- aws:executeScript - 验证快照是否已被删除。

AWSConfigRemediation-DisablePublicAccessToRDSInstance

描述

AWSConfigRemediation-DisablePublicAccessToRDSInstance 运行手册将禁用指定的 Amazon Relational Database Service (Amazon RDS) 数据库 (DB) 实例的公共访问权限。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

类型：字符串

描述：（必需）要为其禁用公共访问权限的数据库实例的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 验证数据库实例是否处于 AVAILABLE 状态。
- aws:executeAwsApi - 禁用数据库实例的公开可访问性。
- aws:waitForAwsResourceProperty - 等待数据库实例变为 MODIFYING 状态。
- aws:waitForAwsResourceProperty - 等待数据库实例变为 AVAILABLE 状态。
- aws:assertAwsResourceProperty - 确认已对数据库实例禁用公开可访问性。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

描述

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster运行手册将对指定的 Amazon Relational Database Service (Amazon RDS) 集群启用 CopyTagsToSnapshot 设置。启用此设置可将所有标签从数据库集群复制到数据库集群的快照。默认设置是不复制它们。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

  类型：布尔值

  默认值：false

  描述：（可选）如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库集群的 `PreferredMaintenanceWindow` 设置如何。
- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用 `CopyTagsToSnapshot` 设置的数据库集群的资源标识符。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`

- rds:ModifyDBCluster

文档步骤

- aws:executeAwsApi - 从数据库集群资源标识符收集数据库集群标识符。
- aws:assertAwsResourceProperty - 确认数据库集群处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库集群启用 CopyTagsToSnapshot 设置。
- aws:assertAwsResourceProperty - 确认已对数据库集群启用 CopyTagsToSnapshot 设置。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

描述

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance 运行手册将对指定的 Amazon Relational Database Service (Amazon RDS) 实例启用 CopyTagsToSnapshot 设置。启用此设置可将所有标签从数据库实例复制到数据库实例快照。默认设置是不复制它们。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

  类型：布尔值

  默认值：false

描述：（可选）如果您为该参数指定 true，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 PreferredMaintenanceWindow 设置如何。

- AutomationAssume角色

  类型：字符串

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

- DbiResource我是

  类型：字符串

  描述：（必需）要对其启用 CopyTagsToSnapshot 设置的数据库实例的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库实例启用 CopyTagsToSnapshot 设置。
- aws:assertAwsResourceProperty - 确认已对数据库实例启用 CopyTagsToSnapshot 设置。

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

描述

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance运行手册对指定的 Amazon RDS 数据库实例启用增强监控。有关增强监控的信息，请参阅《Amazon RDS 用户指南》中的增强监控。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：整数

  有效值：1 | 5 | 10 | 15 | 30 | 60

  描述：（必需）从数据库实例收集增强监控指标时的间隔，以秒为单位。
- MonitoringRoleArn

  类型：字符串

  描述：（必填）允许 Amazon RDS 向亚马逊日志发送增强型监控指标的 IAM 角色的亚马逊资源名称 (ARN)。 CloudWatch
- ResourceId

  类型：字符串

描述：（必需）要对其启用增强监控的数据库实例的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库实例启用增强监控。
- aws:executeScript - 确认已对数据库实例启用增强监控。

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

描述

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS运行手册将对指定的 Amazon RDS 数据库实例启用 AutoMinorVersionUpgrade 设置。启用该设置表示在维护时段期间，将对该数据库实例自动应用次要版本升级。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其进行 AutoMinorVersionUpgrade 设置的数据库实例的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 对数据库实例启用 AutoMinorVersionUpgrade 设置。
- aws:executeScript - 确认已对数据库实例启用 AutoMinorVersionUpgrade 设置。

AWSConfigRemediation-EnableMultiAZOnRDSInstance

描述

AWSConfigRemediation-EnableMultiAZOnRDSInstance运行手册将 Amazon Relational Database Service (Amazon RDS) 数据库 (DB) 实例更改为多可用区部署。更改此设置不会导致中断。更改在下一个维护时段内应用，除非您将 ApplyImmediately 参数设置为 true。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- ApplyImmediately

  类型：布尔值

  默认值：false

  描述：（可选）如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 `PreferredMaintenanceWindow` 设置如何。
- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必填）数据库实例的 AWS 区域唯一不可变标识符，用于启用该设置。`MultiAZ`

所需的 IAM 权限

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

文档步骤

- aws:executeAwsApi - 使用 DBInstanceId 参数中提供的值检索数据库实例名称。
- aws:executeAwsApi - 验证 DBInstanceStatus 是否为 available。
- aws:branch - 检查您在 DbiResourceId 参数中指定的数据库实例上的 MultiAZ 是否已设置为 true。
- aws:executeAwsApi - 将您在 DbiResourceId 参数中指定的数据库实例上的 MultiAZ 设置更改为 true。
- aws:assertAwsResourceProperty - 验证您在 DbiResourceId 参数中指定的数据库实例上 MultiAZ 是否设置为 true。

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

描述

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance 运行手册将对您指定的 Amazon RDS 数据库实例上启用 Performance Insights。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

类型：字符串

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

- DbiResource我是

  类型：字符串

  描述：（必需）要对其启用 Performance Insights 的数据库实例的资源标识符。

- PerformanceInsightsKMS KeyId

  类型：字符串

  默认：`alias/aws/rds`

  描述：（可选）您希望 Performance Insights 用于加密所有潜在敏感数据的亚马逊资源名称 AWS Key Management Service (ARN AWS KMS)、密钥 ID 或 () 客户托管密钥的密钥别名。如果输入此参数的密钥别名，则在值前面加上 **`alias/`**。如果您没有为此参数指定值， AWS 托管式密钥 则使用。

- PerformanceInsightsRetentionPeriod

  类型：整数

  有效值：7、731

  默认：7

  描述：（可选）要保留 Performance Insights 数据的天数。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`

- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例的状态为 available。
- aws:executeAwsApi-收集参数中指定的客户托管密钥 AWS KMS 的 ARN。PerformanceInsightsKMSKeyId
- aws:branch - 检查是否已为数据库实例的 PerformanceInsightsKMSKeyId 属性分配了一个值。
- aws:executeAwsApi - 对您在 DbiResourceId 参数中指定的数据库实例启用 Performance Insights。
- aws:assertAwsResourceProperty - 确认为 PerformanceInsightsKMSKeyId 参数指定的值已用于对数据库实例上的 Performance Insights 启用加密。
- aws:assertAwsResourceProperty - 确认已在数据库实例上启用 Performance Insights。

AWSConfigRemediation-EnableRDSClusterDeletionProtection

描述

该AWSConfigRemediation-EnableRDSClusterDeletionProtection运行手册在您指定的亚马逊关系数据库服务 (Amazon RDS) 集群上启用删除保护。 AWS Config 必须在运行此自动化的 AWS 区域 位置中启用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

- ClusterId

  类型：字符串

  描述：（必需）要对其启用删除保护的数据库集群的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBClusters
- rds:ModifyDBCluster

文档步骤

- aws:executeAwsApi - 从数据库集群资源标识符收集数据库集群名称。
- aws:assertAwsResourceProperty - 验证数据库集群的状态为 available。
- aws:executeAwsApi - 对您在 ClusterId 参数中指定的数据库集群启用删除保护。
- aws:assertAwsResourceProperty - 验证是否已在数据库集群上启用删除保护。

AWSConfigRemediation-EnableRDSInstanceBackup

描述

AWSConfigRemediation-EnableRDSInstanceBackup运行手册将为您指定的 Amazon Relational Database Service (Amazon RDS) 数据库实例启用备份。此运行手册不支持为 Amazon Aurora 数据库实例启用备份。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

  类型：布尔值

  默认值：false

  描述：（可选）如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 `PreferredMaintenanceWindow` 设置如何。
- AutomationAssume角色

  类型：字符串

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

  类型：整数

  有效值：1-35

  描述：（必需）备份的保留天数。
- DbiResource我是

  类型：字符串

  描述：（必需）要为其启用备份的数据库实例的资源标识符。

- PreferredBackup窗口

  类型：字符串

  描述：（可选）创建备份的日常时间范围（采用 UTC 格式）。

  约束：

  - 必须采用 hh24:mi-hh24:mi 格式
  - 必须采用协调世界时 (UTC)
  - 不得与首选维护时段冲突
  - 必须至少为 30 分钟

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeScript - 从数据库实例资源标识符收集数据库实例标识符。为数据库实例启用备份。确认数据库实例上已启用备份。

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

描述

AWSConfigRemediation-EnableRDSInstanceDeletionProtection运行手册将在您指定的 Amazon RDS 数据库实例上启用删除保护。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- ApplyImmediately

  类型：布尔值

  默认值：false

  描述：（可选）如果您为该参数指定 `true`，应尽快异步应用此请求中的修改及任何待处理的修改，无论数据库实例的 `PreferredMaintenanceWindow` 设置如何。
- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用删除保护的数据库实例的资源标识符。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:executeAwsApi - 为您的数据库实例启用删除保护。
- aws:assertAwsResourceProperty - 确认已在数据库实例上启用删除保护。

AWSConfigRemediation-ModifyRDSInstancePortNumber

描述

AWSConfigRemediation-ModifyRDSInstancePortNumber 运行手册将修改 Amazon Relational Database Service (Amazon RDS) 实例接受连接所在的端口号。运行此自动化将重新启动数据库。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（可选）您希望数据库实例接受连接所在的端口号。
- RDSDB 身份证 InstanceResource

  类型：字符串

描述：（必需）要修改其入站端口号的数据库实例的资源标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

文档步骤

- aws:executeAwsApi - 从数据库实例资源标识符收集数据库实例标识符。
- aws:assertAwsResourceProperty - 确认数据库实例处于 AVAILABLE 状态。
- aws:executeAwsApi - 修改数据库实例接受连接所在的入站端口号。
- aws:waitForAwsResourceProperty - 等待数据库实例处于 MODIFYING 状态。
- aws:waitForAwsResourceProperty - 等待数据库实例处于 AVAILABLE 状态。

AWSSupport-ModifyRDSSnapshotPermission

描述

AWSSupport-ModifyRDSSnapshotPermission运行手册可帮助您修改多个 Amazon Relational Database Service (Amazon RDS) 快照的权限。使用此运行手册，您可以制作快照 Public 或 Private 并将其与其他 AWS 账户分享。使用默认 KMS 密钥加密的快照无法与使用此运行手册的其他账户分享。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型: StringList

  默认：无

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

  类型：字符串

  有效值：添加 | 移除

  默认：无

  描述：（可选）要执行的操作类型。
- 专属

  类型：字符串

  有效值：是 | 否

  描述：（必需）如果要与特定账户共享快照，则为该值输入 No。
- SnapshotIdentifiers

  类型: StringList

描述：（必需）要修改其权限的 Amazon RDS 快照名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBSnapshots
- rds:ModifyDBSnapshotAttribute

文档步骤

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

输出

ValidateSnapshots.EncryptedSnapshots

SharewithOther账户. 结果

MakePrivate.Result

MakePrivate. 命令

AWSPremiumSupport-PostgreSQLWorkloadReview

描述

AWSPremiumSupport-PostgreSQLWorkloadReview运行手册将捕获 Amazon Relational Database Service (Amazon RDS) PostgreSQL 数据库使用情况统计数据的多个快照。 AWS Support

主动式服务专家需要收集到的统计数据才能进行运营审查。统计数据使用一组自定义 SQL 和 Shell 脚本进行收集。这些脚本将下载到由本运行手册创建的临时亚马逊弹性计算云 (Amazon EC2) 实例。AWS 账户 运行手册要求您使用包含用户名和密码键值对的 AWS Secrets Manager 密钥提供凭证。用户名必须具有查询标准 PostgreSQL 统计视图和函数的权限。

此运行手册 AWS 账户 使用 AWS CloudFormation 堆栈自动在您中创建以下 AWS 资源。您可以使用 AWS CloudFormation 控制台来监控堆栈的创建。

- 虚拟私有云（VPC）和 Amazon EC2 实例在 VPC 的私有子网中启动，可选择使用 NAT 网关连接到互联网。
- 附加到临时 Amazon EC2 实例的 AWS Identity and Access Management (IAM) 角色，有权检索 Secrets Manager 密钥值。该角色还提供将文件上传到您选择的亚马逊简单存储服务 (Amazon S3) 存储桶的权限，也可以选择上传案例。 AWS Support
- VPC 对等连接，允许在您的数据库实例和临时 Amazon EC2 实例之间建立连接。
- 附加到临时 VPC 的 Systems Manager、Secrets Manager 和 Amazon S3 VPC 端点。
- 包含已注册任务的维护时段，这些任务定期启动和停止临时 Amazon EC2 实例、运行数据收集脚本以及将文件上传到 Amazon S3 存储桶。还会为维护时段创建一个 IAM 角色，该角色提供执行已注册任务的权限。

运行手册完成后，将删除用于创建必要 AWS 资源的 AWS CloudFormation 堆栈，并将报告上传到您选择的 Amazon S3 存储桶，也可以上传一个 AWS Support 案例。

> **Note**
>
> 默认情况下，将保留临时 Amazon EC2 实例的根 Amazon EBS 卷。您可以通过将 `EbsVolumeDeleteOnTermination` 参数设置为 `true` 来覆盖此设置。

先决条件

- Enterprise Support 订阅此运行手册和主动式服务工作负载诊断与审查需要订阅 Enterprise Support。在使用此运行手册之前，请联系您的技术客户经理 (TAM) 或专家 TAM (STAM) 以获取相关说明。有关更多信息，请参阅AWS Support 主动服务。
- 账户和 AWS 区域 配额请确保您尚未达到在账户和使用本运行手册的地区中可以创建的 Amazon EC2 实例或 VPC 的最大数量。如果您需要申请提高限制，请参阅提高服务限制表。
- 数据库配置

1. 您在 DatabaseName 参数中指定的数据库应配置 pg_stat_statements 扩展。如果您尚未在 shared_preload_libraries 中配置 pg_stat_statements，则必须编辑数据库参数组中的值并应用更改。更改参数 shared_preload_libraries 会要求您重启数据库实例。有关更多信息，请参阅 Working with parameter groups。将 pg_stat_statements 添加到 shared_preload_libraries 会增加一些性能开销。但这对于跟踪各个语句的表现很有用。有关 pg_stat_statements 扩展的更多信息，请参阅 PostgreSQL 文档。如果您未配置 pg_stat_statements 扩展，或者用于统计数据收集的数据库中不存在该扩展，则在操作审查中不会显示语句级别的分析。
2. 确保没有关闭 track_counts 和 track_activities 参数。如果这些参数在数据库参数组中关闭，则不会有意义的统计数据可用。更改这些参数需要重启数据库实例。有关更多信息，请参阅使用 Amazon RDS for PostgreSQL 数据库实例上的参数。
3. 如果关闭 track_io_timing 参数，则 I/O 级别统计数据将不包含在操作审查中。更改 track_io_timing 会要求您重启数据库实例，并且会产生额外的性能开销，具体取决于数据库实例的工作负载。尽管关键工作负载会有性能开销，但该参数提供了与每次查询的 I/O 时间相关的有用信息。

账单和费用 AWS 账户 将向您收取与临时的 Amazon EC2 实例、关联的 Amazon EBS 卷、NAT 网关以及此自动化运行期间传输的数据相关的费用。默认情况下，此运行手册会创建一个 t3.micro Amazon Linux 2 实例来收集统计数据。此运行手册在两个步骤之间启动和停止实例以降低成本。

数据安全和治理此运行手册通过查询 PostgreSQL 统计视图和函数来收集统计数据。确保 SecretId 参数中提供的凭证仅允许对统计视图和函数具有只读权限。作为自动化的一部分，收集脚本将上传到 Amazon S3 存储桶，并且可以位于 s3://*DOC-EXAMPLE-BUCKET*/*automation execution id*/queries/。

这些脚本收集的数据供 AWS 专家用来查看对象级别的关键绩效指标。该脚本收集诸如表名、架构名和索引名之类的信息。如果此类任何信息包含收入指标、用户名、电子邮件地址或任何其他个人身份信息等敏感信息，则我们建议您停止此工作负载审查。请联系您的 AWS TAM，讨论工作量审核的替代方法。

确保您获得必要的批准和许可，才能与之共享此自动化收集的统计数据和元数据 AWS。

安全注意事项如果您将 UpdateRdsSecurityGroup 参数设置为 yes，则运行手册会更新与您的数据库实例关联的安全组，以允许来自临时 Amazon EC2 实例私有 IP 地址的入站流量。

如果您将 UpdateRdsRouteTable 参数设置为 yes，则运行手册会更新与您的数据库实例运行所在的子网关联的路由表，以允许通过 VPC 对等连接流向临时 Amazon EC2 实例的流量。

用户创建要允许收集脚本连接到您的 Amazon RDS 数据库，您必须设置一个具有读取统计视图权限的用户。然后您必须将这些凭证存储在 Secrets Manager 中。我们建议为此自动化创建一个新的专门用户。创建单独的用户可让您审计和跟踪此自动化执行的活动。

1. 创建新用户。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "CREATE USER <user_name> PASSWORD '<password>';"
   ```

2. 确保该用户只能进行只读连接。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET default_transaction_read_only=true;"
   ```

3. 设置用户级别限制。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET work_mem=4096;"

   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET statement_timeout=10000;"

   psql -h <database_connection_endpoint> -p <database_port>
   -U <admin_user> -c "ALTER USER <user_name> SET
   idle_in_transaction_session_timeout=60000;"
   ```

4. 向新用户授予 pg_monitor 权限，使其能够访问数据库统计信息。（pg_monitor 角色是 pg_read_all_settings、pg_read_all_stats 和 pg_stat_scan_table 的成员。）

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "GRANT pg_monitor to <user_name>;"
   ```

