aws

Benutzerhandbuch

# AWS Systems Manager Referenz zum Automatisierungs-Runbook

# AWS Systems Manager Referenz zum Automatisierungs-Runbook: Benutzerhandbuch

# Table of Contents

# Referenz zu Systems Manager Automation

AWS Systems Manager Stellt vordefinierte Runbooks bereit, damit Sie schnell loslegen können. Diese Runbooks werden von Amazon Web Services verwaltet, AWS Support, und AWS Config. In der Runbook-Referenz werden alle vordefinierten Runbooks beschrieben, die von Systems Manager AWS Support, und bereitgestellt werden. AWS Config

> **Important**
>
> Wenn Sie einen automatisierten Workflow ausführen, der andere Services mithilfe einer AWS Identity and Access Management -(IAM)-Servicerolle aufruft, muss die Servicerolle mit der Berechtigung zum Aufrufen dieser Services konfiguriert sein. Diese Anforderung gilt für alle AWS Automation-Runbooks (`AWS-*`-Runbooks), wie zum Beispiel `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup` und `AWS-RestartEC2Instance`-Runbooks, um nur einige zu nennen. Diese Anforderung gilt auch für alle benutzerdefinierten Automatisierungs-Runbooks, die Sie erstellen und die andere Dienste mithilfe von Aktionen aufrufen, die andere AWS Dienste aufrufen. Wenn Sie unter anderem `aws:executeAwsApi`-, `aws:createStack`- oder `aws:copyImage`-Aktionen verwenden, dann müssen Sie die Servicerolle mit der Berechtigung zum Aufrufen solcher Services konfigurieren. Sie können Berechtigungen für andere AWS Dienste aktivieren, indem Sie der Rolle eine IAM-Inline-Richtlinie hinzufügen. Weitere Informationen finden Sie unter Hinzufügen einer Automatisierungs-Inline-Richtlinie zum Aufrufen anderer AWS Dienste.

Diese Referenz enthält Themen, in denen die einzelnen Systems Manager Manager-Runbooks beschrieben werden, deren Eigentümer AWS AWS Support, und AWS Config sind. Runbooks sind nach den jeweiligen Benutzern geordnet. AWS-Service Jede Seite enthält eine Erläuterung der erforderlichen und optionalen Parameter, die Sie bei der Verwendung des Runbooks angeben können. Auf jeder Seite sind auch die Schritte im Runbook und gegebenenfalls die Ergebnisse der Automatisierung aufgeführt.

Diese Referenz enthält keine separate Seite für Runbooks, für die eine Genehmigung erforderlich ist, wie z. B. das Runbook `AWS-CreateManagedLinuxInstanceWithApproval` oder`AWS-StopEC2InstanceWithApproval`. Jeder Runbook-Name, der die Aktion enthält`WithApproval`, bedeutet, dass das Runbook die Aktion enthält. `aws:approve` Durch diese Aktion wird eine Automatisierung vorübergehend angehalten, bis bestimmte Hauptbenutzer die Aktion entweder

genehmigen oder ablehnen. Nach Erreichen der erforderlichen Anzahl an Genehmigungen wird die Automatisierung fortgesetzt.

Informationen zum Ausführen von Automatisierungen finden Sie unter Einfache Automatisierung ausführen. Informationen zum Ausführen von Automatisierungen auf mehreren Zielen finden Sie unter Ausführen von Automatisierungen, die Ziele und Ratensteuerungen verwenden.

Themen

- Amazon EMR
- OpenSearch Amazon-Dienst
- EventBridge
- GuardDuty
- IAM
- Amazon-Kinesis-Data-Streams
- AWS KMS
- Lambda
- Amazon Managed Workflows für Apache Airflow
- Neptune
- Amazon RDS
- Amazon-Redshift
- Amazon S3
- SageMaker
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- Drittanbieter
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

# Runbook-Inhalte anzeigen

Sie können den Inhalt für Runbooks in der Systems Manager Manager-Konsole anzeigen.

Um Runbook-Inhalte anzuzeigen

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.

   –oder–

   Wenn die AWS Systems Manager Startseite zuerst geöffnet wird, klicken Sie auf das Menüsymbol (☰), um den Navigationsbereich zu öffnen, und wählen Sie dann im Navigationsbereich Dokumente aus.
3. Wählen Sie im Abschnitt Kategorien die Option Automatisierungsdokumente aus.
4. Wählen Sie ein Runbook aus und anschließend die Option View details.
5. Wählen Sie die Registerkarte Content aus.

# API Gateway

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon API Gateway bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

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

## `AWSConfigRemediation-DeleteAPIGatewayStage`

Beschreibung

Das `AWSConfigRemediation-DeleteAPIGatewayStage` Runbook löscht einen Amazon API Gateway (API Gateway) -Schritt. AWS Configmuss dort aktiviert seinAWS-Region, wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der API-Gateway-Stufe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Löscht den im `StageArn` Parameter angegebenen API-Gateway-Schritt.

## `AWSConfigRemediation-EnableAPIGatewayTracing`

Beschreibung

Das `AWSConfigRemediation-EnableAPIGatewayTracing` Runbook ermöglicht die Protokollierung auf einer Amazon API Gateway-Stufe (API Gateway). AWS Configmuss dort aktiviert seinAWS-Region, wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der API-Gateway-Phase, für die Sie die Protokollierung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die Ablaufverfolgung auf dem im `StageArn` Parameter angegebenen API-Gateway-Schritt.

## AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Beschreibung

Das `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` Runbook aktualisiert die Cache-Methodeneinstellung für eine Amazon API Gateway-Stage-Ressource.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.

- CachingAuthorizedMethods

  Typ: StringList

  Beschreibung: (Erforderlich) Die Methoden, die autorisiert sind, das Caching zu aktivieren. Die Liste muss eine Kombination aus`DELETE`,`GET`,`HEAD`, `OPTIONS` `PATCH`,`POST`, und sein`PUT`. Das Caching ist für ausgewählte Methoden aktiviert und für nicht ausgewählte Methoden deaktiviert. Das Caching ist für alle Methoden aktiviert, wenn `ANY` es ausgewählt ist, und es ist für alle Methoden deaktiviert, wenn `NONE` es ausgewählt ist.

- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der API-Gateway-Stage-ARN für die `REST` API.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

## Dokumentschritte

- `aws:executeScript`- Akzeptiert die Stage-Ressourcen-ID als Eingabe, aktualisiert die Cache-Methodeneinstellung für einen API-Gateway-Schritt mithilfe der `UpdateStage` API-Aktion und überprüft die Aktualisierung.

# AWS Batch

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS Batch Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWSSupport-TroubleshootAWSBatchJob

Beschreibung

Das -`AWSSupport-TroubleshootAWSBatchJob`Runbook hilft Ihnen bei der Behebung von Problemen, die verhindern, dass ein -AWS BatchAuftrag vom `RUNNABLE` `STARTING` Status zum übergeht.

Wie funktioniert es?

Dieses Runbook führt die folgenden Prüfungen durch:

- Wenn sich die Datenverarbeitungsumgebung im `DISABLED` Status `INVALID` oder befindet.
- Wenn der `Max vCPU` Parameter der Datenverarbeitungsumgebung groß genug ist, um das Auftragsvolumen in der Auftragswarteschlange zu berücksichtigen.
- Wenn die Aufträge mehr vCPUs oder Speicherressourcen benötigen, als die Instance-Typen der Datenverarbeitungsumgebung bereitstellen können.
- Wenn die Aufträge auf GPU-basierten Instances ausgeführt werden sollen, die Datenverarbeitungsumgebung jedoch nicht für die Verwendung GPU-basierter Instances konfiguriert ist.
- Wenn die Auto Scaling-Gruppe für die Datenverarbeitungsumgebung keine Instances starten konnte.
- Wenn die gestarteten Instances dem zugrunde liegenden Amazon Elastic Container Service (Amazon ECS)-Cluster beitreten können; wenn nicht, wird das AWSSupport-TroubleshootECSContainerInstance-Runbook ausgeführt.
- Wenn ein Berechtigungsproblem bestimmte Aktionen blockiert, die zum Ausführen des Auftrags erforderlich sind.

**Important**

- Dieses Runbook muss in derselben AWS Region initiiert werden wie Ihr Auftrag, der im `RUNNABLE` Status hängen bleibt.
- Dieses Runbook kann für AWS Batch Aufträge initiiert werden, die auf Amazon-ECS- AWS Fargate oder Amazon Elastic Compute Cloud (Amazon EC2)-Instances geplant sind. Wenn die Automatisierung für einen -AWS BatchAuftrag auf Amazon Elastic Kubernetes Service (Amazon EKS) initiiert wird, wird die Initiierung beendet.
- Wenn Instances verfügbar sind, um den Auftrag auszuführen, aber den Amazon-ECS-Cluster nicht registrieren können, initiiert dieses Runbook das `AWSSupport-TroubleshootECSContainerInstance` Automatisierungs-Runbook, um zu versuchen, den Grund zu ermitteln. Weitere Informationen finden Sie im Runbook AWSSupport-TroubleshootECSContainerInstance.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- JobId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AWS Batch Auftrags, der im RUNNABLE Status hängen bleibt.

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

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

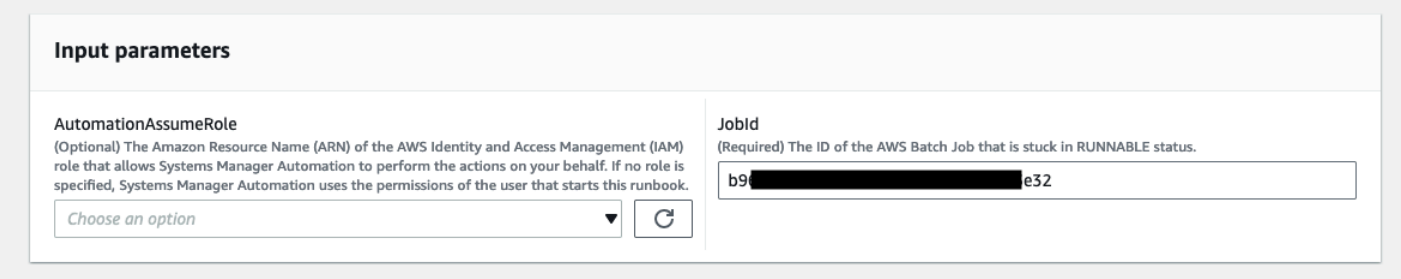
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ecs:DescribeClusters
- ecs:DescribeContainerInstances
- ecs:ListContainerInstances
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sts:GetCallerIdentity

Anweisungen

1. Navigieren Sie in der -AWS Systems ManagerKonsole zu AWSSupport-TroubleshootAWSBatchJob.
2. Wählen Sie Automatisierung ausführen aus
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - JobId (Erforderlich):

     Die ID des AWS Batch Auftrags, der im RUNNABLE Status hängen bleibt.




4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:
   - PreflightPermissionChecks:

     Führt Preflight-IAM-Berechtigungsprüfungen für den initiierenden Benutzer/die initiierende Rolle durch. Wenn Berechtigungen fehlen, enthält dieser Schritt die API-Aktionen, die im Abschnitt Globale Ausgabe fehlen.
   - ProceedOnlyIfUserHasPermission:

     Verzweigungen basierend auf , wenn Sie über Berechtigungen für alle erforderlichen Aktionen für das Runbook verfügen.
   - AWSBatchJobEvaluation:

     Führt Prüfungen für den AWS Batch Auftrag durch, um zu überprüfen, ob er vorhanden ist und sich im `RUNNABLE` Status befindet.
   - ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

     Verzweigungen basierend darauf, ob die Aufträge vorhanden sind und sich im `RUNNABLE` Status befinden.
   - BatchComputeEnvironmentEvaluation:

     Führt Prüfungen für die AWS Batch Datenverarbeitungsumgebung durch.
   - ProceedOnlyIfComputeEnvironmentChecksAreOK:

     Verzweigungen, die darauf basieren, ob die Überprüfung der Datenverarbeitungsumgebung erfolgreich war.
   - UnderlyingInfraEvaluation:

Führt Prüfungen anhand der zugrunde liegenden Auto Scaling-Gruppe oder Spot-Flottenanforderung durch.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Verzweigungen basierend auf , wenn Instances nicht dem Amazon-ECS-Cluster beitreten.

- EcsAutomationRunner:

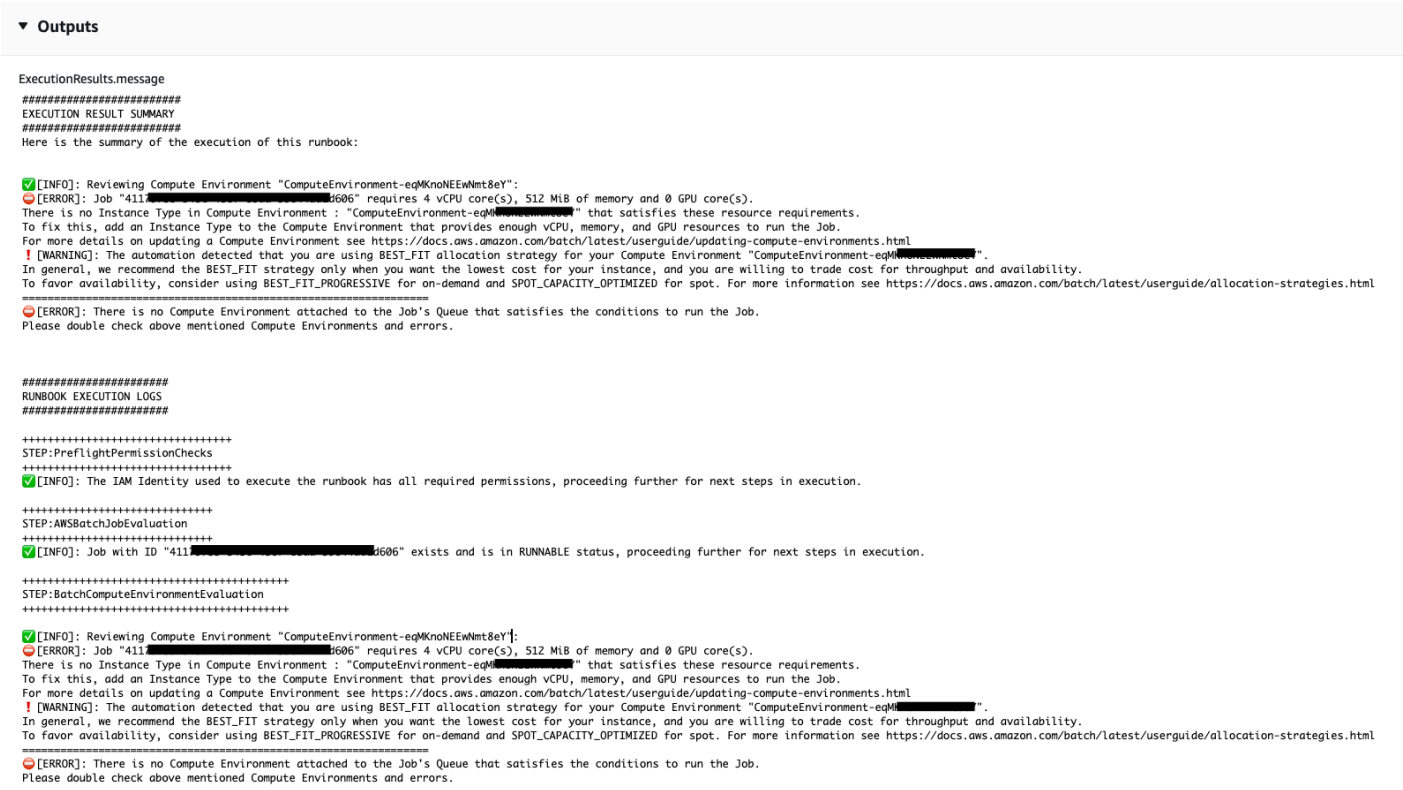
  Führt die Amazon-ECS-Automatisierung für die Instances aus, die nicht dem Cluster beitreten.

- ExecutionResults:

  Generiert Ausgaben basierend auf vorherigen Schritten.

7. Nach Abschluss wird der URI für die HTML-Datei des Bewertungsberichts bereitgestellt:

   S3-Konsolenlink und Amazon S3-URI für den Bericht über die erfolgreiche Ausführung des Runbooks




## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

# AWS CloudFormation

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CloudFormation Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification
- AWS-RunCfnLint
- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

## `AWS-DeleteCloudFormationStack`

Beschreibung

Löschen eines AWS CloudFormation-Stacks.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- StackNameOrId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name oder eindeutige ID des zu löschenden CloudFormation Stacks

## AWS-EnableCloudFormationSNSNotification

Beschreibung

Das `AWS-EnableCloudFormationSNSNotification` Runbook aktiviert Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen für den von Ihnen angegebenen AWS CloudFormation (AWS CloudFormation)-Stack.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der (IAM)-Rolle, mit der AWS Identity and Access Management Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- StackArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN oder Name des AWS CloudFormation Stacks, für den Sie Amazon SNS-Benachrichtigungen aktivieren möchten.

- NotificationArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS-Themas, das Sie dem AWS CloudFormation Stack zuordnen möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

## Dokumentschritte

- CheckCfnSnsLimits (aws:executeScript ) – Überprüft, ob die maximale Anzahl von Amazon SNS-Themen noch nicht mit dem von Ihnen angegebenen AWS CloudFormation Stack verknüpft wurde.

- EnableCfnSnsNotification (aws:executeAwsApi) – Aktiviert Amazon SNS-Benachrichtigungen für den AWS CloudFormation Stack.
- VerificationCfnSnsNotification (aws:executeScript ) – Prüft, ob Amazon SNS-Benachrichtigungen für den AWS CloudFormation Stack aktiviert wurden.

Ausgaben

CheckCfnSnsLimits.NotificationArnList - Eine Liste von ARNs, die Amazon SNS-Benachrichtigungen für den AWS CloudFormation Stack erhalten.

VerificationCfnSnsNotification.VerifySnsTopicsResponse - Antwort des -API-Vorgangs, der bestätigt, dass Amazon SNS-Benachrichtigungen für den AWS CloudFormation Stack aktiviert wurden.

## AWS-RunCfnLint

Beschreibung

Dieses Runbook verwendet einen AWS CloudFormationLinter (`cfn-python-lint`), um YAML- und JSON-Vorlagen anhand der AWS CloudFormation Ressourcenspezifikation zu validieren. Das `AWS-RunCfnLint` Runbook führt zusätzliche Prüfungen durch, z. B. um sicherzustellen, dass gültige Werte für Ressourceneigenschaften eingegeben wurden. Wenn die Validierung nicht erfolgreich ist, schlägt der `RunCfnLintAgainstTemplate`-Schritt fehl und die Ausgabe des Lintertools wird in einer Fehlermeldung bereitgestellt. Dieses Runbook verwendet cfn-lint v0.24.4.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ConfigureRuleFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Konfigurationsoptionen für eine Regel, die an den `--configure-rule`-Parameter übergeben werden soll.

  Beispiel: E2001:strict=false,E3012:strict=false.

- FormatFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Wert, der an den `--format`-Parameter übergeben wird, um das Ausgabeformat anzugeben.

  Gültige Werte: Standard | quiet | parseable | json

  Standard: Standard

- IgnoreChecksFlag

  Typ: Zeichenfolge

  Beschreibung (optional): IDs von Regeln, die an den --ignore-checks-Parameter übergeben werden sollen. Diese Regeln werden nicht überprüft.

  Beispiel: E1001, E1003, W7001

- IncludeChecksFlag

  Typ: Zeichenfolge

  Beschreibung (optional): IDs von Regeln, die an den `--include-checks`-Parameter übergeben werden sollen. Diese Regeln werden überprüft.

  Beispiel: E1001, E1003, W7001

- InfoFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Option für den `--info`-Parameter. Fügen Sie die Option hinzu, um zusätzliche Protokollierungsinformationen zur Vorlagenverarbeitung zu aktivieren.

  Standard: false

- TemplateFileName

  Typ: Zeichenfolge

  Beschreibung: der Name oder der Schlüssel der Vorlagendatei im S3-Bucket.

- Schablonen 3 BucketName

  Typ: Zeichenfolge

  Beschreibung: der Name des S3-Buckets, der die Packer-Vorlage enthält.

- RegionsFlag

  Typ: Zeichenfolge

  Beschreibung: (Optional) Werte, die an den `--regions` Parameter for übergeben werden, um die Vorlage anhand der angegebenen zu testenAWS-Regionen.

  Beispiel: us-east-1,us-west-1

Dokumentschritte

RunCfnLintAgainstTemplate— Führt das `cfn-python-lint` Tool anhand der angegebenen AWS CloudFormation Vorlage aus.

Ausgaben

RunCfnLintAgainstTemplate.output — Der stdout aus dem Tool. `cfn-python-lint`

## AWSSupport-TroubleshootCFNCustomResource

Beschreibung

Das `AWSSupport-TroubleshootCFNCustomResource` Runbook hilft bei der Diagnose, warum ein AWS CloudFormation Stack eine benutzerdefinierte Ressource nicht erstellt, aktualisiert oder gelöscht hat. Das Runbook überprüft das für die benutzerdefinierte Ressource verwendete Service-Token und die zurückgegebene Fehlermeldung. Nachdem die Details für die benutzerdefinierte Ressource überprüft wurden, enthält die Runbook-Ausgabe eine Erläuterung des Stack-Verhaltens und Schritte zur Fehlerbehebung für die benutzerdefinierte Ressource.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- StackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des AWS CloudFormation Stacks, in dem die benutzerdefinierte Ressource ausgefallen ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `validateCloudFormationStack`- Überprüft, ob der AWS CloudFormation Stapel im selben AWS-Konto und AWS-Region vorhanden ist.
- `checkCustomResource`- Analysiert den AWS CloudFormation Stack, überprüft die ausgefallene benutzerdefinierte Ressource und gibt Informationen zur Behebung der ausgefallenen benutzerdefinierten Ressource aus.

## AWS-UpdateCloudFormationStack

Beschreibung

Aktualisieren Sie einen AWS CloudFormation Stack mithilfe einer AWS CloudFormation Vorlage, die in einem Amazon S3 S3-Bucket gespeichert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der von Lambda übernommenen Rolle
- StackNameOrId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name oder eindeutige ID des zu AWS CloudFormation aktualisierenden Stacks
- TemplateUrl

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket-Speicherort, der die aktualisierte CloudFormation Vorlage enthält (z. B. `https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/updated.template`)

# CloudFront

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon CloudFront bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-EnableCloudFrontDefaultRootObject
- AWSConfigRemediation-EnableCloudFrontAccessLogs

- AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity
- AWSConfigRemediation-EnableCloudFrontOriginFailover
- AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

## AWSConfigRemediation-EnableCloudFrontDefaultRootObject

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` Runbook konfiguriert das Standard-Root-Objekt für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie das Standard-Root-Objekt konfigurieren möchten.

- DefaultRootObject

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das Objekt, das Sie zurückgeben CloudFront möchten, wenn eine Viewer-Anfrage auf Ihre Root-URL verweist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Konfiguriert das Standard-Stammobjekt für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben.

## AWSConfigRemediation-EnableCloudFrontAccessLogs

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontAccessLogs` Runbook aktiviert die Zugriffsprotokollierung für die von Ihnen angegebene Amazon CloudFront (CloudFront)-Verteilung.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3)-Buckets, in dem Sie Zugriffsprotokolle speichern möchten. Buckets in af-south-1, ap-east-1, eu-south-1 und me-south-1 AWS-Region werden nicht unterstützt.
- CloudFrontId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Verteilung, für die Sie die Zugriffsprotokollierung aktivieren möchten.
- IncludeCookies

  Typ: Boolesch

  Zulässige Werte: true | false

  Beschreibung: (Erforderlich) Setzen Sie diesen Parameter auf `true` , wenn Cookies in die Zugriffsprotokolle aufgenommen werden sollen.
- Präfix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine optionale Zeichenfolge, die dem Zugriffsprotokoll `filenames` für Ihre Verteilung CloudFront vorangestellt werden soll, z. B. `myprefix/`.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

> **Note**
>
> Die `s3:GetBucketLocation` API kann nur für S3-Buckets im selben Konto verwendet werden. Sie können es nicht für kontoübergreifende S3-Buckets verwenden.

Dokumentschritte

- `aws:executeScript` – Aktiviert die Zugriffsprotokollierung für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben.

## AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` Runbook aktiviert die Origin-Zugriffsidentität für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution. Diese Automatisierung weist allen CloudFront Origins des Amazon Simple Storage Service (Amazon S3) -Origin-Typs dieselbe Origin-Zugriffsidentität ohne Ursprungszugriffsidentität für die von Ihnen angegebene CloudFront Distribution zu. Diese Automatisierung gewährt keine Leseberechtigung für die ursprüngliche Zugriffsidentität für den CloudFront Zugriff auf Objekte in

Ihrem Amazon S3-Bucket. Sie müssen Ihre Amazon S3-Bucket-Berechtigungen aktualisieren, um den Zugriff zu ermöglichen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie Origin-Failover aktivieren möchten.
- OriginAccessIdentityId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront ursprünglichen Zugriffsidentität, die dem Ursprung zugeordnet werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die Ursprungszugriffsidentität für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob die ursprüngliche Zugriffsidentität zugewiesen wurde.

## AWSConfigRemediation-EnableCloudFrontOriginFailover

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontOriginFailover` Runbook aktiviert Origin-Failover für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.

- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie Origin-Failover aktivieren möchten.

- OriginGroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Ursprungsgruppe.

- PrimaryOriginId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des primären Ursprungs in der Ursprungsgruppe.

- SecondaryOriginId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des sekundären Ursprungs in der Ursprungsgruppe.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

## Dokumentschritte

- `aws:executeScript`- Aktiviert das Origin-Failover für die CloudFront Distribution, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob das Failover aktiviert wurde.

## `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS`

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` Runbook aktiviert die Viewer-Protokollrichtlinie für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie die Viewer-Protokollrichtlinie aktivieren möchten.

- ViewerProtocolPolicy

  Typ: Zeichenfolge

  Gültige Werte: https-only, redirect-to-https

  Beschreibung: (Erforderlich) Das Protokoll, mit dem Zuschauer auf die Dateien im Ursprung zugreifen können.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die Viewer-Protokollrichtlinie für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob die Richtlinie zugewiesen wurde.

# CloudTrail

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CloudTrail Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

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

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

## AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

Beschreibung

Das `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` Runbook erstellt einen AWS CloudTrail (CloudTrail) -Trail, der Protokolldateien von mehreren AWS-Regionen an den Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl übermittelt.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- BucketName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Amazon S3-Buckets, in den Sie Protokolle hochladen möchten.

- KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3-Schlüsselpräfix, das nach dem Namen des Buckets steht, den Sie für die Bereitstellung von Protokolldateien angegeben haben.

- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CloudTrail Trails, der erstellt werden soll.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Dokumentschritte

- `aws:executeAwsApi`- Akzeptiert den Trailnamen und den Amazon S3-Bucket-Namen als Eingabe und erstellt einen CloudTrail Trail.
- `aws:executeAwsApi`- Aktiviert die Protokollierung des erstellten Trails und startet die Protokollzustellung an den von Ihnen angegebenen Amazon S3-Bucket.

- `aws:assertAwsResourceProperty`- Überprüft, ob der CloudTrail Trail erstellt wurde.

## AWS-EnableCloudTrail

Beschreibung

Erstellen eines AWS CloudTrail-Trails und Konfiguration der Protokollierung auf einem S3-Bucket.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name des S3-Buckets für die Veröffentlichung von Protokolldateien.

> **Note**
>
> Der S3-Bucket muss vorhanden sein und die Bucket-Richtlinie muss CloudTrail Schreibberechtigung für den Bucket gewähren. Informationen finden Sie in der Amazon S3-Bucket-Richtlinie für CloudTrail.

- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des neuen Trails.

## AWS-EnableCloudTrailCloudWatchLogs

Beschreibung

Dieses Runbook aktualisiert die Konfiguration eines oder mehrerer AWS CloudTrail Trails, um Ereignisse an eine Amazon- CloudWatch Logs-Protokollgruppe zu senden.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der (IAM)-Rolle, mit der AWS Identity and Access Management Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- CloudWatchLogsLogGroupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der CloudWatch Logs-Protokollgruppe, an die die CloudTrail Protokolle übermittelt werden.

- CloudWatchLogsRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, die CloudWatch Logs Logs annimmt, um in die angegebene Protokollgruppe zu schreiben.

- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine kommagetrennte Liste der Namen der CloudTrail Trails, deren Ereignisse Sie an - CloudWatch Protokolle senden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `cloudtrail:UpdateTrail`
- `iam:PassRole`

Dokumentschritte

- `aws:executeScript` – Aktualisiert die angegebenen CloudTrail Trails, um Ereignisse an die angegebene CloudWatch Protokollgruppe zu übermitteln.

## AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Beschreibung

Das `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` Runbook verschlüsselt einen AWS CloudTrail (CloudTrail) -Trail mit dem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel, den Sie angeben. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre CloudTrail Trails gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Trails mit unterschiedlichen KMS-Schlüsseln zu verschlüsseln. CloudTrailDigest-Dateien sind nicht verschlüsselt. Wenn Sie den `EnableLogFileValidation` Parameter bereits auf `true` für den Trail gesetzt haben, finden Sie weitere Informationen im Abschnitt „Serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln verwenden“ im Thema Bewährte Methoden zur CloudTrail präventiven Sicherheit im AWS CloudTrailBenutzerhandbuch.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- KMS KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN, die Schlüssel-ID oder der Schlüsselalias des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln des im `TrailName` Parameter angegebenen Trails verwenden möchten.

- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN oder der Name des Trails, den Sie aktualisieren möchten, der verschlüsselt werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Verschlüsselung auf dem Pfad, den Sie im `TrailName` Parameter angeben.
- `aws:executeAwsApi`- Erfasst den ARN für den vom Kunden verwalteten Schlüssel, den Sie im `KMSKeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Verschlüsselung auf dem CloudTrail Trail aktiviert wurde.

## AWS-EnableCloudTrailKmsEncryption

Beschreibung

Dieses Runbook aktualisiert die Konfiguration eines oder mehrerer AWS CloudTrail Trails zur Verwendung der AWS Key Management Service (AWS KMS)-Verschlüsselung.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- KMSKeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Schlüssel-ID des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln des Trails verwenden möchten, den Sie im `-TrailName`Parameter angeben. Der Wert kann ein Aliasname mit dem Präfix „alias/“, ein vollständig angegebener ARN für einen Alias oder ein vollständig angegebener ARN für einen Schlüssel sein.
- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine kommagetrennte Liste der Trails, die Sie aktualisieren möchten, um verschlüsselt zu werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `cloudtrail:UpdateTrail`
- `kms:DescribeKey`

- `kms:ListKeys`

Dokumentschritte

- `aws:executeScript` – Aktiviert die AWS KMS Verschlüsselung für die Trails, die Sie im `TrailName` Parameter angeben.

## AWSConfigRemediation-EnableCloudTrailLogFileValidation

Beschreibung

Das `AWSConfigRemediation-EnableCloudTrailLogFileValidation` Runbook ermöglicht die Validierung von Protokolldateien für Ihren AWS CloudTrail Trail.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- TrailName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name oder Amazon-Ressourcenname (ARN) des Trails, für den Sie die Protokollvalidierung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi` – Aktiviert die Protokollvalidierung für den AWS CloudTrail Trail, den Sie im `TrailName` Parameter angeben.
- `aws:assertAwsResourceProperty` – Prüft, ob die Protokollvalidierung für Ihren Trail aktiviert ist.

## `AWS-EnableCloudTrailLogFileValidation`

Beschreibung

Das `AWS-EnableCloudTrailLogFileValidation` Runbook ermöglicht die Überprüfung der Protokolldateien für die von Ihnen angegebenen AWS CloudTrail Pfade.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der Namen der CloudTrail Pfade, für die Sie die Protokollvalidierung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die Protokollvalidierung für die AWS CloudTrail Pfade, die Sie im `TrailNames` Parameter angeben.

## AWS-QueryCloudTrailLogs

Beschreibung

Das `AWS-QueryCloudTrailLogs` Runbook erstellt eine Amazon Athena-Tabelle aus dem Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl, die AWS CloudTrail (CloudTrail) -Protokolle

enthält. Nach dem Erstellen der Tabelle führt die Automatisierung von Ihnen angegebene SQL-Abfragen aus und löscht dann die Tabelle.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Abfragen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die SQL-Abfrage, die Sie ausführen möchten.
- SourceBucketPath

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3-Buckets, der die CloudTrail Protokolldateien enthält, die Sie abfragen möchten.
- TableName

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Name der Athena-Tabelle, die durch die Automatisierung erstellt wurde.

Standard: cloudtrail_logs

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

### Dokumentschritte

- `aws:executeAwsApi`- Erzeugt eine Athena-Tabelle.
- `aws:executeAwsApi`- Führt die Abfragezeichenfolge aus, die Sie im `Query` Parameter angeben.
- `aws:executeScript`- Fragt ab und wartet, bis die Abfrage abgeschlossen ist.
- `aws:executeAwsApi`- Ruft die Ergebnisse der Abfrage ab.

- `aws:executeAwsApi`- Löscht die durch die Automatisierung erstellte Tabelle.

# CloudWatch

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon CloudWatch bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

## `AWS-ConfigureCloudWatchOnEC2Instance`

Beschreibung

Aktivieren oder deaktivieren Sie die CloudWatch detaillierte Überwachung von Amazon auf verwalteten Instances.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem

Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, für die Sie die CloudWatch Überwachung aktivieren möchten.

- Eigenschaften

  Typ: Zeichenfolge

  Beschreibung: (Optional) Dieser Parameter wird nicht unterstützt. Er ist hier aus Gründen der Abwärtskompatibilität aufgeführt.

- status

  Gültige Werte: Aktiviert | Deaktiviert

  Beschreibung: (Optional) Gibt an, ob CloudWatch aktiviert oder deaktiviert werden soll.

  Standard: Aktiviert

Dokumentschritte

configureCloudWatch- Wird CloudWatch auf der Amazon EC2-Instance mit dem angegebenen Status konfiguriert.