此 Systems Manager Automation 向临时 Amazon EC2 实例配置文件添加的权限以下权限已添加到与临时 Amazon EC2 实例关联的 IAM 角色。AmazonSSMManagedInstanceCore 托管策略还与 IAM 角色关联，以允许 Systems Manager 管理 Amazon EC2 实例。

```
{
    "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 Automation 向临时维护时段添加的权限以下权限将自动添加到与维护时段任务关联的 IAM 角色。维护时段任务启动、停止并向临时的 Amazon EC2 实例发送命令。

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

[运行此自动化（控制台）]

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）您的数据库实例 ID。
- DatabaseName

  类型：字符串

  描述：（必需）数据库实例上托管的数据库名称。
- SecretId

  类型：字符串

  描述：（必需）包含用户名和密码键值对的 Secrets Manager 密钥的 ARN。 AWS CloudFormation 堆栈创建一个 IAM 策略，该策略具有此 ARN 的`GetSecretValue`操作权限。这些凭证用于允许临时实例收集数据库统计信息。请联系您的 TAM 或 STAM，讨论所需的最低权限。
- 确认

  类型：字符串

  描述：（必需）如果您确认此运行手册将在您的账户中创建临时资源以便从数据库实例收集统计数据，请输入 **`yes`**。我们建议在运行此自动化之前先联系您的 TAM 或 STAM。

- SupportCase

  类型：字符串

  描述：（可选）由您的 TAM 或 STAM 提供的 AWS Support 案例编号。如果已提供，运行手册将更新此案例并附上所收集的数据。此选项要求临时 Amazon EC2 实例具有互联网连接才能访问 AWS Support API 终端节点。您必须将 `AllowVpcInternetAccess` 参数设置为 `true`。案例主题必须包含短语 `AWSPremiumSupport-PostgreSQLWorkloadReview`。

- S3 BucketName

  类型：字符串

  描述：（必需）您的账户中您要上传此自动化收集的数据的 Amazon S3 存储桶名称。验证存储桶策略是否向不需要访问存储桶内容的主体授予任何不必要的读取或写入权限。出于此自动化的目的，我们建议创建一个新的临时 Amazon S3 存储桶。运行手册将为附加到 Amazon EC2 实例的 IAM 角色提供 `s3:PutObject` API 操作的权限。上传的文件将位于 `s3://`*`bucket name`*`/`*`automation execution id`*`/`。

- InstanceType

  类型：字符串

  描述：（可选）将运行自定义 SQL 和 Shell 脚本的临时 Amazon EC2 实例的类型。

  有效值：t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  默认：t3.micro

- VpcCidr

  类型：字符串

  描述：（可选）新 VPC 的 CIDR 表示法中的 IP 地址范围（例如 `172.31.0.0/16`）。确保您选择的 CIDR 不会与任何与数据库实例相连的现有 VPC 重叠或匹配。可创建的最小 VPC 使用 /28 子网掩码，最大 VPC 使用 /16 子网掩码。

  默认：172.31.0.0/16

- StackResourcesNamePrefix

  类型：字符串

描述：（可选）AWS CloudFormation 堆栈资源名称前缀和标签。运行手册使用此前缀作为应用于资源的名称和标签的一部分来创建 AWS CloudFormation 堆栈资源。标签键值对的结构为 *StackResourcesNamePrefix*:{{automation:EXECUTION_ID}}。

默认： AWSPostgreSQLWorkloadReview

- 计划

  类型：字符串

  描述：（可选）维护时段计划。指定维护时段运行任务的频率。默认值为每 1 hour。

  有效值：15 分钟 | 30 分钟 | 1 小时 | 2 小时 | 4 小时 | 6 小时 | 12 小时 | 1 天 | 2 天 | 4 天

  默认：1 小时

- 持续时间

  类型：整数

  描述：（可选）您希望允许自动化运行的最长持续时间（分钟）。支持的最大持续时间为 8,640 分钟（6 天）。默认值为 4,320 分钟（3 天）。

  有效值：30-8640

  默认：4320

- UpdateRdsRouteTable

  类型：字符串

  描述：（可选）如果设置为 true，运行手册将更新与您的数据库实例运行所在的子网关联的路由表。添加 IPv4 路由，用于通过新创建的 VPC 对等连接将流量路由到临时 Amazon EC2 实例私有 IPV4 地址。

  有效值：true | false

  默认：false

- AllowVpcInternetAccess

  类型：字符串

描述：（可选）如果设置为true，运行手册将创建一个 NAT 网关，为临时 Amazon EC2 实例提供互联网连接，从而与 AWS Support API 终端节点通信。如果您只想让运行手册将输出上传到 Amazon S3 存储桶，则可以将此参数保留为 false。

有效值：true | false

默认：false

- UpdateRdsSecurityGroup

  类型：字符串

  描述：（可选）如果设置为 true，运行手册将更新与您的数据库实例关联的安全组，以允许来自临时实例私有 IP 地址的流量。

  有效值：false | true

  默认：false

- EbsVolumeDeleteOn终止

  类型：字符串

  描述：（可选）如果设置为true，则在运行手册完成并删除 AWS CloudFormation 堆栈后，将删除临时 Amazon EC2 实例的根卷。

  有效值：false | true

  默认值：false

所需的 IAM 权限

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

- cloudformation:CreateStack
- cloudformation:DeleteStack
- cloudformation:DescribeStackEvents
- cloudformation:DescribeStackResource
- cloudformation:DescribeStacks
- cloudformation:UpdateStack

- ec2:AcceptVpcPeeringConnection
- ec2:AllocateAddress
- ec2:AssociateRouteTable
- ec2:AssociateVpcCidrBlock
- ec2:AttachInternetGateway
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateEgressOnlyInternetGateway
- ec2:CreateInternetGateway
- ec2:CreateNatGateway
- ec2:CreateRoute
- ec2:CreateRouteTable
- ec2:CreateSecurityGroup
- ec2:CreateSubnet
- ec2:CreateTags
- ec2:CreateVpc
- ec2:CreateVpcEndpoint
- ec2:CreateVpcPeeringConnection
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DeleteInternetGateway
- ec2:DeleteNatGateway
- ec2:DeleteRoute
- ec2:DeleteRouteTable
- ec2:DeleteSecurityGroup
- ec2:DeleteSubnet
- ec2:DeleteTags
- ec2:DeleteVpc
- ec2:DeleteVpcEndpoints

- ec2:DescribeAddresses
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInternetGateways
- ec2:DescribeNatGateways
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DetachInternetGateway
- ec2:DisassociateRouteTable
- ec2:DisassociateVpcCidrBlock
- ec2:ModifySubnetAttribute
- ec2:ModifyVpcAttribute
- ec2:RebootInstances
- ec2:ReleaseAddress
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:StartInstances
- ec2:StopInstances
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile

- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:GetRolePolicy
- iam:PassRole
- iam:PutRolePolicy
- iam:RemoveRoleFromInstanceProfile
- iam:TagPolicy
- iam:TagRole
- rds:DescribeDBInstances
- s3:GetAccountPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:ListBucket
- ssm:AddTagsToResource
- ssm:CancelMaintenanceWindowExecution
- ssm:CreateDocument
- ssm:CreateMaintenanceWindow
- ssm:DeleteDocument
- ssm:DeleteMaintenanceWindow
- ssm:DeregisterTaskFromMaintenanceWindow
- ssm:DescribeAutomationExecutions
- ssm:DescribeDocument
- ssm:DescribeInstanceInformation

- ssm:DescribeMaintenanceWindowExecutions
- ssm:GetCalendarState
- ssm:GetDocument
- ssm:GetMaintenanceWindowExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListTagsForResource
- ssm:RegisterTaskWithMaintenanceWindow
- ssm:RemoveTagsFromResource
- ssm:SendCommand
- support:AddAttachmentsToSet
- support:AddCommunicationToCase
- support:DescribeCases

文档步骤

1. aws:assertAwsResourceProperty - 确认数据库实例处于 available 状态。
2. aws:executeAwsApi - 收集有关数据库实例的详细信息。
3. aws:executeScript - 检查在 S3BucketName 中指定的 Amazon S3 存储桶是否允许匿名访问权限或者公开读取或写入权限。
4. aws:executeScript-从 Automation 运行手册附件中获取 AWS CloudFormation 模板内容，该附件用于在中创建 AWS 账户临时 AWS 资源。
5. aws:createStack-创建 AWS CloudFormation 堆栈资源。
6. aws:waitForAwsResourceProperty-等待 AWS CloudFormation 模板创建的 Amazon EC2 实例开始运行。
7. aws:executeAwsApi - 获取 AWS CloudFormation创建的临时 Amazon EC2 实例和 VPC 对等连接的 ID。
8. aws:executeAwsApi - 获取用于配置与数据库实例连接的临时 Amazon EC2 实例的 IP 地址。
9. aws:executeAwsApi - 标记附加到临时 Amazon EC2 实例的 Amazon EBS 卷。
10. aws:waitForAwsResourceProperty - 等到临时 Amazon EC2 实例通过状态检查。

11. aws:waitForAwsResourceProperty - 等到临时 Amazon EC2 实例由 Systems Manager 管理。如果此步骤超时或失败，则运行手册会重启该实例。
    a. aws:executeAwsApi - 如果上一步失败或超时，则重启临时 Amazon EC2 实例。
    b. aws:waitForAwsResourceProperty - 等到临时 Amazon EC2 实例在重启后由 Systems Manager 管理。
12. aws:runCommand - 在临时 Amazon EC2 实例上安装元数据收集器应用程序要求。
13. aws:runCommand - 通过在临时 Amazon EC2 实例上创建配置文件来配置对数据库实例的访问权限。
14. aws:executeAwsApi - 创建维护时段，以便使用运行命令定期运行元数据收集器应用程序。维护时段会在命令之间启动和停止实例。
15. aws:waitForAwsResourceProperty-等待 AWS CloudFormation 模板创建的维护窗口准备就绪。
16. aws:executeAwsApi-获取由创建的维护时段和更改日历的 ID AWS CloudFormation。
17. aws:sleep - 等到维护时段的结束日期。
18. aws:executeAwsApi - 关闭维护时段。
19. aws:executeScript - 获取在维护时段期间运行的任务的结果。
20. aws:waitForAwsResourceProperty - 等待维护时段完成最后一项任务后再继续。
21. aws:branch - 根据您是否为 SupportCase 参数提供了值对工作流进行分支。
    a. aws:changeInstanceState - 启动临时 Amazon EC2 实例，等待状态检查通过后再上传报告。
    b. aws:waitForAwsResourceProperty - 等到临时 Amazon EC2 实例由 Systems Manager 管理。如果此步骤超时或失败，运行手册将重启该实例。
        i. aws:executeAwsApi - 如果上一步失败或超时，则重启临时 Amazon EC2 实例。
        ii. aws:waitForAwsResourceProperty - 等到临时 Amazon EC2 实例在重启后由 Systems Manager 管理。
    c. aws:runCommand - 如果您为 SupportCase 参数提供了值，则将元数据报告附加到 AWS Support 案例。该脚本将报告压缩并拆分为 5 MB 的文件。该脚本附加到 AWS Support 案例的最大文件数为 12。
22. aws:changeInstanceState-停止临时的 Amazon EC2 实例，以防 AWS CloudFormation 堆栈无法删除。
23. aws:executeAwsApi-描述运行手册无法创建或更新 AWS CloudFormation 堆栈时的 AWS CloudFormation 堆栈事件。

24aws:waitForAwsResourceProperty-等待 AWS CloudFormation 堆栈处于终端状态后再删除。

25aws:executeAwsApi-删除不包括维护时段的 AWS CloudFormation 堆栈。如果 EbsVolumeDeleteOnTermination 参数值设置为 false，则与临时 Amazon EC2 实例关联的 Amazon EBS 根卷将保留。

AWS-RebootRdsInstance

描述

AWS-RebootRdsInstance 运行手册将在 Amazon Relational Database Service (Amazon RDS) 数据库实例未重启时将其重启。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

- InstanceId

  类型：字符串

  描述：（必需）要重启的 Amazon RDS 数据库实例 ID。

文档步骤

RebootInstance -如果数据库实例尚未重启，则重新启动该实例。

WaitForAvailableState -等待数据库实例完成重启过程。

输出

此自动化没有输出。

AWSSupport-ShareRDSSnapshot

描述

AWSSupport-ShareRDSSnapshot 运行手册为知识中心文章如何与其他账户共享加密的 Amazon RDS 数据库快照？概述的过程提供了自动解决方案。如果您的 Amazon Relational Database Service (Amazon RDS) 快照使用默认快照进行加密 AWS 托管式密钥，则无法共享该快照。在这种情况下，您必须使用客户托管密钥复制该快照，然后将其与目标账户共享。此自动化使用您在 SnapshotName 参数中指定的值或为所选 Amazon RDS 数据库实例或集群找到的最新快照执行这些步骤。

> **Note**
>
> 如果您没有为KMSKey参数指定值，则自动化会在您的账户中创建一个用于加密快照的新 AWS KMS 客户托管密钥。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AccountIds

  类型: StringList

  描述：（必需）要与之共享快照的账户 ID 列表（以逗号分隔）。

- AutomationAssumeRole

  类型：字符串

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

- 数据库

  类型：字符串

  描述：（必需）要共享其快照的 Amazon RDS 数据库实例或集群的名称。如果您为 `SnapshotName` 参数指定一个值，则此参数可选。

- KMSKey

  类型：字符串

  描述：（可选）用于加密快照的 AWS KMS 客户托管密钥的完整 Amazon 资源名称（ARN）。

- SnapshotName

  类型：字符串

  描述：（可选）要使用的数据库集群或实例快照的 ID。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

AutomationAssumeRole 需要执行以下操作才能成功启动数据库集群的运行手册。

- ssm:StartAutomationExecution
- rds:DescribeDBClusters
- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

必须将用于运行此自动化的 IAM 角色添加为密钥用户，才能使用 ARNKmsKey 参数中指定的 KMS 密钥。有关添加密钥用户至 KMS 密钥的信息，请参阅AWS Key Management Service 《开发人员指南》中的更改密钥策略。

如果您没有为 KMSKey 参数指定一个值，则 AutomationAssumeRole 需要执行以下额外操作才能成功启动运行手册。

- kms:CreateKey
- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

文档步骤

1. aws:executeScript-检查是否为KMSKey参数提供了值，如果未找到任何值，则创建 AWS KMS 客户托管密钥。
2. aws:branch - 检查是否为 SnapshotName 参数提供了一个值，并相应地进行了分支。
3. aws:executeAwsApi - 检查提供的快照是否来自数据库实例。
4. aws:executeScript - 格式化将冒号替换为连字符的 SnapshotName 参数。
5. aws:executeAwsApi - 使用指定的 KMSKey 复制快照。
6. aws:waitForAwsResourceProperty - 等待复制快照操作完成。
7. aws:executeAwsApi - 与指定 AccountIds 的共享新快照。
8. aws:executeAwsApi - 检查提供的快照是否来自数据库集群。
9. aws:executeScript - 格式化将冒号替换为连字符的 SnapshotName 参数。
10. aws:executeAwsApi - 使用指定的 KMSKey 复制快照。
11. aws:waitForAwsResourceProperty - 等待复制快照操作完成。

12aws:executeAwsApi - 与指定 AccountIds 的共享新快照。

13aws:executeAwsApi - 检查为 Database 参数提供的值是否为数据库实例。

14aws:executeAwsApi - 检查为 Database 参数提供的值是否为数据库集群。

15aws:executeAwsApi - 检索指定 Database 的快照列表。

16aws:executeScript - 从在上一步汇总的列表中确定可用的最新快照。

17aws:executeAwsApi - 使用指定的 KMSKey 复制数据库实例快照。

18aws:waitForAwsResourceProperty - 等待复制快照操作完成。

19aws:executeAwsApi - 与指定 AccountIds 的共享新快照。

20aws:executeAwsApi - 检索指定 Database 的快照列表。

21aws:executeScript - 从在上一步汇总的列表中确定可用的最新快照。

22aws:executeAwsApi - 使用指定的 KMSKey 复制数据库实例快照。

23aws:waitForAwsResourceProperty - 等待复制快照操作完成。

24aws:executeAwsApi - 与指定 AccountIds 的共享新快照。

25aws:executeScript-如果您未为KMSKey参数指定值且自动化失败，则删除由自动化创建的 AWS KMS 客户托管密钥。

AWS-StartRdsInstance

描述

启动 Amazon Relational Database Service (Amazon RDS) 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要启动的 Amazon RDS 实例 ID。

AWS-StartStopAuroraCluster

描述

本运行手册启动或停止 Amazon Aurora 集群。

> **Note**
>
> 要启动集群，它必须处于`stopped`状态。要停止集群，它必须处于`available`状态。本运行手册不能用于启动或停止 Aurora 无服务器集群、Aurora 多主集群、Aurora 全局数据库的一部分或使用 Aurora 并行查询的集群。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

- ClusterName

  类型：字符串

  描述：（必填）要停止或启动的 Aurora 集群的名称。

- 操作

  类型：字符串

  有效值：开始 | 停止

  默认：启动

  描述：（必填）要停止或启动的 Aurora 集群的名称。

所需的 IAM 权限

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

- rds:DescribeDBClusters
- rds:StartDBCluster
- rds:StopDBCluster

文档步骤

- aws:executeScript-根据您为指定的值启动或停止集群。

输出

StartStopAuroraCluster。 ClusterName -Aurora 集群的名称

StartStopAuroraCluster。 CurrentStatus -Aurora 集群的当前状态

StartStopAuroraCluster.message-自动化的详细信息

AWS-StopRdsInstance

描述

停止亚马逊关系数据库服务 (Amazon RDS) 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）要停止的 Amazon RDS 实例的 ID。

AWSSupport-TroubleshootConnectivityToRDS

描述

AWSSupport-TroubleshootConnectivityToRDS 运行手册将诊断 EC2 实例和 Amazon Relational Database Service 实例之间的连接问题。自动化可确保数据库实例可用，然后检查关联的安全组规则、网络访问控制列表（网络 ACL）和路由表是否存在潜在的连接问题。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要测试与其的连接的数据库实例 ID。
- SourceInstance

  类型：字符串

  允许的模式：^i-[a-z0-9]{8,17}$

  描述：（必需）用于进行连接测试的 EC2 实例的 ID。

所需的 IAM 权限

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

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- rds:DescribeDBInstances

文档步骤

- aws:assertAwsResourceProperty - 确认数据库实例的状态为 available。
- aws:executeAwsApi - 获取有关数据库实例的信息。
- aws:executeAwsApi - 获取有关数据库实例网络 ACL 的信息。
- aws:executeAwsApi - 获取数据库实例子网 CIDR。
- aws:executeAwsApi - 获取有关 EC2 实例的信息。
- aws:executeAwsApi - 获取有关 EC2 实例网络 ACL 的信息。
- aws:executeAwsApi - 获取有关与 EC2 实例关联的安全组的信息。
- aws:executeAwsApi - 获取有关与数据库实例关联的安全组的信息。
- aws:executeAwsApi - 获取有关与 EC2 实例关联的路由表的信息。
- aws:executeAwsApi - 获取有关与用于 EC2 实例的 Amazon VPC 关联的主路由表信息。
- aws:executeAwsApi - 获取有关与数据库实例关联的路由表的信息。
- aws:executeAwsApi - 获取有关与用于数据库实例的 Amazon VPC 关联的主路由表信息。
- aws:executeScript - 评估安全组规则。
- aws:executeScript - 评估网络 ACL。
- aws:executeScript - 评估路由表。
- aws:sleep - 结束自动化。

输出

getRDS InstanceProperties .DB InstanceIdentifier -自动化中使用的数据库实例。

getRDS InstanceProperties .DB InstanceStatus -数据库实例的当前状态。

evalSecurityGroup规则。 SecurityGroupEvaluation -将SourceInstance安全组规则与数据库实例安全组规则进行比较的结果。

evalNetworkAcl规则。 NetworkAclEvaluation -将网络 ACL 与数据库实例SourceInstance网络 ACL 进行比较的结果。

evalRouteTable参赛作品。 RouteTableEvaluation -比较SourceInstance路由表和数据库实例路由的结果。

AWSSupport-TroubleshootRDSIAMAuthentication

描述

AWSSupport-TroubleshootRDSIAMAuthentication这有助于对适用于 PostgreSQL 的亚马逊 RDS、适用于 MySQL 的亚马逊 RDS、适用于 MariaDB 的亚马逊 RDS、亚马逊 Aurora PostgreSQL 和亚马逊 Aurora MySQL 实例进行身份验证故障排除 AWS Identity and Access Management (IAM)。使用此运行手册验证使用 Amazon RDS 实例或 Aurora 集群进行 IAM 身份验证所需的配置。它还提供了纠正与 Amazon RDS 实例或 Aurora 集群的连接问题的步骤。

> **Important**
>
> 本运行手册不支持适用于甲骨文的亚马逊 RDS 或适用于微软 SQL Server 的亚马逊 RDS for Microsoft SQL Server。

> **Important**
>
> 如果提供了源 Amazon EC2 实例，而目标数据库是 Amazon RDS，则会调用子自动化AWSSupport-TroubleshootConnectivityToRDS来排除 TCP 连接故障。输出还提供了您可以在 Amazon EC2 实例或源计算机上运行的命令，以便使用 IAM 身份验证连接到 Amazon RDS 实例。

如何工作？

本运行手册包含六个步骤：

- 步骤 1：验证输入：验证自动化的输入。
- 第 2 步：已 branchOnSource提供 EC2：验证输入参数中是否提供了源 Amazon EC2 实例 ID。
- 步骤 3：validaterdsConnectivity：验证来自源 Amazon EC2 实例（如果提供）的 Amazon RDS 连接。
- 第 4 步：validaterdsiamAuthentication：验证 IAM 身份验证功能是否已启用。
- 第 5 步：验证 IAMPolicies：验证提供的 I AM 用户/角色中是否存在所需的 IAM 权限。
- 步骤 6：生成报告：生成先前执行步骤的结果报告。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必填）：选择要连接并进行身份验证的关系数据库的类型。

  允许的值：`Amazon RDS`或 `Amazon Aurora Cluster.`
- 数据库 InstanceIdentifier

类型：字符串

描述：（必填）目标 Amazon RDS 数据库实例或 Aurora 数据库集群的标识符。

允许的模式：^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$

最大字符数：63

- SourceEc2 InstanceIdentifier

  类型：AWS::EC2::Instance::Id

  描述：（可选）如果您从在同一账户和地区运行的 Amazon EC2 实例连接到 Amazon RDS 数据库实例，则为 Amazon EC2 实例 ID。如果源不是 Amazon EC2 实例，或者目标 Amazon RDS 类型是 Aurora 数据库集群，则不要指定此参数。

  默认值：""

- DBIAM RoleName

  类型：字符串

  描述：（可选）用于基于 IAM 的身份验证的 IAM 角色名称。仅在未提供参数DBIAMUserName时提供，否则将其留空。DBIAMUserName必须提供DBIAMRoleName或。

  允许的模式：^[a-zA-Z0-9+=,.@_-]{1,64}$|^$

  最大字符数：64

  默认值：""

- DBIAM UserName

  类型：字符串

  描述：（可选）用于基于 IAM 的身份验证的 IAM 用户名。仅在未提供DBIAMRoleName参数时提供，否则将其留空。DBIAMUserName必须提供DBIAMRoleName或。

  允许的模式：^[a-zA-Z0-9+=,.@_-]{1,64}$|^$

  最大字符数：64

  默认值：""

- 数据库 UserName

  类型：字符串

  描述：（可选）数据库用户名映射到数据库中基于 IAM 的身份验证的 IAM 角色/用户。默认选项用于*评估是否允许数据库中的所有用户拥有该rds-db:connect权限。

  允许的模式：^[a-zA-Z0-9+=,.@*_-]{1,64}$

  最大字符数：64

  默认值：*

所需的 IAM 权限

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

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

说明

1. 在控制台中导航到 AWSSupport-TroubleshotrdsiamAutherticati on。AWS Systems Manager
2. 选择 Execute automation（执行自动化）
3. 要输入参数，请输入内容：
   - AutomationAssumeRole （可选）：

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

     选择您要连接并进行身份验证的 Amazon RDS 的类型。从两个允许的值中进行选择：`Amazon RDS`或 `Amazon Aurora Cluster.`
   - 数据库InstanceIdentifier （必填）：

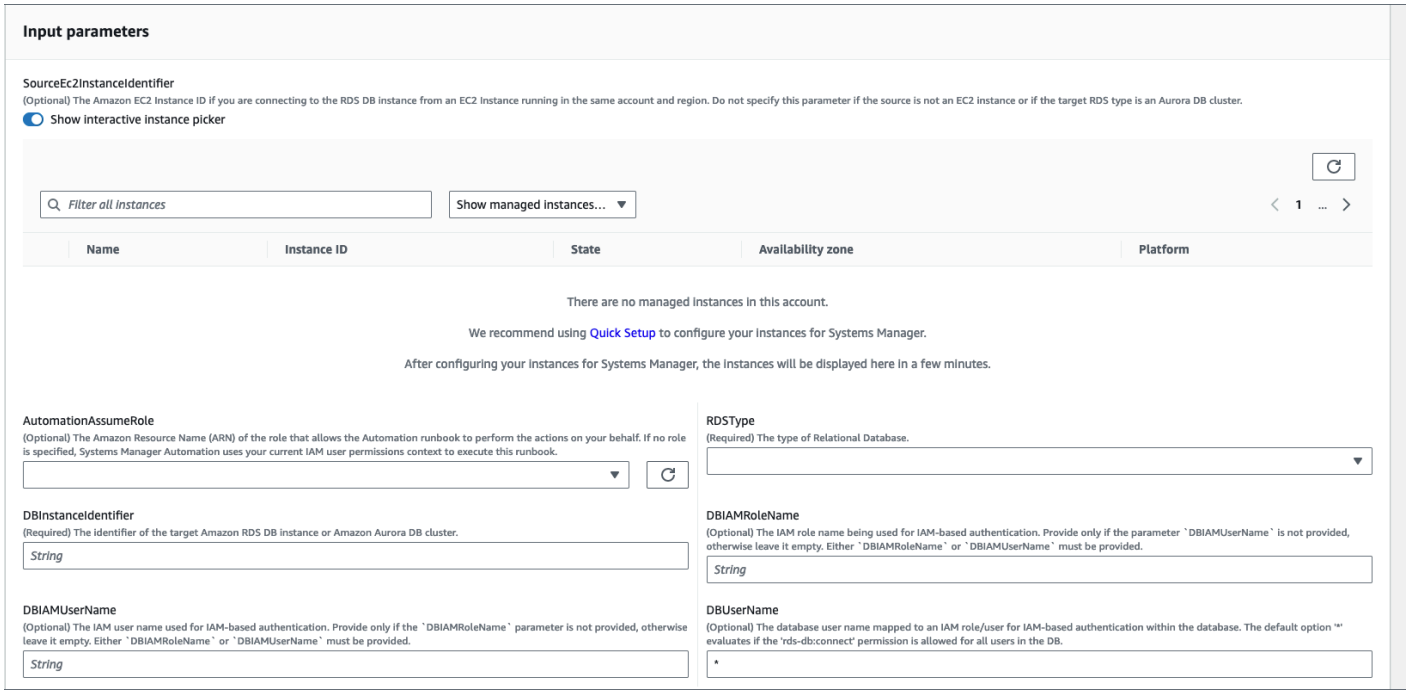
     输入您尝试连接的目标 Amazon RDS 数据库实例或 Aurora 集群的标识符，并使用 IAM 凭证进行身份验证。
   - SourceEc2InstanceIdentifier （可选）：

     如果您要从同一账户和地区的 Amazon EC2 实例连接到 Amazon RDS 数据库实例，请提供 Amazon EC2 实例 ID。如果源不是亚马逊 EC2 或者目标 Amazon RDS 类型是 Aurora 集群，则留空。
   - DBIAMRoleName （可选）：

     输入用于基于 IAM 的身份验证的 IAM 角色名称。仅在未提供`DBIAMUserName`时提供；否则，请留空。`DBIAMUserName`必须提供`DBIAMRoleName`或。
   - DBIAMUserName （可选）：

     输入用于基于 IAM 的身份验证的 IAM 用户。仅`DBIAMRoleName`在未提供时提供，否则留空。`DBIAMUserName`必须提供`DBIAMRoleName`或。
   - 数据库UserName （可选）：

     输入映射到 IAM 角色/用户的数据库用户，以便在数据库中进行基于 IAM 的身份验证。默认选项*用于评估；此字段中未提供任何内容。



4. 选择执行。
5. 请注意，自动化已启动。
6. 文档将执行以下步骤：
   - 步骤 1：验证输入：

     验证自动化的输入-SourceEC2InstanceIdentifier（可选）、DBInstanceIdentifier或ClusterID、DBIAMRoleName或DBIAMUserName。它会验证您输入的输入参数是否存在于您的账户和区域中。它还会验证用户是否输入了其中一个 IAM 参数（例如，DBIAMRoleName或DBIAMUserName）。此外，它还会执行其他验证，例如提及的数据库是否处于“可用”状态。
   - 第 2 步： branchOnSourceEC2 提供：

     验证输入参数中是否提供了源 Amazon EC2 以及数据库是否是 Amazon RDS。如果是，则继续执行步骤 3。否则，它将跳过步骤 3，即 Amazon EC2-Amazon RDS 连接验证，继续执行步骤 4。
   - 步骤 3：验证连接：

     如果输入参数中提供了源 Amazon EC2，并且数据库是 Amazon RDS，则步骤 2 将启动步骤 3。在此步骤中，将调用子自动化AWSSupport-TroubleshootConnectivityToRDS来验证来自源 Amazon EC2 的 Amazon RDS 连接。儿童自动化运行手册AWSSupport-TroubleshootConnectivityToRDS会验证所需的网络配置（Amazon Virtual Private Cloud

[Amazon VPC]、安全组、网络访问控制列表 [NACL]、Amazon RDS 可用性）是否到位，以便您可以从 Amazon EC2 实例连接到亚马逊 RDS 实例。

- 第 4 步：验证 dsiam 身份验证：

  验证是否在 Amazon RDS 实例或 Aurora 集群上启用了 IAM 身份验证功能。

- 第 5 步：验证 IAM 政策：

  验证所传递的 IAM 用户/角色中是否存在所需的 IAM 权限，以允许 IAM 凭证对指定数据库用户（如果有）的 Amazon RDS 实例进行身份验证。

- 步骤 6：生成报告：

  获取前面步骤中的所有信息，并打印每个步骤的结果或输出。它还列出了使用 IAM 凭证连接到 Amazon RDS 实例时需要参考和执行的步骤。

7. 自动化完成后，请查看 “输出” 部分以了解详细结果：

- 检查连接数据库的 IAM 用户/角色权限：

  验证所传递的 IAM 用户/角色中是否存在所需的 IAM 权限，以使 IAM 凭证能够在指定数据库用户（如果有）的 Amazon RDS 实例中进行身份验证。

- 正在检查数据库的基于 IAM 的身份验证属性：

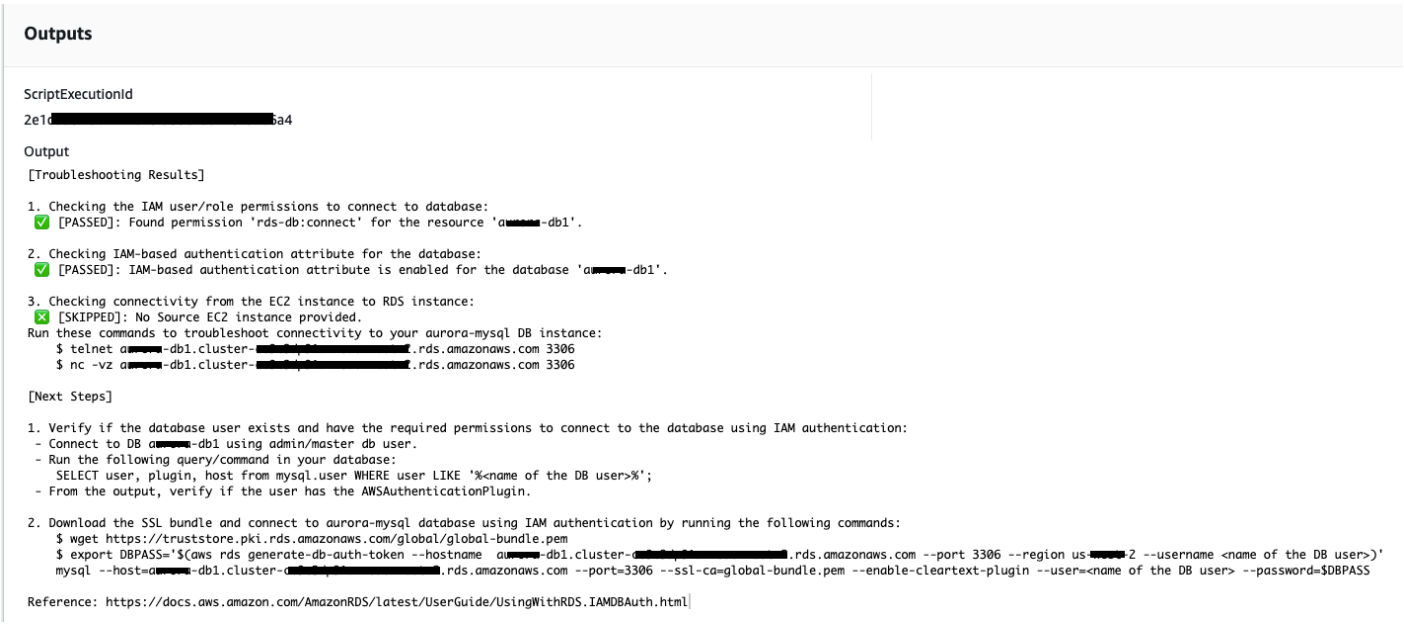
  验证是否为指定的 Amazon RDS 数据库/Aurora 集群启用了 IAM 身份验证功能。

- 检查从 Amazon EC2 实例到 Amazon RDS 实例的连接：

  验证所需的网络配置（亚马逊 VPC、安全组、NACL、Amazon RDS 可用性）是否已到位，以便您可以从 Amazon EC2 实例连接到 Amazon RDS 实例。

- 后续步骤:

  列出了使用 IAM 凭证连接到 Amazon RDS 实例时要参考和执行的命令和步骤。



参考

Systems Manager Automation

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

AWSSupport-ValidateRdsNetworkConfiguration

描述

AWSSupport-ValidateRdsNetworkConfiguration在执行或操作之前，自动化有助于避免现有亚马逊关系数据库服务 (Amazon RDS) /Amazon Aurora/Amazon DocumentDB 实例出现不兼容的网络状态。ModifyDBInstance StartDBInstance如果实例已经处于网络不兼容状态，则运行手册将提供原因。

如何工作？

本运行手册确定您的 Amazon RDS 数据库实例是否会进入网络不兼容状态，或者如果是，则确定其处于网络不兼容状态的原因。

运行手册会对您的 Amazon RDS 数据库实例执行以下检查：

- 每个区域的 Amazon 弹性网络接口 (ENI) 配额。
- 数据库子网组中的所有子网都存在。
- 子网有足够的空闲 IP 地址可用。
- （适用于可公开访问的 Amazon RDS 实例）VPC 属性的设置（`enableDnsSupport`和`enableDnsHostnames`）。

> **Important**
>
> 对亚马逊 Aurora/Amazon DocumentDB 集群使用本文档时，请确保使用`DBInstanceIdentifier`代替。`ClusterIdentifier`否则，文档将在第一步中失败。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

所需的 IAM 权限

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

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

政策示例：

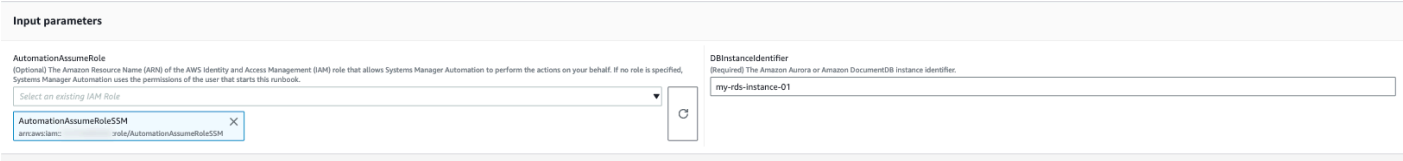
```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "ValidateRdsNetwork",
                    "Effect": "Allow",
                    "Action": [
                        "rds:DescribeDBInstances",
                        "servicequotas:GetServiceQuota",
                        "ec2:DescribeNetworkInterfaces",
                        "ec2:DescribeVpcAttribute",
                        "ec2:DescribeSubnets"
                    ],
                    "Resource": [
                        "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
                    ]
                }
            ]
        }
```

说明

1. 在AWS Systems Manager控制台ValidateRdsNetworkConfiguration中导航到 AWSSupport-。
2. 选择 Execute automation（执行自动化）
3. 要输入参数，请输入内容：
   - AutomationAssumeRole （可选）：

     AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）允许 Systems Manager Automation 代表您执行操作。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
   - 数据库InstanceIdentifier （必填）：

     输入 Amazon Relational Database Service 实例标识符。



4. 选择执行。
5. 请注意，自动化已启动。

6. 文档将执行以下步骤：

   - 步骤 1: assertRdsState:

     检查提供的实例标识符是否存在以及是否具有以下任何状态：`available`、`stopped`、或`incompatible-network`。

   - 第 2 步: gatherRdsInformation:

     收集有关 Amazon RDS 实例的必需信息，以便稍后在自动化中使用。

   - 第 3 步: checkEniQuota:

     检查该地区当前可用的 Amazon ENI 配额。

   - 第 4 步： validateVpcAttributes：

     验证 Amazon VPC 的 DNS 参数（`enableDnsSupport`和`enableDnsHostnames`）是否设置为 true（如果是 Amazon RDS 实例，则不是`PubliclyAccessible`）。

   - 第 5 步： validateSubnetAttributes：

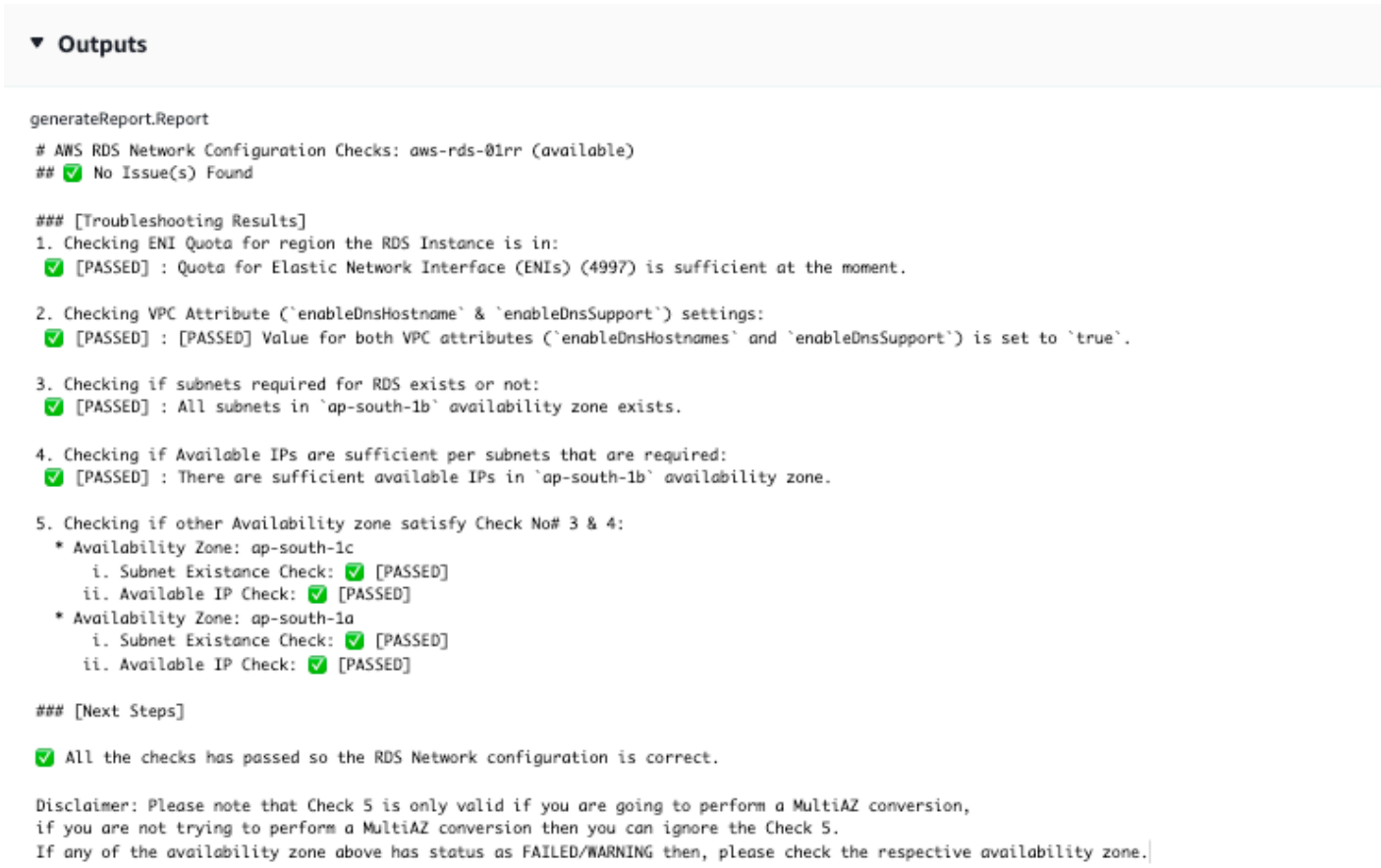
     验证中是否存在子网，`DBSubnetGroup`并检查每个子网是否有可用 IP。

   - 步骤 6：生成报告：

     获取前面步骤中的所有信息，并打印每个步骤的结果或输出。它还列出了使用 IAM 凭证连接到 Amazon RDS 实例时需要参考和执行的步骤。

7. 自动化完成后，请查看 “输出” 部分以了解详细结果：

   具有有效网络配置的 Amazon RDS 实例：



网络配置不正确的 Amazon RDS 实例（VPC 属性设置 enableDnsHostnames 为 false）：

参考

Systems Manager Automation

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

AWS 服务文档

- 如何解决处于网络不兼容状态的 Amazon RDS 数据库的问题？
- 如何解决处于网络不兼容状态的 Amazon DocumentDB 实例的问题？

Amazon Redshift

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

主题

AWSConfigRemediation-DeleteRedshiftCluster

描述

AWSConfigRemediation-DeleteRedshiftCluster 运行手册将删除您指定的 Amazon Redshift 集群。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

- ClusterIdentifier

  类型：字符串

  描述：（必需）要删除的 Amazon Redshift 集群的 ID。
- SkipFinalClusterSnapshot

  类型：布尔值

  默认值：false

  描述：（可选）如果设置为 `false`，则自动化会在删除 Amazon Redshift 集群之前先创建一个快照。如果设置为 `true`，则不会创建最终集群快照。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

文档步骤

- `aws:branch` - 根据您为 `SkipFinalClusterSnapshot` 参数指定的值进行分支。
- `aws:executeAwsApi` - 删除参数 `ClusterIdentifier` 中指定的 Amazon Redshift 集群。
- `aws:assertAwsResourceProperty` - 验证 Amazon Redshift 集群是否已删除。

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

描述

`AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` 运行手册将为指定的 Amazon Redshift 集群禁用公共访问权限。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要为其禁用公共访问权限的集群的唯一标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群禁用公开可访问性。
- aws:waitForAwsResourceProperty - 等待集群的状态变为 available。
- aws:assertAwsResourceProperty - 确认公开可访问性设置已在集群上禁用。

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

描述

AWSConfigRemediation-EnableRedshiftClusterAuditLogging运行手册将为您指定的 Amazon Redshift 集群启用审核日志记录功能。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要将日志上传到的 Amazon Simple Storage Service (Amazon S3) 存储桶的名称。
- ClusterIdentifier

  类型：字符串

  描述：（必需）要对其启用审核日志记录的集群的唯一标识符。
- S3 KeyPrefix

  类型：字符串

描述：（可选）要将日志上传到的 Amazon S3 密钥前缀（子文件夹）。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeLoggingStatus
- redshift:EnableLogging
- s3:GetBucketAcl
- s3:PutObject

文档步骤

- aws:branch - 根据是否为 S3KeyPrefix 参数指定了值进行分支。
- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用审核日志记录。
- aws:assertAwsResourceProperty - 验证集群上是否启用了审核日志记录。

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

描述

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot运行手册将为您指定的 Amazon Redshift 集群启用自动快照。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：整数

  有效值：1-35

  描述：（必需）自动快照保留的天数。
- ClusterIdentifier

  类型：字符串

  描述：（必需）要对其启用自动快照的集群的唯一标识符。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

文档步骤

- `aws:executeAwsApi` - 对 `ClusterIdentifier` 参数中指定的集群启用自动快照。
- `aws:waitForAwsResourceProperty` - 等待集群的状态变为 `available`。
- `aws:executeScript` - 确认已在集群上启用自动快照。

AWSConfigRemediation-EnableRedshiftClusterEncryption

描述

该AWSConfigRemediation-EnableRedshiftClusterEncryption运行手册支持使用 AWS Key Management Service AWS KMS() 客户托管密钥在您指定的 Amazon Redshift 集群上进行加密。此运行手册应仅用作基准，以确保根据建议的最低的安全性最佳实践对 Amazon Redshift 集群进行加密。我们建议使用不同的客户托管密钥对多个集群进行加密。本运行手册无法更改在已加密的集群上使用的 AWS KMS 客户托管密钥。要更改用于加密集群的 AWS KMS 客户托管密钥，必须先在集群上禁用加密。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要对其启用加密的集群的唯一标识符。
- KMSKeyARN

  类型：字符串

  描述：（必需）要用于加密集群数据的 AWS KMS 客户托管密钥的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的 Amazon Redshift 集群启用加密。
- aws:assertAwsResourceProperty - 验证是否已在集群上启用加密。

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

描述

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting运行手册将为您指定的 Amazon Redshift 集群启用增强型虚拟私有云 (VPC) 路由。有关增强型 VPC 路由的信息，请参阅《Amazon Redshift 管理指南》中的Amazon Redshift 增强型 VPC 路由。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

- ClusterIdentifier

  类型：字符串

  描述：（必需）对其启用增强型 VPC 路由的集群的唯一标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用增强型 VPC 路由。
- assertAwsResourceProperty - 确认已在集群上启用增强型 VPC 路由。

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

描述

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster运行手册将要求传入连接对您指定的 Amazon Redshift 集群使用 SSL。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）对其启用增强型 VPC 路由的集群的唯一标识符。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:DescribeClusterParameters
- redshift:ModifyClusterParameterGroup

文档步骤

- aws:executeAwsApi - 从在 ClusterIdentifier 参数中指定的集群收集参数详细信息。
- aws:executeAwsApi - 对 ClusterIdentifier 参数中指定的集群启用 require_ssl 设置。
- aws:assertAwsResourceProperty - 确认已在集群上启用 require_ssl 设置。

- aws:executeScript - 验证集群的 require_ssl 设置。

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

描述

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings运行手册将修改您指定的 Amazon Redshift 集群的维护设置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AllowVersion升级

  类型：布尔值

  描述：（必需）如果设置为 true，将在维护时段期间将主要版本升级自动应用于该集群。
- AutomationAssume角色

  类型：字符串

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

  类型：整数

  有效值：1-35

描述：（必需）自动快照保留的天数。

- ClusterIdentifier

  类型：字符串

  描述：（必需）对其启用增强型 VPC 路由的集群的唯一标识符。

- PreferredMaintenance窗口

  类型：字符串

  描述：（必需）可进行系统维护的每周时间范围（按世界协调时间计算）。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

文档步骤

- aws:executeAwsApi - 修改 ClusterIdentifier 参数中指定的集群的维护设置。
- aws:assertAwsResourceProperty - 确认已为集群配置修改后的维护设置。

AWSConfigRemediation-ModifyRedshiftClusterNodeType

描述

AWSConfigRemediation-ModifyRedshiftClusterNodeType运行手册将修改您指定的 Amazon Redshift 集群的节点类型和节点数。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

数据库

参数

- AutomationAssume角色

  类型：字符串

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

- Classic

  类型：布尔值

  描述：（可选）如果设置为 `true`，则调整大小操作将使用经典的大小调整进程。

- ClusterIdentifier

  类型：字符串

  描述：（必需）要修改其节点类型的集群的唯一标识符。

- ClusterType

  类型：字符串

  有效值：single-node | multi-node

  描述：（必需）要将其分配给您的集群的集群类型。

- NodeType

  类型：字符串

  有效值：ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  描述：（必需）要将其分配给您的集群的节点类型。

- NumberOf节点

  类型：整数

  有效值：2-100

  描述：（可选）要将其分配给集群的节点的数量。如果集群为 `single-node` 类型，请不要为此参数指定值。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

文档步骤

- `aws:executeScript` - 修改 `ClusterIdentifier` 参数中指定的集群的节点类型和节点数。

Amazon S3

AWS Systems Manager Automation 为 Amazon 简单存储服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-ArchiveS3BucketToIntelligentTiering
- AWS-ConfigureS3BucketLogging
- AWS-ConfigureS3BucketVersioning
- AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock
- AWSConfigRemediation-ConfigureS3PublicAccessBlock
- AWS-CreateS3PolicyToExpireMultipartUploads
- AWS-DisableS3BucketPublicReadWrite

- AWS-EnableS3BucketEncryption
- AWS-EnableS3BucketKeys
- AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy
- AWSConfigRemediation-RestrictBucketSSLRequestsOnly
- AWSSupport-TroubleshootS3PublicRead

AWS-ArchiveS3BucketToIntelligentTiering

描述

AWS-ArchiveS3BucketToIntelligentTiering运行手册为您指定的亚马逊简单存储服务 (Amazon S3) 存储桶创建或替换智能分层配置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- BucketName

  类型：字符串

描述：（必填）您要为其创建智能分层配置的 S3 存储桶的名称。

- ConfigurationId

  类型：字符串

  描述：（必填）智能分层配置的 ID。这可以是新的配置 ID，也可以是现有配置的 ID。

- NumberOfDaysTo存档

  类型：字符串

  有效值：90-730

  描述：（必填）存储桶中的对象有资格过渡到存档访问层之后连续经过的天数。

- NumberOfDaysToDeepArchive

  类型：字符串

  有效值：180-730

  描述：（必填）存储桶中的对象有资格过渡到深度存档访问权限层后的连续天数。

- S3Prefix

  类型：字符串

  描述：（可选）要应用配置的对象的键名前缀。

- 标签

  类型: MapList

  描述：（可选）分配给要应用配置的对象的元数据。标签由用户定义的键和值组成。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

文档步骤

- PutsBucketIntelligentTieringConfiguration (aws: ExecuteScript)-为指定存储桶创建或更新 Amazon S3 智能分层配置。
- VerifyBucketIntelligentTiering配置（aws: assert AwsResource 属性）-验证 S3 存储桶智能配置已应用于指定的存储桶。

AWS-ConfigureS3BucketLogging

描述

允许登录 Amazon Simple Storage Service (Amazon S3) 存储桶。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要为其配置日志记录的 Amazon S3 存储桶的名称。

- GrantedPermission

  类型：字符串

  有效值：FULL_CONTROL | READ | WRITE

  描述：（必需）分配给存储桶的被授权者的日志记录权限。
- GranteeEmail地址

  类型：字符串

  （可选）被授权者的电子邮件地址。
- GranteeId

  类型：字符串

  描述：（可选）被授权者的规范用户 ID。
- GranteeType

  类型：字符串

  有效值： CanonicalUser | AmazonCustomerByEmail | 群组

  描述：（必需）被授权者的类型。
- GranteeUri

  类型：字符串

  描述：（可选）被授权者组的 URI。
- TargetBucket

  类型：字符串

  描述：（必需）指定希望 Amazon S3 存储服务器访问日志的存储桶。您可以将日志传输到您拥有的任何存储桶。您也可以配置多个存储桶，以将它们的日志传输到同一目标存储桶。在这种情况下，您应该 TargetPrefix为每个源存储桶选择不同的存储桶，以便可以按密钥区分已交付的日志文件。
- TargetPrefix

  类型：字符串

  默认：/

描述：（可选）指定用于存储日志文件的键的前缀。

AWS-ConfigureS3BucketVersioning

描述

配置 Amazon Simple Storage Service (Amazon S3) 存储桶的版本控制。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要为其配置版本控制的 Amazon S3 存储桶的名称。
- VersioningState

  类型：字符串

  有效值：Enabled | Suspended

默认：Enabled

描述：（可选）应用于 VersioningConfiguration .Status。设置为“Enabled”时，此过程为存储桶中的对象启用版本控制，添加到此存储桶的所有对象都将收到唯一的版本 ID。设置为 Suspended 时，此过程将禁用存储桶中对象的版本控制。添加到存储桶的所有对象都将收到版本 ID null。

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

描述

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 运行手册根据您在运行手册参数中指定的值为 Amazon S3 存储桶配置 Amazon Simple Storage Service (Amazon S3) 公共访问屏蔽设置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：布尔值

  默认：True

描述：（可选）如果设置为 `true`，Amazon S3 会屏蔽 S3 存储桶的公共访问控制列表 (ACL) 以及您在 `BucketName` 参数中指定的 S3 存储桶中存储的对象。

- BlockPublic政策

  类型：布尔值

  默认：True

  描述：（可选）如果设置为 `true`，Amazon S3 会阻止您在 `BucketName` 参数中指定的 S3 存储桶的公有存储桶策略。

- BucketName

  类型：字符串

  描述：（必需）要配置的 S3 存储桶的名称。

- IgnorePublicacls

  类型：布尔值

  默认：True

  描述：（可选）如果设置为 `true`，Amazon S3 会忽略您在 `BucketName` 参数中指定的 S3 存储桶的所有公有 ACL。

- RestrictPublic水桶

  类型：布尔值

  默认：True

  描述：（可选）如果设置为 `true`，Amazon S3 会限制您在 `BucketName` 参数中指定的 S3 存储桶的公有存储桶策略。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`

- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

文档步骤

- aws:executeAwsApi - 创建或修改在 BucketName 参数中指定的 S3 存储桶的 PublicAccessBlock 配置。
- aws:executeScript - 返回在 BucketName 参数中指定的 S3 存储桶的 PublicAccessBlock 配置，并验证是否根据在运行手册参数中指定的值成功进行了更改。

AWSConfigRemediation-ConfigureS3PublicAccessBlock

描述

该AWSConfigRemediation-ConfigureS3PublicAccessBlock运行手册根据你在运行手册参数中指定的值配置 AWS 账户亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的公共访问封锁设置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AccountId

  类型：字符串

  描述：（必填）拥有您正在配置的 S3 存储桶的 ID。 AWS 账户

- AutomationAssume角色

  类型：字符串

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

- BlockPublicacls

  类型：布尔值

  默认：True

  描述：（可选）如果设置为`true`，Amazon S3 会阻止 AWS 账户 您在参数中指定的 S3 存储桶的公共访问控制列表 (ACL)。`AccountId`

- BlockPublic政策

  类型：布尔值

  默认：True

  描述：（可选）如果设置为`true`，Amazon S3 将阻止 AWS 账户 您在`AccountId`参数中指定的拥有的 S3 存储桶的公有存储桶策略。

- IgnorePublicacls

  类型：布尔值

  默认：True

  描述：（可选）如果设置为`true`，Amazon S3 将忽略 AWS 账户 您在参数中指定的拥有的 S3 存储桶的所有公有 ACL。`AccountId`

- RestrictPublic水桶

  类型：布尔值

  默认：True

  描述：（可选）如果设置为`true`，Amazon S3 会限制 AWS 账户 您在参数中指定的拥有的 S3 存储桶的公有存储桶策略。`AccountId`

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock

文档步骤

- aws:executeAwsApi - 为在 AccountId 参数中指定的 AWS 账户 创建或修改 PublicAccessBlock 配置。
- aws:executeScript-返回AccountId参数中 AWS 账户 指定的PublicAccessBlock配置，并根据 runbook 参数中指定的值验证更改是否成功完成。

AWS-CreateS3PolicyToExpireMultipartUploads

描述

AWS-CreateS3PolicyToExpireMultipartUploads运行手册为指定的存储桶创建生命周期策略，该策略将在规定的天数后过期未完成的分段上传。本运行手册将新的生命周期策略与任何已存在的现有生命周期存储桶策略合并。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

类型：字符串

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

- BucketName

  类型：字符串

  描述：（必需）要配置的 S3 存储桶的名称。

- DaysUntil到期

  类型：整数

  描述：（必填）Amazon S3 在永久删除所有上传部分之前等待的天数。

- RuleId

  类型：字符串

  描述：（必填）用于标识生命周期存储桶规则的 ID。这必须是唯一的值。

- S3Prefix

  类型：字符串

  描述：（可选）要应用配置的对象的键名前缀。

所需的 IAM 权限

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

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

文档步骤

- ConfigureExpireMultipartUploads (aws: ExecuteScript)-为存储桶配置生命周期策略。

- VerifyExpireMultipartUploads (aws: ExecuteScript)-验证是否已为存储桶配置生命周期策略。

输出

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

AWS-DisableS3BucketPublicReadWrite

描述

使用 Amazon Simple Storage Service (Amazon S3) `Block Public Access` 禁用公有 S3 存储桶的读写权限。有关更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的使用 Amazon S3 阻止公有访问。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- S3 BucketName

  类型：字符串

描述：（必需）要限制对其的访问的 S3 存储桶。

AWS-EnableS3BucketEncryption

描述

为 Amazon Simple Storage Service (Amazon S3) 存储桶配置默认加密。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

  类型：字符串

  描述：（必需）要加密其内容的 S3 存储桶的名称。
- SSEAlgorithm

  类型：字符串

  默认值：AES256

描述：（可选）用于默认加密的服务器端加密算法。

AWS-EnableS3BucketKeys

描述

AWS-EnableS3BucketKeys运行手册在您指定的亚马逊简单存储服务 (Amazon S3) 存储桶上启用存储桶密钥。此存储桶级密钥在新对象的生命周期中为其创建数据密钥。如果您未为KmsKeyId参数指定值，则默认加密配置将使用使用 Amazon S3 托管密钥 (SSE-S3) 的服务器端加密。

> **Note**
>
> 使用 () 密钥 AWS Key Management Service (DSSE-KMS AWS KMS) 进行双层服务器端加密不支持 Amazon S3 存储桶密钥。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- BucketName

  类型：字符串

  描述：（必填）您要为其启用存储桶密钥的 S3 存储桶的名称。
- KMS KeyId

  类型：字符串

  描述：（可选）您要用于服务器端加密的 Amazon 资源名称 (ARN)、密钥 ID 或 AWS Key Management Service (AWS KMS) 客户托管密钥的密钥别名。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

文档步骤

- ChooseEncryptionType (aws: branch)-评估为`KmsKeyId`参数提供的值以确定将使用 SSE-S3 (AES256) 还是 SSE-KMS。
- PutBucketkeysKMS (aws: executeAwsApi)-使用指定的将指定 S3 存储桶`true`的`BucketKeyEnabled`属性设置为。`KmsKeyId`
- PutBucketkeysaes256 (aws: executeAwsApi)-将具有 AES256 加密的指定 S3 存储桶`true`的`BucketKeyEnabled`属性设置为。
- verifyS3BucketKeysEnabled （aws: assert AwsResource 属性）-验证目标 S3 存储桶上的存储桶密钥是否已启用。

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

描述

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 运行手册将从您的 Amazon Simple Storage Service (Amazon S3) 存储桶策略中移除带有通配符（Principal: * 或 Principal: "AWS": *）的用于 Allow 操作的主体策略语句。带有条件的策略语句也会被删除。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要修改其策略的 Amazon S3 存储桶的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy

- s3:PutBucketPolicy

文档步骤

- aws:executeScript - 修改存储桶策略并验证带有通配符的主体策略语句已从您在 BucketName 参数中指定的 Amazon S3 存储桶中移除。

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

描述

AWSConfigRemediation-RestrictBucketSSLRequestsOnly 运行手册将创建一个 Amazon Simple Storage Service (Amazon S3) 存储桶策略语句，明确拒绝对您指定的 Amazon S3 存储桶的 HTTP 请求。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要拒绝 HTTP 请求的 S3 存储桶的名称。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

文档步骤

- aws:executeScript - 为在 BucketName 参数中指定的 S3 存储桶创建一个明确拒绝 HTTP 请求的存储桶策略。

AWSSupport-TroubleshootS3PublicRead

描述

AWSSupport-TroubleshootS3PublicRead 运行手册将诊断从您在 S3BucketName 参数中指定的公有 Amazon Simple Storage Service (Amazon S3) 存储桶读取对象时遇到的问题。还会分析 S3 存储桶中对象的设置子集。

运行此自动化（控制台）

限制

- 此自动化不会检查是否存在允许对对象进行公共访问的接入点。
- 此自动化不会评估 S3 存储桶策略中的条件密钥。
- 如果您使用的是 AWS Organizations，此自动化不会评估服务控制策略以确认是否允许访问 Amazon S3。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- CloudWatchLogGroup姓名

  类型：字符串

  描述：（可选）您要向其中发送自动化输出的 Amazon CloudWatch 日志组。如果找不到与您指定的值匹配的日志组，此自动化将使用该参数值创建一个日志组。此自动化创建的日志组的保留期为 14 天。

- CloudWatchLogStream姓名

  类型：字符串

  描述：（可选）您要将自动化输出发送到的 CloudWatch 日志日志流。如果找不到与您指定的值匹配的日志流，此自动化将使用该参数值创建一个日志流。如果您未为该参数指定一个值，此自动化将使用 `ExecutionId` 作为日志流的名称。

- HttpGet

  类型：布尔值

  有效值：true | false

  默认：True

  描述：（可选）如果此参数设置为 `true`，此自动化将对您在 `S3BucketName` 中指定的对象发出部分 HTTP 请求。使用 Range HTTP 标头仅返回对象的第一个字节。

- IgnoreBlockPublicAccess

类型：布尔值

有效值：true | false

默认值：false

描述：（可选）如果此参数设置为 `true`，则此自动化将忽略您在 `S3BucketName` 参数中指定的 S3 存储桶的公共访问屏蔽设置。不建议更改该参数的默认值。

- MaxObjects

  类型：整数

  有效值：1-25

  默认：5

  描述：（可选）您在 `S3BucketName` 参数中指定的 S3 存储桶中要分析的对象数量。

- S3 BucketName

  类型：字符串

  描述：（必需）要排查问题的 S3 存储桶的名称。

- S3 PrefixName

  类型：字符串

  描述：（可选）要在 S3 存储桶中分析的对象的密钥名称前缀。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的对象密钥。

- StartAfter

  类型：字符串

  描述：（可选）您希望此自动化开始分析 S3 存储桶中对象的对象密钥名称。

- ResourcePartition

  类型：字符串

  有效值：`aws` |`aws-us-gov` |`aws-cn`

  默认：`aws`

描述：（必需）您的 S3 存储桶所在的分区。

- 详细

  类型：布尔值

  有效值：true | false

  默认值：false

  描述：（可选）要在自动化期间返回更多详细信息，请将此参数设置为 `true`。如果将此参数设置为 `false`，则只会返回警告和错误消息。

所需的 IAM 权限

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

仅当您希望自动化将`logs:CreateLogGroup`日志数据发送到 Log CloudWatch s 时，才需要`logs:CreateLogStream`、和`logs:PutLogEvents`权限。

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

文档步骤

- aws:assertAwsResourceProperty - 确认 S3 存储桶存在并且可以访问。
- aws:executeScript - 返回 S3 存储桶位置和您的规范用户 ID。
- aws:executeScript - 返回对您的账户和 S3 存储桶的公共访问屏蔽设置。
- aws:assertAwsResourceProperty - 确认 S3 存储桶付款方被设置为 BucketOwner。如果在 S3 存储桶上启用 Requester Pays，此自动化将结束。
- aws:executeScript - 返回 S3 存储桶策略状态并确定其是否被视为公开。有关公有 S3 存储桶的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中“公有”的含义。
- aws:executeAwsApi - 返回 S3 存储桶策略。
- aws:executeAwsApi - 返回在 S3 存储桶策略中找到的所有上下文键。
- aws:assertAwsResourceProperty - 确认 S3 存储桶策略中是否有对 GetObject API 操作的明确拒绝。
- aws:executeAwsApi - 返回 S3 桶的访问控制列表 (ACL)。
- aws:executeScript-如果您为CloudWatchLogGroupName参数指定值，则创建 CloudWatch 日志组和日志流。
- aws:executeScript - 根据您在运行手册输入参数中指定的值，评估自动化期间收集的任何 S3 存储桶设置是否阻止对象被公众访问。此脚本执行以下功能：

- 评估公共访问屏蔽设置
- 根据您在 `MaxObjects`、`S3PrefixName` 和 `StartAfter` 参数中指定的值返回 S3 存储桶中的对象。
- 返回 S3 存储桶策略，以模拟从 S3 存储桶返回的对象的自定义 IAM policy。
- 如果 `HttpGet` 参数设置为 `true`，则对返回的对象执行部分 HTTP 请求。使用 Range HTTP 标头仅返回对象的第一个字节。
- 检查返回的对象的键名以确认它是以一个还是两个句点结尾。无法从 Amazon S3 控制台下载以句点结尾的对象键名。
- 检查返回的对象的所有者是否匹配 S3 存储桶的所有者。
- 检查对象的 ACL 是否向匿名用户授予 `READ` 或 `FULL_CONTROL` 权限。
- 返回与对象关联的标签。
- 使用模拟的 IAM policy 确认 `GetObject` API 操作的 S3 存储桶策略中是否明确拒绝此对象。
- 返回对象的元数据以确认是否支持该存储类别。
- 检查对象的服务器端加密设置，以确认是否使用 AWS Key Management Service (AWS KMS) 客户管理的密钥对对象进行加密。

输出

AnalyzeObjects.buck

AnalyzeObjects. 对象

SageMaker

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

主题

- AWS-DisableSageMakerNotebookRootAccess

AWS-DisableSageMakerNotebookRootAccess

描述

AWS-DisableSageMakerNotebookRootAccess运行手册禁用 Amazon SageMaker 笔记本实例的根访问权限。在自动化过程中，notebook 实例将停止以进行所需的更改。 SageMaker 不支持 Studio 笔记本实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- NotebookInstance姓名

  类型：字符串

  描述：（必填）要禁用 root 访问权限的 SageMaker 笔记本实例的名称。

- StartInstanceAfterUpdate

  类型：布尔值

  默认：True

  描述：（可选）确定禁用 root 访问权限后是否启动笔记本实例。此参数的默认设置为`true`。如果设置为`true`，则实例将在禁用 root 访问权限后启动。如果设置为`false`，则禁用 root 访问权限后，实例将保持`stopped`状态。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

文档步骤

- CheckNotebookInstanceStatus (aws: executeAwsApi)：检查笔记本实例的当前状态。
- StopOrUpdateNotebookInstance (aws: branch)：基于笔记本实例状态的分支。
- StopNotebookInstance (aws: executeAwsApi)：如果状态为 ，则启动实例。`stopped`
- WaitForInstanceToStop (aws: wai ForAws ResourceProperty t)：验证实例是否为。`stopped`
- UpdateNotebookInstance (aws: executeAwsApi)：禁用笔记本实例的根访问权限。
- WaitForNotebookUpdate (aws: wait ForAwsResourceProperty)：验证是否已禁用根访问权限以及实例是否处于状态。`stopped`
- ChooseInstanceStart (aws: branch)：根据是否应启动实例进行分支。
- StartNotebookInstance (aws: executeAwsApi)：启动笔记本实例。
- VerifyNotebookInstanceStatus (aws: wait ForAwsResourceProperty)：`available`在禁用 root 访问权限之前验证实例是否已启用。
- VerifyNotebookInstanceRootAccess （ aws: assert AwsResource 属性 ）：验证笔记本实例根访问权限设置是否已成功禁用。

Secrets Manager

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

主题

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

AWSConfigRemediation-DeleteSecret

描述

AWSConfigRemediation-DeleteSecret运行手册会删除一个密钥和存储在中的 AWS Secrets Manager所有版本。您可以选择指定恢复时段，在此期间您可以恢复密钥。如果您没有为 RecoveryWindowInDays 参数指定一个值，则操作将默认为 30 天。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：整数

  有效值：7-30

  默认：30

  描述：（可选）您可以恢复密钥的天数。

- SecretId

  类型：字符串

  描述：（必需）要删除的密钥的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- secretsmanager:DeleteSecret
- secretsmanager:DescribeSecret

文档步骤

- aws:executeAwsApi - 删除您在 SecretId 参数中指定的密钥。
- aws:executeScript - 验证密钥已计划进行删除。

AWSConfigRemediation-RotateSecret

描述

AWSConfigRemediation-RotateSecret运行手册轮换存储在中的密钥。 AWS Secrets Manager

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：间隔

  有效值：1-365

  描述：（必需）密钥两次轮换之间的天数。
- RotationLambdaArn

  类型：字符串

  描述：（必需）可以轮换密钥的 AWS Lambda 函数的 Amazon 资源名称（ARN）。
- SecretId

  类型：字符串

  描述：（必需）要轮换的密钥的 Amazon 资源名称（ARN）。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

文档步骤

- `aws:executeAwsApi` - 轮换您在 `SecretId` 参数中指定的密钥。

- `aws:executeScript` - 验证是否已对密钥启用轮换。

Security Hub

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

主题

- AWSConfigRemediation-EnableSecurityHub

AWSConfigRemediation-EnableSecurityHub

描述

AWSConfigRemediation-EnableSecurityHub运行手册为你运行自动化的 AWS 区域 位置启用 AWS Security Hub （ Sec AWS 账户 urity Hub ）。有关 Security Hub 的信息，请参阅什么是 AWS Security Hub？ 在《AWS Security Hub 用户指南》中。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

- EnableDefault标准

  类型：布尔值

  默认：True

  描述：（必需）如果设置为 `true`，则启用 Security Hub 指定的默认安全标准。

所需的 IAM 权限

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

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

文档步骤

- `aws:executeAwsApi` - 在当前账户和区域中启用 Security Hub。
- `aws:executeAwsApi` - 验证 Security Hub 是否已启用。

AWS Shield

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

主题

- AWSPremiumSupport-DDoSResiliencyAssessment

AWSPremiumSupport-DDoSResiliencyAssessment

描述

`AWSPremiumSupport-DDoSResiliencyAssessment`、AWS Systems Manager 自动化运行手册可帮助您根据 AWS 账户 的 AWS Shield Advanced保护，检查 DDoS 漏洞和资源配置。它为易受分布式拒绝服务 (DDoS) 攻击的资源提供配置设置报告。它用于收集、分析和评估以下资源：Amazon

Route 53、Amazon 负载均衡器、Amazon CloudFront 分配AWS Global Accelerator以及根据推荐的AWS Shield Advanced保护最佳实践进行配置设置的AWS弹性 IP。最终配置报告将以 HTML 文件形式在您选择的 Amazon S3 存储桶中提供。

如何工作？

此运行手册包含一系列检查，用于为公开访问启用的各种类型资源，以及它们是否按照 AWS DDoS 最佳实践白皮书中的建议进行保护措施配置。运行手册将执行以下操作：

- 检查 AWS Shield Advanced 订阅是否已启用。
- 如果已启用，它会查找是否有任何受 Shield Advanced 保护资源。
- 它会在 AWS 账户 中查找所有全球和区域资源，并检查这些资源是否受到 Shield 保护。
- 它需要用于评估的资源类型参数、Amazon S3 存储桶名称和 Amazon S3 存储桶 AWS 账户 ID (S3BucketOwner)。
- 它以 HTML 报告的形式返回调查发现，该报告存储在提供的 Amazon S3 存储桶中。

输入参数 `AssessmentType` 决定是否对所有资源进行检查。默认情况下，运行手册会检查是否有所有类型的资源。如果只选择了 `GlobalResources` 或 `RegionalResources` 参数，运行手册将仅对选定资源类型执行检查。

> **Important**
>
> - 访问 `AWSPremiumSupport-*` 运行手册需要订阅 Enterprise 或 Business Support。有关更多信息，请参阅比较 AWS Support 计划。
> - 此运行手册需要 `ACTIVE`AWS Shield Advanced 订阅。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- AssessmentType

  类型：字符串

  描述：（可选）确定要针对 DDoS 弹性评测进行评估的资源的类型。默认情况下，运行手册将评估全局和区域资源。对于区域资源，运行手册描述了所有应用程序 (ALB) 和网络 (NLB) 负载均衡器，以及您的 AWS 账户/区域的所有 Auto Scaling 组。

  有效值：`['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  默认：全球和区域资源

- S3 BucketName

  类型：`AWS::S3::Bucket::Name`

  描述：（必需）要将报告上传到的 Amazon S3 存储桶名称。

  允许的模式：`^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  类型：字符串

  描述：（可选）拥有 Amazon S3 存储桶的 AWS 账户。如果 Amazon S3 存储桶属于另一个不同的 AWS 账户，请指定此参数，否则可以将此参数留空。

  允许的模式：`^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  类型：`AWS::IAM::Role::Arn`

描述：（可选）具有描述 Amazon S3 存储桶和 AWS 账户 阻止公有访问配置所需权限的 IAM 角色的 ARN（如果存储桶位于其他 AWS 账户）。如果未指定此参数，运行手册将使用 AutomationAssumeRole 或启动此运行手册的 IAM 用户（如果 AutomationAssumeRole 未指定）。请参阅运行手册描述中的“所需权限”部分。

允许的模式：^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$

- S3 BucketPrefix

  类型：字符串

  描述：（可选）Amazon S3 内用于存储结果的路径的前缀。

  允许的模式：^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$

所需的 IAM 权限

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

- autoscaling:DescribeAutoScalingGroups
- cloudfront:ListDistributions
- ec2:DescribeAddresses
- ec2:DescribeNetworkAcls
- ec2:DescribeInstances
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- globalaccelerator:ListAccelerators
- iam:GetRole
- iam:ListAttachedRolePolicies
- route53:ListHostedZones
- route53:GetHealthCheck
- shield:ListProtections
- shield:GetSubscriptionState
- shield:DescribeSubscription

- shield:DescribeEmergencyContactSettings
- shield:DescribeDRTAccess
- waf:GetWebACL
- waf:GetRateBasedRule
- wafv2:GetWebACL
- wafv2:GetWebACLForResource
- waf-regional:GetWebACLForResource
- waf-regional:GetWebACL
- s3:ListBucket
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketEncryption
- s3:GetAccountPublicAccessBlock
- s3:PutObject

自动化承担角色的 IAM policy 示例

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

说明

1. 在控制台中导航到 AWSPremiumSupport-DD ResiliencyAssessment oS。AWS Systems Manager
2. 选择 Execute automation（执行自动化）
3. 要输入参数，请输入内容：
   - AutomationAssumeRole （可选）：

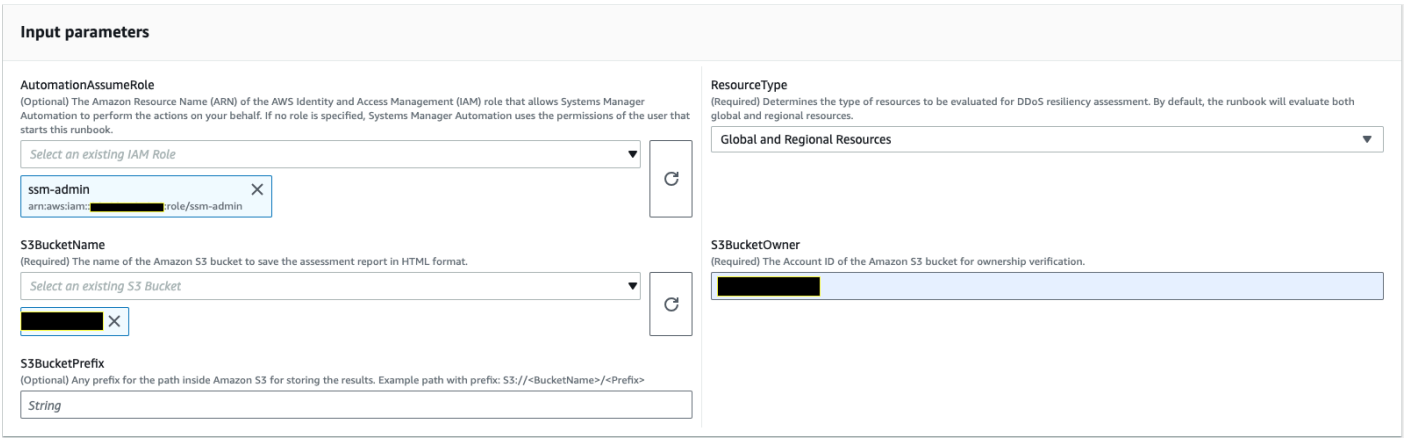
     AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）允许 Systems Manager Automation 代表您执行操作。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
   - AssessmentType （可选）：

     确定要针对 DDoS 弹性评测进行评估的资源的类型。默认情况下，运行手册会评价全球和区域资源。
   - S3BucketName （必填）：

     要将评估报告保存为 HTML 格式的 Amazon S3 存储桶的名称。
   - S3BucketOwner （可选）：

     用于所有权验证的 Amazon S3 存储桶的 AWS 账户 ID。如果报告需要发布到跨账户 Amazon S3 存储桶，则需要提供 AWS 账户 ID；如果 Amazon S3 存储桶与自动化启动处于相同的 AWS 账户，则该 ID 为可选。
   - S3BucketPrefix （可选）：

     Amazon S3 内用于存储结果的路径的前缀。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：

   - CheckShieldAdvancedState:

     检查 “S3BucketName” 中指定的 Amazon S3 存储桶是否允许匿名或公开读取或写入访问权限，该存储桶是否启用了静态加密，以及 “S3BucketOwner” 中提供的 AWS 账户 ID 是否是 Amazon S3 存储桶的所有者。

   - S3BucketSecurityChecks：

     检查 “S3BucketName” 中指定的 Amazon S3 存储桶是否允许匿名或公开读取或写入访问权限，该存储桶是否启用了静态加密，以及 “S3BucketOwner” 中提供的 AWS 账户 ID 是否是 Amazon S3 存储桶的所有者。

   - BranchOnShieldAdvancedStatus:

     根据 AWS Shield Advanced订阅状态和/或 Amazon S3 存储桶所有权状态，对文档步骤进行分支。

   - ShieldAdvancedConfigurationReview:

     审查 Shield Advanced 配置以确保存在最低限度的必要详情。例如：AWS Shield 响应团队 (SRT) 小组的 IAM 访问权限、联系人列表详细信息和 SRT 主动参与状态。