Ausgaben

Diese Automatisierung hat keinen Ausgang.

## AWS-EnableCWAlarm

Beschreibung

Das `AWS-EnableCWAlarm` Runbook erstellt Amazon CloudWatch (CloudWatch)-Alarme für AWS Ressourcen in Ihrem AWS-Konto , die noch keine haben. CloudWatch Alarme werden für die folgenden AWS Ressourcen erstellt:

- Instances von Amazon Elastic Compute Cloud (Amazon EC2)

- Amazon Elastic Block Store (Amazon EBS)-Volumes
- Amazon Simple Storage Service (Amazon S3)-Buckets
- Amazon Relational Database Service (Amazon RDS)-Cluster

## Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ComparisonOperator

  Typ: Zeichenfolge

  Gültige Werte: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshol | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

  Beschreibung: (Erforderlich) Die arithmetische Operation, die beim Vergleich der angegebenen Statistik und des Schwellenwerts verwendet werden soll.
- MetricName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name für die Metrik, die dem Alarm zugeordnet ist.

- Intervall

  Typ: Ganzzahl

  Gültige Werte: 10 | 30 | 60 | Ein Vielfaches von 60

  Beschreibung: (Erforderlich) Der Zeitraum in Sekunden, in dem die Statistik angewendet wird.

- ResourceARNs

  Typ: StringList

  Beschreibung: (Erforderlich) Eine kommagetrennte Liste von ARNs der Ressourcen, für die ein CloudWatch Alarm erstellt werden soll

- Statistik

  Typ: Zeichenfolge

  Gültige Werte: Durchschnitt | Maximum | Minimum | SampleCount | Summe

  Beschreibung: (Erforderlich) Die Statistik für die Metrik, die dem Alarm zugeordnet ist.

- Threshold

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Der Wert, der mit der angegebenen Statistik verglichen werden soll.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `cloudwatch:PutMetricAlarm`

## Dokumentschritte

- `aws:executeScript` – Erstellt einen CloudWatch Alarm gemäß den in den Runbook-Parametern angegebenen Werten für die Ressourcen, die Sie im `ResourceARNs` Parameter angeben.

Ausgaben

EnableCWAlarm .FailedResources: Eine Zuordnungsliste von Ressourcen-ARNs, für die kein CloudWatch Alarm erstellt wurde, und der Grund für den Fehler.

EnableCWAlarm .SuccessfulResources: Eine Liste von Ressourcen-ARNs, für die ein CloudWatch Alarm erfolgreich erstellt wurde.

# Amazon DocumentDB

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon DocumentDB (mit MongoDB-Kompatibilität). Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableDocDbClusterBackupRetentionPeriod

## AWS-EnableDocDbClusterBackupRetentionPeriod

Beschreibung

Das `AWS-EnableDocDbClusterBackupRetentionPeriod` Runbook ermöglicht einen Aufbewahrungszeitraum für Backups für den von Ihnen angegebenen Amazon DocumentDB-Cluster. Diese Funktion legt die Gesamtzahl der Tage fest, für die ein automatisiertes Backup aufbewahrt wird. Um einen Cluster zu ändern, muss sich der Cluster im verfügbaren Zustand mit dem Engine-Typ befinden`docdb`.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DBClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den Amazon DocumentDB-Cluster, für den Sie den Aufbewahrungszeitraum für Backups aktivieren möchten.
- BackupRetentionPeriod

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die automatisierte Backups aufbewahrt werden. Muss ein Wert zwischen 7 und 35 Tagen sein.
- PreferredBackupWindow

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein täglicher Zeitraum in UTC (Universal Time Coordinated) im Format hh24:mm-h24:mm, z. B. 07:14-07:44. Der Wert muss mindestens 30 Minuten betragen und kann nicht mit dem bevorzugten Wartungsfenster in Konflikt geraten.

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

Dokumentschritte

- GetDocDbClusterIdentifier (aws:executeAwsApi) – Gibt die Amazon DocumentDB-Cluster-ID mit der angegebenen Ressourcen-ID zurück.
- VerifyDocDbEngine (aws:assertAwsResourceProperty) – Überprüft, ob der Amazon DocumentDB-Engine-Typ `docdb` versehentliche Änderungen an anderen Amazon-RDS-Engine-Typen verhindern soll.
- VerifyDocDbStatus (aws:waitAwsResourceProperty) – Überprüft, ob der Amazon DocumentDB-Clusterstatus lautet`available`.
- ModifyDocDbRetentionPeriod (aws:executeAwsApi) – Legt den Aufbewahrungszeitraum unter Verwendung der bereitgestellten Werte für den angegebenen Amazon DocumentDB-Cluster fest.
- VerifyDocDbBackupsEnabled (aws:executeScript ) – Prüft, ob der Aufbewahrungszeitraum für den Amazon DocumentDB-Cluster und das bevorzugte Sicherungsfenster, falls angegeben, erfolgreich festgelegt wurden.

Ausgaben

ModifyDocDbRetentionPeriod.ModifyDbClusterResponse - Antwort von der -`ModifyDBCluster`API-Operation.

VerifyDocDbBackupsEnabled.VerifyDbClusterBackupsEnabledResponse - Ausgabe aus dem `VerifyDocDbBackupsEnabled` Schritt zur Bestätigung der erfolgreichen Änderung des Amazon DocumentDB-Clusters.

# CodeBuild

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CodeBuild Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

# AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Beschreibung

Das `AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` Runbook verschlüsselt die Build-Artefakte eines AWS CodeBuild (CodeBuild)-Projekts mit dem von Ihnen angegebenen AWS Key Management Service (AWS KMS) kundenverwalteten Schlüssel. AWS Config muss in der aktiviert sein AWS-Region , in der Sie diese Automatisierung ausführen.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- KMSKeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom Kunden verwalteten Schlüssels, den AWS KMS Sie zum Verschlüsseln des CodeBuild Projekts verwenden möchten, das Sie im -`ProjectId`Parameter angeben.
- ProjectId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des CodeBuild Projekts, dessen Build-Artefakte Sie verschlüsseln möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Dokumentschritte

- `aws:executeAwsApi` – Sammelt den CodeBuild Projektnamen aus der Projekt-ID.
- `aws:executeAwsApi` – Aktiviert die Verschlüsselung für das CodeBuild Projekt, das Sie im -`ProjectId`Parameter angeben.
- `aws:assertAwsResourceProperty` – Prüft, ob die Verschlüsselung für das CodeBuild Projekt aktiviert wurde.

### Ausgaben

UpdateLambdaConfig.UpdateFunctionConfigurationResponse - Antwort auf den `UpdateFunctionConfiguration` API-Aufruf.

## AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

### Beschreibung

Das `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` Runbook löscht die `AWS_SECRET_ACCESS_KEY` Umgebungsvariablen `AWS_ACCESS_KEY_ID` und aus dem von Ihnen angegebenen AWS CodeBuild (CodeBuild) -Projekt. AWS Configmuss dort aktiviert seinAWS-Region, wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des CodeBuild Projekts, dessen Zugriffsschlüssel-Umgebungsvariablen Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Löscht die Umgebungsvariablen des Zugriffsschlüssels für das im `ResourceId` Parameter angegebene CodeBuild Projekt.

# AWS CodeDeploy

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS CodeDeploy Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootCodeDeploy

## `AWSSupport-TroubleshootCodeDeploy`

Beschreibung

Das `AWSSupport-TroubleshootCodeDeploy` Runbook hilft bei der Diagnose, warum eine AWS CodeDeploy Bereitstellung auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance fehlgeschlagen ist. Das Runbook gibt Schritte aus, die Ihnen bei der Lösung des Problems oder bei der weiteren Problembehandlung helfen. CodeDeployEs werden auch bewährte Methoden für bereitgestellt, mit denen Sie ähnliche Probleme in Zukunft vermeiden können.

Dieses Runbook kann Ihnen helfen, die folgenden Probleme zu lösen:

- Der CodeDeploy Agent ist nicht installiert oder läuft nicht auf der Amazon EC2-Instance
- An die Amazon EC2-Instance ist kein AWS Identity and Access Management (IAM-) Instance-Profil angehängt
- Das an die Amazon EC2-Instance angehängte IAM-Instance-Profil verfügt nicht über die erforderlichen Amazon Simple Storage Service (Amazon S3) -Berechtigungen
- Eine in Amazon S3 gespeicherte Revision fehlt, oder der verwendete Amazon S3-Bucket befindet sich in einer AWS-Region anderen als der Amazon EC2-Instance
- Probleme mit der Anwendungsspezifikationsdatei (AppSpec)
- Fehler „Datei ist bereits am Speicherort vorhanden“
- Event-Hooks für den CodeDeploy verwalteten Lebenszyklus fehlgeschlagen

- Fehlgeschlagene vom Kunden verwaltete Lifecycle-Event-Hoo
- Scale-In-Ereignisse während der Bereitstellung

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DeploymentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Bereitstellung, die fehlgeschlagen ist.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, in der die Bereitstellung fehlgeschlagen ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Überprüft die für die `InstanceId` Parameter `DeploymentId` und angegebenen Werte.
- `aws:executeScript`- Sammelt Informationen aus der Amazon EC2-Instance wie den Status der Instance und die Profildetails der IAM-Instance.
- `aws:executeScript`— Überprüft die angegebene Bereitstellung und gibt eine Analyse darüber zurück, warum die Bereitstellung fehlgeschlagen ist.

# AWS Config

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS Config Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-SetupConfig

## `AWSSupport-SetupConfig`

Beschreibung

Das `AWSSupport-SetupConfig` Runbook erstellt eine dienstverknüpfte AWS Identity and Access Management (IAM) -Rolle, einen Konfigurationsrekorder, der von unterstützt wirdAWS Config, und einen Bereitstellungskanal mit einem Amazon Simple Storage Service (Amazon S3) -Bucket, über den Konfigurationssnapshots und Konfigurationsverlaufsdateien AWS Config gesendet werden. Wenn Sie Werte für die `AggregatorAccountRegion` Parameter `AggregatorAccountId` und angeben, erstellt das Runbook auch Autorisierungen für die Datenaggregation, um AWS Config Konfigurations- und Compliance-Daten von mehreren zu sammeln. AWS-Konten AWS-Regionen

Weitere Informationen zum Aggregieren von Daten aus mehreren Konten und Regionen finden Sie unter Datenaggregation für mehrere Konten und Regionen im Entwicklerhandbuch. AWS Config

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AggregatorAccountId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des, AWS-Konto wo ein Aggregator hinzugefügt wird, um AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten zu aggregieren und. AWS-Regionen Dieses Konto wird auch vom Aggregator verwendet, um die Quellkonten zu autorisieren.
- AggregatorAccountRegion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Region, in der ein Aggregator hinzugefügt wird, um AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten und Regionen zu aggregieren.
- IncludeGlobalResourcesRegion

Typ: Zeichenfolge

Standard: us-east-1

Beschreibung: (Erforderlich) Um zu vermeiden, dass globale Ressourcendaten in jeder Region aufgezeichnet werden, geben Sie eine Region an, aus der globale Ressourcendaten aufgezeichnet werden sollen.

- Partition

  Typ: Zeichenfolge

  Standard: `aws`

  Beschreibung: (Erforderlich) Die Partition, von der Sie AWS Config Konfigurations- und Konformitätsdaten sammeln möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Standard: `aws-config-delivery-channel`

  Beschreibung: (Optional) Der Name, den Sie auf den Amazon S3-Bucket anwenden möchten, der für den Lieferkanal erstellt wurde. Die Konto-ID wird an das Ende des Namens angehängt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`- Erzeugt eine dienstverknüpfte IAM-Rolle, AWS Config falls noch keine vorhanden ist.
- `aws:executeScript`- Erzeugt einen Konfigurationsrekorder, falls noch keiner existiert.
- `aws:executeScript`- Erstellt einen Amazon S3-Bucket, der vom Lieferkanal verwendet werden kann, falls noch keiner vorhanden ist.
- `aws:executeScript`- Erzeugt einen Bereitstellungskanal unter Verwendung der vom Runbook erstellten Ressourcen.
- `aws:executeAwsApi`- Startet den Konfigurationsrekorder.
- `aws:executeScript`- Wenn Sie Werte für die `AggregatorAccountRegion` Parameter `AggregatorAccountId` und angegeben haben, werden die Autorisierungen für die Datenaggregation mehrerer Konten und Regionen konfiguriert.

# Amazon Connect

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Connect bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows

## `AWSSupport-AssociatePhoneNumbersToConnectContactFlows`

Beschreibung

Das `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` hilft Ihnen, Telefonnummern mit Kontaktabläufen in Ihrer Amazon Connect Connect-Instance zu verknüpfen.

Durch die Bereitstellung der Zuordnungen von Telefonnummern und Kontaktabläufen in einer CSV-Datei (Comma Separated Values) ordnet das Runbook innerhalb von 14,5 Minuten so viele Telefonnummern wie möglich den Kontaktabläufen zu. Das Runbook erstellt eine CSV-Datei mit allen Telefonnummern- und Kontaktflusspaaren, die innerhalb des Zeitlimits nicht zugeordnet werden konnten, sodass Sie sie beim nächsten Lauf eingeben können.

Wie funktioniert es?

Das Runbook `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` hilft Ihnen dabei, Telefonnummern mit Kontaktabläufen in Ihrer Amazon Connect Connect-Instance zu verknüpfen, indem Sie eine CSV-Datei mit Zuordnungsdaten verwenden, die in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert ist. Die CSV-Eingabedatei sollte dem folgenden Format entsprechen, mit `PhoneNumber` Werten im E.164-Format.

Beispiel für die CSV-Eingabedatei

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

Das Automatisierungs-Runbook erstellt außerdem die folgenden Dateien an dem im `DestinationFileBucket` und `DestinationFilePath` angegebenen Zielverzeichnis.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: Eine temporäre Datei, die die `PhoneNumberId` und `ContactFlowId` -Paare enthält, die für die `AssociatePhoneNumberContactFlow` API erforderlich sind.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: Eine Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aufgrund eines Fehlers nicht verarbeitet werden konnten, z. B. `ResourceNotFoundException` im Format von`PhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: Eine Datei, die die Telefonnummer und die Kontaktflusspaare enthält, die nicht verarbeitet wurden. Das Runbook versucht, innerhalb von 14,5 Minuten (15 Minuten AWS Lambda Funktions-Timeout — 30 Sekunden Puffer) so viele Telefonnummern und Kontaktflüsse wie möglich zu verarbeiten. Falls es einige Telefonnummern/Kontaktflüsse gibt, die aufgrund der Zeitbeschränkung nicht verarbeitet werden konnten, nimmt das Runbook sie in eine CSV-Datei auf, die als Eingabe für die nächste Runbook-Ausführung verwendet werden kann.

Typ des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

```
{
    "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"
            }
        ]
```

```
        }
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie [AWSSupport-AssociatePhoneNumbersToConnectContactFlows]im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ)

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - ConnectInstanceId (Erforderlich)

     Die ID Ihrer Amazon Connect Connect-Instance.
   - SourceFileBucket (Erforderlich)

     Der Amazon S3 S3-Bucket, in dem die CSV-Datei gespeichert wird, die die Telefonnummern- und Kontaktflusspaare enthält.
   - SourceFilePath (Erforderlich)

     Der Amazon S3 S3-Objektschlüssel der CSV-Datei, der die Telefonnummern- und Kontaktflusspaare enthält. z. B. `path/to/input.csv`.
   - DestinationFileBucket (Erforderlich)

     Der Amazon S3 S3-Bucket, in den die Automatisierung eine Zwischendatei und einen Ergebnisbericht einfügt.
   - DestinationFilePath (Fakultativ)

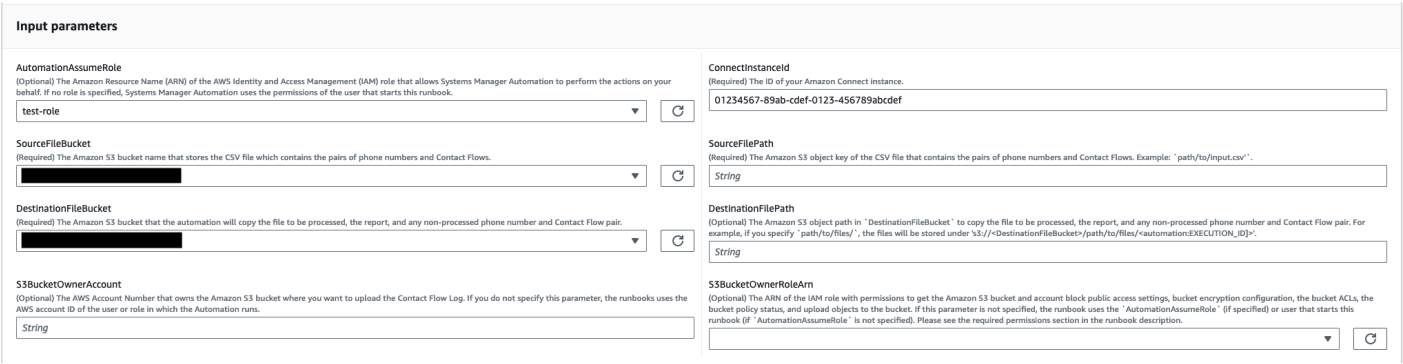
     Der Amazon S3 S3-Objektpfad, `DestinationFileBucket` unter dem eine Zwischendatei und ein Ergebnisbericht gespeichert werden sollen. Wenn Sie beispielsweise angeben`path/to/files/`, werden Dateien unter gespeicherts`3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- S3 BucketOwnerAccount (fakultativ)

  Die AWS Kontonummer, der der Amazon S3 S3-Bucket gehört, in den Sie das Contact Flow Log hochladen möchten. Wenn Sie diesen Parameter nicht angeben, verwenden die Runbooks die AWS Konto-ID des Benutzers oder der Rolle, in der die Automatisierung ausgeführt wird.

- S3 BucketOwnerRoleArn (optional)

  Der ARN der IAM-Rolle mit den Berechtigungen zum Abrufen der Einstellungen für den öffentlichen Zugriff auf den Amazon S3 S3-Bucket und das Konto, zur Konfiguration der Bucket-Verschlüsselung, zu den Bucket-ACLs, zum Status der Bucket-Richtlinie und zum Hochladen von Objekten in den Bucket. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` (falls angegeben) oder den Benutzer, der dieses Runbook startet (falls `AutomationAssumeRole` nicht angegeben). Weitere Informationen finden Sie im Abschnitt „Erforderliche Berechtigungen“ in der Runbook-Beschreibung.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - CheckConnectInstanceExistance

     Prüft, ob die in bereitgestellte Amazon Connect Connect-Instanz `ConnectInstanceId` existiert.

   - Prüft 3 BucketPublicStatus

     Überprüft, ob die in `SourceFileBucket` und angegebenen Amazon S3 S3-Buckets anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen `DestinationFileBucket` zulassen.

   - CheckSourceFileExistenceAndSize

Überprüft, ob die in der angegebene CSV-Quelldatei `SourceFilePath` existiert und ob die Dateigröße das Limit von 25 MiB überschreitet.

- GenerateResourceIdMap

  Lädt die CSV-Quelldatei herunter, die in `SourceFilePath` und identify `PhoneNumberId` und `ContactFlowId` für jede Ressource angegeben ist. Danach wird eine CSV-Datei, die,, und `ContactFlowId` enthält `PhoneNumberPhoneNumberId`, in den Amazon S3 S3-Ziel-Bucket hochgeladen`ContactFlowName`, der in `DestinationFileBucket` angegeben ist. Wenn für eine bestimmte Nummer `PhoneNumberId` nicht identifiziert werden kann, ist das Feld in der CSV-Datei leer.

- AssociatePhoneNumbersToContactFlows

  Erstellt mithilfe eines AWS CloudFormation Stacks eine AWS Lambda Funktion in Ihrem Konto. Die AWS Lambda Funktion ordnet jede Zahl einem Kontaktfluss zu, der in der in und angegebenen CSV-Quelldatei aufgeführt ist, `SourceFileBucket` `SourceFilePath` und der AWS CloudFormation Stapel ruft die Funktion auf. Die AWS Lambda Funktion ordnet so viele Telefonnummern wie möglich den Kontaktströmen zu, bevor das Zeitlimit überschritten wird (15 Minuten). Die Liste der Telefonnummern und Kontaktabläufe, die aufgrund eines Fehlers nicht verarbeitet werden konnten, wird hochgeladen`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Diejenigen, die aufgrund einer Überschreitung der maximalen Anzahl von Telefonnummern, die in einer einzigen Ausführung verarbeitet werden können, nicht verarbeitet werden konnten, werden hochgeladen`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Schlägt dieser Schritt fehl, wird mit dem `DescribeCloudFormationErrorFromStackEvents` Schritt fortgefahren, in dem angegeben wird, warum er aufgrund von AWS CloudFormation Stack-Ereignissen fehlgeschlagen ist.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Wartet, bis die AWS Lambda Funktion, die Telefonnummern Kontaktabläufen zuordnet, erstellt wurde und der AWS CloudFormation Stack seinen Aufruf abgeschlossen hat.

- GenerateReport

  Generiert den Bericht, der die Anzahl der Telefonnummern enthält, die Kontaktabläufen zugeordnet sind, diejenigen, die aufgrund eines Fehlers nicht verarbeitet werden konnten, und die, die aufgrund einer Überschreitung der maximalen Anzahl von Telefonnummern, die in einer einzigen Ausführung verarbeitet werden können, nicht verarbeitet werden

konnten. Der Bericht zeigt auch den Standort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) für `[automation:EXECUTION_ID]/ErrorResourceList.csv` oder`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`, falls zutreffend.

- **`DeleteCloudFormationStack`**

  Löscht den AWS CloudFormation Stack, einschließlich der Lambda-Funktion für das Mapping.

- **`DescribeCloudFormationErrorFromStackEvent`**

  Beschreibt Fehler aus dem AWS CloudFormation Stack des Schritts`AssociatePhoneNumbersToContactFlows`.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - GenerateReport.OutputPayload

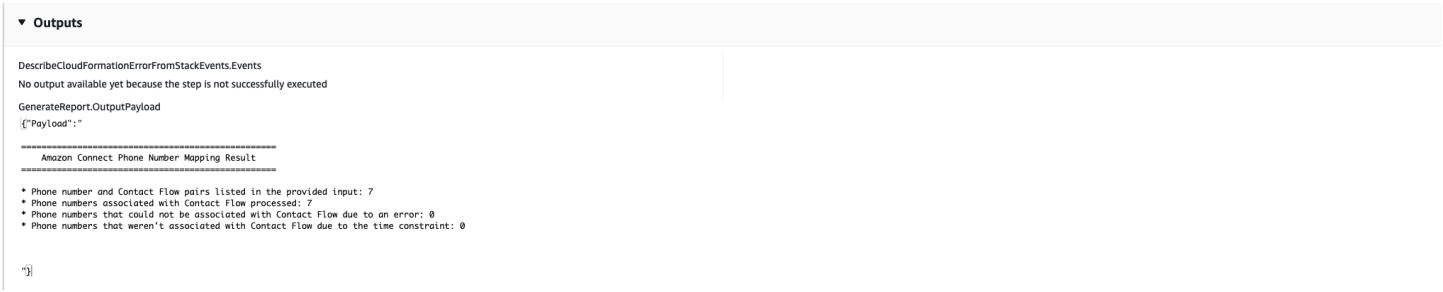
     Ausgabe der Verknüpfungen zwischen Telefonnummer und Kontaktfluss. Dieser Bericht enthält die folgenden Informationen:

     - Die Anzahl der Telefonnummern- und Kontaktflusspaare, die in der CSV-Eingabedatei aufgeführt sind
     - Die Anzahl der Telefonnummern, die mit Kontaktströmen verknüpft sind, wie in der CSV-Eingabedatei angegeben
     - Die Anzahl der Telefonnummern, die aufgrund eines Fehlers nicht mit Kontaktabläufen verknüpft werden konnten
     - Die Anzahl der Telefonnummern, die aus Zeitgründen nicht mit Kontaktabläufen verknüpft wurden
     - Der Speicherort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) der CSV-Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aufgrund eines Fehlers nicht verknüpft werden konnten
     - Der Speicherort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) der CSV-Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aus Zeitgründen nicht verknüpft wurden

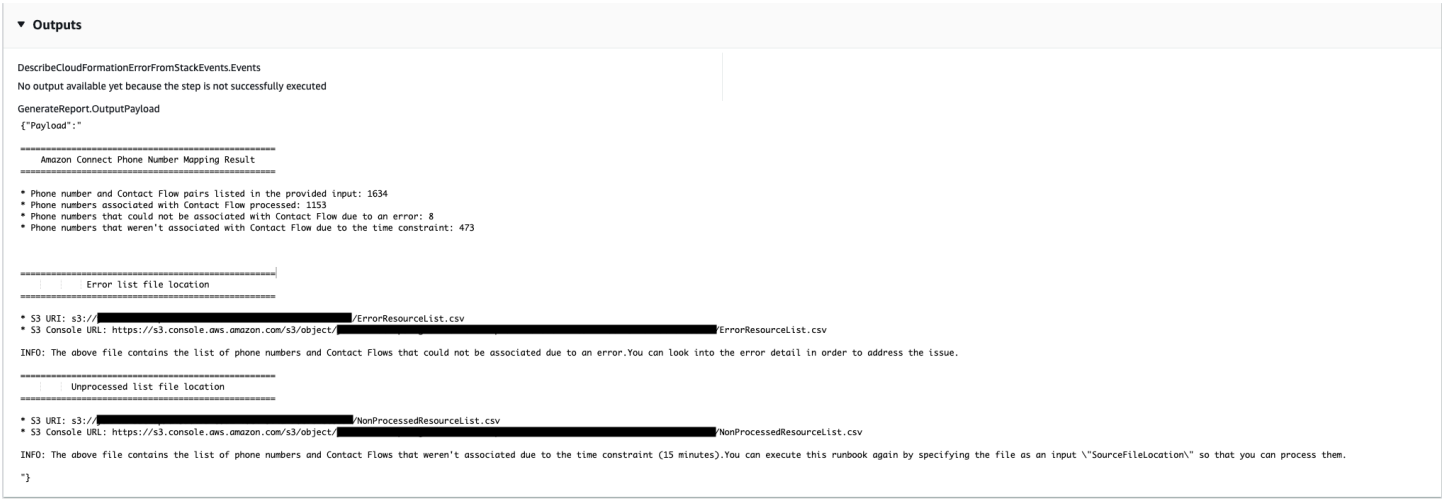
   - DescribeCloudFormationErrorFromStackEvents.Ereignisse

     Ausgabe, die AWS CloudFormation Stack-Ereignisse anzeigt, falls der `AssociatePhoneNumbersToContactFlows` Schritt fehlschlägt.

Ausgabe der Ausführung mit einer kleinen Anzahl von Telefonnummern und Kontaktabläufen




Ergebnis der Ausführung mit einer großen Anzahl von Telefonnummern und Kontaktabläufen sowie Telefonnummern, die aufgrund eines Fehlers oder einer Zeitbeschränkung nicht verknüpft wurden




Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

# AWS Directory Service

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS Directory Service Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-CreateDSManagementInstance
- AWSSupport-TroubleshootADConnectorConnectivity
- AWSSupport-TroubleshootDirectoryTrust

## AWS-CreateDSManagementInstance

Beschreibung

Das `AWS-CreateDSManagementInstance` Runbook erstellt eine Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instance, mit der Sie Ihr Verzeichnis verwalten können. AWS Directory Service Die Verwaltungsinstanz kann nicht zur Verwaltung von AD Connector-Verzeichnissen verwendet werden.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Ein Id

  Typ: Zeichenfolge

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

Beschreibung: (Erforderlich) Die ID der Amazon Machine Image (AMI), die Sie zum Starten der Verwaltungsinstanz verwenden möchten.

- DirectoryId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AWS Directory Service Verzeichnisses, das Sie verwalten möchten. Die Instanz wird mit dem von Ihnen angegebenen Verzeichnis verknüpft.

- IamInstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der von Ihnen angegebene Name wird auf das IAM-Instanzprofil angewendet, das durch die Automatisierung erstellt und an die Verwaltungsinstanz angehängt wird.

- InstanceType

  Typ: Zeichenfolge

  Standard: t3.medium

  Zulässige Werte:

  - 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

Beschreibung: (Erforderlich) Der Instance-Typ, den Sie starten möchten.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselpaar, das beim Erstellen der Instanz verwendet werden soll. Wenn Sie keinen Wert angeben, ist der Instanz kein Schlüsselpaar zugeordnet.

- RemoteAccessCidr

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der CIDR-Block, von dem aus Sie RDP-Verkehr (Port 3389) zulassen möchten. Der von Ihnen angegebene CIDR-Block wird auf eine eingehende Regel angewendet, die der durch die Automatisierung erstellten Sicherheitsgruppe hinzugefügt wird.

- SecurityGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der von Ihnen angegebene Name wird auf die Sicherheitsgruppe angewendet, die durch die Automatisierung erstellt und der Verwaltungsinstanz zugeordnet ist.

- Tags (Markierungen)

  Typ: MapList

  Beschreibung: (Optional) Ein Schlüssel-Wert-Paar, das Sie auf die durch die Automatisierung erstellten Ressourcen anwenden möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeAwsApi- Sammelt Details über das Verzeichnis, das Sie im DirectoryId Parameter angeben.
- aws:executeAwsApi- Ruft den CIDR-Block der Virtual Private Cloud (VPC) ab, in der das Verzeichnis gestartet wurde.
- aws:executeAwsApi- Erstellt eine Sicherheitsgruppe mit dem Wert, den Sie im SecurityGroupName Parameter angeben.
- aws:executeAwsApi- Erstellt eine eingehende Regel für die neu erstellte Sicherheitsgruppe, die RDP-Verkehr von dem CIDR zulässt, den Sie im Parameter angeben. RemoteAccessCidr
- aws:executeAwsApi- Erstellt eine IAM-Rolle und ein Instanzprofil mithilfe des Werts, den Sie im IamInstanceProfileName Parameter angeben.
- aws:executeAwsApi- Startet eine Amazon EC2-Instance auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.
- aws:executeAwsApi- Erstellt ein AWS Systems Manager Dokument, um die neu gestartete Instanz mit Ihrem Verzeichnis zu verbinden.
- aws:runCommand- Fügt die neue Instanz Ihrem Verzeichnis hinzu.
- aws:runCommand- Installiert Tools zur Remote-Serververwaltung auf der neuen Instanz.

## AWSSupport-TroubleshootADConnectorConnectivity

Beschreibung

Das AWSSupport-TroubleshootADConnectorConnectivity Runbook überprüft die folgenden Voraussetzungen für einen AD Connector:

- Prüft, ob der erforderliche Datenverkehr gemäß den Regeln der Sicherheitsgruppe und der Network Access Control List (ACL) zulässig ist, die Ihrem AD Connector zugeordnet sind.
- Prüft AWS Systems ManagerAWS Security Token Service, ob die VPC-Endpunkte der CloudWatch Amazon-Schnittstelle in derselben Virtual Private Cloud (VPC) wie der AD Connector vorhanden sind.

Wenn die erforderlichen Prüfungen erfolgreich abgeschlossen wurden, startet das Runbook zwei Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro-Instances in denselben Subnetzen wie Ihr AD Connector. Netzwerkkonnektivitätstests werden dann mit den `nslookup` Dienstprogrammen `netcat` und durchgeführt.

Diese Automatisierung ausführen (Konsole)

> **Important**
>
> Bei Verwendung dieses Runbooks können zusätzliche Kosten AWS-Konto für Ihre Amazon EC2-Instances, Amazon Elastic Block Store-Volumes und Amazon Machine Image (AMI) anfallen, die während der Automatisierung erstellt wurden. Weitere Informationen finden Sie unter Amazon Elastic Compute Cloud — Preise und Amazon Elastic Block Store — Preise. Wenn der `aws:deletestack` Schritt fehlschlägt, rufen Sie die AWS CloudFormation Konsole auf, um den Stapel manuell zu löschen. Der von diesem Runbook erstellte Stackname beginnt mit`AWSSupport-TroubleshootADConnectorConnectivity`. Informationen zum Löschen von AWS CloudFormation Stacks finden Sie im AWS CloudFormationBenutzerhandbuch unter Löschen eines Stacks.

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DirectoryId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AD Connector-Verzeichnisses, zu dem Sie Verbindungsprobleme beheben möchten.

- Ec2 InstanceProfile

  Typ: Zeichenfolge

  Maximale Anzahl Zeichen: 128

  Beschreibung: (Erforderlich) Der Name des Instanzprofils, das Sie den Instances zuweisen möchten, die zur Durchführung von Konnektivitätstests gestartet werden. Dem von Ihnen angegebenen Instanzprofil müssen die `AmazonSSMManagedInstanceCore` Richtlinie oder gleichwertige Berechtigungen beigefügt sein.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:assertAwsResourceProperty— Bestätigt, dass es sich bei dem im DirectoryId Parameter angegebenen Verzeichnis um einen AD-Connector handelt.
- aws:executeAwsApi- Sammelt Informationen über den AD Connector.
- aws:executeAwsApi- Sammelt Informationen über die Sicherheitsgruppen, die dem AD Connector zugeordnet sind.
- aws:executeAwsApi- Sammelt Informationen über die Netzwerk-ACL-Regeln, die den Subnetzen für den AD Connector zugeordnet sind.
- aws:executeScript- Wertet die AD Connector-Sicherheitsgruppenregeln aus, um sicherzustellen, dass der erforderliche ausgehende Datenverkehr zulässig ist.
- aws:executeScript- Wertet die AD Connector-Netzwerk-ACL-Regeln aus, um sicherzustellen, dass der erforderliche ausgehende und eingehende Netzwerkverkehr zulässig ist.
- aws:executeScript- PrüftAWS Systems Manager, ob die Endpunkte der CloudWatch Amazon-Schnittstelle AWS Security Token Service und die Amazon-Schnittstelle in derselben VPC wie der AD Connector vorhanden sind.

- `aws:executeScript`- Kompiliert die Ergebnisse der in den vorherigen Schritten durchgeführten Prüfungen.
- `aws:branch`- Zweigt die Automatisierung in Abhängigkeit von der Leistung der vorherigen Schritte ab. Die Automatisierung stoppt hier, wenn die erforderlichen Regeln für ausgehende und eingehende Nachrichten für die Sicherheitsgruppen und Netzwerk-ACLs fehlen.
- `aws:createStack`- Erstellt einen AWS CloudFormation Stack zum Starten von Amazon EC2-Instances zur Durchführung von Konnektivitätstests.
- `aws:executeAwsApi`- Erfasst die IDs neu gestarteter Amazon EC2-Instances.
- `aws:waitForAwsResourceProperty`— Wartet darauf, dass die erste neu gestartete Amazon EC2-Instance als verwaltet von gemeldet wird. AWS Systems Manager
- `aws:waitForAwsResourceProperty`— Wartet darauf, dass die zweite neu gestartete Amazon EC2-Instance als verwaltet von gemeldet wird. AWS Systems Manager
- `aws:runCommand`- Führt von der ersten Amazon EC2-Instance aus Netzwerkkonnektivitätstests zu den lokalen DNS-Server-IP-Adressen durch.
- `aws:runCommand`- Führt von der zweiten Amazon EC2-Instance aus Netzwerkkonnektivitätstests zu den lokalen DNS-Server-IP-Adressen durch.
- `aws:changeInstanceState`— Stoppt die Amazon EC2-Instances, die für die Konnektivitätstests verwendet werden.
- `aws:deleteStack`- Löscht den AWS CloudFormation Stapel.
- `aws:executeScript`- Gibt Anweisungen zum manuellen Löschen des AWS CloudFormation Stacks aus, wenn die Automatisierung den Stapel nicht löschen kann.

## AWSSupport-TroubleshootDirectoryTrust

Beschreibung

Das `AWSSupport-TroubleshootDirectoryTrust` Runbook diagnostiziert Probleme bei der Vertrauensbildung zwischen einem AWS Managed Microsoft AD und einem Microsoft Active Directory. Die Automatisierung stellt sicher, dass der Verzeichnistyp Vertrauensstellungen unterstützt, und überprüft dann die zugehörigen Sicherheitsgruppenregeln, Netzwerkzugriffskontrolllisten (Network Access Control Lists, Netzwerk-ACLs) und Routing-Tabellen auf potenzielle Verbindungsprobleme.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DirectoryId

  Typ: Zeichenfolge

  Zulässiges Muster: ^d- [a-z0-9] {10} $

  Beschreibung: (Erforderlich) Die ID des AWS Managed Microsoft AD für die Fehlerbehebung.
- RemoteDomainCidrs

  Typ: StringList

  Zulässiges Muster: ^ (([0-9] | [1-9] [0-9] {2} |2 [0-4] [0-9] |25 [0-5])\.) {3} ([0-9] | [1-9] [0-9] [0-9] {2} |2 [0-4] [0-4] [0-9] |25 [0-5]) (\/(3 [0-2] | [1-2] [0-9] | [1-9])) $

  Beschreibung: (Erforderlich) Die CIDR(s) der Remotedomäne, mit der Sie eine Vertrauensstellung einrichten möchten. Sie können mehrere CIDRs mit durch Kommata getrennten Werten hinzufügen. Zum Beispiel 172.31.48.0/20, 192.168.1.10/32.
- RemoteDomainName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der vollqualifizierte Domänenname der Remotedomäne, mit der Sie eine Vertrauensstellung einrichten.

- RequiredTrafficACL

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Standardportanforderungen für AWS Managed Microsoft AD. In den meisten Fällen sollten Sie den Standardwert nicht ändern.

  Standard: {"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

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Standardportanforderungen für AWS Managed Microsoft AD. In den meisten Fällen sollten Sie den Standardwert nicht ändern.

  Standard: {"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

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Vertrauensstellung für die Fehlerbehebung.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ds:DescribeConditionalForwarders`
- `ds:DescribeDirectories`
- `ds:DescribeTrusts`
- `ds:ListIpRoutes`

- ec2:DescribeNetworkAcls
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

Dokumentschritte

- aws:assertAwsResourceProperty- Bestätigt, dass der Verzeichnistyp istAWS Managed Microsoft AD.
- aws:executeAwsApi- Erhält Informationen über dieAWS Managed Microsoft AD.
- aws:branch- Zweigt die Automatisierung ab, wenn ein Wert für den TrustId Eingabeparameter angegeben wird.
- aws:executeAwsApi- Ruft Informationen über das Vertrauensverhältnis ab.
- aws:executeAwsApi- Ruft die Conditional Forwarder-DNS-IP-Adressen für die RemoteDomainName ab.
- aws:executeAwsApi- Ruft Informationen über IP-Routen ab, die dem hinzugefügt wurdenAWS Managed Microsoft AD.
- aws:executeAwsApi- Ruft die CIDRs der AWS Managed Microsoft AD Subnetze ab.
- aws:executeAwsApi- Ruft Informationen über die Sicherheitsgruppen ab, die dem zugeordnet sindAWS Managed Microsoft AD.
- aws:executeAwsApi- Ruft Informationen über die Netzwerk-ACLs ab, die mit dem AWS Managed Microsoft AD verknüpft sind.
- aws:executeScript- Bestätigt, dass RemoteDomainCidrs es sich um gültige Werte handelt. Bestätigt, dass der AWS Managed Microsoft AD über bedingte Weiterleitungen für die RemoteDomainCidrs verfügt und dass die erforderlichen IP-Routen zu den IP-Adressen hinzugefügt wurden, AWS Managed Microsoft AD falls es sich um Nicht-RFC 1918-IP-Adressen RemoteDomainCidrs handelt.
- aws:executeScript- Wertet die Regeln für Sicherheitsgruppen aus.
- aws:executeScript- Wertet Netzwerk-ACLs aus.

Ausgaben

evalDirectorySecuritygroup.output — Ergebnisse der Bewertung, ob die mit der verknüpften Sicherheitsgruppenregeln den für die AWS Managed Microsoft AD Vertrauensbildung erforderlichen Datenverkehr zulassen.

evalAclEntries.output — Ergebnisse aus der Bewertung, ob die mit dem verknüpften Netzwerk-ACLs den für die Vertrauensbildung erforderlichen Datenverkehr AWS Managed Microsoft AD zulassen.

evaluateRemoteDomaincidr.Output — Ergebnisse der Bewertung, ob es sich um gültige Werte `RemoteDomainCidrs` handelt. Bestätigt, dass der AWS Managed Microsoft AD über bedingte Weiterleitungen für die `RemoteDomainCidrs` verfügt und dass die erforderlichen IP-Routen zu den IP-Adressen hinzugefügt wurden, AWS Managed Microsoft AD falls es sich um Nicht-RFC 1918-IP-Adressen `RemoteDomainCidrs` handelt.

# AWS AppSync

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS AppSync Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableAppSyncGraphQLApiLogging

## `AWS-EnableAppSyncGraphQLApiLogging`

Beschreibung

Das `AWS-EnableAppSyncGraphQLApiLogging` Runbook aktiviert die Protokollierung auf Feldebene und die Protokollierung auf Anforderungsebene für die von Ihnen angegebene AWS AppSync GraphQL-API. Das Runbook wendet Änderungen auf die angegebene GraphQL-API an, auch wenn die Protokollierung bereits aktiviert ist.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ApiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der API, für die Sie die Protokollierung aktivieren möchten.
- FieldLogLevel

  Typ: Zeichenfolge

  Zulässige Werte: FEHLER | ALLE

  Beschreibung: (Erforderlich) Die Feldprotokollierungsebene.
- CloudWatchLogsRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Servicerolle, die AWS AppSync übernimmt, um in Amazon CloudWatch Logs zu veröffentlichen.
- ExcludeVerboseContent

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Setzen Sie auf , `True` um Informationen wie Header, Kontext und ausgewertete Zuweisungsvorlagen unabhängig von der Protokollierungsebene auszuschließen.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- aws:executeAwsApi - Sammelt den Authentifizierungstyp und die Konfigurationsinformationen, die für den primären Authentifizierungstyp relevant sind.
- aws:branch – Verzweigungen basierend auf dem Authentifizierungstyp.
- aws:executeAwsApi - Aktualisiert die Protokollierungskonfiguration für die AWS AppSync GraphQL-API basierend auf den Werten, die für die Eingabeparameter des Runbooks angegeben sind.

Ausgaben

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Antwort auf den -`UpdateGraphqlApi`Aufruf.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Antwort auf den -`UpdateGraphqlApi`Aufruf.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Antwort auf den -`UpdateGraphqlApi`Aufruf.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Antwort auf den -`UpdateGraphqlApi`Aufruf.

# Amazon Athena

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Athena bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



# AWS-EnableAthenaWorkGroupEncryptionAtRest

Beschreibung

Das `AWS-EnableAthenaWorkGroupEncryptionAtRest` Runbook ermöglicht die Verschlüsselung im Ruhezustand für die von Ihnen angegebene Amazon Athena-Arbeitsgruppe.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- WorkGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Arbeitsgruppe, für die Sie die Verschlüsselung im Ruhezustand aktivieren möchten.

- EncryptionOption

  Typ: Zeichenfolge

  Zulässige Werte: SSE_S3 | SSE_KMS | CSE_KMS

  Beschreibung: (Erforderlich) Gibt an, welche Verschlüsselungsoption verwendet wird. Sie können die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE_S3), die serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln (SSE_KMS) oder die clientseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln (CSE_KMS) wählen.

- KmsKeyId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn Sie eine AWS KMSVerschlüsselungsoption verwenden, geben Sie den Schlüssel-ARN, die Schlüssel-ID oder den Schlüsselalias des Schlüssels an, den Sie verwenden möchten.

- EnableMinimumEncryptionConfiguration

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Erzwingt eine minimale Verschlüsselungsstufe für die Arbeitsgruppe für Abfrage- und Berechnungsergebnisse, die in Amazon S3 geschrieben werden. Wenn diese Option aktiviert ist, können Arbeitsgruppenbenutzer die Verschlüsselung nur auf die vom Administrator festgelegte Mindestebene oder höher festlegen, wenn sie Abfragen senden. Diese Einstellung gilt nicht für Spark-fähige Arbeitsgruppen.

- EnforceWorkGroupConfiguration

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Wenn auf festgelegt`True`, überschreiben die Einstellungen für die Arbeitsgruppe clientseitige Einstellungen. Wenn auf festgelegt`False`, werden clientseitige Einstellungen verwendet.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- aws:branch – Verzweigungen basierend auf der im `EncryptionOption` Parameter angegebenen Verschlüsselungsoption.
- aws:executeAwsApi - Dieser Schritt aktualisiert die Athena-Arbeitsgruppe mit der angegebenen Verschlüsselungseinstellung.
- aws:executeAwsApi - Aktualisiert die Athena-Arbeitsgruppe mit der angegebenen Verschlüsselungseinstellung.
- aws:assertAwsResourceProperty - Prüft, ob die Verschlüsselung für die Arbeitsgruppe aktiviert wurde.

# DynamoDB

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon DynamoDB bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

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

- AWS-RestoreDynamoDBTable

## AWS-ChangeDDBRWCapacityMode

Beschreibung

Das AWS-ChangeDDBRWCapacityMode Runbook ändert den Lese-/Schreibkapazitätsmodus für eine oder mehrere Amazon DynamoDB (DynamoDB)-Tabellen entweder in den On-Demand-Modus oder den bereitgestellten Modus.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- CapacityMode

  Typ: Zeichenfolge

  Gültige Werte: PROVISIONED | PIFN_PER_REQUEST

  Beschreibung: (Erforderlich) Der gewünschte Lese-/Schreibkapazitätsmodus. Beim Wechsel von On-Demand(pay-per-request) zu bereitgestellter Kapazität müssen anfänglich bereitgestellte

Kapazitätswerte festgelegt werden. Die anfänglichen bereitgestellten Kapazitätswerte werden auf der Grundlage der verbrauchten Lese- und Schreibkapazität Ihrer Tabelle und globalen sekundären Indizes in den letzten 30 Minuten geschätzt.

- ReadCapacityUnits

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Strongly-Consistent-Lesevorgängen pro Sekunde, bevor DynamoDB eine Drosselungsausnahme zurückgibt.

- TableNames

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Durch Kommata getrennte Liste von DynamoDB-Tabellennamen, für die der Lese-/Schreibkapazitätsmodus geändert werden soll.

- WriteCapacityUnits

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Schreibvorgängen pro Sekunde, bevor DynamoDB eine Drosselungsausnahme zurückgibt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript` – Ändert den Lese-/Schreibkapazitätsmodus für die im `TableNames` Parameter angegebenen DynamoDB-Tabellen.

Ausgaben

ChangeDDBRWCapacityMode .SuccessesTables - Liste der DynamoDB-Tabellennamen, bei denen der Kapazitätsmodus erfolgreich geändert wurde

ChangeDDBRWCapacityMode .FailedTables - Maplist von DynamoDB-Tabellennamen, bei der das Ändern des Kapazitätsmodus fehlgeschlagen ist und der Grund für den Fehler.

## AWS-CreateDynamoDBBackup

Beschreibung

Erstellen Sie eine Sicherungskopie einer Amazon DynamoDB-Tabelle.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BackupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name der zu erstellenden Sicherung.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name der DynamoDB-Tabelle.

## AWS-DeleteDynamoDbBackup

Beschreibung

Löschen Sie das Backup einer Amazon DynamoDB-Tabelle.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BackupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ARN der zu löschenden DynamoDB-Tabelle-Sicherung.

## AWSConfigRemediation-DeleteDynamoDbTable

Beschreibung

Das `AWSConfigRemediation-DeleteDynamoDbTable` Runbook löscht die von Ihnen angegebene Amazon DynamoDB-Tabelle (DynamoDB).

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Löscht die im Parameter angegebene DynamoDB-Tabelle. `TableName`
- `aws:executeScript`— Überprüft, ob die DynamoDB-Tabelle gelöscht wurde.

## AWS-DeleteDynamoDbTableBackups

Beschreibung

Löschen Sie DynamoDB-Tabellen-Backups auf der Grundlage der Aufbewahrungstage oder der Anzahl.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- RetentionCount

  Typ: Zeichenfolge

  Standard: 10

  Beschreibung: (Optional) Die Anzahl der Sicherungen, die für die Tabelle aufbewahrt werden sollen. Wenn mehr als die angegebene Anzahl von Sicherungen vorhanden ist, werden die ältesten Sicherungen jenseits dieser Zahl gelöscht. Entweder RetentionCount oder RetentionDays kann verwendet werden, nicht beides.

- RetentionDays

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Tage für die Aufbewahrung von Sicherungen für die Tabelle. Sicherungen, die älter als die angegebene Zahl von Tagen sind, werden gelöscht. Entweder RetentionCount oder RetentionDays kann verwendet werden, nicht beides.

- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name der DynamoDB-Tabelle.

## AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Beschreibung

Das `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` Runbook verschlüsselt eine Amazon DynamoDB (DynamoDB)-Tabelle mit dem vom Kunden verwalteten Schlüssel AWS Key Management Service (AWS KMS), den Sie für den `KMSKeyId` Parameter angeben.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- KMSKeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln der DynamoDB-Tabelle verwenden möchten, die Sie im `TableName` Parameter angeben.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, die Sie verschlüsseln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi` – Verschlüsselt die DynamoDB-Tabelle, die Sie im `TableName` Parameter angeben.
- `aws:waitForAwsResourceProperty` – Prüft, ob die `true` -`Enabled`Eigenschaft für die DynamoDB-Tabelle auf festgelegt `SSESpecification` ist.
- `aws:assertAwsResourceProperty` – Prüft, ob die DynamoDB-Tabelle mit dem vom Kunden verwalteten Schlüssel verschlüsselt ist, der im `KMSKeyId` Parameter angegeben ist.

## `AWSConfigRemediation-EnablePITRForDynamoDbTable`

Beschreibung

Das `AWSConfigRemediation-EnablePITRForDynamoDbTable` Runbook ermöglicht die point-in-time Wiederherstellung (PITR) in der von Ihnen angegebenen Amazon DynamoDB-Tabelle.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, für die die point-in-time Wiederherstellung aktiviert werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die point-in-time Wiederherstellung der DynamoDB-Tabelle, die Sie im `TableName` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die point-in-time Wiederherstellung in der DynamoDB-Tabelle aktiviert ist.

## AWS-EnableDynamoDbAutoscaling

Beschreibung

Das `AWS-EnableDynamoDbAutoscaling` Runbook aktiviert Application Auto Scaling für die von Ihnen angegebene Amazon-DynamoDB-Tabelle mit bereitgestellter Kapazität. Application Auto

Scaling passt die bereitgestellte Durchsatzkapazität dynamisch an Datenverkehrsmuster an. Weitere Informationen finden Sie unter Automatisches Verwalten der Durchsatzkapazität mit DynamoDB-Auto-Scaling im Amazon-DynamoDB-Entwicklerhandbuch.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, für die Sie Application Auto Scaling aktivieren möchten.
- MinReadCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Mindestanzahl der Lesekapazitätseinheiten für den bereitgestellten Durchsatz für die DynamoDB-Tabelle.
- MaxReadCapacity

  Typ: Ganzzahl

Beschreibung: (Erforderlich) Die maximale Anzahl von Lesekapazitätseinheiten mit bereitgestelltem Durchsatz für die DynamoDB-Tabelle.

- TargetReadCapacityUtilization

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die gewünschte Auslastung der Lesekapazität des Ziels. Die Zielauslastung ist der Prozentsatz des verbrauchten bereitgestellten Durchsatzes zu einem bestimmten Zeitpunkt. Sie können die Zielauslastungswerte für die automatische Skalierung zwischen 20 und 90 Prozent festlegen.

- ReadScaleOutCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeit in Sekunden, die gewartet wird, bis eine vorherige Skalierung der Lesekapazität wirksam wird.

- ReadScaleInCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeit in Sekunden nach Abschluss einer Scale-In-Aktivität der Lesekapazität, bevor eine weitere Scale-In-Aktivität gestartet werden kann.

- MinWriteCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Mindestanzahl von Schreibeinheiten für den bereitgestellten Durchsatz für die DynamoDB-Tabelle.

- MaxWriteCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die maximale Anzahl von Schreibeinheiten für den bereitgestellten Durchsatz für die DynamoDB-Tabelle.

- TargetWriteCapacityUtilization

  Typ: Ganzzahl

Beschreibung: (Erforderlich) Die gewünschte Ziel-Schreibkapazitätsauslastung. Die Zielauslastung ist der Prozentsatz des verbrauchten bereitgestellten Durchsatzes zu einem bestimmten Zeitpunkt. Sie können die Zielauslastungswerte für die automatische Skalierung zwischen 20 und 90 Prozent festlegen.

- WriteScaleOutCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeit in Sekunden, die gewartet wird, bis eine vorherige Skalierung der Schreibkapazität wirksam wird.

- WriteScaleInCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeit in Sekunden nach Abschluss einer Scale-In-Aktivität der Schreibkapazität, bevor eine weitere Scale-In-Aktivität gestartet werden kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi) – Konfiguriert Application Auto Scaling für die von Ihnen angegebene DynamoDB-Tabelle.
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep) – Ruhezustände, um eine API-Drosselung zu vermeiden.
- PutScalingPolicyWrite (aws:executeAwsApi) – Konfiguriert die Auslastung der Zielschreibkapazität für die DynamoDB-Tabelle.

- PutScalingPolicyWriteDelay (aws:sleep) – Ruhezustände, um eine API-Drosselung zu vermeiden.
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi) – Konfiguriert minimale und maximale Lesekapazitätseinheiten für die DynamoDB-Tabelle.
- RegisterAppAutoscalingTargetReadDelay (aws:sleep) – Ruhezustände, um eine API-Drosselung zu vermeiden.
- PutScalingPolicyRead (aws:executeAwsApi) – Konfiguriert die Auslastung der Lesekapazität für die DynamoDB-Tabelle.
- VerifyDynamoDbAutoscalingEnabled (aws:executeScript ) – Prüft, ob Application Auto Scaling für die DynamoDB-Tabelle entsprechend den von Ihnen angegebenen Werten aktiviert ist.

Ausgaben

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

## AWS-RestoreDynamoDBTable

Beschreibung

Das `AWS-RestoreDynamoDBTable` Runbook stellt die Amazon DynamoDB-Tabelle wieder her, die Sie mithilfe der point-in-time Wiederherstellung (PITR) angeben.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EnablePointInTimeRecoverAsNeeded

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Legt fest, ob die Automatisierung die point-in-time Wiederherstellung bei Bedarf aktiviert, um die Tabelle wiederherzustellen.
- GlobalSecondaryIndexOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die neuen globalen Sekundärindizes ersetzen die vorhandenen sekundären Indizes für die neue Tabelle.
- LocalSecondaryIndexOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die neuen lokalen Sekundärindizes ersetzen die vorhandenen sekundären Indizes für die neue Tabelle.
- RestoreDateTime

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die point-in-time Wiederherstellung, auf die Sie Ihre Tabelle in den letzten 35 Tagen wiederherstellen möchten. Geben Sie Datum und Uhrzeit im folgenden Format an: `DD/MM/YYYY HH:MM:SS`
- SourceTableArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der Tabelle, die Sie wiederherstellen möchten.

- SseSpecificationOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die serverseitigen Verschlüsselungseinstellungen, die für die neue Tabelle verwendet werden sollen.

- TargetTableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der wiederherzustellenden Tabelle.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Dokumentschritte

- `aws:executeScript`- Stellt mithilfe der Wiederherstellung die DynamoDB-Tabelle wieder her, die Sie im `TargetTableName` Parameter angeben. point-in-time

# Amazon EBS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Block Store bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWSSupport-AnalyzeEBSResourceUsage

Beschreibung

Das `AWSSupport-AnalyzeEBSResourceUsage` Automation Runbook wird verwendet, um die Ressourcennutzung im Amazon Elastic Block Store (Amazon EBS) zu analysieren. Es analysiert die Datenträgernutzung und identifiziert aufgegebene Volumes, Bilder und Snapshots in einer bestimmten Region. AWS

Wie funktioniert es?

Das Runbook führt die folgenden vier Aufgaben aus:

1. Überprüft, ob ein Amazon Simple Storage Service (Amazon S3) -Bucket existiert, oder erstellt einen neuen Amazon S3-Bucket.
2. Sammelt alle Amazon EBS-Volumes im verfügbaren Status.
3. Sammelt alle Amazon EBS-Snapshots, für die das Quellvolume gelöscht wurde.
4. Sammelt alle Amazon Machine Images (AMIs), die nicht von nicht terminierten Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwendet werden.

Das Runbook generiert CSV-Berichte und speichert sie in einem vom Benutzer bereitgestellten Amazon S3 S3-Bucket. Der bereitgestellte Bucket sollte gemäß den am Ende beschriebenen bewährten AWS Sicherheitsmethoden gesichert werden. Wenn der vom Benutzer angegebene Amazon S3 S3-Bucket nicht im Konto vorhanden ist, erstellt das Runbook einen neuen Amazon S3 S3-Bucket im Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten Schlüssel AWS Key Management Service (AWS KMS), mit aktivierter Objektversionierung, blockiertem öffentlichen Zugriff und erfordert Anfragen zur Verwendung von SSL/TLS.

Wenn Sie Ihren eigenen Amazon S3 S3-Bucket angeben möchten, stellen Sie bitte sicher, dass er gemäß den folgenden bewährten Methoden konfiguriert ist:

- Sperren Sie den öffentlichen Zugriff auf den Bucket (eingestellt `IsPublic` auf`False`).
- Aktivieren Sie die Amazon S3 S3-Zugriffsprotokollierung.
- Erlauben Sie nur SSL-Anfragen an Ihren Bucket.
- Aktivieren Sie die Objektversionierung.
- Verwenden Sie einen Schlüssel AWS Key Management Service (AWS KMS), um Ihren Bucket zu verschlüsseln.

> **Important**
>
> Bei der Verwendung dieses Runbooks können zusätzliche Gebühren für Ihr Konto für die Erstellung von Amazon S3 S3-Buckets und -Objekten anfallen. Weitere Informationen zu den möglicherweise anfallenden Gebühren finden Sie unter Amazon S3 S3-Preise.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

  Typ: `AWS::S3::Bucket::Name`

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket in Ihrem Konto, in den der Bericht hochgeladen werden soll. Stellen Sie sicher, dass die Bucket-Richtlinie Parteien, die keinen Zugriff auf die gesammelten Protokolle benötigen, keine unnötigen Lese-/Schreibberechtigungen gewährt. Wenn der angegebene Bucket nicht im Konto vorhanden ist, erstellt die Automatisierung einen neuen Bucket in der Region, in der die Automatisierung initiiert wird, mit dem Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten AWS KMS Schlüssel.

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

- CustomerManagedKmsKeyArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der benutzerdefinierte AWS KMS Schlüssel Amazon Resource Name (ARN) zur Verschlüsselung des neuen Amazon S3 S3-Buckets, der erstellt wird, wenn der angegebene Bucket nicht im Konto vorhanden ist. Die Automatisierung schlägt fehl, wenn versucht wird, einen Bucket ohne Angabe eines benutzerdefinierten AWS KMS Schlüssel-ARN zu erstellen.

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

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispielrichtlinie mit mindestens erforderlichen IAM-Berechtigungen zum Ausführen dieses Runbooks:

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

Anweisungen

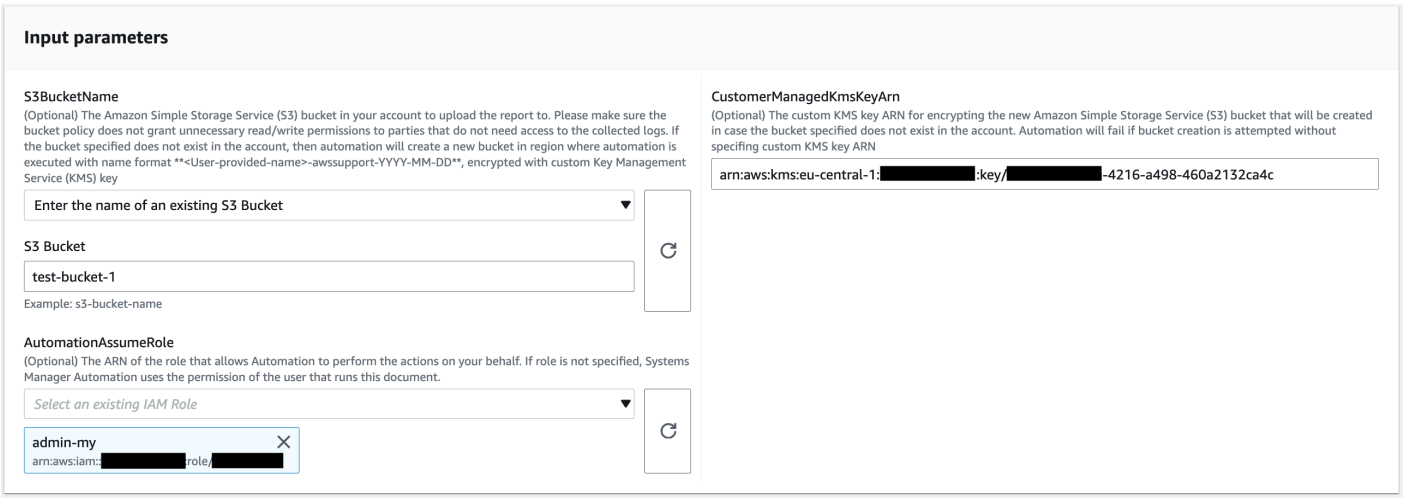
Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie in der Konsole zu AWSSupport-AnalyzeEBS. ResourceUsage AWS Systems Manager
2. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - S3 BucketName (erforderlich):

     Der Amazon S3 S3-Bucket in Ihrem Konto, in den Sie den Bericht hochladen möchten.
   - CustomerManagedKmsKeyArn (Fakultativ):

     Der benutzerdefinierte AWS KMS Schlüssel Amazon Resource Name (ARN) für die Verschlüsselung des neuen Amazon S3 S3-Buckets, der erstellt wird, wenn der angegebene Bucket nicht im Konto vorhanden ist.



3. Wählen Sie Ausführen aus.
4. Die Automatisierung wird eingeleitet.
5. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - Parallelität prüfen:

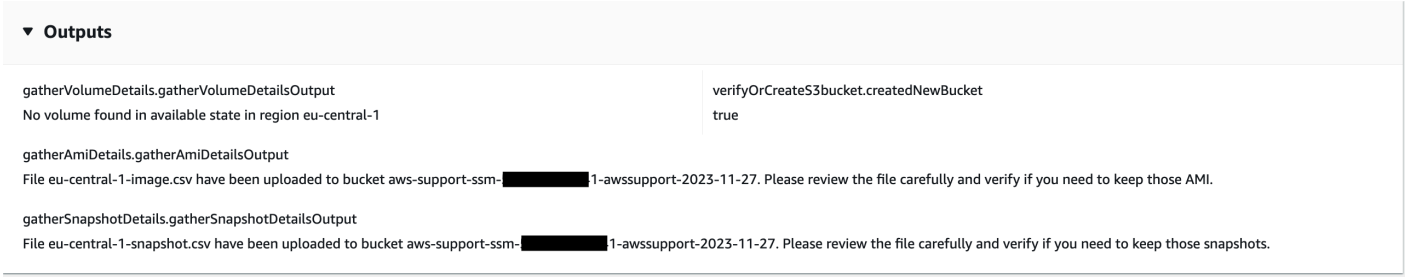
     Stellt sicher, dass dieses Runbook in der Region nur einmal initiiert wird. Wenn das Runbook feststellt, dass gerade eine weitere Ausführung ausgeführt wird, gibt es einen Fehler zurück und wird beendet.
   - verifizieren Sie OrCreate S3Bucket:

     Überprüft, ob der Amazon S3 S3-Bucket existiert. Wenn nicht, erstellt es einen neuen Amazon S3 S3-Bucket in der Region, in der die Automatisierung initiiert wird, mit dem Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten AWS KMS Schlüssel.
   - sammelnAmiDetails:

     Sucht nach AMIs, die von keiner Amazon EC2 EC2-Instance verwendet werden, generiert den Bericht im Namensformat `<region>-images.csv` und lädt ihn in den Amazon S3 S3-Bucket hoch.
   - sammeln: VolumeDetails

     Überprüft Amazon EBS-Volumes im verfügbaren Status, generiert den Bericht im Namensformat `<region>-volume.csv` und lädt ihn in einen Amazon S3 S3-Bucket hoch.
   - sammeln: SnapshotDetails

     Sucht nach den Amazon EBS-Snapshots der Amazon EBS-Volumes, die bereits gelöscht wurden, generiert den Bericht mit dem Namensformat und lädt ihn in den Amazon `<region>-snapshot.csv` S3 S3-Bucket hoch.
6. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

## AWS-ArchiveEBSSnapshots

Beschreibung

Das `AWS-ArchiveEBSSnapshots` Runbook hilft Ihnen beim Archivieren von Snapshots für Amazon Elastic Block Store (Amazon EBS) -Volumes, indem es das Tag angibt, das Sie auf Ihre Snapshots angewendet haben. Alternativ können Sie die ID eines Volumes angeben, wenn Ihre Snapshots nicht markiert sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Beschreibung

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Beschreibung für den Amazon EBS-Snapshot.
- DryRun

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Überprüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anfrage tatsächlich zu stellen, und gibt eine Fehlermeldung aus.
- RetentionCount

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Snapshots, die Sie archivieren möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für `RetentionDays` angeben.
- RetentionDays

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Snapshots aus früheren Tagen, die Sie archivieren möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für `RetentionCount` angeben.
- SnapshotWithTag

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Gibt an, ob die Snapshots, die Sie archivieren möchten, markiert sind.
- TagKey

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Schlüssel des Tags, das den Snapshots zugewiesen ist, die Sie archivieren möchten.
- TagValue

Typ: Zeichenfolge

Beschreibung: (Optional) Der Wert des Tags, das den Snapshots zugewiesen ist, die Sie archivieren möchten.

- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Volumes, dessen Snapshots Sie archivieren möchten. Verwenden Sie diesen Parameter, wenn Ihre Snapshots nicht markiert sind.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:ArchiveSnapshots`
- `ec2:DescribeSnapshots`

Dokumentschritte

`aws:executeScript`- Archiviert Schnappschüsse mit dem Tag, den Sie mit den `TagValue` Parametern `TagKey` und oder dem `VolumeId` Parameter angeben.

## AWS-AttachEBSVolume

Beschreibung

Hängen Sie ein Amazon Elastic Block Store (Amazon EBS) -Volume an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance an.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Gerät

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Gerätename (z. B. dev/sdh oder xvdh).
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance, der Sie das Volume anfügen möchten.
- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes. Volume und Instance müssen sich in derselben Availability Zone befinden.

## AWSSupport-CalculateEBSPerformanceMetrics

Beschreibung

Das `AWSSupport-CalculateEBSPerformanceMetrics` Runbook hilft bei der Diagnose von Amazon-EBS-Leistungsproblemen, indem es Leistungsmetriken berechnet und in einem CloudWatch Dashboard veröffentlicht. Das Dashboard zeigt die geschätzten durchschnittlichen IOPS und den Durchsatz für ein Amazon EBS-Ziel-Volume oder alle Volumes an, die an die

Amazon Elastic Compute Cloud (Amazon EC2)-Ziel-Instance angefügt sind. Für Amazon EC2-Instances werden auch die durchschnittlichen IOPS und der durchschnittliche Durchsatz der Instance angezeigt. Das Runbook gibt den Link zum neu erstellten CloudWatch Dashboard aus, das die relevanten berechneten CloudWatch Metriken anzeigt. Das CloudWatch Dashboard wird in Ihrem Konto mit dem Namen erstellt: `AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Stellt sicher, dass die angegebenen Zeitstempel gültig sind.
- Überprüft, ob die Ressourcen-ID (Amazon-EBS-Volume oder Amazon EC2-Instance) gültig ist.
- Wenn Sie eine Amazon EC2 als ResourceID bereitstellen, wird ein CloudWatch Dashboard mit der tatsächlichen Gesamtzahl der IOPS/Durchsatz für diese Amazon EC2-Instance und dem Diagramm Geschätzte durchschnittliche IOPS/Durchsatz für alle Amazon EBS-Volumes erstellt, die an eine Amazon EC2-Instance angefügt sind.
- Wenn Sie ein Amazon EBS-Volume als ResourceID angeben, wird ein CloudWatch Dashboard mit dem Diagramm Geschätzter durchschnittlicher IOPS/Durchsatz für dieses Volume erstellt.
- Wenn nach der Generierung des CloudWatch Dashboards der geschätzte durchschnittliche IOPS-Durchsatz bzw. der geschätzte durchschnittliche Durchsatz größer als der maximale IOPS- bzw. Maximaldurchsatz ist, ist Mikrobursting für das Volume bzw. die Volumes möglich, die an eine Amazon EC2-Instance angefügt sind.

> **Note**
>
> Bei burstfähigen Volumes (gp2, sc2 und st1) sollte der maximale IOPS/Durchsatz berücksichtigt werden, bis Sie eine Burst-Balance haben. Nachdem die Burst-Balance vollständig ausgelastet ist, d. h. sie wird null, sollten Sie Basis-IOPS/Durchsatzmetriken berücksichtigen.

> **Important**
>
> Das Erstellen des CloudWatch Dashboards kann zu zusätzlichen Gebühren für Ihr Konto führen. Weitere Informationen finden Sie im Amazon CloudWatch -Preisleitfaden.

[Ausführen dieser Automatisierung (Konsole)]

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Beispielrichtlinie

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

### Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

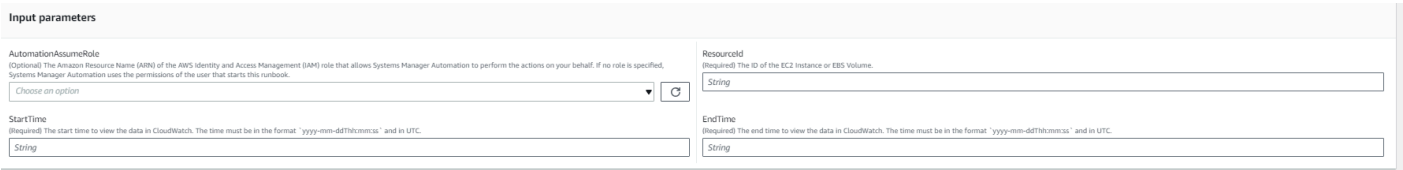
1. Navigieren Sie zu AWSSupport-CalculateEBSPerformanceMetrics in Systems Manager unter Dokumente.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - ResourceID (erforderlich):

     Die ID der Amazon EC2-Instance oder des Amazon-EBS-Volumes.
   - Startzeit (erforderlich):

     Die Startzeit zum Anzeigen der Daten in CloudWatch. Die Uhrzeit muss im Format `yyyy-mm-ddThh:mm:ss` und in UTC vorliegen.
   - Endzeit (erforderlich):

     Die Endzeit zum Anzeigen der Daten in CloudWatch. Die Uhrzeit muss im Format `yyyy-mm-ddThh:mm:ss` und in UTC vorliegen.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckResourceIdAndTimeStamps:

     Prüft um mindestens eine Minute, ob die Endzeit größer als die Startzeit ist und ob die bereitgestellte Ressource vorhanden ist.
   - CreateCloudWatchDashboard:

Berechnet die Amazon EBS-Leistung und zeigt ein Diagramm basierend auf Ihrer Ressourcen-ID an. Wenn Sie eine Amazon-EBS-Volume-ID für den Parameter Resource ID angeben, erstellt dieses Runbook ein Dashboard mit geschätzten durchschnittlichen IOPS und geschätztem durchschnittlichen Durchsatz für das Amazon-EBS-Volume. Wenn Sie eine Amazon EC2-Instance-ID für den Parameter Resource ID angeben, erstellt dieses Runbook ein CloudWatch Dashboard mit durchschnittlicher Gesamt-IOPS und durchschnittlichem Gesamtdurchsatz für Amazon EC2-Instances und mit geschätzten durchschnittlichen IOPS und geschätztem durchschnittlichen Durchsatz für alle Amazon-EBS-Volumes, die an die Amazon EC2-Instance angefügt sind.

7. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten:


Beispiel CloudWatch -Dashboard für Ressourcen-ID als Amazon EC2-Instance

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

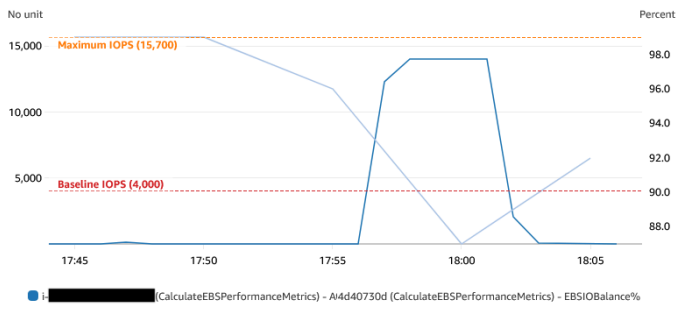
More details on EBS Optimized instances | More details on EBS Volume Types

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

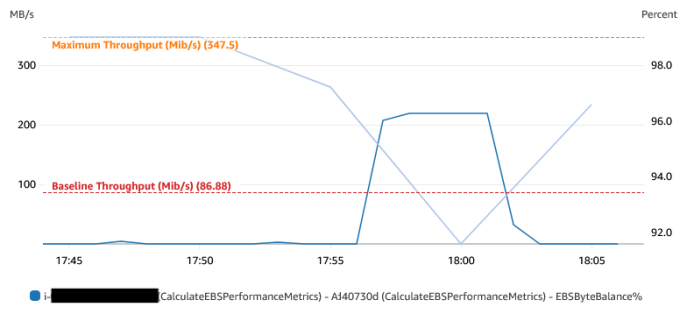
| Calculated Metric | Mathematical Expression | Unit |
|---|---|---|
| Average Total IOPS | SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period | IOPS |
| Average Total Throughput | SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024 | MiB/s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

**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

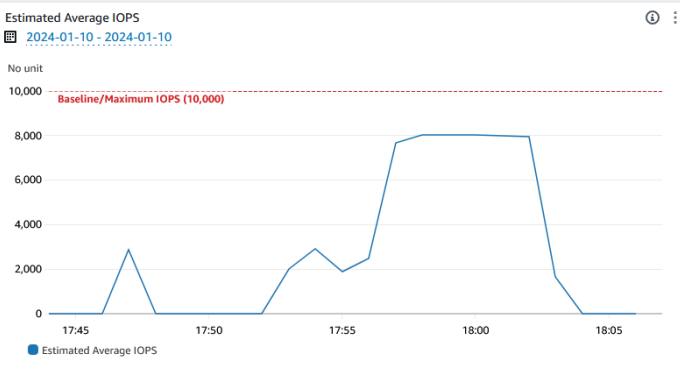
| Calculated Metric | Mathematical Expression | Unit |
|---|---|---|
| Estimated Average IOPS | (SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime)) | IOPS |
| Estimated Average Throughput | (SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024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

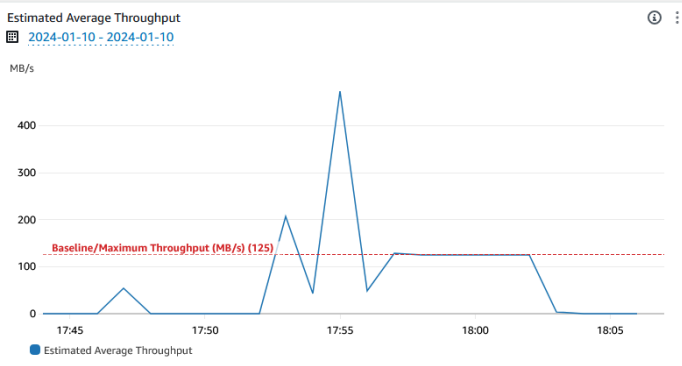
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

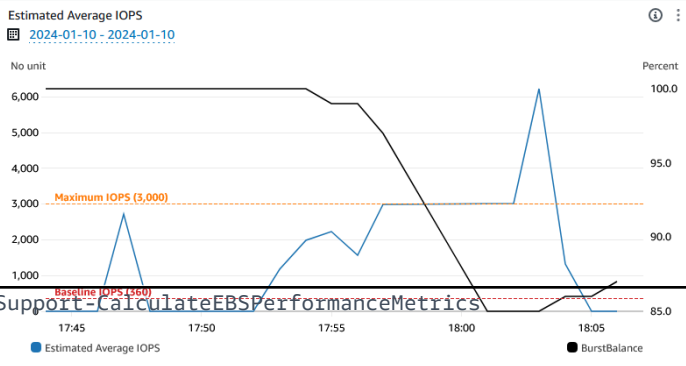



Estimated Average Throughput
2024-01-10 - 2024-01-10

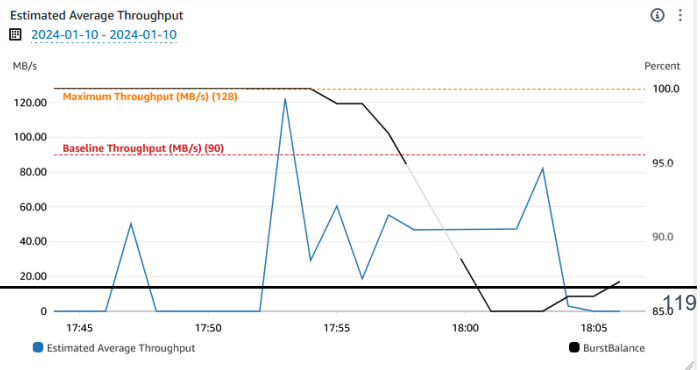



Volume: vol[redacted] | Type: gp2

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




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

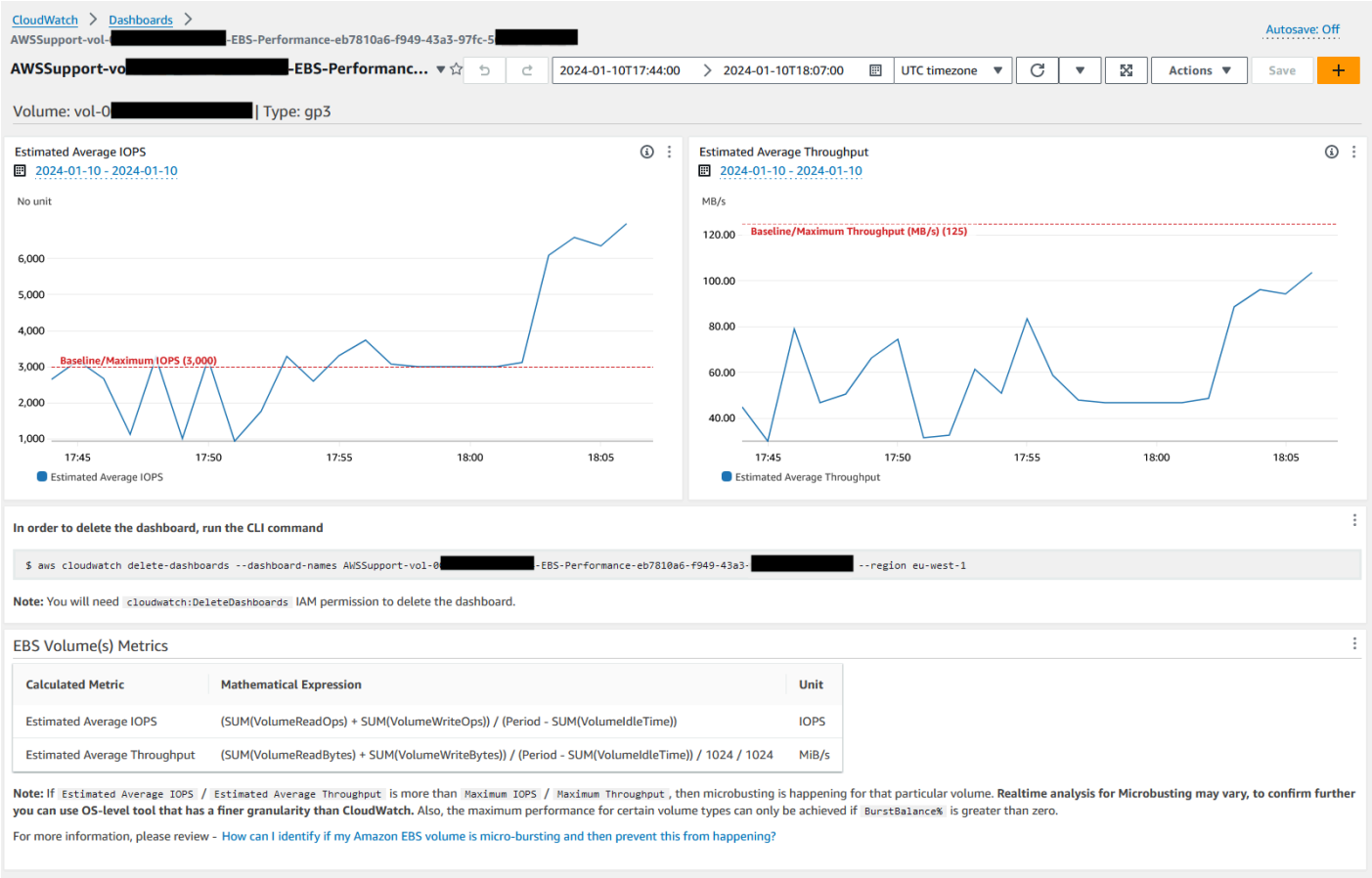



Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

### Beispiel- CloudWatch Dashboard für Ressourcen-ID als Amazon-EBS-Volume-ID




## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

### AWS -Servicedokumentation

- Wie kann ich feststellen, ob mein Amazon-EBS-Volume Micro-Bursting aufweist, und dies dann verhindern?
- Wie verwende ich CloudWatch , um die aggregierten Amazon-EBS-Leistungsmetriken für eine EC2-Instance anzuzeigen?

# AWS-CopySnapshot

Beschreibung

Kopiert einen point-in-time Snapshot eines Amazon Elastic Block Store (Amazon EBS) -Volumes. Sie können den Snapshot innerhalb derselben Region AWS-Region oder von einer Region in eine andere kopieren. Kopien verschlüsselter Amazon EBS-Snapshots bleiben verschlüsselt. Kopien unverschlüsselter Snapshots bleiben unverschlüsselt. Um einen verschlüsselten Snapshot zu kopieren, der von einem anderen Konto gemeinsam genutzt wurde, benötigen Sie Berechtigungen für den KMS-Schlüssel, der zum Verschlüsseln des Snapshots verwendet wurde. Snapshots, die durch Kopieren eines anderen Snapshot erstellt wurden, haben über eine per Zufallsprinzip ausgewählte Volume-ID, die nicht für andere Zwecke verwendet werden sollte.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Beschreibung

  Typ: Zeichenfolge

Beschreibung: (Optional) Eine Beschreibung für den Amazon EBS-Snapshot.

- SnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des zu kopierenden Amazon EBS-Snapshots.

- SourceRegion

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Region, in der sich der Quell-Snapshot zurzeit befindet.

Dokumentschritte

copySnapshot — Kopiert einen Snapshot eines Amazon EBS-Volumes.

Ausgaben

copySnapshot. SnapshotId - Die ID des neuen Snapshots.

## AWS-CreateSnapshot

Beschreibung

Erstellen Sie einen Snapshot eines Amazon EBS-Volumes.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Beschreibung

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Beschreibung für den Snapshot.
- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Volumes.

## AWS-DeleteSnapshot

Beschreibung

Löschen Sie einen Snapshot eines Amazon EBS-Volumes.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- SnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des EBS-Snapshots.

## AWSConfigRemediation-DeleteUnusedEBSVolume

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedEBSVolume` Runbook löscht ein unbenutztes Amazon Elastic Block Store (Amazon EBS) -Volume.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- CreateSnapshot

  Typ: Boolesch

  Beschreibung: (Optional) Wenn auf gesetzt`true`, erstellt die Automatisierung einen Snapshot des Amazon EBS-Volumes, bevor es gelöscht wird.

- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`— Überprüft, ob das Amazon EBS-Volume, das Sie im `VolumeId` Parameter angeben, nicht verwendet wird, und erstellt je nach dem Wert, den Sie für den `CreateSnapshot` Parameter wählen, einen Snapshot.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `CreateSnapshot` Parameter ausgewählt haben.
- `aws:waitForAwsResourceProperty`- Wartet, bis der Snapshot abgeschlossen ist.

- `aws:executeAwsApi`- Löscht den Snapshot, falls die Snapshot-Erstellung fehlgeschlagen ist.
- `aws:executeAwsApi`- Löscht das Amazon EBS-Volume, das Sie im `VolumeId` Parameter angeben.
- `aws:executeScript`— Überprüft, ob das Amazon EBS-Volume gelöscht wurde.

## AWS-DeregisterAMIs

Beschreibung

Das `AWS-DeregisterAMIs` Runbook hilft Ihnen beim Abmelden Amazon Machine Images (AMIs), indem es das Tag angibt, das Sie auf Ihr angewendet haben. AMIs

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DryRun

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

Beschreibung: (Erforderlich) Überprüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anfrage tatsächlich zu stellen, und gibt eine Fehlermeldung aus.

- RetainNumber

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die NummerAMIs, die Sie behalten möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für angeben`Age`.

- Age

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der vorherigen TageAMIs, die Sie behalten möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für angeben`RetainNumber`.

- TagKey

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Schlüssel des Tags, das dem Tag zugewiesen istAMIs, dessen Registrierung Sie aufheben möchten.

- TagValue

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Wert des Tags, das dem Tag zugewiesen istAMIs, dessen Registrierung Sie aufheben möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DeregisterImage`
- `ec2:DescribeImages`

### Dokumentschritte

- `aws:executeAwsApi`- Überprüft die Werte, die Sie für die Runbook-Eingabeparameter angeben.

- `aws:executeAwsApi`- Die Registrierung wird AMIs mit dem Tag aufgehoben, das Sie mit den Parametern und angegeben haben. `TagKey` `TagValue`

## AWS-DetachEBSVolume

Beschreibung

Trennen Sie ein Amazon EBS-Volume von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der von Lambda übernommenen Rolle
- VolumeId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des EBS-Volumes. Volume und Instance müssen sich in derselben Availability Zone befinden.

## AWSConfigRemediation-EnableEbsEncryptionByDefault

Beschreibung

Das `AWSConfigRemediation-EnableEbsEncryptionByDefault` Runbook ermöglicht die Verschlüsselung auf allen neuen Amazon Elastic Block Store (Amazon EBS) -Volumes in AWS-Region dem AWS-Konto und auf dem Sie die Automatisierung ausführen. Volumes, die vor der Ausführung der Automatisierung erstellt wurden, sind nicht verschlüsselt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die standardmäßige Amazon EBS-Verschlüsselungseinstellung für das aktuelle Konto und die Region.
- `aws:assertAwsResourceProperty`— Überprüft, ob die standardmäßige Amazon EBS-Verschlüsselungseinstellung aktiviert wurde.

## AWS-ExtendEbsVolume

Beschreibung

Das `AWS-ExtendEbsVolume` Runbook vergrößert ein Amazon EBS-Volume und erweitert das Dateisystem. Diese Automatisierung unterstützt die `ext4` Dateisysteme `xfs` und.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DriveLetter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Buchstabe des Laufwerks, dessen Dateisystem Sie erweitern möchten. Dieser Parameter ist für Windows Instanzen erforderlich.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Amazon EC2 EC2-Instance, an die das Amazon EBS-Volume angehängt ist, das Sie erweitern möchten.

- KeepSnapshot

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Legt fest, ob der vor der Erhöhung der Größe Ihres Amazon EBS-Volumes erstellte Snapshot beibehalten werden soll.

- MountPoint

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Bereitstellungspunkt des Laufwerks, dessen Dateisystem Sie erweitern möchten. Dieser Parameter ist für Linux-Instances erforderlich.

- SizeGib

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Größe in GiB, auf die Sie Ihr Amazon EBS-Volume ändern möchten.

- VolumeId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des EBS-Volumes, das Sie erweitern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Erhöht die Größe des Volumes auf den Wert, den Sie im `VolumeId` Parameter angeben, und erweitert das Dateisystem.

## AWSSupport-ModifyEBSSnapshotPermission

Beschreibung

Das `AWSSupport-ModifyEBSSnapshotPermission` Runbook hilft Ihnen, die Berechtigungen für mehrere Amazon Elastic Block Store (Amazon EBS) -Snapshots zu ändern. Mit diesem Runbook können Sie Schnappschüsse erstellen `Public` oder `Private` diese mit anderen teilen. AWS-Konten Mit einem Standard-KMS-Schlüssel verschlüsselte Snapshots können nicht mit anderen Konten geteilt werden, die dieses Runbook verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AccountIds

  Typ: StringList

  Standard: keiner

  Beschreibung: (Optional) Die IDs der Konten, mit denen Sie Snapshots teilen möchten. Dieser Parameter ist erforderlich, wenn Sie `No` den Wert des `Private` Parameters eingeben.
- AccountPermissionBetrieb

  Typ: Zeichenfolge

  Gültige Werte: hinzufügen | entfernen

  Standard: keiner

  Beschreibung: (Optional) Die Art des auszuführenden Vorgangs.
- Privat

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

Beschreibung: (Erforderlich) Geben Sie No den Wert ein, wenn Sie Snapshots mit bestimmten Konten teilen möchten.

- SnapshotIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Amazon EBS-Snapshots, deren Berechtigungen Sie ändern möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Dokumentschritte

1. `aws:executeScript`- Überprüft die IDs der im Parameter angegebenen Snapshots. `SnapshotIds` Nach der Überprüfung der IDs sucht das Skript nach verschlüsselten Snapshots und gibt eine Liste aus, falls welche gefunden wurden.
2. `aws:branch`- Verzweigt die Automatisierung auf der Grundlage des Werts, den Sie für den `Private` Parameter eingeben.
3. `aws:executeScript`- Ändert die Berechtigungen der angegebenen Snapshots, um sie für die angegebenen Konten freizugeben.
4. `aws:executeScript`- Ändert die Berechtigungen der Snapshots, um sie von zu zu ändern. `Public` `Private`

### Ausgaben

ValidateSnapshots.EncryptedSnapshots

SharewithOtherKonten. Ergebnis

MakePrivate. Ergebnis

MakePrivate. Befehle

## AWSConfigRemediation-ModifyEBSVolumeType

Beschreibung

Das `AWSConfigRemediation-ModifyEBSVolumeType` Runbook ändert den Volumetyp eines Amazon Elastic Block Store (Amazon EBS) -Volumes. Nachdem der Volumetyp geändert wurde, wechselt das Volume in einen Status. `optimizing` Informationen zur Überwachung des Fortschritts von Volumenänderungen finden Sie unter Überwachen des Fortschritts von Volumenänderungen im Amazon EC2 EC2-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EbsVolumeID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes, das Sie ändern möchten.
- EbsVolumeGeben Sie ein

Typ: Zeichenfolge

Gültige Werte: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

Beschreibung: Der Volumetyp, auf den Sie das Amazon EBS-Volume ändern möchten. Informationen zu Amazon EBS-Volumetypen finden Sie unter Amazon EBS-Volumetypen im Amazon EC2 EC2-Benutzerhandbuch.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Überprüft, ob der Status des Volumes oder ist`available`. `in-use`
- `aws:executeAwsApi`- Ändert das Amazon EBS-Volume, das Sie im `EbsVolumeId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Überprüft, ob der Typ des Volumes auf den Wert geändert wurde, den Sie im Parameter angegeben haben. `EbsVolumeType`

# Amazon EC2

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon Elastic Compute Cloud. Runbooks für Amazon Elastic Block Store befinden sich im Amazon EBS Abschnitt der Runbook-Referenz. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Ändern Sie den Standby-Status einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einer Auto Scaling-Gruppe.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID einer Amazon EC2-Instance, für die Sie den Standby-Status innerhalb einer Auto Scaling-Gruppe ändern möchten.
- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

## AWS-ASGExitStandby

Beschreibung

Ändern Sie den Standby-Status einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einer Auto Scaling-Gruppe.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID einer EC2-Instance, für die Sie den Standby-Status innerhalb einer Auto Scaling-Gruppe ändern möchten.
- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

## AWS-CreateImage

Beschreibung

Erstellen Sie eine neue Amazon Machine Image (AMI) aus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2-Instance.
- NoReboot

  Typ: Boolesch

  Beschreibung: (Optional) Kein Neustart der Instance vor der Erstellung des Abbilds.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

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

## AWS-DeleteImage

Beschreibung

Lösche einen Amazon Machine Image (AMI) und alle zugehörigen Schnappschüsse.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ImageId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des AMI.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