   - ListShieldAdvancedProtections:

     列出受 Shield 保护的资源，并为每个服务创建一组受保护的资源。

   - BranchOnResourceTypeAndCount:

     根据资源类型参数的值和受 Shield 保护的全球资源的数量对文档步骤进行分支。

- ReviewGlobalResources:

  查看 Shield Advanced 受保护的全球资源，例如 Route 53 托管区域、 CloudFront 分布和全球加速器。

- BranchOnResourceType:

  根据资源类型选择对文档记录进行分支（如果是全球、区域或两者）。

- ReviewRegionalResources:

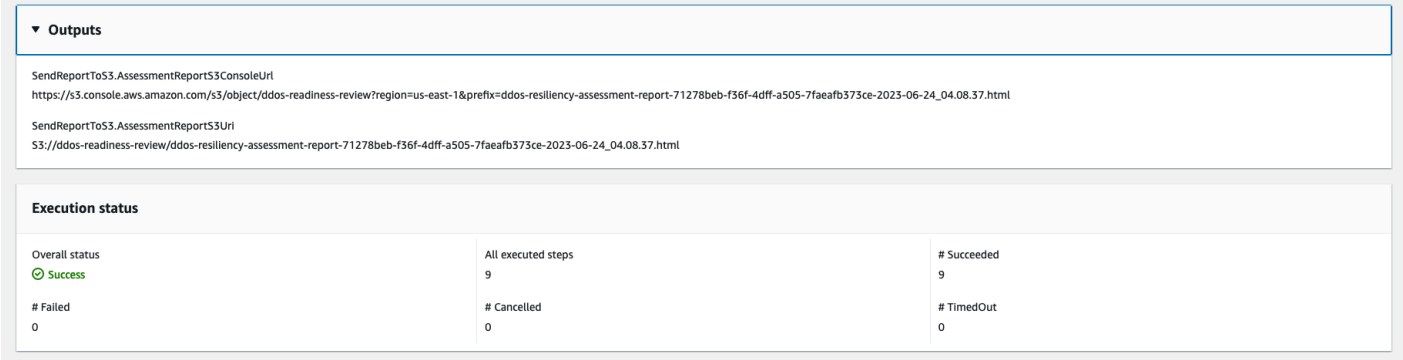
  查看受 Shield Advanced 保护的区域资源，例如应用程序负载均衡器、网络负载均衡器、经典负载均衡器、Amazon Elastic Compute Cloud (Amazon EC2) 实例（弹性 IP）。

- SendReportToS3：

  将 DDoS 评估报告详情上传至 Amazon S3 存储桶。

7. 完成后，将在 Amazon S3 存储桶中提供评估报告 HTML 文件的 URI：

   运行手册成功执行后该报告的 S3 控制台链接和 Amazon S3 URI



参考

Systems Manager Automation

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

AWS服务文档

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager Automation 为 Amazon 简单通知服务提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

AWS-EnableSNSTopicDeliveryStatusLogging

描述

该AWS-EnableSNSTopicDeliveryStatusLogging运行手册为亚马逊 Data Firehose、Lambda 或HTTP亚马逊简单队列服务 (Amazon S Platform application QS) 终端节点配置传输状态日志。这样，Amazon SNS 就可以将失败的警报以及成功警报通知的示例百分比记录到亚马逊。CloudWatch如果已经为该主题配置了交付状态日志，则运行手册将使用您为输入参数指定的新值替换现有配置。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- EndpointType

  类型：字符串

  有效值：

  - HTTP
  - Firehose
  - Lambda
  - 应用程序
  - SQS

  描述：（必填）您要记录其传输状态通知消息的 Amazon SNS 主题终端节点的类型。

- TopicArn

  类型：字符串

  描述：（必填）您要为其配置传送状态日志的 Amazon SNS 主题的 ARN。

- SuccessFeedbackRoleArn

  类型：字符串

  描述：（必填）Amazon SNS 用于向其发送成功通知消息的日志的 IAM 角色的 ARN。 CloudWatch

- SuccessFeedbackSampleRate

  类型：字符串

  有效值：0-100

  描述：（必填）指定 Amazon SNS 主题的成功采样消息的百分比。

- FailureFeedbackRoleArn

  类型：字符串

  描述：（必填）Amazon SNS 用于向其发送失败通知消息日志的 IAM 角色的 ARN。 CloudWatch

所需的 IAM 权限

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

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:PassRole
- sns:GetTopicAttributes
- sns:SetTopicAttributes

文档步骤

- aws:executeAwsApi-将SuccessFeedbackRoleArn参数的值应用于 Amazon SNS 主题。
- aws:executeAwsApi-将SuccessFeedbackSampleRate参数的值应用于 Amazon SNS 主题。
- aws:executeAwsApi-将FailureFeedbackRoleArn参数的值应用于 Amazon SNS 主题。
- aws:executeScript-确认已在 Amazon SNS 主题上启用配送状态记录。

输出

VerifyDeliveryStatusLogging已启用。 GetTopicAttributesResponse -来自 GetTopicAttributes API 操作的响应。

VerifyDeliveryStatusLogging已启用。 VerifyDeliveryStatusLoggingEnabled -表示成功验证传送状态记录的消息。

AWSConfigRemediation-EncryptSNSTopic

描述

该操作AWSConfigRemediation-EncryptSNSTopic手册允许对您使用 () 客户托管密钥指定的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题进行 AWS Key Management Service 加密。AWS KMS此运行手册应仅用作基准，以确保根据建议的最低安全性最佳实践对 Amazon SNS 主题进行加密。我们建议使用不同的客户托管密钥对多个主题进行加密。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

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

  类型：字符串

  描述：（必需）要用于加密 Amazon SNS 主题的 AWS KMS 客户托管密钥的 Amazon 资源名称（ARN）。
- TopicArn

  类型：字符串

  描述：（必需）要加密的 Amazon SNS 主题的 ARN。

所需的 IAM 权限

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

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

文档步骤

- `aws:executeAwsApi` - 加密您在 `TopicArn` 参数中指定的 Amazon SNS 主题。
- `aws:assertAwsResourceProperty` - 确认已对 Amazon SNS 主题启用加密。

AWS-PublishSNSNotification

描述

向 Amazon SNS 发布一个通知。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- 消息

  类型：字符串

  描述：（必需）包含在 SNS 通知中的消息。

- TopicArn

  类型：字符串

描述：（必需）向其发布通知的 SNS 主题的 ARN。

Amazon SQS

AWS Systems Manager Automation 为亚马逊简单队列服务 (Amazon SQS) Simple SQS 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

描述

该AWS-EnableSQSEncryption运行手册支持对亚马逊简单队列服务 (Amazon SQS) 队列进行静态加密。可以使用亚马逊 SQS 托管密钥 (SSE-SQS) 或 () 托管密钥 (SSE-KMS) 对亚马逊 SQS 队列 AWS Key Management Service进行AWS KMS加密。您分配给队列的密钥必须具有密钥策略，其中包括所有有权使用该队列的委托人的权限。启用加密后，匿名ReceiveMessage请求SendMessage和对加密队列的请求将被拒绝。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

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

- QueueUrl

  类型：字符串

  描述：（必填）您要启用加密的 Amazon SQS 队列的 URL。

- KmsKeyId

  类型：字符串

  描述：（可选）用于加密的密AWS KMS钥。此值可以是全局唯一标识符、别名或密钥的 ARN，也可以是以 “alias/” 为前缀的别名。您也可以通过指定别名 aws/sqs 来使用AWS托管密钥。

- KmsDataKeyReusePeriodSeconds

  类型：字符串

  有效值：60-86400

  默认值：300

  描述：（可选）Amazon SQS 队列在再次调用之前可以重复使用数据密钥对消息进行加密或解密的时间长度（以秒为单位）。AWS KMS

所需的 IAM 权限

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

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

文档步骤

- SelectKeyType (aws: branch)：基于指定密钥的分支。

- PutAttributeSseKms (aws:executeAwsApi)-更新 Amazon SQS 队列以使用为加密指定的AWS KMS 密钥。
- PutAttributeSseSqs (aws:executeAwsApi)-更新亚马逊 SQS 队列以使用默认密钥进行加密。
- VerifySqsEncryptionKms (aws: P assertAwsResource roperty)-验证是否已在 Amazon SQS 队列上启用加密。
- VerifySqsEncryptionDefault (aws: P assertAwsResource roperty)-验证是否已在 Amazon SQS 队列上启用加密。

Step Functions

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

主题

- AWS-EnableStepFunctionsStateMachineLogging

AWS-EnableStepFunctionsStateMachineLogging

描述

AWS-EnableStepFunctionsStateMachineLogging运行手册启用或更新您指定的AWS Step Functions状态机上的日志记录。最低日志级别必须设置为ALLERROR、或FATAL。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 级别

  类型：字符串

  有效值：全部 | 错误 | 致命

  描述：（必填）您要启用加密的 Amazon SQS 队列的 URL。

- LogGroupArn

  类型：字符串

  描述：（必填）您要向其发送状态机 CloudWatch 日志的 Amazon 日志组的 ARN。

- StateMachineArn

  类型：字符串

  描述：（必填）要启用登录功能的状态机的 ARN。

- IncludeExecutionData

  类型：布尔值

  默认值：False

  描述：（可选）确定日志中是否包含执行数据。

- TracingConfiguration

  类型：布尔值

  默认值：False

  描述：（可选）确定是否启用AWS X-Ray跟踪。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine
- states:UpdateStateMachine

文档步骤

- EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)-使用指定的日志配置更新指定的状态机。
- VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)-验证是否已为指定状态机启用日志记录。

输出

- EnableStepFunctionsStateMachineLogging.Response-来自 UpdateStateMachine API 调用的响应。

Systems Manager

AWS Systems Manager 自动化为 Systems Manager 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-BulkDeleteAssociation
- AWS-BulkEditOpsItems
- AWS-BulkResolveOpsItems
- AWS-ConfigureMaintenanceWindows
- AWS-CreateManagedLinuxInstance
- AWS-CreateManagedWindowsInstance
- AWSConfigRemediation-EnableCWLoggingForSessionManager
- AWS-ExportOpsDataToS3
- AWS-ExportPatchReportToS3

- AWS-SetupInventory
- AWS-SetupManagedInstance
- AWS-SetupManagedRoleOnEC2Instance
- AWSSupport-TroubleshootManagedInstance
- AWSSupport-TroubleshootPatchManagerLinux
- AWSSupport-TroubleshootSessionManager

AWS-BulkDeleteAssociation

描述

AWS-BulkDeleteAssociation 运行手册可帮助您一次最多删除 50 个 Systems Manager State Manager 关联。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- AssociationIds

类型: StringList

描述：（必需）要删除的关联的 ID 列表（以逗号分隔）。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DeleteAssociation

文档步骤

- aws:executeScript - 删除您在 AssociationIds 参数中指定的关联。

AWS-BulkEditOpsItems

描述

AWS-BulkEditOpsItems运行手册可帮助您编辑的状态、严重性、类别或优先级。 AWS Systems Manager OpsItems此自动化一次最多可以编辑 50 个 OpsItems 。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 类别

  类型：字符串

  有效值：

  - 可用性
  - 费用
  - 无更改
  - Performance
  - 恢复
  - 安全性

  默认：无变化

  描述：（可选）您要为编辑的内容指定的新类别 OpsItems。

- OpsItem身份证

  类型: StringList

  描述：（必填）要编辑的以逗号分隔的 OpsItems ID 列表（例如，oi-xxxxxxxxxxxxx、oi-xxxxxxxxxxxxx）。

- 优先级

  类型：字符串

  有效值：

  - 无更改
  - 1
  - 2
  - 3
  - 4
  - 5

默认：无变化

描述：（可选）编辑的内容 OpsItems 相对于系统 OpsItems 中其他内容的重要性。

- 严重性

  类型：字符串

  有效值：

  - 无更改
  - 1
  - 2
  - 3
  - 4

  默认：无变化

  描述：（可选）已编辑内容的严重性 OpsItems。

- WaitTimeBetweenEditsInSecs

  类型：字符串

  有效值：0.0-2.0

  默认：0.8

  描述：（可选）自动化在调用 `UpdateOpsItems` 操作之间等待的时间。

- Status

  类型：字符串

  有效值：

  - InProgress
  - 无更改
  - 打开
  - 已解决

  默认：无变化

描述：（可选）已编辑内容的新状态 OpsItems。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文档步骤

- aws:executeScript-根据 OpsItems 您为Category、、Priority和OpsItemIds参数指定的值编辑您在Status参数中指定的值。Severity

AWS-BulkResolveOpsItems

描述

AWS-BulkResolveOpsItems运行手册解析的结果与您指定的过滤器 AWS Systems Manager OpsItems 相匹配。您也可以 OpsItems 使用OpsInsightsId参数指定 OpsItemId 要添加到已解析的中。如果您为 S3BucketName 参数指定了一个值，则结果摘要会发送到 Amazon Simple Storage Service (Amazon S3) Service 存储桶。要在结果摘要发送到 Amazon S3 存储桶后收到通知，请为 SnsTopicArn 参数指定一个值。这种自动化一次最多可以解决 1,000 OpsItems 个问题。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- 筛选条件

  类型：字符串

  描述：（必填）用于返回 OpsItems 要解析的过滤器的键值对。例如，`[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`。要详细了解可用于筛选 OpsItems 响应的选项，请参阅 AWS Systems Manager API 参考中的OpsItem过滤器。

- OpsInsight我是

  类型：字符串

  描述：（可选）您要添加到已解析的相关资源标识符 OpsItems。

- S3 BucketName

  类型：字符串

  描述：（可选）要将结果摘要发送到的 Amazon S3 存储桶的名称。

- SnsMessage

  类型：字符串

  描述：（可选）您希望 Amazon Simple Notification Service (Amazon SNS) 在自动化完成时发送的通知。

- SnsTopicArn

  类型：字符串

  描述：（可选）您希望在结果摘要发送到 Amazon S3 时通知的 Amazon SNS 主题的 ARN。

所需的 IAM 权限

~~`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。~~

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

文档步骤

- aws:executeScript- OpsItems 根据您指定的过滤器收集和解析问题。如果您为 OpsInsightId 参数指定了一个值，该值将作为相关资源进行添加。
- aws:executeScript - 如果您为 S3BucketName 参数指定了一个值，则结果摘要随后会发送到 Amazon S3 存储桶。
- aws:executeScript - 如果您为 SnsTopicArn 参数指定了一个值，则在结果摘要发送到 Amazon S3 之后，系统会向 Amazon SNS 主题发送通知，包括 SnsMessage 参数值（如果已指定）。

AWS-ConfigureMaintenanceWindows

描述

AWS-ConfigureMaintenanceWindows 运行手册可帮助您启用或禁用多个 Systems Manager 维护时段。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- MaintenanceWindows

  类型: StringList

  描述：（必需）要启用或禁用的维护时段 ID 的逗号分隔列表。

- MaintenanceWindows状态

  类型：字符串

  有效值："True" | "False"

  默认："False"

  描述：（必需）确定是启用还是禁用维护时段。指定“True”可启用维护时段，指定“False”可禁用维护时段。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

文档步骤

- `aws:executeScript` - 收集您在 `MaintenanceWindows` 参数中指定的维护时段的状态，并启用或禁用维护时段。

AWS-CreateManagedLinuxInstance

描述

创建为 Systems Manager 配置的 Linux EC2 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux

参数

- AmiId

  类型：字符串

  描述：（必需）用于启动实例的 AMI ID。
- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- GroupName

  类型：字符串

  默认：SSM 实例 SecurityGroup ForLinux

  描述：（必需）要创建的安全组名称。
- HttpTokens

类型：字符串

有效值：可选 | 必需

默认：可选

描述：（可选）IMDSv2 使用令牌支持的会话。将 HTTP 令牌的使用设置为 `optional` 或 `required` 以确定 imdsv2 是可选的还是必需的。

- InstanceType

  类型：字符串

  默认：t2.medium

  描述：（必需）要启动的实例类型。默认为 t2.medium。

- KeyPair姓名

  类型：字符串

  描述：（必需）创建实例时使用的密钥对。

- RemoteAccessCidr

  类型：字符串

  默认：0.0.0.0/0

  描述：（必需）创建向 CIDR（默认为 0.0.0.0/0）指定的 IP 开放 SSH 端口（端口范围 22）的安全组。如果安全组已存在，则不会对其进行修改，也不会更改规则。

- RoleName

  类型：字符串

  默认：SSM ManagedInstance ProfileRole

  描述：（必需）要创建的角色名称。

- StackName

  类型：字符串

  默认： CreateManagedInstanceStack{{自动化:execution_ID}}

描述：（可选）指定此运行手册使用的堆栈名称

- SubnetId

  类型：字符串

  默认：Default

  描述：（必需）新实例将部署到此子网；如果未指定，则部署到默认子网。

- VpcId

  类型：字符串

  默认：Default

  描述：（必需）新实例将部署到此 Amazon Virtual Private Cloud (Amazon VPC)；如果未指定，则部署到默认 Amazon VPC。

AWS-CreateManagedWindowsInstance

描述

创建为 Systems Manager 配置的 Windows Server EC2 实例。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Windows

参数

参数

- AmiId

类型：字符串

默认：{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}

描述：（必需）用于启动实例的 AMI ID。

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- GroupName

  类型：字符串

  默认：SSM 实例 SecurityGroup ForLinux

  描述：（必需）要创建的安全组名称。

- HttpTokens

  类型：字符串

  有效值：可选 | 必需

  默认：可选

  描述：（可选）IMDSv2 使用令牌支持的会话。将 HTTP 令牌的使用设置为 optional 或 required 以确定 imdsv2 是可选的还是必需的。

- InstanceType

  类型：字符串

  默认：t2.medium

  描述：（必需）要启动的实例类型。默认为 t2.medium。

- KeyPair姓名

  类型：字符串

描述：（必需）创建实例时使用的密钥对。

- RemoteAccessCidr

  类型：字符串

  默认：0.0.0.0/0

  描述：（必需）创建向 CIDR（默认为 0.0.0.0/0）指定的 IP 开放 RDP 端口（端口范围 3389）的安全组。如果安全组已存在，则不会对其进行修改，也不会更改规则。

- RoleName

  类型：字符串

  默认：SSM ManagedInstance ProfileRole

  描述：（必需）要创建的角色名称。

- StackName

  类型：字符串

  默认： CreateManagedInstanceStack{{自动化:execution_ID}}

  描述：（可选）指定此运行手册使用的堆栈名称

- SubnetId

  类型：字符串

  默认：Default

  描述：（必需）新实例将部署到此子网；如果未指定，则部署到默认子网。

- VpcId

  类型：字符串

  默认：Default

  描述：（必需）新实例将部署到此 Amazon Virtual Private Cloud (Amazon VPC)；如果未指定，则部署到默认 Amazon VPC。

AWSConfigRemediation-EnableCWLoggingForSessionManager

描述

AWSConfigRemediation-EnableCWLoggingForSessionManager运行手册允许 AWS Systems Manager 会话管理器（会话管理器）会话将输出日志存储到 Amazon CloudWatch (CloudWatch) 日志组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- DestinationLog群组

  类型：字符串

  描述：（必填）CloudWatch 日志组的名称。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- ssm:GetDocument
- ssm:UpdateDocument
- ssm:CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

文档步骤

- aws:executeScript-接受 CloudWatch 日志组以更新存储 Session Manager 会话输出日志首选项的文档，如果该首选项不存在，则创建一个。

AWS-ExportOpsDataToS3

描述

本运行手册在 AWS Systems Manager Explorer 中检索 OpsData 摘要列表，并将其导出到指定亚马逊简单存储服务 (Amazon S3) 存储桶中的对象。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- columnFields

  类型: StringList

  描述：（必需）要写入到输出文件的列字段。
- filters

  类型：字符串

  描述：（可选）getOpsSummary 请求的过滤器。
- resultAttribute

  类型：字符串

  描述：（可选）getOpsSummary请求的结果属性。
- s3 BucketName

  类型：字符串

  描述：（必需）要将输出文件下载到的 S3 存储桶。
- sns SuccessMessage

  类型：字符串

  描述：（可选）在运行手册完成时发送的消息。
- sns TopicArn

  类型：字符串

  描述：（必需）下载完成时要通知的 Amazon Simple Notification Service（Amazon SNS）主题 ARN。
- syncName

  类型：字符串

  描述：（可选）资源数据同步的名称。

文档步骤

get OpsSummaryStep — 检索多达 5,000 个操作摘要，立即将其导出为 CSV 文件。

输出

OpsData 对象 — 如果运行手册成功运行，您将在目标 S3 存储桶中找到导出的 OpsData 对象。

AWS-ExportPatchReportToS3

描述

此运行手册在 AWS Systems Manager 补丁管理器中检索补丁摘要数据和补丁详情的列表，并将其导出到指定 Amazon Simple Storage Service (Amazon S3) 存储桶中的 .csv 文件。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- assumeRole

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，则 Systems Manager Automation 使用运行此文档的用户的权限。
- s3 BucketName

  类型：字符串

  描述：（必需）要下载输出文件的 S3 存储桶。
- sns TopicArn

  类型：字符串

描述：（可选）下载完成时要通知的 Amazon Simple Notification Service (Amazon SNS) 主题 Amazon 资源名称（ARN）。

- sns SuccessMessage

  类型：字符串

  描述：（可选）运行手册完成时要发送的消息的文本。

- targets

  类型：字符串

  描述：（必需）实例 ID 或通配符 (*)，用于指示是报告特定实例还是所有实例的补丁数据。

文档步骤

ExportReportStep — 此步骤的操作取决于`targets`参数的值。如果 `targets` 的格式为 `instanceids=*`，则该步骤最多可检索您账户中实例的 10,000 个补丁摘要，并将数据导出到 .csv 文件。

如果 `targets` 的格式为 `instanceids=<instance-id>`，则该步骤会检索您账户中指定实例的补丁摘要和所有补丁，并将其导出到 .csv 文件。

输出

PatchSummary/Patches 对象 — 如果运行手册成功运行，则导出的补丁报告对象将下载到您的目标 S3 存储桶。

AWS-SetupInventory

描述

为一个或多个托管实例创建 Systems Manager Inventory 关联。系统根据关联中的计划从实例收集元数据。有关更多信息，请参阅AWS Systems Manager 清单。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- 应用程序

  类型：字符串

  默认：Enabled

  描述：（可选）收集有关已安装的应用程序的元数据。
- AssociatedDoc姓名

  类型：字符串

  默认：AWS-GatherSoftwareInventory

  描述：（可选）用于从托管实例收集清单的运行手册的名称。
- AssociationName

  类型：字符串

  描述：（可选）将分配给实例的清单关联的名称。
- AssocWait时间

  类型：字符串

  默认值：PT5M

  描述：（可选）到达清单关联开始时间时，清单集合应暂停的时间。时间使用 ISO 8601 格式。
- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- AwsComponents

类型：字符串

默认：Enabled

描述：（可选）收集 AWS 组件的元数据，例如 amazon-ssm-agent。

- CustomInventory

  类型：字符串

  默认：Enabled

  描述：（可选）收集自定义清单元数据。

- 文件

  类型：字符串

  描述：（可选）收集有关实例上的文件的元数据。有关如何收集此类清单数据的更多信息，请参阅使用文件和 Windows 注册表清单。需要 SSMAgent 版本 2.2.64.0 或更高版本。Linux 示例：`[{"Path":"/usr/bin", "Pattern":["aws*", "*ssm*"],"Recursive":false}, {"Path":"/var/log", "Pattern":["amazon*.*"], "Recursive":true, "DirScanLimit":1000}] Windows example: [{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]`

- InstanceDetailed信息

  类型：字符串

  默认：Enabled

  描述：（可选）收集有关实例的其他信息，包括 CPU 型号、速度和内核数等。

- InstanceIds

  类型：字符串

  默认值：*

  描述：（必需）要清点的 EC2 实例。

- LambdaAssume角色

  类型：字符串

描述：（可选）允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- NetworkConfig

  类型：字符串

  默认：Enabled

  描述：（可选）收集有关网络配置的元数据。

- 产出3 BucketName

  类型：字符串

  描述：（可选）要将清单日志数据写入到的 Amazon S3 存储桶的名称。

- 产出3 KeyPrefix

  类型：字符串

  描述：（可选）要将清单日志数据写入到的 Amazon S3 键前缀（子文件夹）。

- OutputS3Region

  类型：字符串

  描述：（可选）Amazon S3 AWS 区域 所在位置的名称。

- 计划

  类型：字符串

  默认值：cron(0 */30 * * * ? *)

  描述：（可选）清单关联计划的 cron 表达式。默认为每 30 分钟一次。

- 服务

  类型：字符串

  默认：Enabled

  描述：（可选，仅限 Windows 操作系统，需要 SSMAgent 版本 2.2.64.0 或更高版本）收集有关服务配置的数据。

- WindowsRegistry

  类型：字符串

  描述：（可选）收集有关 Microsoft Windows 注册表项的元数据。有关如何收集此类清单数据的更多信息，请参阅使用文件和 Windows 注册表清单。需要 SSM Agent 版本 2.2.64.0 或更高版本。示例：[{“路径”: “HKEY_CURRENT_CONFIG\ System”、“Recursive”: true}、{“路径”: “HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ “ , ” “: [" aMiname "]}] MachineImage ValueNames
- WindowsRoles

  类型：字符串

  默认：Enabled

  描述：（可选）收集有关实例上的 Windows 角色的信息。仅适用于 Windows 操作系统。需要 SSMAgent 版本 2.2.64.0 或更高版本。
- WindowsUpdates

  类型：字符串

  默认：Enabled

  描述：（可选）收集有关实例上的所有 Windows 更新的数据。

AWS-SetupManagedInstance

描述

为实例配置一个 AWS Identity and Access Management (IAM) 角色以获得 Systems Manager 访问权限。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

  类型：字符串

  描述：（必需）要配置的 EC2 实例的 ID

- LambdaAssume角色

  类型：字符串

  描述：（可选）允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- RoleName

  类型：字符串

  默认：SSM RoleFor ManagedInstance

  描述：（可选）EC2 实例的 IAM 角色的名称。如果此角色不存在，则创建此角色。指定此值时，请验证该角色是否包含 AmazonSSM ManagedInstance 核心托管策略。

AWS-SetupManagedRoleOnEC2Instance

描述

使用 SSM RoleForManagedInstance 托管 IAM 角色配置实例，以便访问 Systems Manager。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

  类型：字符串

  描述：（必需）要配置的 EC2 实例的 ID

- LambdaAssume角色

  类型：字符串

  描述：（可选）允许 Automation 创建的 Lambda 代表您执行操作的角色的 ARN。如果未指定，将创建临时角色来运行 Lambda 函数。

- RoleName

  类型：字符串

  默认：SSM RoleFor ManagedInstance

  描述：（可选）EC2 实例的 IAM 角色的名称。如果此角色不存在，则创建此角色。指定此值时，请验证该角色是否包含 AmazonSSM ManagedInstance 核心托管策略。

AWSSupport-TroubleshootManagedInstance

描述

AWSSupport-TroubleshootManagedInstance 运行手册可帮助您确定 Amazon Elastic Compute Cloud (Amazon EC2) 实例未报告为由 AWS Systems Manager 管理的原因。此运行手册将审查该实例的 VPC 配置，包括安全组规则、VPC 端点、网络访问控制列表 (ACL) 规则和路由表。它还会确认包含所需权限的 AWS Identity and Access Management (IAM) 实例配置文件是否附加到该实例。

> **Important**
>
> 本自动化操作手册不评估 IPv6 规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

  类型：字符串

  描述：（必需）未报告为由 Systems Manager 管理的 Amazon EC2 实例 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:StartAutomationExecution
- iam:ListRoles
- iam:GetInstanceProfile
- iam:ListAttachedRolePolicies
- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcEndpoints

文档步骤

- aws:executeScript - 收集实例的 PingStatus。
- aws:branch - 根据实例是否已报告为由 Systems Manager 管理的状态进行分支。
- aws:executeAwsApi - 收集有关该实例的详细信息，包括 VPC 配置。
- aws:executeScript - 如果适用，收集与已部署结合 Systems Manager 使用的 VPC 端点相关的其他详细信息，并确认附加到 VPC 端点的安全组允许 TCP 端口 443 上有来自该实例的入站流量。
- aws:executeScript - 检查路由表是否允许流向 VPC 端点或公共 Systems Manager 端点的流量。
- aws:executeScript - 检查网络 ACL 规则是否允许流向 VPC 端点或公共 Systems Manager 端点的流量。

- aws:executeScript - 检查与实例关联的安全组是否允许流向 VPC 端点或公有 Systems Manager 端点的出站流量。
- aws:executeScript - 检查附加到实例的实例配置文件是否包含提供所需权限的托管策略。
- aws:branch - 根据实例的操作系统进行分支。
- aws:executeScript - 提供对 ssmagent-toolkit-linux Shell 脚本的引用。
- aws:executeScript-提供ssmagent-toolkit-windows PowerShell 脚本参考。
- aws:executeScript - 生成自动化的最终输出。
- aws:executeScript - 如果实例 PingStatus 的为 Online，则返回该实例已由 Systems Manager 管理。

AWSSupport-TroubleshootPatchManagerLinux

描述

该AWSSupport-TroubleshootPatchManagerLinux运行手册使用 “补丁管理器” AWS Systems Manager 功能对可能导致基于 Linux 的托管节点上出现补丁失败的常见问题进行故障排除。本运行手册的主要目标是确定补丁命令失败的根本原因并提出补救计划。

如何工作？

AWSSupport-TroubleshootPatchManagerLinux运行手册会考虑您提供的几个实例 ID/命令 ID 以进行故障排除。如果未提供命令 ID，则它会在所提供的实例上选择最近 30 天内最新失败的补丁命令。检查命令状态、先决条件满足情况和操作系统分发后，运行手册会下载并运行日志分析器软件包。输出包括问题的根本原因以及修复问题所需的操作。

文档类型

自动化

所有者

Amazon

平台

- 亚马逊 Linux 2 和 2023
- 红帽企业 Linux 8.X 和 9.X

- Centos 8.X 和 9.X
- SUSE 15.X

参数

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:SendCommand
- ssm:DescribeDocument
- ssm:GetCommandInvocation
- ssm:ListCommands
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:GetDocument
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

说明

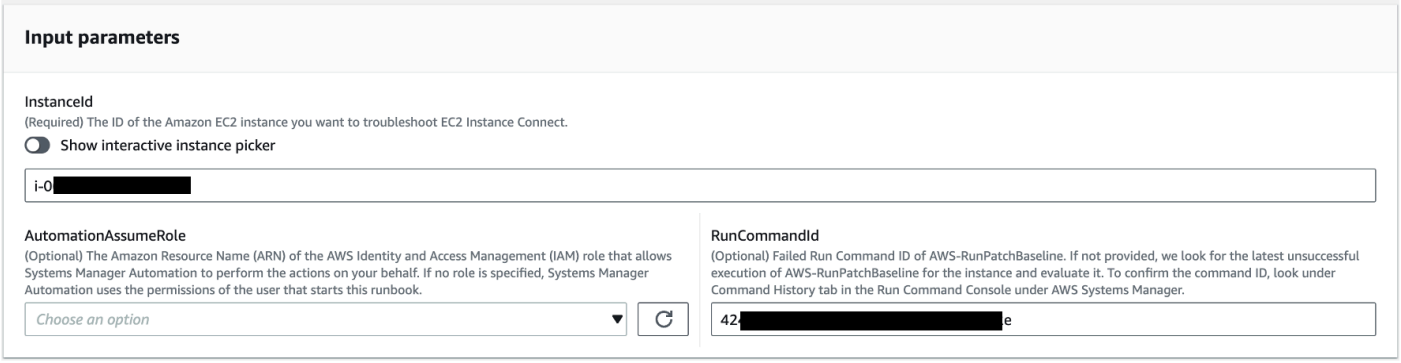
按照这些步骤对自动化进行配置：

1. 在AWS Systems Manager控制台AWSSupport-TroubleshootPatchManagerLinux中导航到。
2. 选择 Execute automation（执行自动化）。
3. 对于输入参数，请输入以下内容：
   - InstanceId （必填）：

     使用交互式实例选择器选择补丁命令失败的基于 Linux 的 SSM 托管节点（亚马逊弹性计算云 (Amazon EC2) 或混合激活服务器）的 ID，或者手动输入 SSM 托管实例的 ID。
   - AutomationAssumeRole （可选）：

     输入允许 Automation 代表您执行操作的 IAM 角色的 ARN。如果未指定角色，Automation 将使用启动此运行手册的用户的权限。
   - RunCommandId （可选）：

输入AWS-RunPatchBaseline文档的失败运行命令 ID。如果您未提供命令 ID，则运行手册将在选定实例上查找最近 30 天内最新的失败补丁命令。



4. 选择执行。
5. 自动化启动。
6. 文档将执行以下步骤：
   - CheckConcurrency:

     确保只有一次针对同一个实例执行此运行手册。如果 runbook 发现针对同一实例的另一个执行正在进行中，则会返回错误并结束。
   - ValidateCommand身份证:

     验证是否已为 AWS-RunPatchBaseline SSM 文档执行了作为输入参数的命令 ID。如果未提供命令 ID，则运行手册将考虑在过去 30 天AWS-RunPatchBaseline内在选定实例上最近一次执行失败的情况。
   - BranchOnCommandStatus:

     确认所提供命令的状态为失败。否则，运行手册将结束执行并生成一份报告，说明所提供的命令已成功执行。
   - VerifyPrerequistes:

     确认上述先决条件已满足。
   - GetPlatformDetails:

     检索操作系统 (OS) 的发行版和版本。
   - GetDownload网址：

     检索 L PatchManager og Analyzer 软件包的下载 URL。
   - EvaluatePatchManagerLogs:

在实例上下载并执行 PatchManager Log Analyzer python 软件包以评估日志文件。

- GenerateReport:

  生成运行手册执行的最终报告，其中包括已发现的问题和建议的解决方案。

7. 完成后，请查看 “输出” 部分，了解执行的详细结果：

参考

Systems Manager Automation

- 运行此自动化（控制台）
- 运行自动化
- 设置自动化
- 支持自动化工作流登录页面

AWSSupport-TroubleshootSessionManager

描述

AWSSupport-TroubleshootSessionManager 运行手册可帮助您排除导致您无法使用会话管理器连接到托管 Amazon Elastic Compute Cloud (Amazon EC2) 实例的常见问题。会话管理器是一项功能 AWS Systems Manager。此运行手册检查以下各项：

- 检查实例是否正在运行并报告为由 Systems Manager 管理。
- 如果实例未报告为由 Systems Manager 管理，则运行 AWSSupport-TroubleshootManagedInstance 运行手册。

- 检查安装在该实例上的 SSM Agent 的版本。
- 检查包含建议的会话管理器 AWS Identity and Access Management (IAM) 策略的实例配置文件是否已附加到 Amazon EC2 实例。
- 从实例收集 SSM 代理日志。
- 分析您的会话管理器首选项。
- `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`运行手册以分析实例与会话管理器、 AWS Key Management Service (AWS KMS)、亚马逊简单存储服务 (Amazon S3) 和 CloudWatch 亚马逊CloudWatch 日志（日志）的终端节点的连接。

注意事项

- 不支持混合托管节点。
- 此运行手册仅检查建议的托管 IAM policy 是否已附加到实例配置文件。它不会分析 IAM 或实例配置文件中包含的 AWS KMS 权限。

> **Important**
>
> `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 运行手册使用 VPC Reachability Analyzer 分析来源和服务端点之间的网络连接。每次在来源和目标之间运行分析时，您需要支付费用。有关详细信息，请参阅 Amazon VPC 定价。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- InstanceId

  类型：字符串

  描述：（必需）您无法使用会话管理器连接到的 Amazon EC2 实例的 ID。

- SessionPreference文档

  类型：字符串

  默认：SSM-SessionManager RunShell

  描述：（可选）会话首选项文档的名称。如果您在启动会话时未指定自定义会话首选项文档，则使用默认值。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateNetworkInsightsPath
- ec2:DeleteNetworkInsightsAnalysis
- ec2:DeleteNetworkInsightsPath
- ec2:StartNetworkInsightsAnalysis
- tiros:CreateQuery
- ec2:DescribeAvailabilityZones
- ec2:DescribeCustomerGateways
- ec2:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInternetGateways

- ec2:DescribeManagedPrefixLists
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInsightsAnalyses
- ec2:DescribeNetworkInsightsPaths
- ec2:DescribeNetworkInterfaces
- ec2:DescribePrefixLists
- ec2:DescribeRegions
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTransitGatewayAttachments
- ec2:DescribeTransitGatewayConnects
- ec2:DescribeTransitGatewayPeeringAttachments
- ec2:DescribeTransitGatewayRouteTables