```
{
    "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

Beschreibung

Patchen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einer Auto Scaling-Gruppe.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance für das Patching. Geben Sie keine Instanz-ID an, die so konfiguriert ist, dass sie während eines Wartungsfensters ausgeführt wird.
- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die es dem von Automation erstellten Lambda ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn nicht angegeben, wird eine transiente Rolle erstellt, um die Lambda-Funktion auszuführen.
- WaitForInstance

  Typ: Zeichenfolge

  Standard: PT2M

  Beschreibung: (Optional) Dauer, für die die Automatisierung in den Ruhezustand versetzt werden soll, damit die Instance wieder in Betrieb genommen werden kann.
- WaitForReboot

Typ: Zeichenfolge

Standard: PT5M

Beschreibung: (Optional) Dauer, für die die Automatisierung in den Ruhezustand versetzt werden soll, damit eine gepatchte Instanz neu gestartet werden kann.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beschreibung

Sorgt dafür, dass eine EC2-Instance der geltenden Patch-Baseline entspricht. Macht das Root-Volume bei einem Ausfall rückgängig.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) EC2, InstanceId auf das wir die Patch-Baseline anwenden.
- LambdaAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- ReportS3Bucket

  Typ: Zeichenfolge

  Beschreibung: (Optional) Amazon S3-Bucket-Ziel für den während des Prozesses generierten Compliance-Bericht.

Dokumentschritte

| Schrittnummer | Name des Schritts | Automation-Aktion |
|---|---|---|
| 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` |

| Schrittnummer | Name des Schritts | Automation-Aktion |
|---|---|---|
| 10 | DeleteSnapshot | `aws:invokeLambdaFunction` |
| 11 | deleteCloudFormationVorlage | `aws:deleteStack` |

Ausgaben

IdentifyRootVolume.Nutzlast

PrePatchSnapshot.Ausgang

SaveComplianceReportToS3. Nutzlast

RestoreFromSnapshot.Nutzlast

CheckCompliance.Nutzlast

## `AWS-QuarantineEC2Instance`

Beschreibung

Mit dem `AWS-QuarantineEC2Instance` Runbook können Sie einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die keinen eingehenden oder ausgehenden Datenverkehr zulässt, eine Sicherheitsgruppe zuweisen.

> **Important**
>
> Änderungen an den RDP-Einstellungen sollten sorgfältig geprüft werden, bevor dieses Runbook ausgeführt wird.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der verwalteten Instance, deren RDP-Einstellungen verwaltet werden sollen.
- IsolationSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Sicherheitsgruppe, die Sie der Instance zuweisen möchten, um eingehenden oder ausgehenden Datenverkehr zu verhindern.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `autoscaling:DescribeAutoScalingInstances`
- `autoscaling:DetachInstances`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSnapshot`
- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeSnapshots`
- `ec2:ModifyInstanceAttribute`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeAwsApi`- Sammelt Details über die Instanz.
- `aws:executeScript`— Überprüft, dass die Instanz nicht Teil einer Auto Scaling-Gruppe ist.
- `aws:executeAwsApi`— Erstellt einen Snapshot des an die Instance angehängten Root-Volumes.
- `aws:waitForAwsResourceProperty`- Wartet, bis der Snapshot-Status erreicht ist. `completed`
- `aws:executeAwsApi`- Weist Ihrer Instance die im `IsolationSecurityGroup` Parameter angegebene Sicherheitsgruppe zu.

Ausgaben

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

## AWS-ResizeInstance

Beschreibung

Ändern Sie den Instance-Typ einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance.
- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Typ der Instance.
- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der von Lambda übernommenen Rolle.

## AWS-RestartEC2Instance

Beschreibung

Starten Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances neu.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Amazon EC2-Instances, die neu gestartet werden sollen.

## `AWS-SetupJupyter`

Beschreibung

Das `AWS-SetupJupyter` Runbook hilft Ihnen bei der Einrichtung von Jupyter Notebook auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Sie können entweder eine vorhandene Instance angeben oder eine Amazon Machine Image (AMI) ID für die Automatisierung angeben, um eine neue Instance zu starten und einzurichten. Bevor Sie beginnen, müssen Sie im `SecureString` Parameter Store einen Parameter erstellen, der als Passwort für Jupyter Notebook verwendet werden kann. Parameter Store ist eine Fähigkeit vonAWS Systems Manager. Informationen zum Erstellen von Parametern finden Sie im AWS Systems ManagerBenutzerhandbuch unter Parameter erstellen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AmiId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID derAMI, die Sie verwenden möchten, um eine neue Instance zu starten und Jupyter Notebook einzurichten.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, auf der Sie Jupyter Notebook einrichten möchten.
- InstanceType

  Typ: Zeichenfolge

  Standard: t3.medium

  Beschreibung: (Optional) Wenn Sie eine neue Instance starten, um Jupyter Notebook einzurichten, geben Sie den Instance-Typ an, den Sie verwenden möchten.
- JupyterPasswordSSM-Schlüssel

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des `SecureString` Parameters im Parameter Store, den Sie als Passwort für Jupyter Notebook verwenden möchten.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselpaar, das Sie der neu gestarteten Instance zuordnen möchten.

- RemoteAccessCidr

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Optional) Der CIDR-Bereich, aus dem Sie SSH-Verkehr zulassen möchten.

- RoleName

  Typ: Zeichenfolge

  Standard: SSM ManagedInstanceProfileRole

  Beschreibung: (Optional) Der Name des Instanzprofils für die neu gestartete Instance.

- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{Automation:Execution_ID}}

  Beschreibung: (Optional) Der AWS CloudFormation Stack-Name, den die Automatisierung verwenden soll.

- SubnetId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Optional) Das Subnetz, in dem Sie die zu verwendende neue Instance starten möchten.

- VpcId

  Typ: Zeichenfolge

  Standard: Standard

Beschreibung: (Optional) Die ID der Virtual Private Cloud (VPC), in der Sie die neue Instance starten möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`- Richtet Jupyter Notebook auf der von Ihnen angegebenen Instanz oder auf einer neu gestarteten Instance ein und verwendet dabei die Werte, die Sie für die Runbook-Eingabeparameter angeben.

## AWS-StartEC2Instance

Beschreibung

Starten Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: (Erforderlich) Zu startende EC2-Instances.

## AWS-StopEC2Instance

Beschreibung

Stoppt eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: (Erforderlich) EC2-Instances zum Stoppen.

## AWS-TerminateEC2Instance

Beschreibung

Beenden Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: (Erforderlich) IDs einer oder mehrerer zu beendender EC2-Instances.

## AWS-UpdateLinuxAmi

Beschreibung

Aktualisieren Sie an Amazon Machine Image (AMI) mit Linux-Distributionspaketen und Amazon-Software.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ExcludePackages

  Typ: Zeichenfolge

  Standard: keiner

  Beschreibung: (Optional) Namen der Pakete, die bei Updates unter allen Umständen zurückgehalten werden müssen. Standardmäßig wird kein (\„none\“) Paket ausgeschlossen.
- IamInstanceProfileName

  Typ: Zeichenfolge

  Standard: ManagedInstanceProfile

  Beschreibung: (Erforderlich) Das Instanzprofil, mit dem Systems Manager die Instanz verwalten kann.
- IncludePackages

  Typ: Zeichenfolge

  Standard: alle

  Beschreibung: (Optional) Nur diese benannten Pakete aktualisieren. Standardmäßig werden alle (\„all\“) verfügbaren Updates übernommen.
- InstanceType

Typ: Zeichenfolge

Standard: t2.micro

Beschreibung (Optional) Der Typ der als Workspace-Host zu startenden Instance. Die Instance-Typen sind je nach Region unterschiedlich.

- MetadataOptions

  Typ: StringMap

  Standard: {“ HttpEndpoint „: „aktiviert“, "HttpTokens„: „optional"}

  Beschreibung: (Optional) Die Metadatenoptionen für die Instanz. Weitere Informationen finden Sie unter InstanceMetadataOptionsRequest.

- PostUpdateScript

  Typ: Zeichenfolge

  Standard: keiner

  Beschreibung: (Optional) Die URL eines Skripts, das ausgeführt werden muss, nachdem Paketupdates angewendet werden. Standard („none“) ist die Ausführung keines Skripts.

- PreUpdateScript

  Typ: Zeichenfolge

  Standard: keiner

  Beschreibung: (Optional) Die URL eines Skripts, das ausgeführt werden muss, bevor Updates angewendet werden. Standard („none“) ist die Ausführung keines Skripts.

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs der Sicherheitsgruppen, auf die AMI Sie sich beziehen möchten.

- SourceAmiId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Quell-Amazon Machine Image-ID.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die Instance starten möchten. Wenn Sie Ihre Standard-VPC gelöscht haben, ist dieser Parameter erforderlich.

- TargetAmiName

  Typ: Zeichenfolge

  Standard: UpdateLinuxAmi _from_ {{SourceAmiId}} _am_ {{global:Date_Time}}

  Beschreibung: (Optional) Der Name des neuen AMIs, das erstellt wird. Der Standard ist eine systemgenerierte Zeichenfolge, die die Quell-AMI-ID sowie Uhrzeit und Datum der Erstellung enthält.

## AWS-UpdateWindowsAmi

Beschreibung

Aktualisieren Sie ein Microsoft Windows Amazon Machine Image (AMI). Standardmäßig installiert dieses Runbook alle Windows-Updates, Amazon-Software und Amazon-Treiber. Anschließend wird mit Sysprep ein neues AMI erstellt. Unterstützt Windows Server 2008 R2 oder höher.

> **Important**
>
> Wenn Ihre Instances AWS Systems Manager mithilfe von VPC-Endpunkten eine Verbindung herstellen, schlägt dieses Runbook fehl, sofern es nicht in der Region us-east-1 verwendet wird. Für Instances muss TLS 1.2 aktiviert sein, um dieses Runbook verwenden zu können.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Kategorien

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe von mindestens einer Updatekategorie. Sie können Kategorien anhand kommaseparierter Werte filtern. Optionen: Anwendung, Konnektoren CriticalUpdates DefinitionUpdates, DeveloperKits,, TreiberFeaturePacks, Anleitung, Microsoft, SecurityUpdates ServicePacks,, ToolsUpdateRollups, Updates. Gültige Formate beinhalten einen einzigen Eintrag, zum Beispiel:CriticalUpdates. Oder Sie können eine durch Kommas getrennte Liste angeben:CriticalUpdates,SecurityUpdates. HINWEIS: Um die Kommata herum dürfen keine Leerzeichen stehen.

- ExcludeKbs

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe mindestens einer Microsoft Knowledge Base (KB)-Artikel-ID, die ausgeschlossen werden soll. Sie können mehrere IDs anhand kommaseparierter Werte ausschließen. Gültige Formate: KB9876543 oder 9876543.

- IamInstanceProfileName

  Typ: Zeichenfolge

  Standard: ManagedInstanceProfile

Beschreibung: (Erforderlich) Der Name der Rolle, mit der Systems Manager die Instanz verwalten kann.

- IncludeKbs

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe mindestens einer Microsoft Knowledge Base (KB)-Artikel-ID, die eingeschlossen werden soll. Sie können mehrere IDs anhand kommaseparierter Werte installieren. Gültige Formate: KB9876543 oder 9876543.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung (Optional) Der Typ der als Workspace-Host zu startenden Instance. Die Instance-Typen sind je nach Region unterschiedlich. Standard ist t2.medium.

- MetadataOptions

  Typ: StringMap

  Standard: {“ HttpEndpoint „: „aktiviert“, "HttpTokens„: „optional"}

  Beschreibung: (Optional) Die Metadatenoptionen für die Instanz. Weitere Informationen finden Sie unter InstanceMetadataOptionsRequest.

- PostUpdateScript

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein als Zeichenfolge bereitgestelltes Skript. Es wird nach der Installation von Betriebssystemaktualisierungen ausgeführt.

- PreUpdateScript

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein als Zeichenfolge bereitgestelltes Skript. Es wird vor der Installation von Betriebssystemaktualisierungen ausgeführt.

- PublishedDateAfter

Typ: Zeichenfolge

Beschreibung: (Optional) Angabe des Datums, nach dem die Aktualisierungen veröffentlicht werden sollen. Beispiel: Wenn 01.01.2017 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die am oder nach dem 01.01.2017 veröffentlicht wurden, zurückgegeben.

- PublishedDateBefore

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe des Datums, vor dem die Aktualisierungen veröffentlicht werden sollen. Beispiel: Wenn 01.01.2017 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die am oder vor dem 01.01.2017 veröffentlicht wurden, zurückgegeben.

- PublishedDaysOld

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe des erforderlichen Alters der Aktualisierungen in Tagen ab dem Veröffentlichungsdatum. Beispiel: Wenn 10 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die vor 10 oder mehr Tagen veröffentlicht wurden, zurückgegeben.

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs der Sicherheitsgruppen, auf die AMI Sie sich beziehen möchten.

- SeverityLevels

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe mindestens einer MSRC-Ebene, die einem Update zugeordnet ist. Sie können Dringlichkeitsstufen anhand kommaseparierter Werte filtern. Standardmäßig werden Patches für alle Sicherheitsstufen ausgewählt sind. Wenn Werte angegeben sind, wird die Update-Liste nach diesen Werten gefiltert. Optionen: Kritisch, Wichtig, Niedrige, Mittel oder Nicht angegeben. Zu den gültigen Formaten gehört ein einzelner Eintrag. Beispiel: Wichtig. Sie können auch eine kommaseparierte Liste angeben: Kritisch,Wichtig,Niedrig.

- SourceAmiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die AMI Quell-ID.
- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die Instance starten möchten. Wenn Sie Ihre Standard-VPC gelöscht haben, ist dieser Parameter erforderlich.
- TargetAmiName

  Typ: Zeichenfolge

  Standard: UpdateWindowsAmi _from_ {{SourceAmiId}} _am_ {{global:Date_Time}}

  Beschreibung: (Optional) Der Name des neuen AMIs, das erstellt wird. Der Standard ist eine systemgenerierte Zeichenfolge, die die Quell-AMI-ID sowie Uhrzeit und Datum der Erstellung enthält.

## AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Beschreibung

Das `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` Runbook ermöglicht Zustandsprüfungen für die von Ihnen angegebene Amazon EC2 Auto Scaling (Auto Scaling) -Gruppe.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.

- AutoScalingGroupARN

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der Auto Scaling-Gruppe, für die Sie Integritätsprüfungen aktivieren möchten.

- HealthCheckGracePeriod

  Typ: Ganzzahl

  Standard: 300

  Beschreibung: (Optional) Die Zeit in Sekunden, die Auto Scaling abwartet, bevor der Integritätsstatus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance überprüft wird, die in Betrieb genommen wurde.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert Zustandsprüfungen für die Auto Scaling-Gruppe, die Sie im `AutoScalingGroupARN` Parameter angeben.

## `AWSConfigRemediation-EnforceEC2InstanceIMDSv2`

Beschreibung

Das `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` Runbook erfordert, dass die von Ihnen angegebene Amazon Elastic Compute Cloud (Amazon EC2)-Instance Instance Metadata Service Version 2 (IMDSv2) verwendet.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, die Sie für die Verwendung von IMDSv2 benötigen möchten.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.

- HttpPutResponseHopLimit

  Typ: Ganzzahl

  Beschreibung: (Optional) Das Hop-Antwortlimit vom IMDS-Service zurück an den Anforderer. Legen Sie für EC2-Instances, die Container hosten, auf 2 oder höher fest. Setzen Sie auf 0, um nicht zu ändern (Standard).

  Zulässiges Muster: `^([1-5]?\d|6[0-4])$`

  Standard: 0

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript` – Legt die `HttpTokens` Option `required` auf der Amazon EC2, die Sie im `InstanceId` Parameter angeben, auf fest.
- `aws:assertAwsResourceProperty` – Prüft, ob IMDSv2 auf der Amazon EC2 erforderlich ist.

## AWSEC2-CloneInstanceAndUpgradeSQLServer

Beschreibung

Erstellen Sie eine AMI aus einer EC2-Instance, um SQL Server 2008 oder höher Windows Server auszuführen, und aktualisieren Sie dann das AMI auf eine neuere Version von SQL Server.

Die folgenden Upgrade-Pfade werden unterstützt:

- SQL Server 2008 auf SQL Server 2017, 2016 oder 2014

- SQL Server 2008 R2 auf SQL Server 2017, 2016 oder 2014
- SQL Server 2012 auf SQL Server 2019, 2017, 2016 oder 2014
- SQL Server 2014 bis SQL Server 2019, 2017 oder 2016
- SQL Server 2016 auf SQL Server 2019 oder 2017
- SQL Server 2017 bis SQL Server 2019

Wenn Sie eine frühere Version von Windows Server verwenden, die nicht mit SQL Server 2019 kompatibel ist, muss das Automatisierungsdokument Ihre Windows Server-Version auf 2016 aktualisieren.

Das Upgrade ist ein aus mehreren Schritten bestehender Prozess, der 2 Stunden in Anspruch nehmen kann. Die Automatisierung erstellt das AMI aus der Instance und startet dann eine temporäre Instance aus der neuen Instance AMI in der angegebenen Instanz`SubnetID`. Die Sicherheitsgruppen, die Ihrer ursprünglichen Instance zugeordnet sind, werden auf die temporäre Instance angewendet. Die Automatisierung führt dann ein direktes Upgrade `TargetSQLVersion` auf die auf der temporären Instanz durch. Nach dem Upgrade erstellt die Automatisierung eine neue AMI aus der temporären Instanz und beendet dann die temporäre Instanz.

Sie können die Anwendungsfunktionalität testen, indem Sie die neue AMI in Ihrer VPC starten. Nachdem Sie den Test abgeschlossen haben, und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

> **Note**
>
> Informationen zum Ändern des Computernamens der EC2-Instance, die von der neuen aus gestartet wurdeAMI, finden Sie unter Umbenennen eines Computers, der eine eigenständige Instanz von SQL Server hostet.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Voraussetzungen

- TLS-Version 1.2.
- Die EC2-Instance muss eine Version von Windows Server verwenden, die Windows Server 2008 R2 (oder höher) und SQL Server 2008 (oder höher) ist.
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installation und Konfiguration des SSM-Agenten auf EC2-Instances für Windows Server.
- Konfigurieren Sie die Instanz so, dass sie eine AWS Identity and Access Management (IAM) Instance-Profilrolle verwendet. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Instance-Boot-Datenträger hat.
- Für Instances, die eine Bring Your Own License (BYOL) SQL Server-Version verwenden, gelten die folgenden zusätzlichen Voraussetzungen:
  - Geben Sie eine EBS-Snapshot-ID an, die das SQL Server-Zielinstallationsmedium enthält. So gehen Sie vor:

    1. Überprüfen Sie, ob die EC2-Instance Windows Server 2008 R2 oder höher ausführt.
    2. Erstellen Sie ein 6 GB EBS-Volume in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
    3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
    4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
    5. Erstellen Sie einen EBS-Snapshot des 6 GB-Volumes, das Sie in Schritt 2 erstellt haben.

Einschränkungen

- Das Upgrade ist nur auf einem SQL Server mit Windows-Authentifizierung möglich.

- Stellen Sie sicher, dass keine Sicherheits-Patch-Updates auf den Instances ausstehen. Öffnen Sie Control Panel (Systemsteuerung), und wählen Sie dann Check for updates (Auf Aktualisierungen prüfen).
- SQL Server-Bereitstellungen in HA und der Spiegelungsmodus werden nicht unterstützt.

Parameter

- IamInstanceProfile

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das IAM-Instanzprofil.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Instance auf Windows Server 2008 R2 (oder höher) oder SQL Server 2008 (oder höher).
- KeepPreUpgradeImageBackUp

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, löscht die Automatisierung das vor dem Upgrade aus der Instance erstellte AMI nicht. Wenn auf gesetzt`true`, müssen Sie das AMI löschen. Das AMI wird standardmäßig gelöscht.
- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (erforderlich) Geben Sie ein Subnetz für den Upgrade-Prozess an. Stellen Sie sicher, dass das Subnetz über ausgehende Verbindungen zu AWS Services, Amazon S3 und Microsoft verfügt (um Patches herunterzuladen).
- SQL ServerSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Bedingte) Snapshot-ID für das SQL Server-Zielinstallationsmedium. Dieser Parameter ist für Instances erforderlich, die eine BYOL SQL Server-Version verwenden. Dieser Parameter ist optional für Instances mit enthaltener SQL Server-Lizenz (Instances, die mit einem

von AWS bereitgestellten Amazon Machine Image für Windows Server mit Microsoft SQL Server gestartet werden).

- RebootInstanceBeforeTakingImage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, startet die Automatisierung die Instance neu, bevor ein AMI vor dem Upgrade erstellt wird. Standardmäßig wird die Automatisierung vor dem Upgrade nicht neu gestartet.

- Ziel-SQL-Version

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wählen Sie die SQL Server-Zielversion aus.

  Mögliche Ziele:

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

  Standardziel: SQL Server 2016

Ausgaben

AmiId: Die ID des AMIs, das aus der Instanz erstellt wurde, die auf eine neuere Version von SQL Server aktualisiert wurde.

## AWSEC2-CloneInstanceAndUpgradeWindows

Beschreibung

Erstellen Sie ein Amazon Machine Image (AMI) aus einer Instance von Windows Server 2008 R2, 2012 R2, 2016 oder 2019 und aktualisieren Sie dann AMI auf Windows Server 2016, 2019 oder 2022. Die unterstützten Upgrade-Pfade sind wie folgt.

- Windows Server 2008 R2 bis Windows Server 2016.
- Windows Server 2012 R2 zu Windows Server 2016.

- Windows Server 2012 R2 zu Windows Server 2019.
- Windows Server 2012 R2 bis Windows Server 2022.
- Windows Server 2016 zu Windows Server 2019.
- Windows Server 2016 bis Windows Server 2022.
- Windows Server 2019 bis Windows Server 2022.

Die Upgrade-Operation ist ein aus mehreren Schritten bestehender Prozess, der 2 Stunden in Anspruch nehmen kann. Wir empfehlen, für Instances mit mindestens zwei vCPUs und 4 GB RAM ein Betriebssystem-Upgrade durchzuführen. Die Automatisierung erstellt ein AMI aus der Instance und startet dann eine temporäre Instance aus dem neu erstellten AMI in der von `SubnetId` Ihnen angegebenen . Die Sicherheitsgruppen, die Ihrer ursprünglichen Instance zugeordnet sind, werden auf die temporäre Instance angewendet. Die Automatisierung führt dann ein direktes Upgrade auf die `TargetWindowsVersion` auf der temporären Instance durch. Um Ihre Windows Server 2008 R2-Instance auf Windows Server 2016, 2019 oder 2022 zu aktualisieren, wird ein direktes Upgrade zweimal durchgeführt, da das direkte Upgrade Windows Server von 2008 R2 auf Windows Server 2016, 2019 oder 2022 nicht unterstützt wird. Die Automatisierung aktualisiert oder installiert auch die AWS Treiber, die für die temporäre Instance erforderlich sind. Nach dem Upgrade erstellt die Automatisierung ein neues AMI aus der temporären Instance und beendet dann die temporäre Instance.

Sie können die Anwendungsfunktionalität testen, indem Sie eine Test-Instance über das aktualisierte AMI in Ihrer Amazon Virtual Private Cloud (Amazon VPC) starten. Nachdem Sie den Test abgeschlossen haben, und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zum aktualisierten AMI wechseln.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Windows Server 2008 R2, 2012 R2, 2016 oder 2019 Standard- und Datacenter-Editionen

Voraussetzungen

- TLS-Version 1.2.
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installieren und Konfigurieren von SSM Agent auf EC2-Instances für Windows Server.
- Windows PowerShell 3.0 oder höher muss auf Ihrer Instance installiert sein.
- Für Instances, die einer Microsoft Active Directory-Domain angehören, empfehlen wir, eine `SubnetId` anzugeben, die keine Verbindung zu Ihren Domain-Cntrollern aufweist, um Hostnamenkonflikte zu vermeiden.
- Das Instance-Subnetz muss über ausgehende Konnektivität zum Internet verfügen, das Zugriff auf AWS-Services wie Amazon S3 und Zugriff auf das Herunterladen von Patches von Microsoft bietet. Diese Anforderung ist erfüllt, wenn das Subnetz entweder ein öffentliches Subnetz ist und die Instance eine öffentliche IP-Adresse hat, oder wenn es sich bei dem Subnetz um ein privates Subnetz mit einer Route handelt, die Internetverkehr an ein öffentliches NAT-Gerät sendet.
- Diese Automatisierung funktioniert nur mit Instances von Windows Server 2008 R2, 2012 R2, 2016 und 2019.
- Konfigurieren Sie die Windows Server Instance mit einem AWS Identity and Access Management (IAM)-Instance-Profil, das die erforderlichen Berechtigungen für Systems Manager bereitstellt. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Boot-Datenträger hat.
- Wenn die Instance keine von bereitgestellte Windows AWS-Lizenz verwendet, geben Sie eine Amazon EBS-Snapshot-ID an, die Windows Server 2012 R2-Installationsmedien enthält. So gehen Sie vor:
  - Überprüfen Sie, dass die EC2-Instance Windows Server 2012 oder höher ausführt.
  - Erstellen Sie ein 6 GB EBS-Volume in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
  - Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
  - Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
  - Erstellen Sie einen EBS-Snapshot des 6 GB-Volumes, das Sie oben in Schritt 2 erstellt haben.

Einschränkungen

Diese Automatisierung unterstützt keine Upgrades von Windows Domänencontrollern, Clustern oder von Windows-Desktop-Betriebssystemen. Diese Automation unterstützt auch keine EC2-Instances für Windows Server mit den folgenden installierten Rollen.

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Parameter

- AlternativeKeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name eines alternativen Schlüsselpaars, das während des Upgrade-Prozesses verwendet werden soll. Dies ist in Situationen nützlich, in denen das der ursprünglichen Instance zugewiesene Schlüsselpaar nicht verfügbar ist. Wenn der ursprünglichen Instance kein Schlüsselpaar zugewiesen wurde, müssen Sie einen Wert für diesen Parameter angeben.
- BYOLWindowsMediaSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des zu kopierenden Amazon-EBS-Snapshots, der Windows Server 2012R2-Installationsmedien enthält. Nur erforderlich, wenn Sie eine BYOL-Instance aktualisieren.
- IamInstanceProfile

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des IAM-Instance-Profils, mit dem Systems Manager die Instance verwalten kann.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die EC2-Instance, auf der Windows Server 2008 R2, 2012 R2, 2016 oder 2019 ausgeführt wird.
- KeepPreUpgradeImageBackUp

  Typ: Zeichenfolge

Beschreibung: (Optional) Wenn True festgelegt ist, löscht die Automatisierung das AMI, das vor dem Upgrade von der EC2-Instance erstellt wurde, nicht. Bei „True“ müssen Sie das AMI löschen. Das AMI wird standardmäßig gelöscht.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und der Ort, an dem sich Ihre EC2-Quell-Instance befindet. Stellen Sie sicher, dass das Subnetz über ausgehende Konnektivität zu - AWS Services, Amazon S3 und Microsoft verfügt (zum Herunterladen von Patches).

- TargetWindowsVersion

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Wählen Sie die Windows-Zielversion aus.

  Standard: 2022

- RebootInstanceBeforeTakingImage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Bei „True“ startet die Automation die Instance vor der Erstellung eines Pre-Upgrade-AMI neu. Standardmäßig startet die Automation vor dem Upgrade nicht neu.

## AWSEC2-ConfigureSTIG

Security Technical Implementation Guides (STIGs) sind die Standards zur Konfigurationsverdichtung, die von der Defense Information Systems Agency (DISA) zur Sicherung von Informationssystemen und Software erstellt wurden. Um Ihre Systeme mit STIG-Standards konform zu machen, müssen Sie eine Vielzahl von Sicherheitseinstellungen installieren, konfigurieren und testen.

Amazon EC2 stellt ein Systems Manager-Runbook bereit, AWSEC2-ConfigureSTIG, mit dem Sie STIG-Einstellungen auf eine Instance anwenden können. Dieses Dokument hilft Ihnen, schnell konforme Images für STIG-Standards zu erstellen. Das STIG Systems Manager-Dokument sucht nach Fehlkonfigurationen und führt ein Korrekturskript aus. Es wird auch InstallRoot vom US-Verteidigungsministerium (Department of Defense, DoD) auf Windows-AMIs installiert, um die DoD-Zertifikate zu installieren und zu aktualisieren und unnötige Zertifikate zu entfernen, um die STIG-

Compliance aufrechtzuerhalten. Für die Verwendung des STIG Systems Manager-Dokuments fallen keine zusätzlichen Gebühren an.

> **Important**
>
> Mit wenigen Ausnahmen installieren die STIG-Hardening-Komponenten, die das Systems Manager-Dokument herunterlädt, keine Pakete von Drittanbietern. Wenn Pakete von Drittanbietern bereits auf der Instance installiert sind und verwandte STIGs vorhanden sind, die Amazon EC2 für dieses Paket unterstützt, werden diese STIGs angewendet.

Auf dieser Seite werden alle STIGs aufgeführt, die Amazon EC2 unterstützt und die STIG-Hardening-Komponenten für Ihre EC2-Instance gelten.

Sie können auswählen, welche STIG-Compliance-Kategorie angewendet werden soll.

Compliance-Stufen

- Hoch (Kategorie I)

  Das schwerwiegendste Risiko. Schließt jede Schwachstelle ein, die zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität führen kann.
- Mittel (Kategorie II)

  Beinhaltet jede Schwachstelle, die zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität führen kann, aber das Risiko kann verringert werden.
- Niedrig (Kategorie III)

  Beinhaltet jede Schwachstelle, die Maßnahmen zum Schutz vor einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt.

Themen

## Downloads von STIG-Hardening-Komponenten

Amazon gruppiert STIG-Harding-Komponenten für jede Version in betriebssystembezogene Pakete. Pakete sind Archivdateien, die für das Zielbetriebssystem geeignet sind, auf das sie heruntergeladen und ausgeführt werden. Linux-Komponentenpakete werden als TAR-Dateien (.tgz-Dateierweiterung) gespeichert. Windows-Komponentenpakete werden als ZIP-Dateien (ZIP-Dateierweiterung) gespeichert.

Amazon speichert die Komponentenpakete im Image-Builder-S3-`STIG`Bucket in jeder AWS-Region. Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

Muster und Beispiele für Komponentenspeicherpfade und Bundle-Dateinamen lauten wie folgt:

Komponentenspeicherpfad

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

Komponentenpfadvariablen

region

AWS-Region (Jede Region hat ihren eigenen Komponenten-Bucket.)

bundle file name

Das Format ist *`<os bundle name>`*_*`<YYYY>`*_Q*`<CCP>`*[_*`<release>`*].*`<file extension>`*. Beachten Sie, dass der Name Unterstriche zwischen den Knoten hat, keine Punkte.

os bundle name

Das Standardnamenpräfix für das Betriebssystem-Bundle ist entweder `LinuxAWSConfigureSTIG` oder `AWSConfigureSTIG`. Um die Abwärtskompatibilität aufrechtzuerhalten, enthält der Download für Windows kein Plattformpräfix.

YYYY

Das vierstellige Jahr der Version.

quarter

Identifiziert das Quartal des Jahres: 1, 2, 3 oder 4.

release

Inkrementelle Zahl, die bei eins beginnt und für jede neue Version um eins erhöht wird. Die Version ist für die erste Version eines Quartals nicht enthalten und wird nur für nachfolgende Versionen hinzugefügt.

file extension

Komprimiertes Dateiformat `tgz` (Linux) oder `zip` (Windows).

Beispiel für Bundle-Dateinamen

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

## Windows-STIG-Einstellungen

Amazon EC2 Windows STIG AMIs und Hardening-Komponenten sind für eigenständige Server konzipiert und wenden die lokale Gruppenrichtlinie an. STIG-konforme Komponenten installieren InstallRoot Sie vom US-Verteidigungsministerium (Department of Defense, DoD ) auf Windows-AMIs, um die DoD-Zertifikate herunterzuladen, zu installieren und zu aktualisieren. Sie entfernen auch unnötige Zertifikate, um die STIG-Compliance aufrechtzuerhalten. Derzeit unterstützt Amazon EC2 STIG-Baselines für die folgenden Versionen von Windows Server: 2012 R2, 2016, 2019 und 2022.

In diesem Abschnitt werden die aktuellen STIG-Einstellungen aufgeführt, die Amazon EC2 für Ihre Windows-Infrastruktur unterstützt, gefolgt von einem Versionsverlaufsprotokoll.

Sie können niedrige, mittlere oder hohe STIG-Einstellungen anwenden.

Windows STIG Low (Kategorie III)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

- Windows Server 2022 STIG Version 1 Version 1

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 und V-254481
- Windows Server 2019 STIG Version 2 Version 5

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 und V-205923
- Windows Server 2016 STIG Version 2 Version 5

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 und V-225060
- Windows Server 2012 R2 MS STIG Version 3 Version 5

  V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 und V-225250
- Microsoft .NET Framework 4.0 STIG Version 2 Version 2

  Für das Microsoft .NET Framework für Schwachstellen der Kategorie III gelten keine STIG-Einstellungen.
- Windows Firewall STIG Version 2 Version 1

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 und V-242008
- Internet Explorer 11 STIG Version 2 Version 3

  V-46477, V-46629 und V-97527
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)

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

Windows STIG Medium (Kategorie II)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch

beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Windows STIG Medium enthält alle aufgelisteten STIG-Hardening-Einstellungen, die für Windows STIG Low (Category III) gelten, sowie die STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie II unterstützt.

- Windows Server 2022 STIG Version 1 Version 1

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

  V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511, und V-254512
- Windows Server 2019 STIG Version 2 Version 5

Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

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

- Windows Server 2016 STIG Version 2 Version 5

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040,

V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 und V-236000

- Windows Server 2012 R2 MS STIG Version 3 Version 5

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

  V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225347, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259, und V-225239

- Microsoft .NET Framework STIG 4.0 Version 2 Version 2

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

V-225238

- Windows Firewall STIG Version 2 Version 1

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

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

- Internet Explorer 11 STIG Version 2 Version 3

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

  V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593, V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46615, V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46685, V-46689, V-46691, V-46693, V-46695, V-46701, V-46705, V-46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46781, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46869, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005, V-47009, V-64711, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169 und V-75171

- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 V-2467363

- Defender STIG Version 2 Release 4 (nur Windows Server 2022)

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445,

V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 V-2134664

Windows STIG High (Kategorie I)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Windows STIG High enthält alle aufgelisteten STIG-Hardening-Einstellungen, die für die Kategorien Windows STIG Medium und Low gelten, sowie die STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie I unterstützt.

- Windows Server 2022 STIG Version 1 Version 1

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 und V-254500
- Windows Server 2019 STIG Version 2 Version 5

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 und V-205919
- Windows Server 2016 STIG Version 2 Version 5

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 und V-225079

- Windows Server 2012 R2 MS STIG Version 3 Version 5

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 und V-225274
- Microsoft .NET Framework STIG 4.0 Version 2 Version 2

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) für das Microsoft .NET Framework unterstützt. Für Schwachstellen der Kategorie I gelten keine zusätzlichen STIG-Einstellungen.
- Windows Firewall STIG Version 2 Version 1

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-241992, V-241997 und V-242002
- Internet Explorer 11 STIG Version 2 Version 3

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) für Internet Explorer 11 unterstützt. Für Schwachstellen der Kategorie I gelten keine zusätzlichen STIG-Einstellungen.
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-235758 und V-235759
- Defender STIG Version 2 Release 4 (nur Windows Server 2022)

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-213426, V-213452 und V-213453

## Windows-STIG-Versionsverlauf

In diesem Abschnitt wird der Versionsverlauf der Windows-Komponenten für die vierteljährlichen STIG-Updates protokolliert. Um die Änderungen und veröffentlichten Versionen für ein Quartal anzuzeigen, wählen Sie den Titel aus, um die Informationen zu erweitern.

Änderungen 2024 Q1 – 02/23/2024 (keine Änderungen):

Für die Veröffentlichung des ersten Quartals 2024 wurden keine Änderungen an der Windows-Komponente STIGS vorgenommen.

Änderungen für Q4 2023 – 12/07/2023 (keine Änderungen):

Für die Veröffentlichung des vierten Quartals 2023 wurden keine Änderungen an der Windows-Komponente STIGS vorgenommen.

Änderungen im Q3 2023 – 10/04/2023 (keine Änderungen):

Für die Veröffentlichung des dritten Quartals 2023 wurden keine Änderungen an der Windows-Komponente STIGS vorgenommen.

Änderungen für Q2 2023 – 05/03/2023 (keine Änderungen):

Für die Veröffentlichung des zweiten Quartals 2023 wurden keine Änderungen für die Windows-Komponente STIGS vorgenommen.

Änderungen für Q1 2023 – 03/27/2023 (keine Änderungen):

Für die Veröffentlichung des ersten Quartals 2023 wurden keine Änderungen für die Windows-Komponente STIGS vorgenommen.

Änderungen für Q4 2022 – 02/01/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Q4-Version 2022 wie folgt:

STIG-Build-Windows-Low-Version 2022.4.0

- Windows Server 2022 STIG Version 1 Release 1
- Windows Server 2019 STIG Version 2 Release 5
- Windows Server 2016 STIG Version 2 Release 5
- Windows Server 2012 R2 MS STIG Version 3 Release 5

- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 2 Release 3
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)

STIG-Build-Windows-Medium Version 2022.4.0

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

STIG-Build-Windows-High-Version 2022.4.0

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

Änderungen für Q3 2022 – 09/30/2022 (keine Änderungen):

Für die Veröffentlichung des dritten Quartals 2022 wurden keine Änderungen für die Windows-Komponente STIGS vorgenommen.

Änderungen für Q2 2022 – 08/02/2022:

Aktualisierte STIG-Versionen und angewandte STIGS für die Q2-Version 2022.

STIG-Build-Windows-Low Version 1.5.0

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

STIG-Build-Windows-Medium Version 1.5.0

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

STIG-Build-Windows-High-Version 1.5.0

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

Änderungen für Q1 2022 – 08/02/2022 (keine Änderungen):

Für die Veröffentlichung des ersten Quartals 2022 wurden keine Änderungen an der Windows-Komponente STIGS vorgenommen.

Änderungen für Q4 2021 – 12/20/2021:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des vierten Quartals 2021.

STIG-Build-Windows-Low Version 1.5.0

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

STIG-Build-Windows-Medium Version 1.5.0

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

STIG-Build-Windows-High-Version 1.5.0

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

Änderungen am Q3 2021 – 09/30/2021:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des dritten Quartals 2021.

STIG-Build-Windows-Low Version 1.4.0

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

STIG-Build-Windows-Medium Version 1.4.0

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

STIG-Build-Windows-High-Version 1.4.0

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

## Linux-STIG-Einstellungen

Dieser Abschnitt enthält Informationen zu den von Amazon EC2 unterstützten Linux-STIG-Hardening-Einstellungen, gefolgt von einem Versionsverlaufsprotokoll. Wenn die Linux-Distribution keine eigenen STIG-Hardening-Einstellungen hat, verwendet Amazon EC2 RHEL-Einstellungen. Unterstützte STIG-Harding-Einstellungen gelten für Amazon EC2 Linux-AMIs und -Komponenten, die auf der Linux-Distribution basieren, wie folgt:

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

### Linux STIG Low (Kategorie III)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Harding-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

RHEL 7 STIG Version 3 Version 14

- RHEL 7/CentOS 7

  V-204452, V-204576 und V-204605
- AL2

  V-204452, V-204576 und V-204605

RHEL 8 STIG Version 1 Version 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-230499999 und V-230281-202020499

Ubuntu 18.04 STIG Version 2 Version 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 und V-2193333

Ubuntu 20.04 STIG Version 1 Version 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 und V-238308

Linux STIG Medium (Kategorie II)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Harding-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Linux STIG Medium enthält alle aufgelisteten STIG-Hardening-Einstellungen, die für Linux STIG Low (Category III) gelten, zusätzlich zu den STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie II unterstützt.

RHEL 7 STIG Version 3 Version 14

Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

- RHEL 7/CentOS 7

  V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204579, V-204631, V-204633, und V-256970

- AL2:

  V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204579, V-204631, V-204633, und V-256970

RHEL 8 STIG Version 1 Version 13

Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (niedrig) unterstützt, sowie:

- RHEL 8/CentOS 8/AL 2023

  V-230257, V-230258, V-230259, V-230550, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-230228, V-230298, V-230387, V-230231, V-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244554, V-250317, V-251718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230368, V-230369, V-230375, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230334, V-230336, V-230338, V-230340, V-230342, V-230344, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230240, V-230282, V-250315, V-250316, V-230255, V-230277, V-230278, V-230348, V-230353, V-230386, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, V-230483, V-244542, V-230503, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-237643, V-251711, V-230238, V-230239, V-230273, V-230275, V-230478, V-230488, V-230489, V-230559, V-230560, V-230561, V-237640, und V-256974

Ubuntu 18.04 STIG Version 2 Version 13

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219303, V-219326, V-219328, V-219330, V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, V-219298, V-219299, V-219300, V-219309, V-219310, V-219311, V-219312, V-233779, V-233780, V-255906,

V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219155, V-219156, V-219160, V-219306, V-219149, V-219166, V-219176, V-219339, V-219331, V-219337, und V-219335

Ubuntu 20.04 STIG Version 1 Version 11

V-238205, V-238207, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-251505, V-238360, V-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238358, V-238356, V-238359, V-238370, und V-238334

Linux STIG High (Kategorie I)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Harding-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Linux STIG High enthält alle aufgelisteten STIG-Hardening-Einstellungen, die für die Kategorien Linux STIG Medium und Low gelten, sowie die STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie I unterstützt.

RHEL 7 STIG Version 3, Version 14

Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

- RHEL 7/CentOS 7

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

- AL2:

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

RHEL 8 STIG Version 1 Version 13

Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

- RHEL 8/CentOS 8/AL 2023

  V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533 und V-230558

Ubuntu 18.04 STIG Version 2 Version 13

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316 und V-251507

Ubuntu 20.04 STIG Version 1 Version 11

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

## Linux-STIG-Versionsverlauf

In diesem Abschnitt wird der Versionsverlauf der Linux-Komponenten für die vierteljährlichen STIG-Updates protokolliert. Um die Änderungen und veröffentlichten Versionen für ein Quartal anzuzeigen, wählen Sie den Titel aus, um die Informationen zu erweitern.