- ec2:DescribeTransitGateways
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetManagedPrefixListEntries
- ec2:GetTransitGatewayRouteTablePropagations
- ec2:SearchTransitGatewayRoutes
- elasticloadbalancing:DescribeListeners
- elasticloadbalancing:DescribeLoadBalancerAttributes

- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeRules
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- iam:GetInstanceProfile
- iam:ListAttachedRolePolicies
- iam:ListRoles
- iam:PassRole
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:StartAutomationExecution
- tiros:GetQueryAnswer
- tiros:GetQueryExplanation

文档步骤

1. aws:waitForAwsResourceProperty：最多等 6 分钟，目标实例就能通过状态检查。
2. aws:executeScript：解析会话首选项文档。
3. aws:executeAwsApi：获取附加到您的实例的实例配置文件的 ARN。
4. aws:executeAwsApi：检查您的实例是否报告为由 Systems Manager 管理。
5. aws:branch：根据您的实例是否报告为由 Systems Manager 管理进行分支。
6. aws:executeScript：检查您的实例上安装的SSM Agent 是否支持会话管理器。
7. aws:branch：根据用于收集 ssm-cli 日志的实例的平台进行分支。
8. aws:runCommand：从 Linux 或 macOS 实例收集 ssm-cli 的输出日志。

9. aws:runCommand：从 Windows 实例收集 ssm-cli 的输出日志。

10aws:executeScript：解析 ssm-cli 日志。

11aws:executeScript：检查建议的 IAM policy 是否已附加到实例配置文件。

12aws:branch：确定是否根据 ssm-cli 日志评估 ssmmessages 端点连接。

13aws:executeAutomation：评估实例是否可以连接到 ssmmessages 端点。

14aws:branch：根据 ssm-cli 日志和会话首选项，确定是否评估 Amazon S3 端点连接。

15aws:executeAutomation：评估实例是否可以连接到 Amazon S3 端点。

16aws:branch：决定是否根据ssm-cli日志和会话首选项评估 AWS KMS 端点连接。

17aws:executeAutomation：评估实例是否可以连接到 AWS KMS 终端节点。

18aws:branch：根据 CloudWatch 日志和您的会话首选项确定是否评估ssm-cli日志端点连接。

19aws:executeAutomation：评估实例是否可以连接到 L CloudWatch ogs 端点。

20aws:executeAutomation: 运行 AWSSupport-TroubleshootManagedInstance 运行手册。

21aws:executeScript：编译先前步骤的输出并输出一个报告。

输出

- generateReport.EvalReport - 运行手册以纯文本形式执行的检查结果。

第三方

AWS Systems Manager 自动化为第三方产品和服务提供预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

AWS-CreateJiraIssue

描述

在 Jira 中创建问题。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AssigneeName

  类型：字符串

  描述：（必需）应向其分配问题的人员的用户名。
- DueDate

  类型：字符串

  描述：（可选）问题的截止日期（ yyyy-mm-dd格式为）。
- IssueDescription

  类型：字符串

  描述：（必需）问题的详细说明。
- IssueSummary

  类型：字符串

  描述：（必需）问题的小结。
- IssueType姓名

  类型：字符串

  描述：（必需）您要创建的问题的类型名称（例如，任务、子任务、错误等）。
- JiraURL

类型：字符串

描述：（必需）Jira 实例的 URL。

- JiraUsername

  类型：字符串

  描述：（必需）创建问题将使用的用户的名称。

- PriorityName

  类型：字符串

  描述：（可选）问题的优先级的名称。

- ProjectKey

  类型：字符串

  描述：（必需）应在其中创建问题的项目的密钥。

- SSM ParameterName

  类型：字符串

  描述：（必需）包含 Jira 用户的 API 密钥或密码的加密 SSM 参数的名称。

文档步骤

aws:createStack-创建 CloudFormation 堆栈以创建 Lambda IAM 角色和函数。

aws:invokeLambdaFunction - 调用 Lambda 函数以创建 Jira 问题

aws:deleteStack-删除创建的 CloudFormation 堆栈。

输出

IssueId: 新创建的 Jira 事务的 ID

AWS-CreateServiceNowIncident

描述

在事件表中创建 ServiceNow 事件。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- 类别

  类型：字符串

  描述：（可选）事件的类别。

  有效值：None | Inquiry/Help | Software | Hardware | Network | Database

  默认值：None
- 描述

  类型：字符串

  描述：（必需）有关事件的详细说明。
- 影响

  类型：字符串

描述：（可选）事件对业务的影响。

有效值：High | Medium | Low

默认值：Low

- ServiceNowInstanceUsername

  类型：字符串

  描述：（必需）创建事件时使用的用户的名称。

- ServiceNowInstancePassword

  类型：字符串

  描述：（必填）包含 ServiceNow 用户密码的加密 SSM 参数的名称。

- ServiceNow实例网址

  类型：字符串

  描述：（必填） ServiceNow 实例的 URL

- ShortDescription

  类型：字符串

  描述：（必需）事件的简要描述。

- 子类别

  类型：字符串

  描述：（可选）事件的子类别。

  有效值：None | Antivirus | Email | Internal Application | Operating System | CPU | Disk | Keyboard | Hardware | Memory | Monitor | Mouse | DHCP | DNS | IP Address | VPN | Wireless | DB2 | MS SQL Server | Oracle

  默认值：None

文档步骤

push_incident — 将事件信息推送到。 ServiceNow

输出

Push_incident.incidentID – 创建的事件 ID。

AWS-RunPacker

描述

本运行手册使用 HashiCorp Packer 工具来验证、修复或构建用于创建机器映像的打包程序模板。该运行手册使用 Packer v1.7.2。

> **Note**
>
> 如果您指定了 vpc_id 值，则还必须指定公有子网的 subnet_id 值。除非您修改子网的 IPv4 公有寻址属性，否则还必须将 associate_public_ip_address 设置为 true。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- Force

类型：布尔值

描述：在以前生成中的构件禁止生成运行时，强制生成器运行的 Packer 选项。

- Mode

  类型：字符串

  描述：在根据模板进行验证时使用 Packer 的模式或命令。选项包括 `Build`、`Validate` 和 `Fix`。

- TemplateFile姓名

  类型：字符串

  描述：S3 存储桶中的模板文件的名称或键。

- 模板3 BucketName

  类型：字符串

  描述：包含 Packer 模板的 S3 存储桶的名称。

文档步骤

RunPackerProcessTemplate — 使用 Packer 工具对模板运行所选模式。

输出

RunPackerProcessTemplate.output — Packer 工具中的标准输出。

RunPackerProcessTemplate.fixed_template_key — 存储在 S3 存储桶中的模板的名称，仅在 “修复” 模式下运行时使用。

RunPackerProcessTemplate.s3_bucket — 包含仅在 “修复” 模式下运行时使用的固定模板的 S3 存储桶的名称。

Amazon VPC

AWS Systems Manager Automation 为亚马逊 Virtual Private Cloud 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-CloseSecurityGroup
- AWSSupport-ConfigureDNSQueryLogging
- AWSSupport-ConfigureTrafficMirroring
- AWSSupport-ConnectivityTroubleshooter
- AWSSupport-TroubleshootVPN
- AWSConfigRemediation-DeleteEgressOnlyInternetGateway
- AWSConfigRemediation-DeleteUnusedENI
- AWSConfigRemediation-DeleteUnusedSecurityGroup
- AWSConfigRemediation-DeleteUnusedVPCNetworkACL
- AWSConfigRemediation-DeleteVPCFlowLog
- AWSConfigRemediation-DetachAndDeleteInternetGateway
- AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway
- AWS-DisableIncomingSSHOnPort22
- AWS-DisablePublicAccessForSecurityGroup
- AWSConfigRemediation-DisableSubnetAutoAssignPublicIP
- AWSSupport-EnableVPCFlowLogs
- AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch
- AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket
- AWS-ReleaseElasticIP
- AWS-RemoveNetworkACLUnrestrictedSSHRDP
- AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules
- AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules
- AWSSupport-SetupIPMonitoringFromVPC
- AWSSupport-TerminateIPMonitoringFromVPC

AWS-CloseSecurityGroup

描述

此运行手册将从您指定的安全组中删除所有入口和出口规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- SecurityGroup我是

  类型：字符串

  描述：（必填）要关闭的安全组的 ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

文档步骤

- `aws:executeScript`-从您在参数中指定的安全组中删除所有入口和出口规则。`SecurityGroupId`

AWSSupport-ConfigureDNSQueryLogging

描述

AWSSupport-ConfigureDNSQueryLogging 运行手册为源自虚拟私有云 (VPC) 的或为 Amazon Route 53 托管区的 DNS 查询配置日志记录。您可以选择将查询日志发布到亚马逊日 CloudWatch 志、亚马逊简单存储服务 (Amazon S3) Service 或亚马逊 Data Firehose。有关查询日志记录和解析器查询日志的更多信息，请参阅公共 DNS 查询日志记录和解析器查询日志记录。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LogDestinationArn

  类型：字符串

  描述：（可选）您要向其发送查询日志的 CloudWatch 日志组、Amazon S3 存储桶或 Firehose 流的 ARN。请注意，Route 53 公共 DNS 查询日志记录仅支持 CloudWatch 日志组。如果您未为此参数指定值，则自动化会创建一个格式为的 CloudWatch 日志组 AWSSupport-ConfigureDNSQueryLogging-{automation: *EXECUTION_ID* } ，以及用于发布查询日志的 IAM 资源策略。自动化创建的 CloudWatch 日志组的保留期为 14 天。

- QueryLog类型

  类型：字符串

  描述：（可选）要记录的查询的类型。

  有效值：公共 | 解析器/私有

  默认：公共

- ResourceId

  类型：字符串

  描述：（必需）要记录其查询的资源的 ID。如果您为 QueryLogType 参数指定 Public，则资源必须是 Route 53 私有托管区的 ID。如果您 为 QueryLogType 参数指定 Resolver/Private，则资源必须是 VPC 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeVpcs
- firehose:ListTagsForDeliveryStream
- firehose:PutRecord
- firehose:PutRecordBatch
- firehose:TagDeliveryStream
- iam:AttachRolePolicy
- iam:CreatePolicy
- iam:CreateRole
- iam:CreateServiceLinkedRole
- iam:DeletePolicy
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole

- iam:PassRole
- iam:PutRolePolicy
- iam:TagRole
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:DescribeResourcePolicies
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:PutRetentionPolicy
- logs:UpdateLogDelivery
- route53:CreateQueryLoggingConfig
- route53:DeleteQueryLoggingConfig
- route53:GetHostedZone
- route53resolver:AssociateResolverQueryLogConfig
- route53resolver:CreateResolverQueryLogConfig
- route53resolver:DeleteResolverQueryLogConfig
- s3:GetBucketAcl

文档步骤

- aws:executeScript - 验证您为 ResourceId 参数指定的资源是否存在，并检查资源类型是否匹配所需的 QueryLogType 选项。
- aws:executeScript - 验证您为 LogDestinationArn 参数指定的值是否匹配所需的 QueryLogType 值。
- aws:executeScript-验证 Route 53 向日志组发布日志所需的权限，如果不存在所需的 IAM 资源策略，则创建所需的 IAM 资源策略。 CloudWatch

- aws:executeScript - 对所选目标启用 DNS 查询日志记录。

AWSSupport-ConfigureTrafficMirroring

描述

AWSSupport-ConfigureTrafficMirroring 运行手册将配置流量镜像，以帮助您解决负载均衡器与 Amazon Elastic Compute Cloud (Amazon EC2) 实例之间的连接问题。流量镜像会复制来自附加到您的实例的网络接口的入站和出站流量。要配置流量镜像，此运行手册将创建所需的目的地、筛选条件和会话。默认情况下，运行手册会为除 Amazon DNS 之外的所有协议的所有入站和出站流量配置镜像。如果您希望镜像来自特定来源和目的地的流量，则可以在自动化完成后修改入站和出站规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- SourceENI

  类型：字符串

  描述：（必需）要为其配置流量镜像的弹性网络接口。

- 目标

类型：字符串

描述：（必需）镜像流量的目的地。必须指定网络接口、网络负载均衡器或网关负载均衡器端点的 ID。如果您指定了网络负载均衡器，则端口 4789 上必须有 UDP 侦听器。

- SessionNumber

  类型：字符串

  有效值：1-32766

  描述：（必需）要使用的镜像会话的数量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:CreateTrafficMirrorTarget
- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilter
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

文档步骤

- aws:executeScript - 运行脚本以创建一个目标。
- aws:executeAwsApi - 创建一个筛选规则。
- aws:executeAwsApi - 为所有入站流量创建一个镜像筛选规则。
- aws:executeAwsApi - 为所有出站流量创建一个镜像筛选规则。

- aws:executeAwsApi - 创建流量镜像会话。
- aws:executeAwsApi - 在筛选器或会话创建失败时删除筛选器。
- aws:executeAwsApi - 在筛选器或会话创建失败时删除目标。

输出

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.targetIDOutput

AWSSupport-ConnectivityTroubleshooter

描述

AWSSupport-ConnectivityTroubleshooter 运行手册可诊断以下各项之间的连接问题：

- AWS 亚马逊虚拟私有云（亚马逊 VPC）中的资源
- AWS 同一个 Amazon VPC 中使用 VPC AWS 区域 对等互连连接的资源
- AWS Amazon VPC 中的资源和使用互联网网关的互联网资源
- AWS Amazon VPC 中的资源和使用网络地址转换 (NAT) 网关的互联网资源

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- DestinationIP

  类型：字符串

  描述：（必需）要连接到的资源的 IPv4 地址。
- DestinationPort

  类型：字符串

  默认：True

  描述：（必需）要在目的地资源上连接的端口号。
- DestinationVpc

  类型：字符串

  默认：全部

  描述：（可选）要测试与之连接性的 Amazon VPC 的 ID。
- SourceIP

  类型：字符串

  描述：（必填）您想要测试连接的 Amazon VPC 中 AWS 资源的私有 IPv4 地址。
- SourcePort射程

  类型：字符串

  描述：（可选）您的 Amazon VPC 中您想要测试连接的 AWS 资源使用的端口范围。
- SourceVpc

  类型：字符串

  默认：全部

描述：（可选）要从其测试连接性的 Amazon VPC 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

文档步骤

- aws:executeScript-收集有关您在SourceIP参数中指定的 AWS 资源的详细信息。
- aws:executeScript-使用上一步收集的路由，确定来自 AWS 资源的网络流量的目的地。
- aws:branch - 根据网络流量的目的地进行分支。
- aws:executeAwsApi - 收集有关目的地资源的详细信息。
- aws:executeScript - 确认为目的地 Amazon VPC 返回的 ID 匹配在 DestinationVpc 参数中指定的值（如果有）。
- aws:executeAwsApi - 收集源资源和目的地资源的安全组规则。
- aws:executeScript - 确认安全组规则是否允许来源资源和目的地资源之间所需的流量。
- aws:executeAwsApi - 收集与来源资源和目的地资源的子网关联的网络访问控制列表 (NACL)。
- aws:executeScript - 确认 NACL 是否允许来源资源和目的地资源之间所需的流量。
- aws:executeScript - 在路由目的地是互联网网关时确认来源是否拥有与资源关联的公有 IP 地址。
- aws:executeAwsApi - 收集来源资源的安全组规则。
- aws:executeScript - 确认安全组规则是否允许从来源资源到目的地资源的所需流量。
- aws:executeAwsApi - 为来源资源收集与子网关联的 NACL。
- aws:executeScript - 确认 NACL 是否允许来自来源资源的所需流量。
- aws:executeAwsApi - 收集 NAT 网关的详细信息。

- aws:executeAwsApi - 为 NAT 网关收集与 NAT 网关的子网关联的 NACL。
- aws:executeScript - 确认 NACL 是否允许来自 NAT 网关的子网的所需流量。
- aws:executeScript - 收集与 NAT 网关的子网关联的路由。
- aws:executeScript - 确认 NAT 网关是否具有到互联网网关的路由。
- aws:executeAwsApi - 收集有关 VPC 对等连接的详细信息。
- aws:executeScript - 确认两个 VPC 位于同一区域，并且为目的地 VPC 返回的 ID 匹配 DestinationVpc 参数中指定的值（若有）。
- aws:executeAwsApi - 返回目的地资源的子网。
- aws:executeScript - 收集与对等连接 VPC 的子网关联的路由。
- aws:executeScript - 确认对等连接 VPC 是否有到对等连接的路由。
- aws:executeScript - 确认当自动化不支持目的地时是否允许来自源资源的流量。

AWSSupport-TroubleshootVPN

描述

AWSSupport-TroubleshootVPN 运行手册可帮助您跟踪和解决 AWS Site-to-Site VPN 连接中的错误。自动化包括多项自动化的检查，旨在跟踪与 AWS Site-to-Site VPN 连接隧道相关的 IKEv1 或 IKEv2错误。自动化将尝试匹配特定的错误及其相应的解决方案，从而形成常见问题列表。

注意：此自动化并不能纠正错误。它在上述时间范围内运行，并扫描日志组中是否存在 VPN CloudWatch 日志组中的错误。

如何工作？

运行手册运行参数验证，以确认输入参数中包含的 Amazon CloudWatch 日志组是否存在、日志组中是否存在与 VPN 隧道日志记录相对应的日志流、VPN 连接 ID 是否存在以及隧道 IP 地址是否存在。它会在配置为 VPN 日志记录的 CloudWatch 日志组上进行 Logs Insights API 调用。

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- LogGroupName

  类型：字符串

  描述：（必填）为AWS Site-to-Site VPN连接 CloudWatch 日志配置的 Amazon 日志组名称

  允许的模式：`^[\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

  类型：字符串

  说明：（必需）要排查问题的 AWS Site-to-Site VPN 连接。

  允许的模式：`^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

  类型：字符串

  描述：（必需）与您的AWS Site-to-Site VPN关联的隧道编号 1 的 IPv4 地址。

  允许的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}$`

- TunnelBIPAddress

  类型：字符串

  描述：（可选）与 AWS Site-to-Site VPN 关联的隧道编号 2 的 IPv4 地址。

  允许的模式：`^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

  类型：字符串

  描述：（必需）选择您正在使用的 IKE 版本。允许的值：IKEv1、IKEv2

  有效值：`['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  类型：字符串

  描述：（可选）日志分析的开始时间。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 进行日志分析

  允许的模式：`^\d{10}|^$`

- EndTimeinEpoch

  类型：字符串

  描述：（可选）日志分析的结束时间。您可以使用 StartTimeinEpoch/EndTimeinEpoch 或 LookBackPeriod 进行日志分析。如果同时给出 StartTimeinEpoch/EndTimeinEpoch LookBackPeriod 然后优 LookBackPeriod 先

  允许的模式：`^\d{10}|^$`

- LookBackPeriod

  类型：字符串

  描述：（可选）以小时为单位的两位数时间，用于回顾日志分析。有效范围：01 - 99 如果您还给出 StartTimeinEpoch 和，则此值优先 EndTime

  允许的模式：`^(\d?[1-9]|[1-9]0)|^$`

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`

- logs:StartQuery
- ec2:DescribeVpnConnections

说明

注意：当 CloudWatch 日志输出格式为 JSON 时，此自动化适用于为 VPN 隧道日志记录配置的日志组。

按照这些步骤对自动化进行配置：

1. 在控制台中导航到 AWSSupport-故障排除VPN。AWS Systems Manager
2. 要输入参数，请输入以下内容：
   - AutomationAssumeRole （可选）：

     AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）允许 Systems Manager Automation 代表您执行操作。如果未指定任何角色，则 Systems Manager Automation 使用启动此运行手册的用户的权限。
   - LogGroupName （必填）：

     要验证的 Amazon CloudWatch 日志组名称。这必须是为 VPN 配置的要向其发送日志的日志组。CloudWatch
   - VpnConnectionId （必填）：

     因 VPN 错误而跟踪其日志组的 AWS Site-to-Site VPN 连接 ID。
   - 隧道 IP 地址（必需）：

     与您的 AWS Site-to-Site VPN 连接关联的隧道 A IP 地址。
   - TunnelBIPAddress（可选）：

     与您的 AWS Site-to-Site VPN 连接关联的隧道 B IP 地址。
   - ike版本（必需）：

     选择您正在使用的 IKEVersion。允许的值：IKEv1、IKEv2。
   - StartTimeinEpoch （可选）：

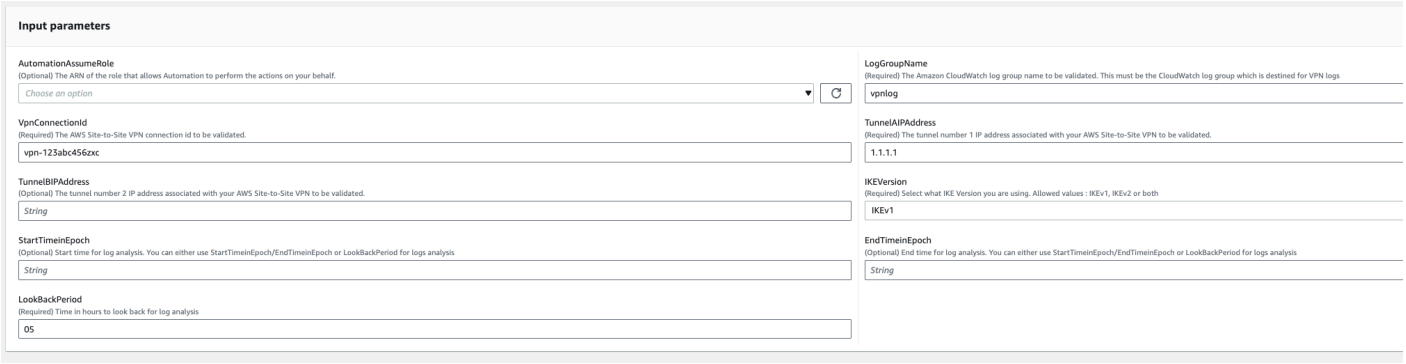
     查询错误的时间范围的起点。该范围包括在内，因此查询中包含了指定的开始时间。指定为纪元时间，即自 1970 年 1 月 1 日 00:00:00 UTC 以来的秒数。
   - EndTimeinEpoch （可选）：

查询错误的时间范围的结束时间。该范围包括在内，因此查询中包含了指定的结束时间。指定为纪元时间，即自 1970 年 1 月 1 日 00:00:00 UTC 以来的秒数。

- LookBackPeriod （必填）：

  回顾错误查询所需的时间（以小时为单位）。

注意：配置 StartTimeinEpoch EndTimeinEpoch、或 LookBackPeriod 以固定日志分析的时间范围。给出一个以小时为单位的两位数数字，以检查从自动化开始时间起过去是否有错误。或者，如果错误发生在特定的时间范围内，请使用 StartTimeinEpoch 和 EndTimeinEpoch，而不是 LookBackPeriod。



3. 选择执行。
4. 自动化启动。
5. 自动化运行手册执行以下步骤：

   - parameterValidation：

     对自动化中包含的输入参数运行一系列验证。

   - branchOnValidationOfLogGroup:

     检查参数中提到的日志组是否有效。如果无效，它会停止进一步启动自动化步骤。

   - branchOnValidationOfLogStream:

     检查包含的日志组中是否存在 CloudWatch 日志流。如果无效，它会停止进一步启动自动化步骤。

   - branchOnValidationOfVpnConnectionId:

     检查参数中包含的 VPN 连接 ID 是否有效。如果无效，它会停止进一步启动自动化步骤。

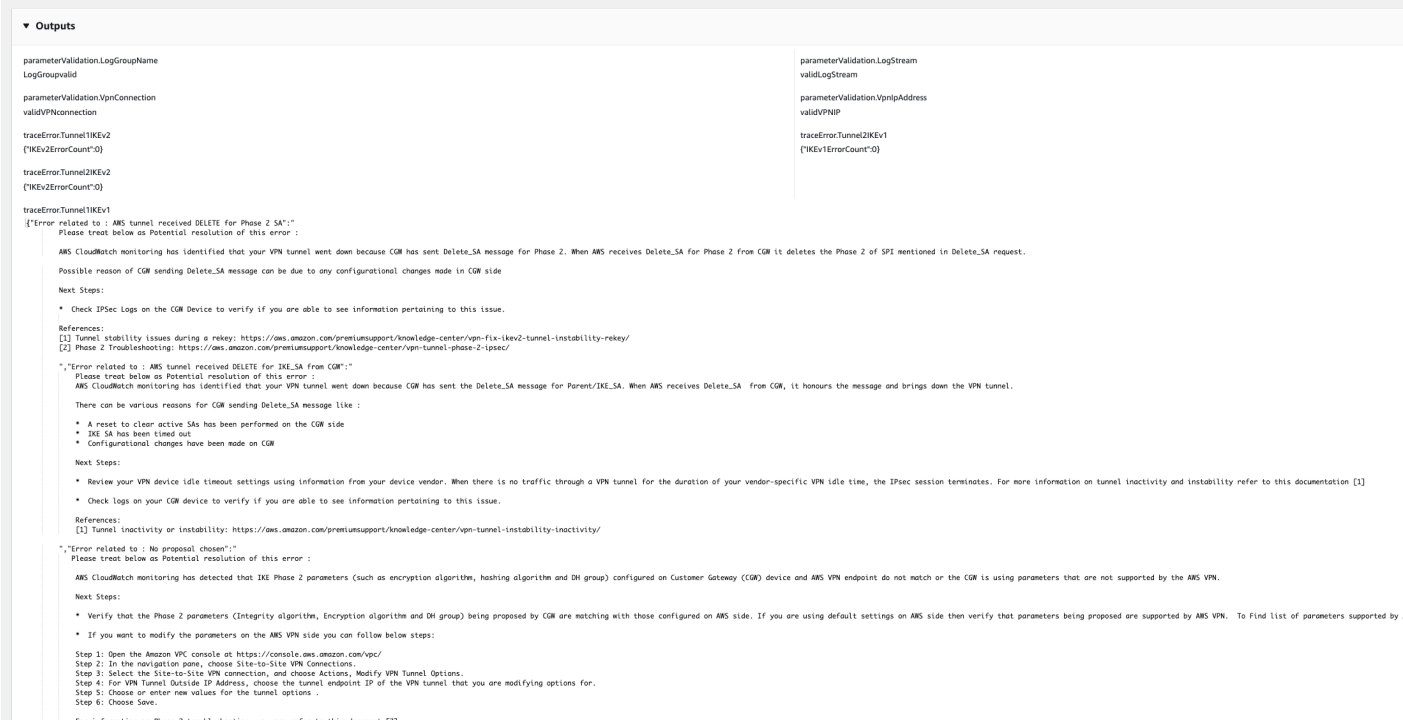
   - branchOnValidationOfVpnIp:

检查参数中提到的隧道 IP 地址是否有效。如果无效，它会停止进一步执行自动化步骤。

- traceError：

  在包含的 CloudWatch 日志组中调用 logs insight API，然后搜索与 IKEv1/IKEv2 相关的错误以及相关的建议解决方案。

6. 完成后，查看“输出”部分以了解执行的详细结果。



参考

Systems Manager Automation

- 运行此自动化（控制台）
- 运行自动化
- 设置自动化
- 支持自动化工作流登录页面

AWS 服务文档

- 点对点 VPN 日志的内容

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

描述

AWSConfigRemediation-DeleteEgressOnlyInternetGateway 运行手册删除指定的仅出口互联网网关。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- EgressOnlyInternetGateway我是

  类型：字符串

  描述：（必需）要删除的仅出口互联网网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

文档步骤

- aws:executeScript - 删除 EgressOnlyInternetGatewayId 参数中指定的仅出口互联网网关。
- aws:executeScript - 验证仅出口互联网网关是否已被删除。

AWSConfigRemediation-DeleteUnusedENI

描述

AWSConfigRemediation-DeleteUnusedENI 运行手册将删除连接状态为 detached 的弹性网络接口 (ENI)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- NetworkInterface我是

类型：字符串

描述：（必需）要删除的 ENI ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

文档步骤

- aws:executeAwsApi - 删除您在 NetworkInterfaceId 参数中指定的 ENI。
- aws:executeScript - 验证 ENI 是否已被删除。

AWSConfigRemediation-DeleteUnusedSecurityGroup

描述

AWSConfigRemediation-DeleteUnusedSecurityGroup 运行手册将删除您在 GroupId 参数中指定的安全组。如果您尝试删除与 Amazon Elastic Compute Cloud (Amazon EC2) 实例关联的安全组或由另一个安全组引用的安全组，则自动化将失败。此自动化不会删除默认的安全组。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- GroupId

  类型：字符串

  描述：（必需）要删除的安全组 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:DeleteSecurityGroup

文档步骤

- aws:executeAwsApi - 使用您在 GroupId 参数中提供的值返回安全组名称。
- aws:branch - 确认群组名称不是“default”。
- aws:executeAwsApi - 删除 GroupId 参数中指定的安全组。
- aws:executeScript - 确认安全组已删除。

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

描述

AWSConfigRemediation-DeleteUnusedVPCNetworkACL 运行手册删除将删除不与子网关联的网络访问控制列表 (ACL)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- NetworkAcl我是

  类型：字符串

  描述：（必需）要删除的网络 ACL 的 ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

文档步骤

- `aws:executeAwsApi` - 删除 `NetworkAclId` 参数中指定的网络 ACL。
- `aws:executeScript` - 确认 `NetworkAclId` 参数中指定的网络 ACL 已删除。

AWSConfigRemediation-DeleteVPCFlowLog

描述

AWSConfigRemediation-DeleteVPCFlowLog运行手册将删除您指定的虚拟私有云（VPC）流日志。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- FlowLog我是

  类型：字符串

  描述：（必需）要删除的流日志的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteFlowLogs

- ec2:DescribeFlowLogs

文档步骤

- aws:executeAwsApi - 删除您在 FlowLogId 参数中指定的流日志。
- aws:executeScript - 验证流日志是否已删除。

AWSConfigRemediation-DetachAndDeleteInternetGateway

描述

AWSConfigRemediation-DetachAndDeleteInternetGateway 运行手册将分离并删除您指定的互联网网关。如果您的虚拟私有云（VPC）中的任何 Amazon EC2 实例具有与之关联的弹性 IP 地址或公有 IPv4 地址，运行手册将失败。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- InternetGateway我是

  类型：字符串

描述：（必需）要删除的互联网网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteInternetGateway
- ec2:DescribeInternetGateways
- ec2:DetachInternetGateway

文档步骤

- aws:waitForAwsResourceProperty - 接受虚拟专用网关的 ID，然后等到虚拟专用网关的状态属性变为 available 或超时。
- aws:executeAwsApi - 检索指定的虚拟专用网关配置。
- aws:branch-基于 VpcAttachments .state 参数值的分支。

- aws:waitForAwsResourceProperty-接受虚拟专用网关的 ID，并等待虚拟专用网关的 VpcAttachments .state 属性更改为attached或超时。
- aws:executeAwsApi - 接受虚拟专用网关 ID 和 Amazon VPC 的 ID 作为输入，并将虚拟专用网关与 Amazon VPC 分离。
- aws:waitForAwsResourceProperty-接受虚拟专用网关的 ID，并等待虚拟专用网关的 VpcAttachments .state 属性更改为detached或超时。

- aws:executeAwsApi - 接受虚拟专用网关的 ID 作为输入并将其删除。

- aws:waitForAwsResourceProperty - 接受虚拟专用网关的 ID 作为输入，并验证是否将其删除。

aws:executeAwsApi - 从 互联网网关 ID 收集 VPC ID。

- aws:executeAwsApi - 将互联网网关 ID 与 VPC 分离。

- aws:executeAwsApi - 删除互联网网关。

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

描述

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 运行手册将分离并删除给定的 Amazon Elastic Compute Cloud (Amazon EC2) 虚拟专用网关，该网关附加到通过 Amazon Virtual Private Cloud (Amazon VPC) 创建的虚拟私有云（VPC）。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- VpnGateway我是

  类型：字符串

  描述：（必需）要删除的虚拟专用网关的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteVpnGateway
- ec2:DetachVpnGateway
- ec2:DescribeVpnGateways

文档步骤

- aws:waitForAwsResourceProperty - 接受虚拟专用网关的 ID，然后等到虚拟专用网关的状态属性变为 available 或超时。
- aws:executeAwsApi - 检索指定的虚拟专用网关配置。
- aws:branch-基于 VpcAttachments .state 参数值的分支。

- aws:waitForAwsResourceProperty-接受虚拟专用网关的 ID，并等待虚拟专用网关的 VpcAttachments .state 属性更改为attached或超时。
- aws:executeAwsApi - 接受虚拟专用网关 ID 和 Amazon VPC 的 ID 作为输入，并将虚拟专用网关与 Amazon VPC 分离。
- aws:waitForAwsResourceProperty-接受虚拟专用网关的 ID，并等待虚拟专用网关的 VpcAttachments .state 属性更改为detached或超时。

- aws:executeAwsApi - 接受虚拟专用网关的 ID 作为输入并将其删除。

- aws:waitForAwsResourceProperty - 接受虚拟专用网关的 ID 作为输入，并验证是否将其删除。

AWS-DisableIncomingSSHOnPort22

描述

该AWS-DisableIncomingSSHOnPort22运行手册删除了允许安全组在 TCP 端口 22 上不受限制地传入 SSH 流量的规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- SecurityGroup身份证

  类型：字符串

  描述：（必填）要限制 SSH 流量的安全组的 ID 列表，以逗号分隔。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

文档步骤

- `aws:executeAwsApi`-从您在`SecurityGroupIds`参数中指定的安全组中移除允许通过 TCP 端口 22 传入 SSH 流量的所有规则。

输出

DisableIncomingSSHTemplate。 RestrictedSecurityGroupIds -已移除入站 SSH 规则的安全组的 ID 列表。

AWS-DisablePublicAccessForSecurityGroup

描述

本运行手册禁用对所有 IP 地址开放的默认 SSH 和 RDP 端口。

> **Important**
>
> 此运行手册失败，并显示 “InvalidPermission。 NotFound“符合以下两个条件的安全组会出错：1) 安全组位于非默认 VPC 中；2) 安全组的入站规则未使用以下所有四个模式指定开放端口：
>
> - `0.0.0.0/0`
> - `::/0`
> - `SSH or RDP port + 0.0.0.0/0`
> - `SSH or RDP port + ::/0`

> **Note**
>
> 本运行手册在中国 AWS 区域 境内尚不可用。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- GroupId

  类型：字符串

  描述：（必需）端口应被禁用的安全组的 ID。

- IpAddressToBlock

  类型：字符串

  描述：（可选）访问应被阻止的其他 IPv4 地址，格式为 `1.2.3.4/32`。

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

描述

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 运行手册将禁用您指定的子网的公有 IPv4 寻址属性。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- SubnetId

  类型：字符串

  描述：（必需）要对其禁用自动分配公有 IPv4 地址属性的子网的 ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

文档步骤

- `aws:executeAwsApi` - 禁用您在 `SubnetId` 参数中指定的子网的自动分配公有 IPv4 地址属性。
- `aws:assertAwsResourceProperty` - 验证该属性是否已被禁用。

AWSSupport-EnableVPCFlowLogs

描述

`AWSSupport-EnableVPCFlowLogs` 运行手册为 AWS 账户中的子网、网络接口和 VPC 创建 Amazon Virtual Private Cloud (Amazon VPC)流日志。如果您为子网或 VPC 创建流日志，则会监控该子网或 Amazon VPC 中的每个网络接口。流日志数据将发布到亚马逊 CloudWatch 日志组或您指定的亚马逊简单存储服务 (Amazon S3) 存储桶。有关流日志的更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 流日志。

> **Important**
>
> 当您将流日志发布到 Logs 或 Amazon S3 时，会收取已售日志的数据摄取 CloudWatch 和存档费用。有关更多信息，请参阅流日志定价

运行此自动化（控制台）

> **Note**
>
> 选择s3作为日志目标时，请确保存储桶策略允许日志传输服务访问存储桶。有关更多信息，请参阅流日志的 Amazon S3 存储桶权限

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- DeliverLogsPermissionArn

  类型：字符串

  描述：（可选）允许亚马逊弹性计算云 (Amazon EC2) 将流日志发布到您账户中的日志组的 IAM 角色的 ARN。 CloudWatch 如果您为 LogDestinationType 参数指定了 s3，则不要为该参数提供值。有关更多信息，请参阅 Amazon VPC 用户指南中的向 CloudWatch 日志发布流日志。
- LogDestinationARN

  类型：字符串

  描述：（可选）要向其发布流日志数据的资源的 ARN。如果cloud-watch-logs为LogDestinationType参数指定，请提供要向其发布流 CloudWatch 日志数据的日志组的

ARN。或者，改用 LogGroupName。如果为 LogDestinationType 参数指定了 s3，则必须为此参数指定您要向其发布流日志数据的 Amazon S3 存储桶的 ARN。您还可以指定存储桶中的文件夹。

> **Important**
>
> 选择s3作为时，LogDestinationType您应确保所选存储段遵循 Amazon S3 存储桶安全最佳实践，并遵守您所在组织和地理区域的数据隐私法。

- LogDestinationType

  类型：字符串

  有效值： cloud-watch-logs | s3

  描述：（必需）确定流日志数据的发布位置。如果将 LogDestinationType 指定为 s3，则不要指定 DeliverLogsPermissionArn 或 LogGroupName。

- LogFormat

  类型：字符串

  描述：（可选）要包含在流日志中的字段，以及它们在记录中出现的顺序。有关可用字段的列表，请参阅《Amazon VPC 用户指南》中的流日志记录。如果不为该参数指定值，则使用默认的格式创建流日志。如果指定此参数，则必须至少指定一个字段。

- LogGroupName

  类型：字符串

  描述：（可选）发布流 CloudWatch 日志数据的日志日志组的名称。如果您为 LogDestinationType 参数指定了 s3，则不要为该参数提供值。

- ResourceIds

  类型: StringList

  描述：（必需）要为其创建流日志的子网、弹性网络接口或 VPC 的 ID 列表（以逗号分隔）。

- TrafficType

  类型：字符串

  有效值：ACCEPT | REJECT | ALL

描述：（必需）要记录的流量的类型。您可以记录资源接受或拒绝的流量，或者记录所有流量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs
- iam:AttachRolePolicy
- iam:CreateRole
- iam:CreatePolicy
- iam:DeletePolicy
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:TagRole
- iam:PassRole
- iam:PutRolePolicy
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- s3:GetBucketLocation
- s3:GetBucketAcl

- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

政策示例