Änderungen für Q1 2024 – 02/06/2024:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des ersten Quartals 2024 wie folgt:

STIG-Build-Linux-Low Version 2024.1.x

- RHEL 7 STIG Version 3 Version 14
- RHEL 8 STIG Version 1 Version 13
- Ubuntu 18.04 STIG Version 2 Version 13
- Ubuntu 20.04 STIG Version 1 Version 11

STIG-Build-Linux-Medium Version 2024.1.x

- RHEL 7 STIG Version 3 Version 14
- RHEL 8 STIG Version 1 Version 13
- Ubuntu 18.04 STIG Version 2 Version 13
- Ubuntu 20.04 STIG Version 1 Version 11

STIG-Build-Linux-High-Version 2024.1.x

- RHEL 7 STIG Version 3 Version 14
- RHEL 8 STIG Version 1 Version 13
- Ubuntu 18.04 STIG Version 2 Version 13
- Ubuntu 20.04 STIG Version 1 Version 11

Änderungen für Q4 2023 – 12/07/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des vierten Quartals 2023 wie folgt:

STIG-Build-Linux-Low Version 2023.4.x

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG Version 2 Version 12
- Ubuntu 20.04 STIG Version 1 Version 10

STIG-Build-Linux-Medium Version 2023.4.x

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG Version 2 Version 12
- Ubuntu 20.04 STIG Version 1 Version 10

STIG-Build-Linux-High Version 2023.4.x

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG Version 2 Version 12
- Ubuntu 20.04 STIG Version 1 Version 10

Änderungen am Q3 2023 – 10/04/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des dritten Quartals 2023 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 9

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 9

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 9

Änderungen für Q2 2023 – 05/03/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des zweiten Quartals 2023 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 8

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 8

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG Version 2 Version 11
- Ubuntu 20.04 STIG Version 1 Version 8

Änderungen für Q1 2023 – 03/27/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des ersten Quartals 2023 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG Version 2 Version 10
- Ubuntu 20.04 STIG Version 1 Version 7

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG Version 2 Version 10
- Ubuntu 20.04 STIG Version 1 Version 7

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG Version 2 Version 10
- Ubuntu 20.04 STIG Version 1 Version 7

Änderungen für Q4 2022 – 02/01/2023:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des vierten Quartals 2022 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG Version 2 Version 9

- Ubuntu 20.04 STIG Version 1 Version 6

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG Version 2 Version 9
- Ubuntu 20.04 STIG Version 1 Version 6

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG Version 2 Version 9
- Ubuntu 20.04 STIG Version 1 Version 6

Änderungen für Q3 2022 – 09/30/2022 (keine Änderungen):

Für die Veröffentlichung des dritten Quartals 2022 wurden keine Änderungen für die Linux-Komponente STIGS vorgenommen.

Änderungen für Q2 2022 – 08/02/2022:

Ubuntu-Unterstützung eingeführt, STIG-Versionen aktualisiert und STIGS für das zweite Quartal 2022 angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 7
- RHEL 8 STIG Version 1 Version 6
- Ubuntu 18.04 STIG Version 2 Version 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 7

- RHEL 8 STIG Version 1 Version 6
- Ubuntu 18.04 STIG Version 2 Version 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 7
- RHEL 8 STIG Version 1 Version 6
- Ubuntu 18.04 STIG Version 2 Version 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Änderungen für Q1 2022 – 04/26/2022:

Faktorwechsel, um eine bessere Unterstützung für Container einzuschließen. Das vorherige AL2-Skript wurde mit RHEL 7 kombiniert. Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des ersten Quartals 2022 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Änderungen für Q4 2021 – 12/20/2021:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des vierten Quartals 2021 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 5
- RHEL 8 STIG Version 1 Version 4

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 5
- RHEL 8 STIG Version 1 Version 4

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 5
- RHEL 8 STIG Version 1 Version 4

Änderungen am Q3 2021 – 09/30/2021:

Aktualisierte STIG-Versionen und angewandte STIGS für die Veröffentlichung des dritten Quartals 2021 wie folgt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Version 4
- RHEL 8 STIG Version 1 Version 3

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Version 4
- RHEL 8 STIG Version 1 Version 3

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Version 4
- RHEL 8 STIG Version 1 Version 3

# AWSEC2-PatchLoadBalancerInstance

Beschreibung

Aktualisieren und patchen Sie eine Nebenversion einer Amazon EC2-Instance (Windows oder Linux), die an einen beliebigen Load Balancer (Classic, ALB oder NLB) angeschlossen ist. Die Standardzeit für den Verbindungsabbau wird angewendet, bevor die Instanz gepatcht wird. Sie können die Wartezeit überschreiben, indem Sie Ihre benutzerdefinierte Entleerungszeit in Minuten (1-59) für den ConnectionDrainTimeParameter eingeben.

Der Automatisierungsablauf sieht wie folgt aus:

1. Der Load Balancer oder die Zielgruppe, an die die Instance angehängt ist, wird bestimmt, und die Instance wird als fehlerfrei verifiziert.
2. Die Instance wird aus dem Load Balancer oder der Zielgruppe entfernt.
3. Die Automatisierung wartet auf den angegebenen Zeitraum, in dem die Verbindung leerläuft.
4. Die RunPatchBaselineAWS-Automatisierung wird aufgerufen, um die Instance zu patchen.
5. Die Instance wird erneut an den Load Balancer oder die Zielgruppe angehängt.

Diese Automatisierung ausführen (Konsole)

Dokumenttyp

-Automatisierung

Eigentümer

Amazon

Voraussetzungen

- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agenten auf EC2-Instances für Windows Server.

Parameter

- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) ID der zu patchenden Instanz, die einem Load Balancer (Classic, ALB oder NLB) zugeordnet ist.

- ConnectionDrainTime

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Zeit, in der der Load Balancer die Verbindung verbraucht, in Minuten (1-59).

## AWSEC2-SQLServerDBRestore

Beschreibung

Das `AWSEC2-SQLServerDBRestore` Runbook stellt in Amazon S3 gespeicherte Microsoft SQL Server-Datenbanksicherungen auf SQL Server 2017 wieder her, die auf einer Amazon Elastic Compute Cloud (EC2) Linux-Instance ausgeführt werden. Sie können Ihre eigene EC2-Instance mit SQL Server 2017 Linux bereitstellen. Wenn keine EC2-Instance bereitgestellt wird, startet und konfiguriert die Automatisierung eine neue Ubuntu 16.04 EC2-Instance mit SQL Server 2017. Die Automatisierung unterstützt die Wiederherstellung vollständiger, differenzierter und transaktionaler Protokollsicherungen. Diese Automatisierung akzeptiert mehrere Datenbank-Sicherungsdateien und stellt die neueste gültige Sicherung der einzelnen Datenbanken in den bereitgestellten Dateien wieder her.

Um sowohl die Sicherung als auch die Wiederherstellung einer lokalen SQL Server-Datenbank auf einer EC2-Instance zu automatisieren, auf der SQL Server 2017 Linux ausgeführt wird, können Sie das AWS PowerShell -signierte Skript verwenden. `MigrateSQLServerToEC2Linux`

> **Important**
>
> Dieses Runbook setzt das Benutzerkennwort des SQL Server-Server-Administrators (SA) bei jeder Ausführung der Automatisierung zurück. Nach Abschluss der Automatisierung müssen Sie erneut Ihr eigenes SA-Benutzerkennwort festlegen, bevor Sie eine Verbindung zur SQL Server-Instanz herstellen.

Diese Automatisierung ausführen (Konsole)

Dokumenttyp

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

## Voraussetzungen

Um diese Automatisierung auszuführen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Dem IAM-Benutzer oder der IAM-Rolle, der diese Automatisierung ausführt, muss eine Inline-Richtlinie mit den unter beschriebenen Berechtigungen zugeordnet sein. Erforderliche IAM-Berechtigungen
- Wenn Sie Ihre eigene EC2-Instance bereitstellen:
  - Die von Ihnen bereitgestellte EC2-Instance muss eine Linux-Instance sein, auf der Microsoft SQL Server 2017 ausgeführt wird.
  - Die von Ihnen bereitgestellte EC2-Instance muss mit einem AWS Identity and Access Management (IAM-) Instance-Profil konfiguriert sein, an das die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie angehängt ist. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
  - Der SSM-Agent muss auf Ihrer EC2-Instance installiert sein. Weitere Informationen finden Sie unter Installation und Konfiguration des SSM-Agenten auf EC2-Instances für Linux.
  - Die EC2-Instance muss über ausreichend freien Speicherplatz verfügen, um die SQL Server-Backups herunterzuladen und wiederherzustellen.

## Einschränkungen

Diese Automatisierung unterstützt keine Wiederherstellung auf SQL Server auf EC2-Instances für Windows Server. Diese Automatisierung stellt nur Datenbanksicherungen wieder her, die mit SQL Server Linux 2017 kompatibel sind. Weitere Informationen finden Sie unter Editionen und unterstützte Funktionen von SQL Server 2017 auf Linux.

## Parameter

Diese Automatisierung hat die folgenden Parameter:

- DatabaseNames

  Typ: Zeichenfolge

  Beschreibung: (Optional) Durch Komma getrennte Liste der Namen der wiederherzustellenden Datenbanken.
- DataDirectorySize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-Datenverzeichnisses für die neue EC2-Instance.

  Standardwert: 100
- KeyPair

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das beim Erstellen der neuen EC2-Instance zu verwendende Schlüsselpaar.
- IamInstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das IAM-Instance-Profil, das an die neue EC2-Instance angehängt werden soll. An das IAM-Instanzprofil muss die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie angehängt sein.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Instance mit SQL Server 2017 auf Linux. Wenn keine Angabe InstanceId erfolgt, startet die Automatisierung eine neue EC2-Instance unter Verwendung der ServerEdition bereitgestellten InstanceType und SQL-Anweisungen.
- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ der zu startenden EC2-Instance.
- iSS 3 PresignedUrl

Typ: Zeichenfolge

Beschreibung: (Optional) Geben Sie an, ob S3Input eine vorsignierte S3-URL ist. `yes`

Standardwert: nein

Gültige Werte: ja | nein

- LogDirectorySize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-Protokollverzeichnisses für die neue EC2-Instance.

  Standardwert: 100

- S3-Eingang

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket-Name, durch Komma getrennte Liste der S3-Objektschlüssel oder durch Komma getrennte Liste der vorsignierten S3-URLs mit den SQL-Sicherungsdateien für die Wiederherstellung.

- SQL ServerEdition

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Edition von SQL Server 2017 zur Installation auf der neu erstellten EC2-Instance.

  Gültige Werte: Standard | Enterprise | Web | Express

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Subnetz, in dem die neue EC2-Instance gestartet wird. Das Subnetz muss ausgehende Konnektivität zu den AWS-Services aufweisen. Wenn kein Wert für angegeben SubnetId wird, verwendet die Automatisierung das Standardsubnetz.

- TempDbDirectorySize

Typ: Zeichenfolge

Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-TempDB-Verzeichnisses für die neue EC2-Instance.

Standardwert: 100

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

### Dokumentschritte

Um diese Automatisierung zu verwenden, folgen Sie den Schritten, die für Ihren Instance-Typ gelten:

Für neue EC2-Instances:

1. `aws:executeAwsApi`- Rufen Sie die AMI-ID für SQL Server 2017 auf Ubuntu 16.04 ab.
2. `aws:runInstances`- Starten Sie eine neue EC2-Instance für Linux.
3. `aws:waitForAwsResourceProperty`- Warten Sie, bis die neu erstellte EC2-Instance bereit ist.
4. `aws:executeAwsApi`- Starten Sie die Instanz neu, falls die Instanz nicht bereit ist.
5. `aws:assertAwsResourceProperty`- Stellen Sie sicher, dass der SSM Agent installiert ist.
6. `aws:runCommand`- Führen Sie das SQL Server-Wiederherstellungsskript in ausPowerShell.

Für vorhandene EC2-Instances:

1. `aws:waitForAwsResourceProperty`- Stellen Sie sicher, dass die EC2-Instance bereit ist.
2. `aws:executeAwsApi`- Starten Sie die Instanz neu, falls die Instanz nicht bereit ist.
3. `aws:assertAwsResourceProperty`- Stellen Sie sicher, dass der SSM Agent installiert ist.
4. `aws:runCommand`- Führen Sie das SQL Server-Wiederherstellungsskript in ausPowerShell.

### Ausgaben

Instanz abrufen. InstanceId

restoreToNewInstanz.Output

restoreToExistingInstanz.Output

## AWSSupport-ActivateWindowsWithAmazonLicense

### Beschreibung

Das `AWSSupport-ActivateWindowsWithAmazonLicense` Runbook aktiviert eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance für Windows Server mit einer von Amazon bereitgestellten Lizenz. Die Automatisierung überprüft und konfiguriert die erforderlichen Betriebssystemeinstellungen des Schlüsselverwaltungsdienstes und versucht die Aktivierung.

Dazu gehören Betriebssystemrouten zu den Schlüsselverwaltungsservern von Amazon und die Betriebssystemeinstellungen des Schlüsselverwaltungsdienstes. Das Festlegen des `AllowOffline`-Parameter auf „`true`“ kann die Automatisierung erfolgreich auf Instances abzielen lassen, die nicht von AWS Systems Manager verwaltet werden, dafür ist jedoch ein Stopp und ein Start der Instance erforderlich.

> **Note**
>
> Dieses Runbook kann nicht für Bring Your Own License (BYOL) Windows Server - Modellinstanzen verwendet werden. Informationen zur Verwendung Ihrer eigenen Lizenz finden Sie unter Microsoft-Lizenzierung in AWS.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Legen Sie fest, `true` ob Sie eine Offline-Windows-Aktivierung zulassen, falls die Online-Problembehandlung fehlschlägt oder wenn es sich bei der bereitgestellten Instanz nicht um eine verwaltete Instanz handelt.

> **Important**
>
> Die Offline-Methode erfordert, die bereitgestellte EC2-Instance anzuhalten und dann neu zu starten. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ForceActivation

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Stellen Sie es auf, `true` wenn Sie fortfahren möchten, auch wenn Windows bereits aktiviert ist.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer verwalteten EC2-Instance für Windows Server.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Nur offline – Die Subnetz-ID für die EC2Rescue-Instance zum Ausführen der Offline-Fehlerbehebung. Verwenden Sie `SelectedInstanceSubnet` es, um dasselbe Subnetz wie Ihre Instance zu verwenden, oder verwenden Sie `CreateNewVPC` es, um eine neue

VPC zu erstellen. WICHTIG: Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Wir empfehlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Sie benötigen mindestens ssm: StartAutomationExecution und ssm:, SendCommand um die Automatisierung auszuführen und den Befehl an die Instanz zu senden, sowie ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können. Informationen zur Offline-Korrektur finden Sie in den erforderlichen Berechtigungen von`AWSSupport-StartEC2RescueWorkflow`.

### Dokumentschritte

1. `aws:assertAwsResourceProperty`- Überprüfen Sie, ob die Plattform der bereitgestellten Instanz Windows ist.
2. `aws:assertAwsResourceProperty`— Bestätigen Sie, dass es sich bei der bereitgestellten Instanz um eine verwaltete Instanz handelt:
   a. (Online-Aktivierungsfix) Wenn es sich bei der Eingabeinstanz um eine verwaltete Instanz handelt, führen Sie den Befehl aus, `aws:runCommand` um das PowerShell Skript auszuführen und zu versuchen, die Windows-Aktivierung zu korrigieren.
   b. (Offline-Aktivierungsreparatur) Wenn die Eingabe-Instance keine verwaltete Instance ist:
      i. `aws:assertAwsResourceProperty`- Überprüft, ob die `AllowOffline` Flagge auf `true` gesetzt ist. Wenn ja, beginnt der Offline-Fix; andernfalls endet die Automatisierung.
      ii. `aws:executeAutomation`- `AWSSupport-StartEC2RescueWorkflow` Mit dem Offline-Fix-Skript für die Windows-Aktivierung aufrufen. Das Skript verwendet je nach Betriebssystemversion entweder EC2Config oder EC2Launch.
      iii. `aws:executeAwsApi`- Lesen Sie das Ergebnis von`AWSSupport-StartEC2RescueWorkflow`.

### Ausgaben

activateWindows.Output

getActivateWindowsOfflineResult.Ausgang

## AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Beschreibung

Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook analysiert die Konnektivität von einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance oder Elastic Network-Schnittstelle zu einem AWS-Service Endpunkt. IPv6 wird nicht unterstützt. Das Runbook verwendet den Wert, den Sie für den `ServiceEndpoint` Parameter angeben, um die Konnektivität zu einem Endpunkt zu analysieren. Wenn in Ihrer VPC kein AWS PrivateLink Endpunkt gefunden werden kann, verwendet das Runbook eine öffentliche IP-Adresse für den Service in der aktuellen AWS-Region. Diese Automatisierung verwendet Reachability Analyzer von Amazon Virtual Private Cloud . Weitere Informationen finden Sie unter Was ist Reachability Analyzer? in Reachability Analyzer.

Diese Automatisierung überprüft Folgendes:

- Prüft, ob Ihre Virtual Private Cloud (VPC) für die Verwendung des von Amazon bereitgestellten DNS-Servers konfiguriert ist.
- Prüft, ob in der VPC ein AWS PrivateLink Endpunkt für die AWS-Service von Ihnen angegebene vorhanden ist. Wenn ein Endpunkt gefunden wird, überprüft die Automatisierung, ob das `privateDns` Attribut aktiviert ist.
- Prüft, ob der AWS PrivateLink Endpunkt die Standard-Endpunktrichtlinie verwendet.

Überlegungen

- Sie zahlen pro Analyselauf zwischen einer Quelle und einem Ziel. Weitere Informationen dazu finden Sie unter Amazon VPC – Preise.
- Während der Automatisierung werden ein Netzwerkerkenntnispfad und eine Netzwerkerkenntnisanalyse erstellt. Wenn die Automatisierung erfolgreich abgeschlossen wurde, löscht das Runbook diese Ressourcen. Wenn der Bereinigungsschritt fehlschlägt, wird der Pfad für Netzwerkerkenntnisse nicht vom Runbook gelöscht und Sie müssen ihn manuell löschen. Wenn Sie den Netzwerkerkenntnispfad nicht manuell löschen, wird er weiterhin auf das Kontingent für Ihr angerechnet AWS-Konto. Weitere Informationen zu Kontingenten für Reachability Analyzer finden Sie unter Kontingente für Reachability Analyzer in Reachability Analyzer.

- Konfigurationen auf Betriebssystemebene wie die Verwendung eines Proxys, eines lokalen DNS-Resolvers oder einer Hostdatei können sich auf die Konnektivität auswirken, auch wenn Reachability Analyzer zurückgibt`PASS`.
- Überprüfen Sie die Bewertung aller vom Reachability Analyzer durchgeführten Prüfungen. Wenn eine der Prüfungen den Status zurückgibt`FAIL`, kann sich dies auf die Konnektivität auswirken, auch wenn die gesamte Erreichbarkeitsprüfung den Status zurückgibt`PASS`.

## Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Quelle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance oder der Netzwerkschnittstelle, von der aus Sie die Erreichbarkeit analysieren möchten.
- ServiceEndpoint

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Hostname des Service-Endpunkts, für den Sie die Erreichbarkeit analysieren möchten.

- RetainVpcReachabilityAnalysis

  Typ: Zeichenfolge

  Standard: false

  Beschreibung: (Optional) Bestimmt, ob der Netzwerkerkenntnispfad und die erstellte zugehörige Analyse beibehalten werden. Standardmäßig werden die Ressourcen, die für die Analyse der Erreichbarkeit verwendet werden, nach erfolgreicher Analyse gelöscht. Wenn Sie die Analyse beibehalten möchten, löscht das Runbook die Analyse nicht und Sie können sie in der Amazon-VPC-Konsole visualisieren. Ein Konsolenlink ist in der Automatisierungsausgabe verfügbar.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:executeScript`: Validiert den Service-Endpunkt, indem versucht wird, den Hostnamen aufzulösen.
2. `aws:executeScript`: Sammelt Details zur VPC und zum Subnetz.
3. `aws:executeScript`: Wertet die DNS-Konfiguration der VPC aus.
4. `aws:executeScript`: Wertet die VPC-Endpunktprüfungen aus.
5. `aws:executeScript`: Lokalisiert ein Internet-Gateway, um eine Verbindung zum öffentlichen Service-Endpunkt herzustellen.
6. `aws:executeScript`: Bestimmt das Ziel, das für die Erreichbarkeitsanalyse verwendet werden soll.
7. `aws:executeScript`: Analysiert die Erreichbarkeit von der Quelle zum Endpunkt mithilfe von Reachability Analyzer und bereinigt die Ressourcen, wenn die Analyse erfolgreich ist.
8. `aws:executeScript`: Generiert einen Bericht zur Bewertung der Erreichbarkeit.
9. `aws:executeScript`: Generiert die Ausgabe in JSON.

Ausgaben

- `generateReport.EvalReport` – Die Ergebnisse der von der Automatisierung durchgeführten Prüfungen im Textformat.
- `generateJsonOutput.Output` – Eine minimale Version der Ergebnisse im JSON-Format.

## AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Beschreibung

Das `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` Runbook automatisiert Migrationen von von Intel betriebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu den entsprechenden von AMD betriebenen Instance-Typen. Dieses Runbook unterstützt General Purpose (M), Burstable General Purpose (T), rechenoptimierte (C) und speicheroptimierte (R)

Instances, die auf dem Nitro-System basieren. Dieses Runbook kann auf Instanzen verwendet werden, die nicht von Systems Manager verwaltet werden.

Um das potenzielle Risiko von Datenverlusten und Ausfallzeiten zu reduzieren, überprüft das Runbook das Stoppverhalten der Instance, ob sich die Instance in einer Amazon EC2 Auto Scaling-Gruppe befindet, den Zustand der Instance und ob der entsprechende von AMD betriebene Instance-Typ in derselben Availability Zone verfügbar ist. Standardmäßig ändert dieses Runbook den Instance-Typ nicht, wenn Instance-Speicher-Volumes angehängt sind oder wenn die Instance Teil eines AWS CloudFormation Stacks ist. Wenn Sie dieses Verhalten ändern möchten, geben Sie `yes` für einen der `AllowCloudFormationInstances` Parameter `AllowInstanceStoreInstances` und an.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist entweder ein Enterprise- oder ein Business Support-Abonnement erforderlich. Weitere Informationen finden Sie unter AWS SupportTarife vergleichen.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden.
- Wenn Sie den Instance-Typ ändern, muss das Runbook Ihre Instance stoppen. Wenn eine Instance gestoppt wird, gehen alle im RAM oder auf den Instance-Speichervolumes gespeicherten Daten verloren und die automatische öffentliche IPv4-Adresse wird freigegeben. Weitere Informationen finden Sie unter Anhalten und Starten Ihrer Instance.
- Wenn Sie keinen Wert für den `TargetInstanceType` Parameter angeben, versucht das Runbook, die entsprechende AMD-Instance in Bezug auf virtuelle CPUs und Arbeitsspeicher innerhalb derselben Instance-Familie zu identifizieren. Das Runbook wird beendet, wenn es keinen gleichwertigen AMD-Instance-Typ identifizieren kann.
- Mithilfe der `DryRun` Option können Sie den entsprechenden AMD-Instance-Typ erfassen und die Anforderungen validieren, ohne den Instance-Typ tatsächlich zu ändern.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Bestätigen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Geben Sie ein, `yes` um zu bestätigen, dass Ihre Zielinstanz gestoppt wird, falls sie läuft.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, deren Typ Sie ändern möchten.
- TargetInstanceType

  Typ: Zeichenfolge

  Standard: automatisch

  Beschreibung: (Optional) Der AMD-Instance-Typ, auf den Sie Ihre Instance ändern möchten. Der `automatic` Standardwert verwendet den entsprechenden Instance-Typ in Bezug auf virtuelle CPUs und Arbeitsspeicher. Beispielsweise würde ein m5.large in m5a.large geändert werden.
- AllowInstanceStoreInstances

  Typ: Zeichenfolge

Gültige Werte: nein | ja

Standard: no

Beschreibung: (Optional) Wenn Sie angebenyes, wird das Runbook auf Instances ausgeführt, an die Instance-Speicher-Volumes angehängt sind.

- AllowCloudFormationInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn auf gesetztyes, wird das Runbook auf Instanzen ausgeführt, die Teil eines AWS CloudFormation Stacks sind.

- AllowCrossGeneration

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn diese Option auf gesetzt istyes, versucht das Runbook, den neuesten äquivalenten AMD-Instance-Typ innerhalb derselben Instance-Familie zu finden.

- DryRun

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn auf gesetztyes, gibt das Runbook den entsprechenden AMD-Instance-Typ zurück und validiert die Migrationsanforderungen, ohne Änderungen am Instance-Typ vorzunehmen.

- SleepWait

  Typ: Zeichenfolge

Standard: PT3S

Beschreibung: (Optional) Die Zeit, die das Runbook warten sollte, bevor eine neue Automatisierung gestartet wird. Der Wert, den Sie für diesen Parameter angeben, muss der Norm ISO 8601 entsprechen. Weitere Informationen zum Erstellen von ISO 8601-Zeichenketten finden Sie unter Formatieren von Datums- und Uhrzeitzeichenfolgen für Systems Manager.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

### Dokumentschritte

1. `aws:assertAwsResourceProperty`: Bestätigt, dass der Status der Amazon EC2-Zielinstanz`running`, `pending``stopped`, oder `stopping` lautet. Andernfalls endet die Automatisierung.
2. `aws:executeAwsApi`: Ruft Eigenschaften von der Amazon EC2-Zielinstanz ab.
3. `aws:branch`: Zweigt die Automatisierung auf der Grundlage des Status der Amazon EC2-Instance ab.

   a. Falls `stopped` oder`stopping`, wird die Automatisierung ausgeführt, `aws:waitForAwsResourceProperty` bis die Amazon EC2-Instance vollständig gestoppt ist.

   b. Falls `running` oder`pending`, wird die Automatisierung ausgeführt, `aws:waitForAwsResourceProperty` bis die Amazon EC2-Instance die Statusprüfungen bestanden hat.

4. `aws:assertAwsResourceProperty`: Bestätigt, dass die Amazon EC2-Instance nicht Teil einer Auto Scaling-Gruppe ist, indem überprüft wird, ob das `aws:autoscaling:groupName` Tag angewendet wurde.
5. `aws:executeAwsApi`: Sammelt die aktuellen Instance-Typ-Eigenschaften, um den entsprechenden AMD-Instance-Typ zu finden.
6. `aws:assertAwsResourceProperty`: Bestätigt, dass kein AWS Marketplace Produktcode mit der Amazon EC2-Instance verknüpft ist. Einige Produkte sind nicht für alle Instance-Typen verfügbar.
7. `aws:branch`: Zweigt die Automatisierung ab, je nachdem, ob die Automatisierung überprüfen soll, ob die Amazon EC2-Instance Teil eines AWS CloudFormation Stacks ist

   a. Wenn das `aws:cloudformation:stack-name` Tag auf die Instanz angewendet wird, wird die Automatisierung ausgeführt, `aws:assertAwsResourceProperty` um zu bestätigen, dass die Instanz nicht Teil eines AWS CloudFormation Stacks ist.

8. `aws:branch`: Die Automatisierung erfolgt in Abhängigkeit davon, ob es sich bei dem Instance-Root-Volumetyp um Amazon Elastic Block Store (Amazon EBS) handelt.
9. `aws:assertAwsResourceProperty`: Bestätigt, dass das Verhalten beim Herunterfahren der Instanz ist `stop` und nicht`terminate`.
10. `aws:executeScript`: Bestätigt, dass es nur eine Automatisierung dieses Runbooks gibt, die auf die aktuelle Instanz abzielt. Wenn bereits eine weitere Automatisierung läuft, die auf dieselbe Instanz abzielt, gibt sie einen Fehler zurück und wird beendet.
11. `aws:executeAwsApi`: Gibt eine Liste der AMD-Instance-Typen mit derselben Menge an Arbeitsspeicher und vCPUs zurück.
12. `aws:executeScript`: Prüft, ob der aktuelle Instance-Typ unterstützt wird, und gibt den entsprechenden AMD-Instance-Typ zurück. Wenn es kein Äquivalent gibt, endet die Automatisierung.
13. `aws:executeScript`: Bestätigt, dass der AMD-Instance-Typ in derselben Availability Zone verfügbar ist, und überprüft die bereitgestellten IAM-Berechtigungen.
14. `aws:branch`: Verzweigt die Automatisierung je nachdem, ob der `DryRun` Parameterwert ist`yes`.

15. `aws:branch`: Prüft, ob der ursprüngliche Instance-Typ und der Ziel-Instance-Typ identisch sind. Wenn sie identisch sind, endet die Automatisierung.
16. `aws:executeAwsApi`: Ruft den aktuellen Instanzstatus ab.
17. `aws:changeInstanceState`: Stoppt die Amazon EC2-Instance.
18. `aws:changeInstanceState`: Erzwingt das Stoppen der Instanz, wenn sie im Stopping-Status feststeckt.
19. `aws:executeAwsApi`: Ändert den Instance-Typ in den Ziel-AMD-Instance-Typ.
20. `aws:sleep`: Wartet nach dem Ändern des Instanztyps 3 Sekunden, um die Konsistenz sicherzustellen.
21. `aws:branch`: Zweigt die Automatisierung auf der Grundlage des vorherigen Instanzstatus ab. Wenn ja`running`, wird die Instanz gestartet.
    a. `aws:changeInstanceState`: Startet die Amazon EC2-Instance, falls sie vor der Änderung des Instance-Typs ausgeführt wurde.
    b. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2-Instance die Statusprüfungen bestanden hat. Wenn die Instance die Statusprüfungen nicht besteht, wird die Instance wieder auf ihren ursprünglichen Instance-Typ zurückgesetzt.
        i. `aws:changeInstanceState`: Stoppt die Amazon EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird.
        ii. `aws:changeInstanceState`: Erzwingt das Stoppen der Amazon EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird, falls sie in einem Stopp-Zustand stecken bleibt.
        iii. `aws:executeAwsApi`: Ändert die Amazon EC2-Instance auf ihren ursprünglichen Typ.
        iv. `aws:sleep`: Wartet nach dem Ändern des Instanztyps 3 Sekunden, um die Konsistenz sicherzustellen.
        v. `aws:changeInstanceState`: Startet die Amazon EC2-Instance, falls sie vor der Änderung des Instance-Typs ausgeführt wurde.
        vi. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2-Instance die Statusprüfungen bestanden hat.
22. `aws:sleep`: Wartet, bevor das Runbook beendet wird.

## AWSSupport-CheckXenToNitroMigrationRequirements

Beschreibung

Das `AWSSupport-CheckXenToNitroMigrationRequirements` Runbook überprüft, ob eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance die Voraussetzungen erfüllt, um den Instance-Typ erfolgreich von einer Xen-Instance in einen Nitro-basierten Instance-Typ zu ändern. Diese Automatisierung überprüft Folgendes:

- Das Root-Gerät ist ein Amazon Elastic Block Store (Amazon EBS) -Volume.
- Das `enaSupport` Attribut ist aktiviert.
- Das ENA-Modul ist auf der Instance installiert.
- Das NVMe-Modul ist auf der Instance installiert. Falls ja, ist das Modul installiert und ein Skript überprüft, ob das Modul in das `initramfs` Image geladen ist.
- Analysiert `/etc/fstab` und sucht nach Blockgeräten, die mithilfe von Gerätenamen gemountet werden.
- Legt fest, ob das Betriebssystem (OS) standardmäßig vorhersehbare Netzwerkschnittstellennamen verwendet.

Dieses Runbook unterstützt die folgenden Betriebssysteme:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server15 SP2
- SUSE Linux Enterprise Server12 SP5

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Standard: false

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, für die Sie die Voraussetzungen überprüfen möchten, bevor Sie zu einem Nitro-basierten Instance-Typ migrieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeAwsApi`- Sammelt Details über die Instanz.
- `aws:executeAwsApi`- Sammelt Informationen über den Hypervisor für die Instanz.
- `aws:branch`- Branches basierend darauf, ob auf der Ziel-Instance bereits ein Nitro-basierter Instance-Typ ausgeführt wird.
- `aws:branch`- Prüft, ob das Betriebssystem der Instance von Nitro-basierten Instances unterstützt wird.
- `aws:assertAwsResourceProperty`- Überprüft, ob die von Ihnen angegebene Instanz vom Systems Manager verwaltet wird und ob der Status lautet`Online`.
- `aws:branch`— Branches basierend darauf, ob es sich bei dem Root-Gerät der Instance um ein Amazon EBS-Volume handelt.
- `aws:branch`- Verzweigungen basierend darauf, ob das ENA-Attribut für die Instanz aktiviert ist.
- `aws:runCommand`- Sucht auf der Instance nach ENA-Treibern.
- `aws:runCommand`- Sucht auf der Instance nach NVMe-Treibern.
- `aws:runCommand`- Prüft die `fstab` Datei auf unbekannte Formate.
- `aws:runCommand`- Prüft, ob die Konfiguration des Schnittstellennamens auf der Instanz vorhersehbar ist.
- `aws:executeScript`- Generiert eine Ausgabe auf der Grundlage früherer Schritte.

Ausgaben

finalOutput.Output — Die Ergebnisse der von der Automatisierung durchgeführten Prüfungen.

## AWSSupport-ConfigureEC2Metadata

Beschreibung

Dieses Runbook hilft Ihnen bei der Konfiguration von IMDS-Optionen (Instance Metadata Service) für Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Mit diesem Runbook können Sie Folgendes konfigurieren:

- Erzwingen Sie die Verwendung von IMDSv2 für Instanzmetadaten.
- Konfigurieren Sie den Wert`HttpPutResponseHopLimit`.
- Erlauben oder verweigern Sie den Zugriff auf Instanz-Metadaten.

Weitere Informationen zu Instance-Metadaten finden Sie unter Configuring the Instance Metadata Service im Amazon EC2 EC2-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Erzwingen Sie IMDSv2

  Typ: Zeichenfolge

  Gültige Werte: erforderlich | optional

Standard: optional

Beschreibung: (Optional) IMDSv2 erzwingen. Wenn Sie möchten`required`, verwendet die Amazon EC2 EC2-Instance nur IMDSv2. Wenn Sie möchten`optional`, können Sie für den Zugriff auf Metadaten zwischen IMDSv1 und IMDSv2 wählen.

> **Important**
>
> Wenn Sie IMDSv2 erzwingen, funktionieren Anwendungen, die IMDSv1 verwenden, möglicherweise nicht richtig. Bevor Sie IMDSv2 durchsetzen, stellen Sie sicher, dass Ihre Anwendungen, die IMDS verwenden, auf eine Version aktualisiert wurden, die IMDSv2 unterstützt. Informationen zu Instance Metadata Service Version 2 (IMDSv2) finden Sie unter Configuring the Instance Metadata Service im Amazon EC2 EC2-Benutzerhandbuch.

- HttpPutResponseHopLimit

  Typ: Ganzzahl

  Gültige Werte: 0-64

  Standard: 0

  Beschreibung: (Optional) Der gewünschte Grenzwert (1—64) für HTTP-PUT-Antwort-Hop-Anfragen für Instance-Metadaten. Dieser Wert steuert die Anzahl der Hops, die die PUT-Antwort durchlaufen kann. Um zu verhindern, dass die Antwort die Instanz verlässt, geben Sie 1 für den Parameter einen Wert an.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, deren Metadateneinstellungen Sie konfigurieren möchten.