```
       {
           "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}/*"
                ]
            }
        ]
    }
```

文档步骤

- aws:branch - 根据为 LogDestinationType 参数指定的值进行分支。
- aws:executeScript-检查目标亚马逊简单存储服务 (Amazon S3) Simple Storage Service 是否有可能授予对其对象的读取或public写入权限。
- aws:executeScript - 在没有为 LogDestinationARN 参数指定任何值但为 LogDestinationType 参数指定了 cloud-watch-logs 时创建一个日志组值。
- aws:executeScript - 根据运行手册参数中指定的值创建流日志。

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

描述

该AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch运行手册将向亚马逊简单存储服务 (Amazon S3) Simple Storage Service 发布流日志数据的现有 Amazon VPC 流日志替换为将流日志数据发布到您指定的 CloudWatch 亚马逊日志CloudWatch （ 日志 ）日志组的流日志。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- DestinationLog群组

  类型：字符串

  描述：（必填）要向其发布流 CloudWatch 日志数据的日志组的名称。

- DeliverLogsPermissionArn

  类型：字符串

  描述：（必填）您要使用的 AWS Identity and Access Management (IAM) 角色的 ARN，该角色为亚马逊弹性计算云 (Amazon EC2) 提供向日志发布流日志数据的必要权限。 CloudWatch

- FlowLog我是

  类型：字符串

  描述：（必需）要替换的发布到 Amazon S3 的流日志的 ID。

- MaxAggregation间隔

  类型：整数

  有效值：60 | 600

  描述：（可选）捕获数据包流并聚合到流日志记录中的最长时间间隔（以秒为单位）。

- TrafficType

  类型：字符串

  有效值：ACCEPT | REJECT | ALL

  描述：（必需）要记录和发布的流日志数据的类型。

所需的 IAM 权限

~~AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。~~

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs

文档步骤

- aws:executeAwsApi - 从您在 FlowLogId 参数中指定的值收集有关 VPC 的详细信息。
- aws:executeAwsApi - 根据您为运行手册参数指定的值创建一个流日志。
- aws:assertAwsResourceProperty-验证新创建的流日志已发布到 CloudWatch 日志。
- aws:executeAwsApi - 删除发布到 Amazon S3 的流日志。
- aws:executeScript - 确认发布到 Amazon S3 的流日志已删除。

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

描述

该AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket运行手册将向亚马逊 CloudWatch 日志（日志）发布流日志数据的现有 Amazon VPC 流CloudWatch 日志替换为将流日志数据发布到您指定的亚马逊简单存储服务 (Amazon S3) 存储桶的流日志。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- 目的地 3 BucketArn

  类型：字符串

  描述：（必需）要将流日志数据发布到的 Amazon S3 存储桶的 ARN。

- FlowLog我是

  类型：字符串

  描述：（必填）发布到要替换的 CloudWatch 日志的流日志的 ID。

- MaxAggregation间隔

  类型：整数

  有效值：60 | 600

  描述：（可选）捕获数据包流并聚合到流日志记录中的最长时间间隔（以秒为单位）。

- TrafficType

  类型：字符串

  有效值：ACCEPT | REJECT | ALL

  描述：（必需）要记录和发布的流日志数据的类型。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2:DeleteFlowLogs

- ec2:DescribeFlowLogs

文档步骤

- aws:executeAwsApi - 从您在 FlowLogId 参数中指定的值收集有关 VPC 的详细信息。
- aws:executeAwsApi - 根据您为运行手册参数指定的值创建一个流日志。
- aws:assertAwsResourceProperty - 验证新创建的流日志是否发布到 Amazon S3。
- aws:executeAwsApi-删除发布到日志的流 CloudWatch 日志。
- aws:executeScript-确认已删除发布到 CloudWatch 日志的流日志。

AWS-ReleaseElasticIP

描述

使用分配 ID 释放指定的弹性 IP 地址。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- AllocationId

类型：字符串

描述：（必需）弹性 IP 地址的分配 ID。

AWS-RemoveNetworkACLUnrestrictedSSHRDP

描述

AWS-RemoveNetworkACLUnrestrictedSSHRDP运行手册从指定的网络 ACL 中删除了所有网络访问控制列表 (ACL) 规则，这些规则允许从所有源地址到默认 SSH 和 RDP 端口的入口流量。包含与默认 SSH 和 RDP 端口重叠的端口范围的规则不会被删除。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- NetworkAcl我是

  类型：字符串

  描述：（必填）要删除的网络 ACL 的 ID，这些规则允许从所有源地址到默认 SSH 和 RDP 端口的入口流量。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAclEntry
- ec2:DescribeNetworkAcls

文档步骤

- aws:executeScript - 从您在 SecurityGroupId 参数中指定的安全组中移除所有允许流量来自任何源地址的入口规则。

输出

RemoveNaclEntriesAnd验证。 VerificationMessage -成功删除网络 ACL 规则的验证消息。

RemoveNaclEntriesAnd验证。 RulesDeletedAndApiResponses -已删除的网络 ACL 规则以及 DeleteNetworkAclEntry API 操作响应。

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

描述

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 运行手册将从您指定的安全组中移除所有允许流量来自任何源地址的入口规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。

- SecurityGroup我是

  类型：字符串

  描述：（必需）要从中移除入口规则的安全组的 ID，该入口规则允许流量来自任何源地址。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

文档步骤

- `aws:executeScript` - 从您在 `SecurityGroupId` 参数中指定的安全组中移除所有允许流量来自任何源地址的入口规则。

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

描述

`AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` 运行手册将从您指定的虚拟私有云（VPC）的默认安全组中移除所有规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- GroupId

  类型：字符串

  描述：（必需）要从其中移除所有规则的安全组的 ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

文档步骤

- `aws:assertAwsResourceProperty` - 确认您在 `GroupId` 参数中指定的安全组命名为 default。
- `aws:executeScript` - 从您在 `GroupId` 参数中指定的安全组中移除所有规则。

AWSSupport-SetupIPMonitoringFromVPC

描述

AWSSupport-SetupIPMonitoringFromVPC 在指定子网中创建一个 Amazon Elastic Compute Cloud (Amazon EC2) 实例，然后通过持续运行 ping、MTR、traceroute 和 tracetcp 测试来监控选定的目标 IP（IPv4 或 IPv6）。结果存储在 Amazon CloudWatch Logs 日志中，并应用指标筛选器在 CloudWatch 控制面板中快速可视化延迟和丢包统计数据。

附加信息

CloudWatch 日志数据可用于网络故障排除和模式/趋势分析。此外，当数据包丢失和/或延迟达到阈值时，您可以使用 Amazon SNS 通知配置 CloudWatch 警报。这些数据也可以在开案时使用 AWS Support，以帮助快速隔离问题，并在调查网络问题时缩短解决时间。

> **Note**
>
> 要清理由 AWSSupport-SetupIPMonitoringFromVPC 创建的资源，您可以使用运行手册 AWSSupport-TerminateIPMonitoringFromVPC。有关更多信息，请参阅 AWSSupport-TerminateIPMonitoringFromVPC。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。

- CloudWatchLogGroupNamePrefix

  类型：字符串

  默认：/ AWSSupport-SetupIPMonitoringFromVPC

  描述：（可选）用于为测试结果创建的每个 CloudWatch 日志组的前缀。

- CloudWatchLogGroupRetentionIn天数

  类型：字符串

  有效值：1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  默认：7

  描述：（可选）要保留网络监控结果的天数。

- InstanceType

  类型：字符串

  有效值：t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

  默认：t2.micro

  描述：（可选）EC2Rescue 实例的 EC2 实例类型。建议大小：t2.micro。

- SubnetId

  类型：字符串

  描述：（必需）监控实例的子网 ID。请注意，如果您指定私有子网，则必须确保可以访问 Internet 才能允许监控实例设置测试（也就是说，安装 CloudWatch 日志代理，与 Systems Manager 交互和 CloudWatch）。

- TargetIPs

  类型：字符串

描述：（必需）要监控的以逗号分隔的 IPv4 和/或 IPv6 列表。不允许使用空格。最大大小为 255 个字符。注意，如果提供的 IP 无效，则 Automation 将失败并回滚测试设置。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

建议运行自动化的用户附加 AmazonSS AutomationRole M IAM 托管策略。此外，用户还必须将以下策略附加到其用户账户、组或角色：

```
            {
    "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"
        }
    ]
}
```

文档步骤

1. **aws:executeAwsApi** - 描述提供的子网。
2. **aws:branch** - 评估 TargetIPs 输入。

   (IPv6) 如果 TargetIPs 包含 IPv6：

   aws:assertAwsResourceProperty - 检查提供的子网是否关联了 IPv6 池
3. **aws:executeScript** - 获取最新 Amazon Linux 2 AMI 的实例类型和公共参数路径的架构。
4. **aws:executeAwsApi** - 从 Parameter Store 获取最新的亚马逊 Amazon Linux 2 AMI。
5. **aws:executeAwsApi** - 在子网的 VPC 中为测试创建一个安全组。

   （清理）如果安全组创建失败：

   aws:executeAwsApi - 删除自动化创建的安全组（如果存在）。
6. **aws:executeAwsApi** - 允许测试安全组中的所有出站流量。

   （清理）如果安全组出口规则创建失败：

   aws:executeAwsApi - 删除自动化创建的安全组（如果存在）。
7. **aws:executeAwsApi** - 为测试 EC2 实例创建一个 IAM 角色

   （清理）如果角色创建失败：

   a. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色（如果存在）。

   b. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。
8. **aws:executeAwsApi**-附上 AmazonSSM 托管政策 ManagedInstanceCore

   （清理）如果附加策略失败：

a. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色（如果已连接）分离。

b. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

c. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

9. **aws:executeAwsApi**-附加内联策略以允许设置 CloudWatch 日志组保留和创建仪表板 CloudWatch

（清理）如果附加内联策略失败：

a. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略（如果已创建）。

b. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

d. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

10. **aws:executeAwsApi** - 创建 IAM 实例配置文件。

（清理）如果实例配置文件创建失败：

a. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件（如果存在）。

b. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

c. **aws:executeAwsApi**-从自动化创建的角色中删除 AmazonSSM ManagedInstanceCore 托管策略。

d. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

e. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

11. **aws:executeAwsApi** - 将 IAM 实例配置文件关联至 IAM 角色。

（清理）如果实例配置文件和角色关联失败：

a. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件（如果已关联）。

b. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

c. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

d. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

e. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

f. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

12. **aws:sleep** - 等待实例配置文件变为可用。

13. **aws:runInstances** - 在指定的子网中创建测试实例，并附加先前创建的实例配置文件。

    （清理）如果步骤失败：

    a. **aws:changeInstanceState** - 终止测试实例。

    b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

    c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

    d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

    e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

    f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

    g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

14. **aws:branch** - 评估 TargetIPs 输入。

    (IPv6) 如果 TargetIPs 包含 IPv6：

    aws:executeAwsApi - 为测试实例分配 IPv6。

15. **aws:waitForAwsResourceProperty** - 等待测试实例变为托管实例。

    （清理）如果步骤失败：

    a. **aws:changeInstanceState** - 终止测试实例。

    b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

    c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

    d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

    e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

    f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

    g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

16. **aws:runCommand** - 安装测试先决条件：

    （清理）如果步骤失败：

    a. **aws:changeInstanceState** - 终止测试实例。

    b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

    c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

    d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

17 **aws:runCommand** - 验证提供的 IP 是不是语法正确的 IPv4 和/或 IPv6 地址：

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

18 **aws:runCommand** - 为提供的每个 IP 定义 MTR 测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

19 **aws:runCommand** - 为提供的每个 IP 定义第一个 ping 测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

20 **aws:runCommand** - 为提供的每个 IP 定义第二个 ping 测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

21 **aws:runCommand** - 为提供的每个 IP 定义 tracepath 测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

22 **aws:runCommand** - 为提供的每个 IP 定义 traceroute 测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

23**aws:runCommand**-配置 CloudWatch 日志。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

24**aws:runCommand** - 安排 cronjobs 每分钟运行一次测试。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

25**aws:sleep** - 等待测试生成一些数据。

26**aws:runCommand**-设置所需的 CloudWatch 日志组保留时间。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

27 **aws:runCommand**-设置 CloudWatch 日志组指标筛选器。

（清理）如果步骤失败：

a. **aws:changeInstanceState** - 终止测试实例。

b. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

c. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

d. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

e. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

f. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

g. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

28 **aws:runCommand**-创建 CloudWatch 仪表板。

（清理）如果步骤失败：

a. **aws:executeAwsApi**-删除 CloudWatch 仪表板（如果存在）。

b. **aws:changeInstanceState** - 终止测试实例。

c. **aws:executeAwsApi** - 从角色中删除 IAM 实例配置文件。

d. **aws:executeAwsApi** - 删除自动化创建的 IAM 实例配置文件。

e. **aws:executeAwsApi**-从自动化创建的角色中删除 CloudWatch 内联策略。

f. **aws:executeAwsApi**-将 AmazonSSM ManagedInstanceCore 托管策略与自动化创建的角色分离。

g. **aws:executeAwsApi** - 删除自动化创建的 IAM 角色。

h. **aws:executeAwsApi** - 删除自动化创建的安全组（如果存在）。

输出

创建CloudWatch仪表板。输出-仪表板的 URL。 CloudWatch

创建ManagedInstance。 InstanceIds -测试实例 ID。

AWSSupport-TerminateIPMonitoringFromVPC

描述

AWSSupport-TerminateIPMonitoringFromVPC 终止先前由 AWSSupport-SetupIPMonitoringFromVPC 启动的 IP 监控测试。将删除与指定测试 ID 相关的数据。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- AutomationExecution我是

  类型：字符串

  描述：（必需）您之前运行 AWSSupport-SetupIPMonitoringFromVPC 运行手册时的自动化执行 ID。与该执行 ID 关联的所有资源都被删除。

- InstanceId

  类型：字符串

  描述：（必需）监控实例的实例 ID。

- SubnetId

  类型：字符串

  描述：（必需）监控实例的子网 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

建议运行自动化的用户附加 AmazonSS AutomationRole M IAM 托管策略。此外，用户还必须将以下策略附加到其用户、组或角色：

```
{
"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"
    ]
}
```

文档步骤

1. aws:assertAwsResourceProperty-检查 AutomationExecutionId 并 InstanceId 与同一个测试相关。
2. aws:assertAwsResourceProperty-检查 SubnetId 并 InstanceId与同一个测试相关。
3. aws:executeAwsApi - 检索测试安全组。
4. aws:executeAwsApi-删除 CloudWatch 仪表板。
5. aws:changeInstanceState - 终止测试实例。
6. aws:executeAwsApi - 从角色中删除 IAM 实例配置文件。
7. aws:executeAwsApi - 删除自动化创建的 IAM 实例配置文件。
8. aws:executeAwsApi-从自动化创建的角色中删除 CloudWatch 内联策略。

9. aws:executeAwsApi-将 AmazonSSM ManagedInstance Core 托管策略与自动化创建的角色分离。
10. aws:executeAwsApi - 删除自动化创建的 IAM 角色。
11. aws:executeAwsApi - 删除自动化创建的安全组（如果存在）。

输出

无

AWS WAF

AWS Systems Manager 自动化为用户提供了预定义的运行手册。 AWS WAF有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

描述

该AWS-AddWAFRegionalRuleToRuleGroup操作手册将现有的 AWS WAF 区域规则添加到 AWS WAF 区域规则组中。仅支持 AWS WAF 经典区域规则组。 AWS WAF 经典区域规则组最多可以有 10 条规则。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- RuleGroup我是

  类型：字符串

  描述：（必填）要更新的规则组的 ID。
- RulePriority

  类型：整数

  描述：（必填）新规则的优先级。规则优先级决定了评估区域组中规则的顺序。值较低的规则比值较高的规则具有更高的优先级。值必须是整数。如果您向一个区域规则组添加多条规则，则这些值不必是连续的。
- RuleId

  类型：字符串

  描述：（必填）您要添加到区域规则组的规则的 ID。
- RuleAction

  类型：字符串

  描述：（必填）指定 Web 请求符合规则条件时 AWS WAF 采取的操作。

  有效值：允许 | 阻止 | 计数

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetChangeTokenStatus
- waf-regional:ListActivatedRulesInRuleGroup
- waf-regional:UpdateRuleGroup

文档步骤

- getWaf ChangeToken (aws: executeAwsApi)-检索 AWS WAF 更改令牌以确保运行手册不会向服务提交冲突的请求。
- addWAF RuleTo WAF RegionalRuleGroup (aws: ExecuteScript)-将指定的规则添加到区域规则组。AWS WAF
- VerifyChangeTokenPropagating (aws: wait ForAwsResourceProperty)-验证更改令牌的状态为或。PENDING INSYNC
- VerifyRuleAddedToRuleGroup (aws: executeScript)-验证指定的 AWS WAF 规则是否已添加到目标区域规则组。

输出

- VerifyRuleAddedToRuleGroup。 VerifyRuleAddedToRuleGroupResponse -验证新规则是否已添加到区域规则组的步骤的输出。
- VerifyRuleAddedToRuleGroup。 ListActivatedRulesInRuleGroupResponse -ListActivatedRulesInRuleGroup API 操作的输出。

AWS-AddWAFRegionalRuleToWebAcl

描述

该AWS-AddWAFRegionalRuleToWebAcl运行手册将现有的 AWS WAF 区域规则、规则组或基于速率的规则添加到 AWS WAF 经典区域 Web 访问控制列表 (ACL) 中。本运行手册不会更新由 AWS Firewall Manager管理的现有 AWS WAF 经典区域 Web ACL。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- WebACLId

  类型：字符串

  描述：（必填）要更新的网络 ACL 的 ID。
- ActivatedRule优先级

  类型：整数

  描述：（必填）新规则的优先级。规则优先级决定评估 Web ACL 中规则的顺序。值较低的规则比值较高的规则具有更高的优先级。值必须是整数。如果您向区域 Web ACL 添加多条规则，则这些值不必是连续的。
- ActivatedRuleRuleId

  类型：字符串

  描述：（必填）要添加到 Web ACL 的常规规则、基于速率的规则或组的 ID。
- ActivatedRule行动

  类型：字符串

  有效值：允许 | 阻止 | 计数

描述：（可选）指定 Web 请求符合规则条件时 AWS WAF 采取的操作。

- ActivatedRule类型

  类型：字符串

  有效值：常规 | 基于费率 | 群组

  默认：常规

  描述：（可选）您要添加到 Web ACL 的规则类型。尽管此字段是可选字段，但请注意，如果您尝试在 Web ACL 中添加RATE_BASED规则而不设置类型，则请求会失败，因为请求默认为REGULAR规则。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

文档步骤

- DetermineWebACL NotIn FMS AndRulePriority (AWS: ExecuteScript)-验证 AWS WAF Web ACL 是否在 Firewall Manager 安全策略中，并验证优先级 ID 是否与现有 ACL 冲突。
- AddRuleOrRuleGroupToWebACL (aws: ExecuteScript)-将指定的规则添加到 Web ACL。 AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws: executeScript)-验证指定的 AWS WAF 规则是否已添加到目标 Web ACL 中。

输出

- DetermineWebACL NotIn FMS AndRule 优先级。
  PrereqResponse：DetermineWebACLNotInFMSAndRulePriority步骤的输出。

- VerifyRuleOrRuleGroupAddedToWebAcl。 VerifyRuleOrRuleGroupAddedToWebaclResponse：步骤的输出。AddRuleOrRuleGroupToWebACL
- VerifyRuleOrRuleGroupAddedToWebAcl。 ListActivatedRulesOrRuleGroupsInWebaclResponse：步骤的VerifyRuleOrRuleGroupAddedToWebAcl输出。

AWSConfigRemediation-EnableWAFClassicLogging

描述

该AWSConfigRemediation-EnableWAFClassicLogging运行手册允许您登录到亚马逊数据 Firehose (Firehose)，以 AWS WAF 获取您指定的网络访问控制列表 (Web ACL)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- DeliveryStream姓名

  类型：字符串

  描述：（必填）您要向其发送日志的 Firehose 传输流的名称。
- WebACLId

  类型：字符串

描述：（必填）要启用登录功能的 AWS WAF Web ACL 的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf:GetLoggingConfiguration
- waf:GetWebAcl
- waf:PutLoggingConfiguration

文档步骤

- aws:executeAwsApi - 确认您在 DeliveryStreamName 中指定的传送流存在。
- aws:executeAwsApi-收集参数中指定的 Web ACL 的 ARN。 AWS WAF WebACLId
- aws:executeAwsApi - 为 Web ACL 启用日志记录。
- aws:assertAwsResourceProperty-验证是否已在 AWS WAF Web ACL 上启用日志记录。

AWSConfigRemediation-EnableWAFClassicRegionalLogging

描述

该AWSConfigRemediation-EnableWAFClassicRegionalLogging运行手册允许您登录到亚马逊数据 Firehose (Firehose)，以获取您 AWS WAF 指定的网络访问控制列表 (ACL)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- LogDestination配置

  类型：字符串

  描述：（必填）您要向其发送日志的 Firehose 传输流的亚马逊资源名称 (ARN)。
- WebACLId

  类型：字符串

  描述：（必填）要启用登录功能的 AWS WAF Web ACL 的 ID。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

文档步骤

- `aws:executeAwsApi`-收集参数中指定的 Web ACL 的 ARN。 AWS WAF `WebACLId`
- `aws:executeAwsApi` - 为 Web ACL 启用日志记录。

- aws:assertAwsResourceProperty-验证是否已在 AWS WAF Web ACL 上启用日志记录。

AWSConfigRemediation-EnableWAFV2Logging

描述

该AWSConfigRemediation-EnableWAFV2Logging运行手册允许使用指定的 Amazon Dat AWS WAF a Firehose (Firehose) 传输流记录 (AWS WAF V2) 网络访问控制列表 (Web ACL)。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- LogDestination配置

  类型：字符串

  描述：（必填）您要与网页 ACL 关联的 Firehose 传送流 ARN。

> **Note**
>
> Firehose 传送流 ARN 必须以前缀开头。aws-waf-logs-例如，aws-waf-logs-us-east-2-analytics。有关更多信息，请参阅 Amazon Data Firehose。

- WebAclArn

  类型：字符串

  描述：（必需）要为其启用日志记录的 Web ACL 的 ARN。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

文档步骤

- `aws:executeScript`-启用 AWS WAF V2 Web ACL 的日志记录并验证日志记录是否具有指定的配置。

Amazon WorkSpaces

AWS Systems Manager 自动化为 Amazon WorkSpaces 提供了预定义的运行手册。有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

AWS-CreateWorkSpace

描述

AWS-CreateWorkSpace运行手册会根据您为输入参数指定的值创建一个新的 Amazon WorkSpaces 虚拟桌面，称为 a WorkSpace。有关信息 WorkSpaces，请参阅 Amazon WorkSpaces 是什么？ 在《亚马逊 WorkSpaces 管理指南》中。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- BundleId

  类型：字符串

  描述：（必填）要用于的捆绑包的 ID WorkSpace。
- ComputeType姓名

  类型：字符串

  有效值：VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  描述：（可选）您的计算类型 WorkSpace。
- DirectoryId

类型：字符串

描述：（必填）要添加您的 WorkSpace目录的 ID。

- RootVolumeEncryptionEnabled

  类型：布尔值

  有效值：true | false

  默认：false

  描述：（可选）确定是否对的根卷进行加密。 WorkSpace

- RootVolumeSizeGib

  类型：整数

  描述：（必填）的根卷的大小 WorkSpace。

- RunningMode

  类型：字符串

  有效值：ALWAYS_ON | AUTO_STOP

  描述：（必填）的运行模式 WorkSpace。

- RunningModeAutoStopTimeoutIn分钟

  类型：整数

  描述：（可选）用户注销后 WorkSpaces停止的时间。以 60 分钟为间隔指定一个值。

- 标签

  类型：字符串

  描述：（可选）要应用于的标签 WorkSpace。

- UserName

  类型：字符串

  描述：（必填）要与关联的用户名 WorkSpace。

- UserVolumeEncryptionEnabled

类型：布尔值

有效值：true | false

默认：false

描述：（可选）确定是否对的用户卷进行加密。 WorkSpace

- UserVolumeSizeGib

  类型：整数

  描述：（必填）的用户音量大小 WorkSpace。

- VolumeEncryption钥匙

  类型：字符串

  描述：（可选）您要用来加密存储在上的数据的对称密 AWS Key Management Service 钥。 WorkSpace

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

文档步骤

- `aws:executeScript`- WorkSpace 根据您为输入参数指定的值创建。
- `aws:waitForAwsResourceProperty`-验证 is 的 WorkSpace 状态`AVAILABLE`。

输出

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

描述

AWSSupport-RecoverWorkSpace运行手册在您指定的 Amazon WorkSpaces 虚拟桌面（称为 a WorkSpace）上执行恢复步骤。运行手册会重新启动 WorkSpace，如果状态静止UNHEALTHY，则 WorkSpace 根据您为输入参数指定的值恢复或重建。在使用本运行手册之前，我们建议您查看《Amazon WorkSpaces 管理指南》中的 “疑难解答 WorkSpaces ”。

> **Important**
>
> 恢复或重建 WorkSpace 是一种潜在的破坏性操作，可能会导致数据丢失。这是因为是从上次可用的快照中恢复的，而从快照中恢复的数据可能长达 12 小时。 WorkSpace 恢复选项会根据最新的快照重新创建根卷和用户卷。rebuild 选项根据最新的快照重新创建用户卷，并 WorkSpace 从与创建该分发包关联的映像中重新创建用户卷。 WorkSpace 已安装的应用程序或在创建后更改的 WorkSpace 系统设置都将丢失。有关恢复和重建的更多信息 WorkSpaces，请参阅《Amazon WorkSpaces 管理指南》 WorkSpace中的 “还原 a” WorkSpace 和 “重建 a”。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssumeRole

  类型：字符串

  描述：（可选）允许 Systems Manager Automation 代表您执行操作 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。如果未指定角色，Systems Manager Automation 将使用启动此运行手册的用户的权限。
- 确认

类型：字符串

有效值：是

描述：（必填）输入 “是” 表示您知道还原和重建操作将尝试 WorkSpace 从最新的快照中恢复，并且从这些快照恢复的数据可能最长为 12 小时。

- Reboot

  类型：字符串

  有效值：是 | 否

  默认：是

  描述：（必填）确定 WorkSpace 是否重新启动。

- 重建

  类型：字符串

  有效值：是 | 否

  默认：否

  描述：（必填）确定 WorkSpace 是否重建。

- 还原

  类型：字符串

  有效值：是 | 否

  默认：否

  描述：（必填）确定 WorkSpace 是否恢复。

- WorkspaceId

  类型：字符串

  描述：（必填） WorkSpace 要恢复的 ID。

所需的 IAM 权限

AutomationAssumeRole 参数需要执行以下操作才能成功使用运行手册。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- workspaces:DescribeWorkspaces
- workspaces:DescribeWorkspaceSnapshots
- workspaces:RebootWorkspaces
- workspaces:RebuildWorkspaces
- workspaces:RestoreWorkspace
- workspaces:StartWorkspaces

文档步骤

- aws:executeAwsApi-收集 WorkSpace 您在WorkspaceId参数中指定的状态。
- aws:assertAwsResourceProperty-验证 WorkSpace 是AVAILABLE、、ERRORIMPAIREDSTOPPED、或UNHEALTHY的状态。
- aws:branch-基于状态的分支 WorkSpace。
- aws:executeAwsApi-启动 WorkSpace。
- aws:branch - 根据您为 Action 参数指定的值进行分支。
- aws:waitForAwsResourceProperty-启动后等待 WorkSpace 状态。
- aws:waitForAwsResourceProperty-等待 WorkSpace 状态更改为AVAILABLE、ERRORIMPAIRED、或启动UNHEALTHY后。
- aws:executeAwsApi-收集启动 WorkSpace 后的状态。
- aws:branch-基于启动 WorkSpace 后的状态的分支。
- aws:executeAwsApi-收集用于恢复或重建的可用快照。 WorkSpace
- aws:branch - 根据您为 Reboot 参数指定的值进行分支。
- aws:executeAwsApi-重新启动。 WorkSpace
- aws:executeAwsApi-收集启动 WorkSpace 后的状态。
- aws:waitForAwsResourceProperty-等待状态变 WorkSpace 为。REBOOTING
- aws:waitForAwsResourceProperty-等待 WorkSpace 状态更改为AVAILABLEERROR、或重新启动UNHEALTHY后。
- aws:executeAwsApi-收集重启 WorkSpace 后的状态。

- aws:branch-根据重启 WorkSpace 后的状态进行分支。
- aws:branch - 根据您为 Restore 参数指定的值进行分支。
- aws:executeAwsApi-恢复。 WorkSpace如果恢复失败，运行手册将尝试重建。 WorkSpace
- aws:waitForAwsResourceProperty-等待状态变 WorkSpace 为。RESTORING
- aws:waitForAwsResourceProperty-等待 WorkSpace 状态更改为AVAILABLEERROR、或恢复UNHEALTHY后。
- aws:executeAwsApi-收集恢复 WorkSpace 后的状态。
- aws:branch-基于恢复 WorkSpace 后的状态的分支。
- aws:branch - 根据您为 Rebuild 参数指定的值进行分支。
- aws:executeAwsApi-重建。 WorkSpace
- aws:waitForAwsResourceProperty-等待状态变 WorkSpace 为。REBUILDING
- aws:waitForAwsResourceProperty-等待 WorkSpace 状态更改为AVAILABLEERROR、或重建UNHEALTHY后。
- aws:executeAwsApi-收集重建 WorkSpace 后的状态。
- aws:assertAwsResourceProperty-确认 WorkSpace is 的状态AVAILABLE。

X-Ray

AWS Systems Manager 自动化为用户提供了预定义的运行手册。 AWS X-Ray有关运行手册的更多信息，请参阅使用运行手册。有关如何查看运行手册内容的信息，请参阅 查看运行手册内容。

主题

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

描述

AWSConfigRemediation-UpdateXRayKMSKey运行手册支持使用 AWS Key Management Service (AWS KMS) 密钥对您的 AWS X-Ray 数据进行加密。本运行手册应仅用作基准，以确保您的 AWS X-Ray 数据按照建议的最低安全最佳实践进行加密。我们建议使用不同的 KMS 密钥对多组数据进行加密。

运行此自动化（控制台）

文档类型

自动化

所有者

Amazon

平台

Linux、macOS、Windows

参数

- AutomationAssume角色

  类型：字符串

  描述：（必需）允许 Systems Manager Automation 代表您执行操作的 AWS Identity and Access Management (IAM) 角色的 Amazon 资源名称（ARN）。
- KeyId

  类型：字符串

  描述：（必填）您要 AWS X-Ray 用于加密数据的 Amazon 资源名称 (ARN)、密钥 ID 或 KMS 密钥的密钥别名。

所需的 IAM 权限

`AutomationAssumeRole` 参数需要执行以下操作才能成功使用运行手册。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

文档步骤

- `aws:executeAwsApi` - 使用您在 `KeyId` 参数中指定的 KMS 密钥对 X-Ray 数据启用加密。

- aws:waitForAwsResourceProperty - 等待 X-Ray 的加密配置状态变为 ACTIVE。
- aws:executeAwsApi - 收集您在 KeyId 参数中指定的密钥的 ARN。
- aws:assertAwsResourceProperty - 验证是否已对您的 X-Ray 启用加密。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。