- MetadataAccess

  Typ: Zeichenfolge

  Gültige Werte: aktiviert | deaktiviert

  Standard: aktiviert

Beschreibung: (Optional) Erlauben oder verweigern Sie den Zugriff auf Instance-Metadaten in der Amazon EC2 EC2-Instance. Wenn Sie dies angeben`disabled`, werden alle anderen Parameter ignoriert und der Metadatenzugriff für die Instance verweigert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

1. branch OnMetadataAccess — Verzweigt die Automatisierung auf der Grundlage des `MetadataAccess` Parameterwerts.
2. disableMetadataAccess — Ruft die ModifyInstanceMetadataOptions API-Aktion auf, um den Zugriff auf Metadaten-Endpunkte zu deaktivieren.
3. branch OnHttpPutResponseHopLimit — Verzweigt die Automatisierung auf der Grundlage des `HttpPutResponseHopLimit` Parameterwerts.
4. maintain HopLimitAndConfigureImdsVersion — Wenn 0 `HttpPutResponseHopLimit` ist, wird das aktuelle Hop-Limit beibehalten und andere Metadatenoptionen geändert.
5. wait BeforeAsserting IMDSv2State — Wartet 30 Sekunden, bevor der IMDSv2-Status bestätigt wird.
6. set HopLimitAndConfigureImdsVersion - Wenn größer als 0 `HttpPutResponseHopLimit` ist, werden die Metadatenoptionen unter Verwendung der angegebenen Eingabeparameter konfiguriert.
7. wait BeforeAssertingHopLimit — Wartet 30 Sekunden, bevor die Metadatenoptionen aktiviert werden.
8. assertHopLimit — Bestätigt, dass die `HttpPutResponseHopLimit` Eigenschaft auf den von Ihnen angegebenen Wert gesetzt ist.

9. branch VerificationOn IMDSv2Option — Überprüfung von Zweigen auf der Grundlage des Parameterwerts. `EnforceIMDSv2`
10. assertImDSv2 — Bestätigt den WertIsOptional , der auf gesetzt ist. `HttpTokens optional`
11. assertImDSv2 — Bestätigt den WertIsEnforced , der auf gesetzt ist. `HttpTokens required`
12. wait BeforeAssertingMetadataState — Wartet 30 Sekunden, bevor bestätigt wird, dass der Metadatenstatus deaktiviert ist.
13. assert MetadataIsDisabled — Bestätigt, dass Metadaten. `disabled`
14. describeMetadataOptions — Ruft die Metadatenoptionen ab, nachdem die von Ihnen angegebenen Änderungen übernommen wurden.

Ausgaben

beschreibe MetadataOptions .State

beschreibenMetadataOptions. MetadataAccess

beschreibe MetadataOptions .IMDSv2

MetadataOptionsbeschreiben. HttpPutResponseHopBegrenzen

## AWSSupport-CopyEC2Instance

Beschreibung

Das `AWSSupport-CopyEC2Instance` Runbook bietet eine automatisierte Lösung für das Verfahren, das im Knowledge Center-Artikel Wie verschiebe ich meine EC2-Instance in ein anderes Subnetz, eine Availability Zone oder VPC beschrieben wird? Die Automatisierung verzweigt sich je nach den Werten, die Sie für die `SubnetId` Parameter `Region` und angeben.

Wenn Sie einen Wert für den `SubnetId` Parameter angeben, aber keinen Wert für den `Region` Parameter, erstellt die Automatisierung eine Amazon Machine Image (AMI) der Ziel-Instance und startet eine neue Instance von der AMI in dem von Ihnen angegebenen Subnetz aus.

Wenn Sie einen Wert für den `SubnetId` Parameter und den `Region` Parameter angeben, erstellt die Automatisierung eine AMI der Zielinstanzen, kopiert sie in die AMI von AWS-Region Ihnen angegebene Instance und startet eine neue Instance von der AMI in dem von Ihnen angegebenen Subnetz.

Wenn Sie einen Wert für den `Region` Parameter angeben, aber keinen Wert für den `SubnetId` Parameter, erstellt die Automatisierung eine AMI der Zielinstanzen, kopiert sie AMI in die von Ihnen angegebene Region und startet eine neue Instance aus dem Standardsubnetz Ihrer Virtual Private Cloud (VPC) in der Zielregion. AMI

Wenn für die `SubnetId` Parameter `Region` oder kein Wert angegeben wird, erstellt die Automatisierung eine AMI der Ziel-Instances und startet eine neue Instance aus AMI dem Standardsubnetz Ihrer VPC.

Um eine AMI in eine andere Region zu kopieren, müssen Sie einen Wert für den `AutomationAssumeRole` Parameter angeben. Wenn bei der Automatisierung während des `waitForAvailableDestinationAmi` Schritts ein Timeout auftritt, wird AMI möglicherweise immer noch kopiert. In diesem Fall können Sie warten, bis der Kopiervorgang abgeschlossen ist, und die Instance manuell starten.

Bevor Sie diese Automatisierung ausführen, beachten Sie Folgendes:

- AMIs basieren auf Amazon Elastic Block Store (Amazon EBS) -Snapshots. Bei großen Dateisystemen ohne vorherigen Snapshot kann AMI die Erstellung mehrere Stunden dauern. Um die AMI Erstellungszeit zu verkürzen, erstellen Sie einen Amazon EBS-Snapshot, bevor Sie den AMI erstellen.
- Durch das Erstellen eines AMI wird kein Snapshot für Instance-Speicher-Volumes auf der Instance erstellt. Informationen zur Sicherung von Instance-Speicher-Volumes auf Amazon EBS finden Sie unter Wie sichere ich ein Instance-Speichervolume auf meiner Amazon EC2-Instance in Amazon EBS?
- Die neue Amazon EC2-Instance hat eine andere private IPv4- oder öffentliche IPv6-IP-Adresse. Sie müssen alle Verweise auf die alten IP-Adressen (z. B. in DNS-Einträgen) mit den neuen IP-Adressen aktualisieren, die der neuen Instanz zugewiesen sind. Wenn Sie in Ihrer Quell-Instance eine Elastic IP-Adresse verwenden, stellen Sie sicher, dass Sie sie an die neue Instance anhängen.
- Probleme mit dem Domain Security Identifier (SID) können auftreten, wenn die Kopie gestartet wird und versucht, die Domain zu kontaktieren. Bevor Sie das AMI erfassen, verwenden Sie Sysprep oder entfernen Sie die domänengebundene Instance aus der Domäne, um Konfliktprobleme zu vermeiden. Weitere Informationen finden Sie unter Wie kann ich Sysprep verwenden, um benutzerdefinierte wiederverwendbare Windows-AMIs zu erstellen und zu installieren?

Diese Automatisierung ausführen (Konsole)

> **Important**
>
> Es wird nicht empfohlen, dieses Runbook zum Kopieren von Microsoft Active Directory-Domänencontroller-Instanzen zu verwenden.

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, die Sie kopieren möchten.
- KeyPair

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselpaar, das Sie der neuen kopierten Instanz zuordnen möchten. Wenn Sie die Instance in eine andere Region kopieren, stellen Sie sicher, dass das Schlüsselpaar in der angegebenen Region vorhanden ist.

- Region

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Region, in die Sie die Instanz kopieren möchten. Wenn Sie einen Wert für diesen Parameter angeben, aber keine Werte für die `SecurityGroupIds` Parameter `SubnetId` und angeben, versucht die Automatisierung, die Instance in der Standard-VPC mit der Standardsicherheitsgruppe zu starten. Wenn EC2-Classic in der Zielregion aktiviert ist, schlägt der Start fehl.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in das Sie die Instance kopieren möchten. Wenn EC2-Classic in der Zielregion aktiviert ist, müssen Sie einen Wert für diesen Parameter angeben.

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ, als der die kopierte Instance gestartet werden soll. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Quellinstanztyp verwendet. Wenn der Quellinstanztyp in der Region, in die die Instanz kopiert wird, nicht unterstützt wird, schlägt die Automatisierung fehl.

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine durch Kommas getrennte Liste von Sicherheitsgruppen-IDs, die Sie der kopierten Instanz zuordnen möchten. Wenn Sie keinen Wert für diesen Parameter angeben und die Instanz nicht in eine andere Region kopiert wird, werden die der Quellinstanz zugeordneten Sicherheitsgruppen verwendet. Wenn Sie die Instance in eine andere Region kopieren, wird die Standardsicherheitsgruppe für die Standard-VPC in der Zielregion verwendet.

- KeepImageSourceRegion

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, löscht die Automatisierung die AMI der Quellinstanz nicht. Wenn Sie `false` für diesen Parameter angeben, hebt die Automatisierung die Registrierung der Snapshots auf AMI und löscht die zugehörigen Snapshots.

- KeepImageDestinationRegion

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, löscht die Automatisierung nicht dieAMI, die in die von Ihnen angegebene Region kopiert wurde. Wenn Sie `false` für diesen Parameter angeben, hebt die Automatisierung die Registrierung der Snapshots auf AMI und löscht die zugehörigen Snapshots.

- NoRebootInstanceBeforeTakingImage

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, wird die Quellinstanz nicht neu gestartet, bevor der AMI erstellt wird. Wenn diese Option verwendet wird, kann die Integrität des Dateisystems auf dem erstellten Image nicht garantiert werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`

- `ec2:RunInstances`

Wenn Sie die Instanz in eine andere Region kopieren, benötigen Sie außerdem die folgenden Berechtigungen.

- `ec2:CopyImage`

Dokumentschritte

- describeOriginalInstanceDetails — Ruft Details von der Instanz ab, die kopiert werden sollen.
- assertRootVolumeIsEbs- Prüft, ob der Root-Volume-Gerätetyp ist`ebs`, und beendet andernfalls die Automatisierung.
- evalInputParameters- Wertet die für die Eingabeparameter bereitgestellten Werte aus.
- createLocalAmi- Erzeugt eine AMI der Quellinstanzen.
- tagLocalAmi- Markiert das, AMI was im vorherigen Schritt erstellt wurde.
- branchAssertRegionIsSame- Branches, je nachdem, ob die Instanz innerhalb derselben Region oder in eine andere Region kopiert wird.
- branchAssertSameRegionWithKeyPair- Verzweigungen basierend darauf, ob ein Wert für den `KeyPair` Parameter für eine Instanz angegeben wurde, die innerhalb derselben Region kopiert wird.
- sameRegionLaunchInstanceWithKeyPair- Startet eine Amazon EC2-Instance AMI von der Quell-Instance aus im selben Subnetz oder in dem von Ihnen angegebenen Subnetz mithilfe des von Ihnen angegebenen Schlüsselpaars.
- sameRegionLaunchInstanceWithoutKeyPair- Startet eine Amazon EC2-Instance AMI von der Quell-Instance aus im selben Subnetz oder in dem von Ihnen angegebenen Subnetz ohne Schlüsselpaar.
- copyAmiToRegion — Kopiert AMI die in die Zielregion.
- waitForAvailableDestinationAmi- Wartet darauf, dass der kopierte AMI Zustand erreicht wird`available`.
- destinationRegionLaunchInstance — Startet eine Amazon EC2-Instance mithilfe der kopierten AMI Instance.
- branchAssertDestinationAmiToDelete- Zweige, die auf dem Wert basieren, den Sie für den `KeepImageDestinationRegion` Parameter angegeben haben.

- deregisterDestinationAmiAndDeleteSnapshots- Deregistriert die kopierten Snapshots AMI und löscht die zugehörigen Schnappschüsse.
- branchAssertSourceAmiTodelete- Zweige, die auf dem Wert basieren, den Sie für den `KeepImageSourceRegion` Parameter angegeben haben.
- deregisterSourceAmiAndDeleteSnapshots- Deregistriert die von der Quellinstanz AMI erstellten Snapshots und löscht die zugehörigen Snapshots.
- sleep — Die Automatisierung wird 2 Sekunden lang in den Ruhezustand versetzt. Dies ist ein letzter Schritt.

Ausgaben

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstanz. DestinationInstanceId

## AWSSupport-EnableWindowsEC2SerialConsole

Beschreibung

Das Runbook `AWSSupport-EnableWindowsEC2SerialConsole` hilft Ihnen, serielle Amazon EC2-Konsole, spezielle Admin-Konsole (SAC) und das Startmenü auf Ihrer Amazon EC2-Windows-Instance zu aktivieren. Mit der seriellen Konsolenfunktion von Amazon Elastic Compute Cloud (Amazon EC2) haben Sie Zugriff auf den seriellen Port Ihrer Amazon EC2-Instance, um Boot-, Netzwerkkonfigurations- und andere Probleme zu beheben. Das Runbook automatisiert die Schritte, die erforderlich sind, um die Funktion auf Instances zu aktivieren, die sich im laufenden Zustand befinden und von verwaltet werden AWS Systems Manager, sowie auf Instances, die sich im angehaltenen Zustand befinden oder nicht von verwaltet werden AWS Systems Manager.

Wie funktioniert es?

Das `AWSSupport-EnableWindowsEC2SerialConsole` Automatisierungs-Runbook hilft bei der Aktivierung von SAC und dem Startmenü auf Amazon EC2-Instances, auf denen Microsoft Windows Server ausgeführt wird. Für Instances, die sich im Ausführungsstatus befinden und von verwaltet werden AWS Systems Manager, führt das Runbook ein AWS Systems Manager Run Command- PowerShell Skript aus, um das SAC- und das Startmenü zu aktivieren. Für Instances im angehaltenen Zustand oder nicht von verwaltet AWS Systems Manager, verwendet das Runbook

AWSSupport-StartEC2RescueWorkflow, um eine temporäre Amazon EC2-Instance zu erstellen, um die erforderlichen Änderungen offline durchzuführen.

Weitere Informationen finden Sie unter Serielle Amazon EC2-Konsole für Windows-Instances.

**Important**

- Wenn Sie SAC auf einer Instance aktivieren, funktionieren die Amazon EC2-Services, die auf dem Passwortabruf angewiesen sind, nicht über die Amazon EC2Konsole. Weitere Informationen finden Sie unter SAC zur Fehlerbehhebung von Windows-Instances verwenden.
- Um den Zugriff auf die serielle Konsole zu konfigurieren, müssen Sie seriellen Konsolenzugriff auf Kontoebene gewähren und dann AWS Identity and Access Management (IAM)-Richtlinien konfigurieren, um Ihren Benutzern Zugriff zu gewähren. Sie müssen auch einen passwortbasierten Benutzer für jede Instance konfigurieren, damit Ihre Benutzer die serielle Konsole zur Fehlerbehebung verwenden können. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle Amazon EC2-Konsole.
- Informationen dazu, ob die serielle Konsole in Ihrem Konto aktiviert ist, finden Sie unter Anzeigen des Kontozugriffsstatus für die serielle Konsole.
- Der serielle Konsolenzugriff wird nur auf virtualisierten Instances unterstützt, die auf dem Nitro-System basieren.

Weitere Informationen finden Sie unter Voraussetzungen für die serielle Amazon EC2-Konsole. https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-serial-console-prerequisites.html

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

## Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie zur `AWSSupport-EnableWindowsEC2SerialConsole` in der - AWS Systems Manager Konsole.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId: (Erforderlich)

     Die ID der Amazon EC2-Instance, die die serielle Amazon EC2Konsole, (SAC) und das Startmenü aktivieren soll.
   - AutomationAssumeRole: (Optional)

     Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - HelperInstanceType: (bedingt)

     Der Typ der Amazon EC2-Instance, die das Runbook zur Konfiguration der seriellen Amazon EC2-Konsole für eine Offline-Instance bereitstellt.
   - HelperInstanceProfileName: (bedingt)

     Der Name eines vorhandenen IAM-Instance-Profils für die Hilfs-Instance. Wenn Sie das SAC- und Startmenü auf einer Instance aktivieren, die sich im angehaltenen Zustand befindet oder nicht von verwaltet wird AWS Systems Manager, ist dies erforderlich. Wenn kein IAM-Instance-Profil angegeben ist, erstellt die Automatisierung eines in Ihrem Namen.
   - SubnetId: (bedingt)

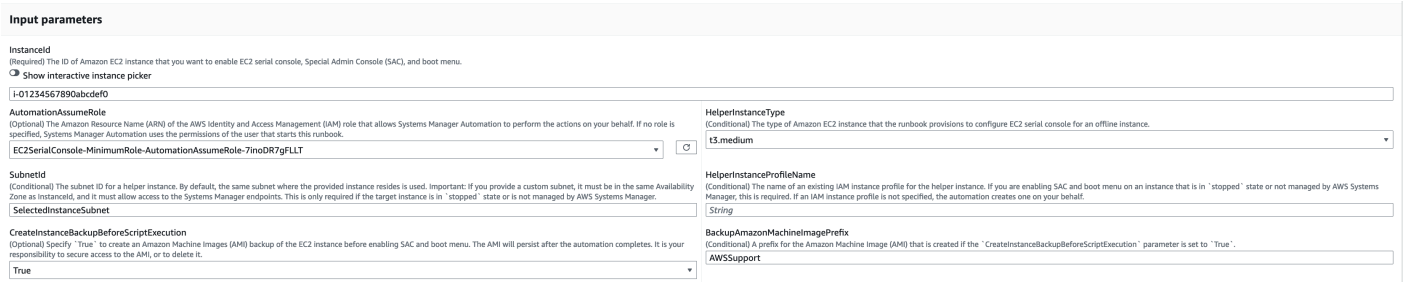
     Die Subnetz-ID für eine Hilfsinstanz. Standardmäßig wird dasselbe Subnetz verwendet, in dem sich die bereitgestellte Instance befindet.

     > **Important**
     >
     > Wenn Sie ein benutzerdefiniertes Subnetz bereitstellen, muss es sich in derselben Availability Zone wie befinden InstanceIdund den Zugriff auf die Systems Manager-Endpunkte erlauben. Dies ist nur erforderlich, wenn sich die Ziel-Instance im angehaltenen Zustand befindet oder nicht von verwaltet wird AWS Systems Manager.
   - CreateInstanceBackupBeforeScriptExecution: (Optional)

Geben Sie True an, um ein Amazon Machine Images (AMI)-Backup der Amazon EC2-Instance zu erstellen, bevor Sie das SAC- und das Startmenü aktivieren. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu sichern oder es zu löschen.

- BackupAmazonMachineImagePrefix: (bedingt)

  Ein Präfix für das Amazon Machine Image (AMI), das erstellt wird, wenn der `CreateInstanceBackupBeforeScriptExecution` Parameter auf festgelegt ist`True`.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckIfEc2SerialConsoleAccessEnabled:

     Prüft, ob der Zugriff auf die serielle Amazon EC2-Konsole auf Kontoebene aktiviert ist. Hinweis: Der Zugriff auf die serielle Konsole ist standardmäßig nicht verfügbar. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle Amazon EC2-Konsole.
   - CheckIfEc2InstanceIsWindows:

     Prüft, ob die Ziel-Instance-Plattform Windows ist.
   - GetInstanceType:

     Ruft den Instance-Typ der Ziel-Instance ab.
   - CheckIfInstanceTypeIsNitro:

     Prüft, ob der Hypervisor des Instance-Typs Nitro-basiert ist. Der serielle Konsolenzugriff wird nur auf virtualisierten Instances unterstützt, die auf dem Nitro-System basieren.
   - CheckIfInstanceIsInAutoScalingGruppe:

     Prüft, ob die Amazon EC2-Instance Teil einer Amazon EC2-Auto Scaling-Gruppe ist, indem die `DescribeAutoScalingInstances`-API aufgerufen wird. Wenn die Instance Teil einer

Amazon EC2 Auto Scaling-Gruppe ist, wird sichergestellt, dass sich die Portierungsassistent für .NET-Instance im Standby-Lebenszyklusstatus befindet.

- WaitForEc2InstanceStateStablized:

  Wartet, bis sich die Instance im laufenden oder angehaltenen Zustand befindet.

- GetEc2InstanceState:

  Ruft den aktuellen Status der Instance ab.

- BranchOnEc2InstanceState:

  Verzweigungen basierend auf dem Instance-Status, der im vorherigen Schritt abgerufen wurde. Wenn dieser Instance-Status ausgeführt wird, wird er zum `CheckIfEc2InstanceIsManagedBySSM` Schritt und andernfalls zum `CheckIfHelperInstanceProfileIsProvided` Schritt .

- CheckIfEc2InstanceIsManagedBySSM:

  Prüft, ob die Instance von verwaltet wird AWS Systems Manager. Wenn das Runbook verwaltet wird, aktiviert es das SAC- und Startmenü mithilfe eines PowerShell Run Command.

- BranchOnPreEC2RescueBackup:

  Verzweigungen, die auf dem `CreateInstanceBackupBeforeScriptExecution` Eingabeparameter basieren.

- CreateAmazonMachineImageBackup:

  Erstellt eine AMI-Sicherung der Instance.

- EnableSACAndBootMenu

  Aktiviert SAC und das Bootmenü durch Ausführen eines PowerShell Run Command-Skripts.

- RebootInstance:

  Startet die Amazon EC2-Instance neu, um die Konfiguration anzuwenden. Dies ist der letzte Schritt, wenn die Instance online ist und von verwaltet wird AWS Systems Manager.

- CheckIfHelperInstanceProfileIsProvided:

  Prüft, ob das `HelperInstanceProfileName` angegebene vorhanden ist, bevor SAC und das Startmenü mit einer temporären Amazon EC2-Instance offline aktiviert werden.

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu

Führt aus`AWSSupport-StartEC2RescueWorkflow`, um SAC und das Startmenü zu aktivieren, wenn sich die Instance im angehaltenen Zustand befindet oder nicht von verwaltet wird AWS Systems Manager.

- GetExecutionDetails:

  Ruft die Image-ID der Backup- und Offline-Skriptausgabe ab.

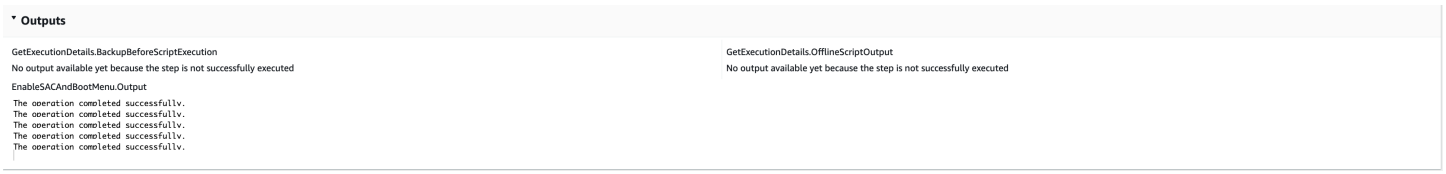
7. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten:
   - EnableSACAndBootMenu.Output:

     Ausgabe der Befehlsausführung im `EnableSACAndBootMenu` Schritt .
   - GetExecutionDetails.OfflineScriptOutput:

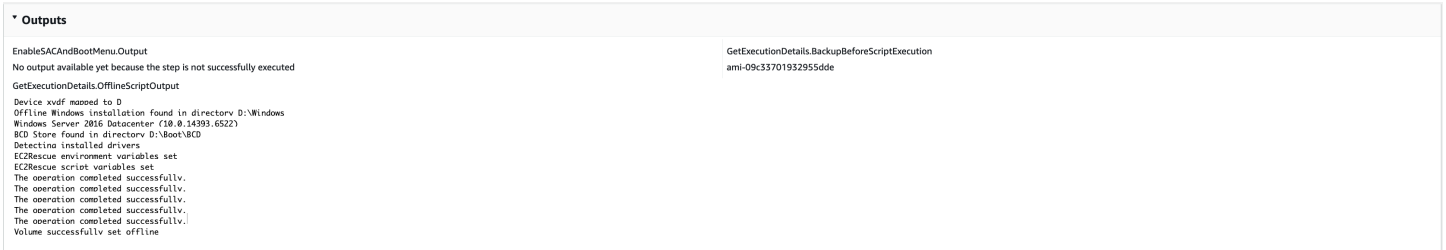
     Ausgabe des Offline-Skripts, das im `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` Schritt ausgeführt wurde.
   - GetExecutionDetails.BackupBeforeScriptExecution:

     Image-ID des AMI-Backups, wenn der `CreateInstanceBackupBeforeScriptExecution` Eingabeparameter True ist.

Ausgabe der Ausführung auf einer Instance, die von ausgeführt und verwaltet wird AWS Systems Manager




Ausgabe der Ausführung auf einer Instance, die angehalten oder nicht von verwaltet wird AWS Systems Manager



Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

## AWSSupport-ExecuteEC2Rescue

Beschreibung

Dieses Runbook verwendet das EC2Rescue Tool, um häufig auftretende Verbindungsprobleme mit der angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance für Linux oder zu beheben, sofern möglich. Windows Server Instanzen mit verschlüsselten Root-Volumes werden nicht unterstützt.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem

Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- EC2 RescueInstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.small | t2.medium | t2.large

  Standard: t2.small

  Beschreibung: (Erforderlich) Der EC2-Instance-Typ für die EC2Rescue Instance. Empfohlene Größe: `t2.small`

- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Amazon S3-Bucket-Name in Ihrem Konto, in das Sie die Fehlerbehebungsprotokolle hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Die Subnetz-ID für die EC2Rescue Instance. Standardmäßig erstellt AWS Systems Manager Automation eine neue VPC. Verwenden Sie alternativ, dasselbe Subnetz wie Ihre Instance `SelectedInstanceSubnet` zu verwenden, oder geben Sie eine benutzerdefinierte Subnetz-ID an.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone befinden wie `UnreachableInstanceId` und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

- UnreachableInstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) ID Ihrer nicht erreichbaren EC2-Instance.

> **Important**
>
> Systems Manager Automation stoppt diese Instanz und erstellt ein AMI, bevor ein Vorgang versucht wird. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP-Adresse verwenden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Sie müssen mindestens `ssm:StartAutomationExecution` und habens`sm:GetAutomationExecution`, um die Automatisierungsausgabe lesen zu können. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter [AWSSupport-StartEC2RescueWorkflow].

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Bestätigt, ob die angegebene Instanz: Windows Server
   a. (EC2RescuefürWindows Server) Wenn es sich bei der bereitgestellten Instanz um eine Windows Server Instanz handelt:
      i. `aws:executeAutomation`- Wird `AWSSupport-StartEC2RescueWorkflow` mit dem EC2Rescue-for Windows Server Offline-Skript aufgerufen.
      ii. `aws:executeAwsApi`— Ruft die Backup-AMI-ID aus der verschachtelten Automatisierung ab.
      iii. `aws:executeAwsApi`- Ruft die EC2Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab.
   b. (EC2Rescuefür Linux) Wenn es sich bei der bereitgestellten Instanz um eine Linux-Instanz handelt:
      i. `aws:executeAutomation`- Wird `AWSSupport-StartEC2RescueWorkflow` mit den Offline-Skripten von EC2Rescue für Linux aufgerufen
      ii. `aws:executeAwsApi`— Ruft die Backup-AMI-ID aus der verschachtelten Automatisierung ab.

iii. `aws:executeAwsApi`- Ruft die EC2Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab.

Ausgaben

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

## AWSSupport-ListEC2Resources

Beschreibung

Das `AWSSupport-ListEC2Resources` Runbook gibt Informationen über Amazon EC2-Instances und verwandte Ressourcen wie Amazon Elastic Block Store (Amazon EBS) -Volumes, Elastic IP-Adressen und Amazon EC2 Auto Scaling-Gruppen aus den von Ihnen angegebenen Gruppen zurück. AWS-Regionen Standardmäßig werden die Informationen aus allen Regionen gesammelt und in der Ausgabe der Automatisierung angezeigt. Optional können Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket angeben, in den die Informationen als Datei mit kommagetrennten Werten (.csv) hochgeladen werden sollen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Bucket

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des S3-Buckets, in den die gesammelten Informationen hochgeladen werden.

- DisplayResourceDeletionDocumentation

  Typ: Zeichenfolge

  Standard: true

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, erstellt die Automatisierung in der Ausgabe Links zur Dokumentation, die sich auf das Löschen Ihrer Ressourcen bezieht.

- RegionsToQuery

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die Regionen, aus denen Sie Amazon EC2-bezogene Informationen sammeln möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`

- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeVolumes
- ec2:DescribeSnapshots
- elasticloadbalancing:DescribeLoadBalancers

Um die gesammelten Informationen erfolgreich in den von Ihnen angegebenen S3-Bucket hochzuladen, sind außerdem die folgenden Aktionen AutomationAssumeRole erforderlich:

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

Dokumentschritte

- aws:executeAwsApi- Sammelt die für das Konto aktivierten Regionen.
- aws:executeScript— Bestätigt, dass die für das Konto aktivierten Regionen die im RegionsToQuery Parameter angegebenen Regionen unterstützen.
- aws:branch- Wenn keine Regionen für das Konto aktiviert sind, endet die Automatisierung.
- aws:executeScript- Listet alle EC2-Instances für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript— Listet alle Amazon Machine Images (AMI) für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript- Listet alle EBS-Volumes für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript— Listet alle Elastic IP-Adressen für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript— Listet alle Elastic Network-Interfaces für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript- Listet alle Auto Scaling-Gruppen für das Konto und die von Ihnen angegebenen Regionen auf.
- aws:executeScript- Listet alle Load Balancer für das Konto und die von Ihnen angegebenen Regionen auf.

- `aws:executeScript`- Lädt die gesammelten Informationen in den angegebenen S3-Bucket hoch, wenn Sie einen Wert für den `Bucket` Parameter angeben.

## AWSSupport-ManageRDPSettings

Beschreibung

Das `AWSSupport-ManageRDPSettings` Runbook ermöglicht es dem Benutzer, allgemeine Remote Desktop Protocol (RDP) -Einstellungen wie den RDP-Port und die Network Layer Authentication (NLA) zu verwalten. Standardmäßig liest das Runbook die Werte der Einstellungen und gibt sie aus.

> **Important**
>
> Änderungen an den RDP-Einstellungen sollten sorgfältig geprüft werden, bevor dieses Runbook ausgeführt wird.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der verwalteten Instance, deren RDP-Einstellungen verwaltet werden sollen.

- NLA SettingAction

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren | Deaktivieren

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion zur Ausführung auf der NLA-Einstellung: Check, Aktivieren, Deaktivieren.

- RDPPort

  Typ: Zeichenfolge

  Standard: 3389

  Beschreibung: (Optional) Angabe des neuen RDP-Ports. Wird nur verwendet, wenn die Aktion auf „Modify“ gesetzt ist. Die Portnummer muss zwischen 1025 und 65535 liegen. Hinweis: Nachdem der Port geändert wurde, wird der RDP-Service neu gestartet.

- RDP PortAction

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Ändern

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion, die auf den RDP-Port angewendet wird.

- RemoteConnections

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren | Deaktivieren

  Standard: Check

Beschreibung: (Erforderlich) Eine Aktion, die mit der Einstellung fDenytsConnections ausgeführt werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die EC2-Instance, die den Befehl empfängt, muss über eine IAM-Rolle verfügen, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Der Benutzer muss mindestens ssm: haben, SendCommand um den Befehl an die Instanz zu senden, plus ssm:, GetCommandInvocation um die Befehlsausgabe lesen zu können.

Dokumentschritte

`aws:runCommand`- Führen Sie das PowerShell Skript aus, um die RDP-Einstellungen auf der Zielinstanz zu ändern oder zu überprüfen.

Ausgaben

manageRDPSettings.Output

## `AWSSupport-ManageWindowsService`

Beschreibung

Das `AWSSupport-ManageWindowsService` Runbook ermöglicht es Ihnen, jeden Windows-Dienst auf der Zielinstanz zu beenden, zu starten, neu zu starten, anzuhalten oder zu deaktivieren.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der verwalteten Instanz, von der die Dienste verwaltet werden sollen.
- ServiceAction

  Typ: Zeichenfolge

  Gültige Werte: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion, die auf den Windows-Dienst angewendet wird. Beachten Sie, dass `Force-Restart` und verwendet werden `Force-Stop` kann, um einen Dienst neu zu starten und zu beenden, der abhängige Dienste hat.
- StartupType

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Automatisch | Nachfrage | Deaktiviert | DelayedAutoStart

  Standard: Check

  Beschreibung: (Erforderlich) Ein Starttyp, der auf den Windows-Dienst angewendet werden soll.
- WindowsServiceName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein gültiger Windows-Service-Name.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Der Benutzer muss mindestens über ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instanz zu senden, sowie über ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können.

Dokumentschritte

`aws:runCommand`- Führen Sie das PowerShell Skript aus, um die gewünschte Konfiguration auf den Windows-Dienst auf der Zielinstanz anzuwenden.

Ausgaben

manageWindowsService.Ausgang

## AWSSupport-MigrateEC2ClassicToVPC

Beschreibung

Das `AWSSupport-MigrateEC2ClassicToVPC` Runbook migriert eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance von EC2-Classic zu einer Virtual Private Cloud (VPC). Dieses Runbook unterstützt die Migration von Amazon EC2-Instances des Virtualisierungstyps Hardware Virtual Machine (HVM) mit Root-Volumes von Amazon Elastic Block Store (Amazon EBS).

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen.

- IAM genehmigen

  Typ: StringList

  Beschreibung: (Optional) Die Amazon-Ressourcennamen (ARNs) der IAM-Benutzer, die die Aktion genehmigen oder ablehnen können. Dieser Parameter gilt nur, wenn Sie den `CutOver` Wert für den `MigrationType` Parameter angeben.

- DestinationSecurityGroupId

  Typ: StringList

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die Sie der Amazon EC2-Instance zuordnen möchten, die in Ihrer VPC gestartet wird. Wenn Sie keinen Wert für diesen Parameter angeben, erstellt die Automatisierung eine Sicherheitsgruppe in Ihrer VPC und kopiert die Regeln aus der Sicherheitsgruppe in EC2-Classic. Wenn die Regeln nicht in die neue Sicherheitsgruppe kopiert werden können, wird die Standardsicherheitsgruppe Ihrer VPC mit der Amazon EC2-Instance verknüpft.

- DestinationSubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in das Sie Ihre Amazon EC2-Instance migrieren möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wählt die Automatisierung nach dem Zufallsprinzip ein Subnetz aus Ihrer VPC aus.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, die Sie migrieren möchten.

- MigrationType

  Typ: Zeichenfolge

Gültige Werte: CutOver | Test

Beschreibung: (Erforderlich) Die Art der Migration, die Sie durchführen möchten.

Für die `CutOver` Option ist eine Genehmigung erforderlich, um Ihre Amazon EC2-Instance zu beenden, die in EC2-Classic ausgeführt wird. Nachdem diese Aktion genehmigt wurde, wird die Amazon EC2-Instance gestoppt und die Automatisierung erstellt eine Amazon Machine Image (AMI). Wenn der AMI Status lautet`available`, wird von dieser AMI in der von `DestinationSubnetId` Ihnen in Ihrer VPC angegebenen Instanz eine neue Amazon EC2-Instance gestartet. Wenn Ihrer Amazon EC2-Instance, die in EC2-Classic ausgeführt wird, eine Elastic IP-Adresse angehängt ist, wird die Instance auf die neu erstellte Amazon EC2-Instance in Ihrer VPC verschoben. Wenn die Amazon EC2-Instance, die in Ihrer VPC gestartet wird, aus irgendeinem Grund nicht erstellt werden kann, wird sie beendet und es wird eine Genehmigung für den Start Ihrer Amazon EC2-Instance in EC2-Classic angefordert.

Die `Test` Option erstellt eine AMI Ihrer Amazon EC2-Instances, die in EC2-Classic ohne Neustart ausgeführt wird. Da die Amazon EC2-Instance nicht neu gestartet wird, können wir die Dateisystemintegrität des erstellten Images nicht garantieren. Wenn der AMI Status lautet`available`, wird von dieser aus in der von Ihnen AMI in Ihrer VPC angegebenen Instanz eine neue Amazon EC2-Instance gestartet. `DestinationSubnetId` Wenn an Ihre Amazon EC2-Instance, die in EC2-Classic ausgeführt wird, eine Elastic IP-Adresse angehängt ist, überprüft die Automatisierung, ob die von `DestinationSubnetId` Ihnen angegebene IP-Adresse öffentlich ist. Wenn die Amazon EC2-Instance, die in Ihrer VPC gestartet wird, aus irgendeinem Grund nicht erstellt werden kann, wird sie beendet und die Automatisierung wird beendet.

- SNS-Benachrichtigung AR NforApproval

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN des Amazon Simple Notification Service (Amazon SNS) - Themas, an das Sie Genehmigungsanfragen senden möchten. Dieser Parameter gilt nur, wenn Sie den `CutOver` Wert für den `MigrationType` Parameter angeben.

- TargetInstanceType

  Typ: Zeichenfolge

  Standard: t2.2xlarge

Beschreibung: (Optional) Der Typ der Amazon EC2-Instance, die Sie in Ihrer VPC starten möchten. Es werden nur Xen-basierte Instance-Typen wie T2, M4 oder C4 unterstützt.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeAwsApi- Erfasst Details über die Amazon EC2-Instance, die Sie im InstanceId Parameter angeben.
- aws:assertAwsResourceProperty— Bestätigt, dass der Instanztyp, den Sie im TargetInstanceType Parameter angeben, Xen-basiert ist.
- aws:assertAwsResourceProperty— Bestätigt, dass es sich bei der Amazon EC2-Instance, die Sie im InstanceId Parameter angeben, um den HVM-Virtualisierungstyp handelt.
- aws:assertAwsResourceProperty— Bestätigt, dass die Amazon EC2-Instance, die Sie im InstanceId Parameter angeben, über ein Amazon EBS-Root-Volume verfügt.
- aws:executeScript- Erstellt je nach Bedarf je nach dem Wert, den Sie für den DestinationSecurityGroupId Parameter angeben, eine Sicherheitsgruppe.
- aws:branch- Zweige, die auf dem Wert basieren, den Sie im DestinationSubnetId Parameter angeben.
- aws:executeAwsApi— Identifiziert die Standard-VPC in demAWS-Region, in dem Sie diese Automatisierung ausführen.
- aws:executeAwsApi- Wählt nach dem Zufallsprinzip die ID eines Subnetzes aus, das sich in der Standard-VPC befindet.
- aws:createImage— Erstellt eine, AMI ohne die Amazon EC2-Instance neu zu starten.
- aws:branch- Zweige, die auf dem Wert basieren, den Sie für den MigrationType Parameter angeben.
- aws:branch- Zweige, die auf dem Wert basieren, den Sie für den DestinationSubnetId Parameter angeben.
- aws:runInstances- Startet eine neue Instance aus der AMI erstellten Instance, ohne die Amazon EC2-Instance in EC2-Classic neu zu starten.

- `aws:changeInstanceState`- Beendet die neu gestartete Amazon EC2-Instance, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:runInstances`- Startet eine neue Instance von der AMI erstellten Instance aus, ohne die Amazon EC2-Instance in EC2-Classic in den angegebenen Fällen neu zu starten. `DestinationSubnetId`
- `aws:changeInstanceState`- Beendet die neu gestartete Amazon EC2-Instance, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:assertAwsResourceProperty`— Bestätigt das Stoppverhalten für die Amazon EC2-Instance, die in EC2-Classic ausgeführt wird.
- `aws:approve`— Wartet auf die Genehmigung, um die Amazon EC2-Instance zu stoppen.
- `aws:changeInstanceState`- Stoppt die Amazon EC2-Instance, die in EC2-Classic ausgeführt wird.
- `aws:changeInstanceState`- Force stoppt die Amazon EC2-Instance, die in EC2-Classic ausgeführt wird, falls erforderlich.
- `aws:createImage`— Erzeugt eine AMI der Amazon EC2-Instances, nachdem sie beendet wurde.
- `aws:branch`- Zweige, die auf dem für den `DestinationSubnetId` Parameter angegebenen Wert basieren.
- `aws:runInstances`- Startet eine neue Instance aus der AMI erstellten oder gestoppten Amazon EC2-Instance in EC2-Classic.
- `aws:approve`- Wartet auf die Genehmigung, um die neu gestartete Instance zu beenden, und startet die Amazon EC2-Instance in EC2-Classic, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:changeInstanceState`- Beendet die neu gestartete Amazon EC2-Instance.
- `aws:runInstances`- Startet eine neue Instance aus der AMI erstellten oder gestoppten Amazon EC2-Instance in EC2-Classic über den Parameter. `DestinationSubnetId`
- `aws:approve`- Wartet auf die Genehmigung, um die neu gestartete Instance zu beenden, und startet die Amazon EC2-Instance in EC2-Classic, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:changeInstanceState`- Beendet die neu gestartete Amazon EC2-Instance.
- `aws:changeInstanceState`- Startet die Amazon EC2-Instance, die in EC2-Classic gestoppt wurde.
- `aws:branch`— Branches, die darauf basieren, ob die Amazon EC2-Instance eine öffentliche IP-Adresse hat.

- `aws:executeAwsApi`— Überprüft, ob es sich bei der öffentlichen IP-Adresse um eine Elastic IP-Adresse handelt.
- `aws:branch`- Zweige, die auf dem Wert basieren, den Sie im `MigrationType` Parameter angeben.
- `aws:executeAwsApi`- Verschiebt die Elastic IP-Adresse auf Ihre VPC.
- `aws:executeAwsApi`— Erfasst die Zuweisungs-ID der Elastic IP-Adresse, die in Ihre VPC verschoben wurde.
- `aws:branch`- Branches basierend auf dem Subnetz, auf dem die in Ihrer VPC ausgeführte Amazon EC2-Instance gestartet wurde.
- `aws:executeAwsApi`- Hängt die Elastic IP-Adresse an die neu gestartete Instance in Ihrer VPC an.
- `aws:executeScript`— Bestätigt, dass das Subnetz Ihrer neu gestarteten Amazon EC2-Instance, die in Ihrer VPC ausgeführt wird, öffentlich ist.

Ausgaben

g `etInstanceProperties.virtualizationType` — Der Virtualisierungstyp der Amazon EC2-Instance, die in EC2-Classic ausgeführt wird.

`getInstanceProperties.rootDeviceType`- Der Root-Gerätetyp der Amazon EC2-Instance, die in EC2-Classic ausgeführt wird.

`createAMIWithoutReboot.ImageId`- Die ID der AMI erstellten Amazon EC2-Instance, die in EC2-Classic ausgeführt wird, ohne einen Neustart durchzuführen.

`getDefaultVPC.VpcId`- Die ID der Standard-VPC, auf der die neue Amazon EC2-Instance gestartet wird, falls kein Wert für den `DestinationSubnetId` Parameter angegeben wird.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- Die ID des Subnetzes in der Standard-VPC, in dem die neue Amazon EC2-Instance gestartet wird, falls kein Wert für den `DestinationSubnetId` Parameter angegeben wird.

`launchTestInstanceDefaultVPC.InstanceIds`- Die ID der neu gestarteten Amazon EC2-Instance in Ihrer Standard-VPC während des `Test` Migrationstyps.

`launchTestInstanceProvidedSubnet.InstanceIds`- Die ID der neu gestarteten Amazon EC2-Instance in der`DestinationSubnetId`, die Sie während des `Test` Migrationstyps angegeben haben.

`createAMIAfterStoppingInstance.ImageId`- Die ID der, die nach dem Stoppen der in EC2-Classic laufenden Amazon EC2-Instance AMI erstellt wurde.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- Die ID der neu gestarteten Amazon EC2-Instance in der`DestinationSubnetId`, die Sie während des `CutOver` Migrationstyps angegeben haben.

`launchCutOverInstanceDefaultVPC.InstanceIds`- Die ID der neu gestarteten Amazon EC2-Instance in Ihrer Standard-VPC während des `CutOver` Migrationstyps.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Ob das von der Automatisierung in Ihrer Standard-VPC gewählte Subnetz öffentlich ist.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Ob das Subnetz, das Sie in der angegeben haben, öffentlich `DestinationSubnetId` ist.

## AWSSupport-MigrateXenToNitroLinux

Beschreibung

Das `AWSSupport-MigrateXenToNitroLinux` Runbook klont, bereitet eine Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen-Instance zu einem Instance-Typ vor und migriert sie. Nitro Dieses Runbook bietet zwei Optionen für Operationstypen:

- `Clone&Migrate`— Der Arbeitsablauf dieser Option besteht aus den Vorprüfungen, Tests und Clone&MigratePhasen. Der Workflow wird mit dem `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` Runbook ausgeführt.
- `FullMigration`— Diese Option führt den `Clone&Migrate` Workflow aus und führt dann den zusätzlichen Schritt des Ersetzens von Amazon EBS-Root-Volumes aus.

> **Important**
>
> Wenn Sie dieses Runbook verwenden, fallen Ihrem Konto Kosten für die Laufzeit von Amazon EC2-Instances, die Erstellung von Amazon Elastic Block Store (Amazon EBS) - Volumes und an. AMIs Weitere Informationen finden Sie unter Amazon EC2-Preise und Amazon EBS-Preise.

Vorläufige Kontrollen

Die Automatisierung führt die folgenden Vorprüfungen durch, bevor mit der Migration fortgefahren wird. Schlägt eine der Prüfungen fehl, endet die Automatisierung. Diese Phase ist nur ein Teil des `Clone&Migrate` Workflows.

- Prüft, ob die Zielinstanz bereits ein Nitro Instanztyp ist.
- Prüft, ob die Kaufoption für Spot-Instances für die Ziel-Instance verwendet wurde.
- Prüft, ob Instance-Speicher-Volumes an die Ziel-Instance angehängt sind.
- Überprüft, ob das Betriebssystem (OS) der Zielinstanz Linux ist.
- Prüft, ob die Ziel-Instance Teil einer Amazon EC2 Auto Scaling-Gruppe ist. Wenn sie Teil einer Auto Scaling-Gruppe ist, überprüft die Automatisierung, ob sich die Instanz im `standby` Status befindet.
- Überprüft, ob die Instanz von AWS Systems Manager verwaltet wird.

Testen

Die Automatisierung erstellt eine Amazon Machine Image (AMI) aus der Zielinstanz und startet eine Testinstanz von der neu erstellten Instanz ausAMI. Diese Phase ist nur Teil des `Clone&Migrate` Workflows.

Wenn die Testinstanz alle Statusprüfungen bestanden hat, wird die Automatisierung unterbrochen und die Genehmigung durch die benannten Principals wird über die Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung angefordert. Wenn die Genehmigung erteilt wird, beendet die Automatisierung die Testinstanz, stoppt die Zielinstanz und setzt die Migration fort, während die neu erstellte Instanz am Ende des Workflows deregistriert AMI wird. `Clone&Migrate`

> **Note**
>
> Bevor Sie die Genehmigung erteilen, sollten Sie überprüfen, ob alle auf der Zielinstanz ausgeführten Anwendungen ordnungsgemäß geschlossen wurden.

Klonen und Migrieren

Die Automatisierung erstellt eine weitere Instance AMI aus der Ziel-Instance und startet eine neue Instance, um zu einem Nitro Instance-Typ zu wechseln. Die Automatisierung erfüllt die folgenden Voraussetzungen, bevor Sie mit der Migration fortfahren. Schlägt eine der Prüfungen fehl, endet die Automatisierung. Diese Phase ist ebenfalls nur ein Teil des `Clone&Migrate` Workflows.

- Schaltet das Enhanced Networking (ENA) -Attribut ein.
- Installiert die neueste Version der ENA-Treiber, falls diese noch nicht installiert sind, oder aktualisiert die ENA-Treiberversion auf die neueste Version. Um eine maximale Netzwerkleistung zu gewährleisten, ist ein Update auf die neueste ENA-Treiberversion erforderlich, wenn es sich bei dem Nitro Instance-Typ um die 6. Generation handelt.
- Überprüft, ob das NVMe-Modul installiert ist. Wenn das Modul installiert ist, überprüft die Automatisierung, dass das Modul geladen ist. `initramfs`
- Analysiert `/etc/fstab` und ersetzt Einträge mit Blockgerätenamen (`/dev/sd*`oder`/dev/xvd*`) durch ihre jeweiligen UUIDs. Bevor die Konfiguration geändert wird, erstellt die Automatisierung eine Sicherungskopie der Datei im Pfad`/etc/fstab*`.
- Deaktiviert die vorhersehbare Benennung von Schnittstellen, indem die `net.ifnames=0` Option zur `GRUB_CMDLINE_LINUX` Zeile in der `/etc/default/grub` Datei hinzugefügt wird, falls sie existiert, oder zum Kernel in`/boot/grub/menu.lst`.
- Löscht die `/etc/udev/rules.d/70-persistent-net.rules` Datei, falls sie existiert. Vor dem Entfernen der Datei erstellt die Automatisierung eine Sicherungskopie der Datei im Pfad`/etc/udev/rules.d/`.

Nachdem alle Anforderungen überprüft wurden, wird der Instanztyp in den von Ihnen angegebenen Nitro Instanztyp geändert. Die Automatisierung wartet darauf, dass die neu erstellte Instanz alle Statusprüfungen bestanden hat, nachdem sie als Nitro Instanztyp gestartet wurde. Die Automatisierung wartet dann auf die Genehmigung der designierten Principals, um eine AMI der erfolgreich gestarteten Nitro Instances zu erstellen. Wenn die Genehmigung verweigert wird, wird die Automatisierung beendet und die neu erstellte Instanz läuft weiter, und die Zielinstanz bleibt angehalten.

Ersetzen Sie das Amazon EBS-Root-Volume

Wenn Sie `FullMigration` als die auswählen`OperationType`, migriert die Automatisierung die Amazon EC2-Zielinstanz auf den von Ihnen Nitro angegebenen Instance-Typ. Automation fordert von bestimmten Principals die Genehmigung an, das Amazon EBS-Root-Volume der Amazon EC2-Ziel-Instance durch das Root-Volume der geklonten Amazon EC2-Instance zu ersetzen. Nach erfolgreicher Migration wird die geklonte Amazon EC2-Instance beendet. Wenn die Automatisierung fehlschlägt, wird das ursprüngliche Amazon EBS-Root-Volume an die Amazon EC2-Zielinstanz angehängt. Wenn das Amazon EBS-Root-Volume, das an die Amazon EC2-Zielinstanz angehängt ist, Tags mit dem angewendeten `aws:` Präfix enthält, wird der `FullMigration` Vorgang nicht unterstützt.

Bevor Sie beginnen

Die Zielinstanz muss über einen ausgehenden Internetzugang verfügen. Dies dient dazu, auf Repositorys für Treiber und Abhängigkeiten wiekernel-devel,gcc,patch,rpm-build, wget dracutmake, linux-headers und zuzugreifen. unzip Bei Bedarf wird der Paketmanager verwendet.

Für das Senden von Benachrichtigungen über Genehmigungen und Aktualisierungen ist ein Amazon SNS-Thema erforderlich. Weitere Informationen zum Erstellen eines Amazon SNS-Themas finden Sie unter Erstellen eines Amazon SNS-Themas im Amazon Simple Notification Service Developer Guide.

Dieses Runbook unterstützt die folgenden Betriebssysteme:

- RHEL7,x - 8,5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS und 20.10 STR
- SUSE Linux Enterprise Server(SUSE 12 SP5, SUSE 15 SP2)

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem

Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Anerkennung

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Lesen Sie die vollständigen Details der Aktionen, die von diesem Automatisierungs-Runbook ausgeführt werden, und geben Sie ein, **`Yes, I understand and acknowledge`** um mit der Verwendung des Runbooks fortzufahren.

- IAM genehmigen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ARNs der IAM-Rollen, Benutzer oder Benutzernamen, die Genehmigungen für die Automatisierung erteilen können. Sie können maximal 10 Genehmiger angeben.

- DeleteResourcesOnFailure

  Typ: Boolesch

  Beschreibung: (Optional) Legt fest, ob die neu erstellte Instanz und AMI die Migration gelöscht werden, falls die Automatisierung fehlschlägt.

  Gültige Werte: True | False

  Standard: True

- MinimumRequiredApprovals

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Mindestanzahl von Genehmigungen, die erforderlich sind, um die Automatisierung fortzusetzen, wenn Genehmigungen angefordert werden.

  Gültige Werte: 1-10

  Standard: 1

- NitroInstanceType

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Nitro Instanztyp, in den Sie die Instanz ändern möchten. Zu den unterstützten Instance-Typen gehören M5, M6, C5, C6, R5, R6 und T3.

Standard: m5.xlarge

- OperationType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Vorgang, den Sie ausführen möchten. Die `FullMigration` Option erfüllt dieselben Aufgaben wie das Root-Volume Ihrer Ziel-Instance `Clone&Migrate` und ersetzt es zusätzlich. Das Root-Volume der Ziel-Instance wird nach dem Migrationsprozess durch das Root-Volume der neu erstellten Instance ersetzt. Der `FullMigration` Vorgang unterstützt keine von Logical Volume Manager (LVM) definierten Root-Volumes.

  Gültige Werte: Clone&Migrate | FullMigration

- SNS TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS-Themas für die Genehmigungsbenachrichtigung. Das Amazon SNS-Thema wird verwendet, um während der Automatisierung erforderliche Genehmigungsbenachrichtigungen zu senden.

- TargetInstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der zu migrierenden Amazon EC2-Instances.

Clone&Migrate-Workflow

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- startOfPreliminaryChecksBranch- Abzweigungen zum Arbeitsablauf für Vorprüfungen.
- getTargetInstanceProperties- Sammelt Details von der Zielinstanz.
- checkIfNitroInstanceTypeIsSupportedInAZ— Stellt fest, ob der Amazon EC2-Zielinstance-Typ in derselben Availability Zone wie die Ziel-Instance unterstützt wird.

- `getXenInstanceTypeDetails`- Sammelt Details über den Quell-Instance-Typ.
- `checkIfInstanceHypervisorIsNitroAlready`- Prüft, ob die Zielinstanz bereits als Nitro Instanztyp läuft.
- `checkIfTargetInstanceLifecycleIsSpot`- Prüft, ob die Kaufoption der Ziel-Instance Spot ist.
- `checkIfOperatingSystemIsLinux`- Prüft, ob das Betriebssystem der Zielinstanz Linux ist.
- `verifySSMConnectivityForTargetInstance`- Überprüft, ob die Zielinstanz vom Systems Manager verwaltet wird.
- `checkIfEphemeralVolumeAreSupported`- Prüft, ob der aktuelle Instance-Typ der Ziel-Instance Instance-Speicher-Volumes unterstützt.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`- Prüft, ob an die Zielinstanz Instance-Speicher-Volumes angehängt sind.
- `checkIfRootVolumeIsEBS`- Prüft, ob der Root-Volume-Typ der Ziel-Instance EBS ist.
- `checkIfTargetInstanceIsInASG`- Prüft, ob die Zielinstanz Teil einer Auto Scaling-Gruppe ist.
- `endOfPreliminaryChecksBranch`- Ende der Abteilung für Vorprüfungen.
- `startOfTestBranch`- Abzweigungen zum Test-Workflow.
- `createTestImage`- Erstellt einen Test AMI der Zielinstanz.
- `launchTestInstanceInSameSubnet`- Startet aus dem Test heraus eine Testinstanz AMI mit derselben Konfiguration wie die Zielinstanz.
- `cleanupTestInstance`- Beendet die Testinstanz.
- `endOfTestBranch`- Ende der Testabteilung.
- `checkIfTestingBranchSucceeded`- Prüft den Status der Testing-Abteilung.
- `approvalToStopTargetInstance`- Wartet auf die Genehmigung der designierten Principals, um die Zielinstanz zu stoppen.
- `stopTargetEC2Instance`- Stoppt die Zielinstanz.
- `forceStopTargetEC2Instance`- Force stoppt die Zielinstanz nur, wenn der vorherige Schritt die Instanz nicht stoppen konnte.
- `startOfCloneAndMigrateBranch`- Abzweigungen zum Clone&Migrate Arbeitsablauf.
- `createBackupImage`- Erzeugt eine AMI der Zielinstanzen, die als Backup dient.
- `launchInstanceInSameSubnet`- Startet eine neue Instance aus dem Backup AMI mit derselben Konfiguration wie die Quell-Instance.

- `waitForClonedInstanceToPassStatusChecks`- Wartet darauf, dass die neu erstellte Instanz alle Statusprüfungen bestanden hat.
- `verifySSMConnectivityForClonedInstance`- Überprüft, ob die neu erstellte Instanz vom Systems Manager verwaltet wird.
- `checkAndInstallENADrivers`- Prüft, ob ENA-Treiber auf der neu erstellten Instanz installiert sind, und installiert die Treiber bei Bedarf.
- `checkAndAddNVMEDrivers`- Prüft, ob NVMe-Treiber auf der neu erstellten Instanz installiert sind, und installiert die Treiber bei Bedarf.
- `checkAndModifyFSTABEntries`- Prüft, ob Gerätenamen verwendet werden, `/etc/fstab` und ersetzt sie bei Bedarf durch UUIDs.
- `stopClonedInstance`- Stoppt die neu erstellte Instanz.
- `forceStopClonedInstance`- Force stoppt die neu erstellte Instanz nur, wenn der vorherige Schritt die Instanz nicht stoppen konnte.
- `checkENAAttributeForClonedInstance`- Prüft, ob das erweiterte Netzwerkattribut für die neu erstellte Instanz aktiviert ist.
- `setNitroInstanceTypeForClonedInstance`- Ändert den Instanztyp für die neu erstellte Instanz in den von Ihnen angegebenen Nitro Instanztyp.
- `startClonedInstance`- Startet die neu erstellte Instanz, deren Instanztyp Sie geändert haben.
- `approvalForCreatingImageAfterDriversInstallation`- Wenn die Instance erfolgreich als Nitro Instance-Typ gestartet wird, wartet die Automatisierung auf die Genehmigung durch die erforderlichen Principals. Wenn die Genehmigung erteilt wird, AMI wird eine erstellt, die als Golden verwendet werden kannAMI.
- `createImageAfterDriversInstallation`- Erzeugt AMI und kann als Golden verwendet werdenAMI.
- `endOfCloneAndMigrateBranch`- Ende der Clone&Migrate Filiale.
- `cleanupTestImage`- Deregistriert die zum Testen AMI erstellten Dateien ab.
- `failureHandling`- Prüft, ob Sie sich dafür entschieden haben, Ressourcen bei einem Ausfall zu beenden.
- `onFailureTerminateClonedInstance`- Beendet die neu erstellte Instanz, falls die Automatisierung fehlschlägt.
- `onFailurecleanupTestImage`- Deregistriert die zum Testen AMI erstellten Dateien ab.
- `onFailureApprovalToStartTargetInstance`- Wenn die Automatisierung fehlschlägt, wird auf die Genehmigung der angegebenen Principals gewartet, um die Zielinstanz zu starten.

- onFailureStartTargetInstance- Wenn die Automatisierung fehlschlägt, wird die Zielinstanz gestartet.

FullMigration-Workflow

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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

Dokumentschritte

Der FullMigration Workflow führt dieselben Schritte wie der Clone&Migrate Workflow aus und führt zusätzlich die folgenden Schritte aus:

- checkConcurrency— Überprüft, ob es nur eine Automatisierung dieses Runbooks gibt, die auf die von Ihnen angegebene Amazon EC2-Instance abzielt. Wenn das Runbook feststellt, dass gerade eine weitere Automatisierung ausgeführt wird, die auf dieselbe Instanz abzielt, wird die Automatisierung beendet.
- getTargetInstanceProperties- Sammelt Details von der Zielinstanz.
- checkRootVolumeTags— Ermittelt, ob das Root-Volume der Amazon EC2-Zielinstanz AWS reservierte Tags enthält.
- cloneTargetInstanceAndMigrateToNitro- Startet eine untergeordnete Automatisierung mithilfe des AWS-CloneXenInstanceToNitro Runbooks.
- branchOnTheOperationType- Verzweigt sich nach dem Wert, den Sie für den OperationType Parameter angeben.
- getClonedInstanceId- Ruft die ID der neu gestarteten Instanz aus der Child-Automation ab.
- checkIfRootVolumeIsBasedOnLVM- Stellt fest, ob die Root-Partition von LVM verwaltet wird.
- branchOnTheRootVolumeLVMStatus- Liegen die erforderlichen Mindestgenehmigungen von den Principals vor, wird die Automatisierung mit dem Austausch des Root-Volumes fortgesetzt.
- manualInstructionsInCaseOfLVM- Wenn das Root-Volume von LVM verwaltet wird, sendet die Automatisierung eine Ausgabe mit Anweisungen, wie die Root-Volumes manuell ersetzt werden können.
- startOfReplaceRootEBSVolumeBranch- Startet den Workflow „Replace Root EBS Volume Branch“.

- `checkIfTargetInstanceIsManagedByCFN`- Ermittelt, ob die Zielinstanz von einem AWS CloudFormation Stack verwaltet wird.
- `branchOnCFNStackStatus`- Zweige basierend auf dem Status des CloudFormation Stacks.
- `approvalForRootVolumesReplacement(WithCFN)`- Wenn die Zielinstanz von gestartet wurdeCloudFormation, wartet die Automatisierung auf die Genehmigung, nachdem die neu gestartete Instance erfolgreich als Nitro Instance-Typ gestartet wurde. Wenn Genehmigungen vorliegen, werden die Amazon EBS-Volumes der Ziel-Instance durch die Root-Volumes der neu gestarteten Instance ersetzt.
- `approvalForRootVolumesReplacement`- Wartet auf die Genehmigung, nachdem die neu gestartete Instance erfolgreich als Nitro Instance-Typ gestartet wurde. Wenn Genehmigungen vorliegen, werden die Amazon EBS-Volumes der Ziel-Instance durch die Root-Volumes der neu gestarteten Instance ersetzt.
- `assertIfTargetEC2InstanceIsStillStopped`- Überprüft, ob sich die Zielinstanz in einem bestimmten `stopped` Zustand befindet, bevor das Root-Volume ersetzt wird.
- `stopTargetInstanceForRootVolumeReplacement`— Wenn die Zielinstanz läuft, stoppt die Automatisierung die Instance, bevor das Root-Volume ersetzt wird.
- `forceStopTargetInstanceForRootVolumeReplacement`- Force stoppt die Zielinstanz, wenn der vorherige Schritt fehlschlägt.
- `stopClonedInstanceForRootVolumeReplacement`- Stoppt die neu erstellte Instance, bevor die Amazon EBS-Volumes ersetzt werden.
- `forceStopClonedInstanceForRootVolumeReplacement`- Force stoppt die neu erstellte Instanz, wenn der vorherige Schritt fehlschlägt.
- `getBlockDeviceMappings`- Ruft die Blockgerätezuordnungen sowohl für die Zielinstanz als auch für die neu erstellte Instanz ab.
- `replaceRootEbsVolumes`- Ersetzt das Root-Volume der Ziel-Instance durch das Root-Volume der neu erstellten Instance.
- `EndOfReplaceRootEBSVolumeBranch`- Ende des Workflows zum Ersetzen von Root EBS Volume Branch.
- `checkENAAttributeForTargetInstance`— Prüft, ob das Enhanced Networking (ENA) -Attribut für die Amazon EC2-Zielinstanz aktiviert ist.
- `enableENAAttributeForTargetInstance`— Aktiviert bei Bedarf das ENA-Attribut für die Amazon EC2-Zielinstanz.
- `setNitroInstanceTypeForTargetInstance`- Ändert die Zielinstanz auf den von Ihnen angegebenen Nitro Instance-Typ.

- `replicateRootVolumeTags`— Repliziert die Tags auf dem Amazon EBS-Root-Volume von der Amazon EC2-Zielinstanz.
- `startTargetInstance`- Startet die Amazon EC2-Ziel-Instance, nachdem der Instance-Typ geändert wurde.
- `onFailureStopTargetEC2Instance`- Stoppt die Amazon EC2-Ziel-Instance, wenn sie nicht als Nitro Instance-Typ gestartet werden kann.
- `onFailureForceStopTargetEC2Instance`- Force stoppt die Amazon EC2-Zielinstanz, wenn der vorherige Schritt fehlschlägt.
- `OnFailureRevertOriginalInstanceType`- Setzt die Amazon EC2-Ziel-Instance auf den ursprünglichen Instance-Typ zurück, wenn die Ziel-Instance nicht als Nitro Instance-Typ gestartet werden kann.
- `onFailureRollbackRootVolumeReplacement`- Macht bei Bedarf alle durch den `replaceRootEbsVolumes` Schritt vorgenommenen Änderungen rückgängig.
- `onFailureApprovalToStartTargetInstance`- Wartet auf die Genehmigung des designierten Principals, um die Amazon EC2-Zielinstanz zu starten, nachdem die vorherigen Änderungen rückgängig gemacht wurden.
- `onFailureStartTargetInstance`— Startet die Amazon EC2-Zielinstanz.
- `terminateClonedEC2Instance`— Beendet die geklonte Amazon EC2-Instance, nachdem das Amazon EBS-Root-Volume ersetzt wurde.

## AWSSupport-ResetAccess

Beschreibung

Dieses Runbook verwendet das EC2Rescue-Tool auf der angegebenen EC2-Instance, um die Passwortentschlüsselung mithilfe der EC2-Konsole (Windows) erneut zu aktivieren oder um ein neues SSH-Schlüsselpaar zu generieren und hinzuzufügen (Linux). Wenn Sie Ihr Schlüsselpaar verloren haben, erstellt diese Automatisierung ein passwortfähiges AMI, mit dem Sie eine neue EC2-Instance mit einem eigenen Schlüsselpaar starten können (Windows).

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EC2 RescueInstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.small | t2.medium | t2.large

  Standard: t2.small

  Beschreibung: (Erforderlich) Der EC2-Instance-Typ für die EC2Rescue-Instance. Empfohlene Größe: t2.small.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2-Instance, für die Sie den Zugriff zurücksetzen möchten.

> **Important**
>
> Systems Manager Automation stoppt diese Instanz und erstellt ein AMI, bevor ein Vorgang versucht wird. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Die Subnetz-ID für die EC2Rescue-Instance. Standardmäßig erstellt Systems Manager Automation eine neue VPC. Verwenden Sie alternativ, SelectedInstanceSubnet um dasselbe Subnetz wie Ihre Instance zu verwenden, oder geben Sie eine benutzerdefinierte Subnetz-ID an.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Sie müssen mindestens ssm:StartAutomationExecution, ssm: GetParameter (um den Namen des SSH-Schlüsselparameters abzurufen) und ssm: haben, GetAutomationExecution um die Automatisierungsausgabe lesen zu können. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter `AWSSupport-StartEC2RescueWorkflow`.

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Bestätigen Sie, ob es sich bei der bereitgestellten Instanz um Windows handelt.
   a. (EC2Rescue für Windows) Wenn die Plattform der bereitgestellten Instance Windows ist
      i. `aws:executeAutomation`- `AWSSupport-StartEC2RescueWorkflow` Mit dem Offline-Skript zum Zurücksetzen des Passworts von EC2Rescue für Windows aufrufen
      ii. `aws:executeAwsApi`- Rufen Sie die Backup-AMI-ID aus der verschachtelten Automatisierung ab
      iii. `aws:executeAwsApi`- Rufen Sie die kennwortfähige AMI-ID aus der verschachtelten Automatisierung ab

iv. `aws:executeAwsApi`- Rufen Sie die EC2Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab

b. (EC2Rescue für Linux) Wenn die Plattform der bereitgestellten Instance Linux ist

i. `aws:executeAutomation`- `AWSSupport-StartEC2RescueWorkflow` Mit dem Offline-SSH-Schlüsselinjektionsskript von ec2Rescue für Linux aufrufen

ii. `aws:executeAwsApi`- Rufen Sie die Backup-AMI-ID aus der verschachtelten Automatisierung ab

iii. `aws:executeAwsApi`- Ruft den SSM-Parameternamen für den injizierten SSH-Schlüssel ab

iv. `aws:executeAwsApi`- Rufen Sie die EC2Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab

Ausgaben

Holen Sie sich EC2RescueForWindowsResult. Output

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

Holen Sie sich EC2RescueForLinuxResult. Output

getLinuxBackupAmi. ImageId

Holen Sie sich LinuxSSH .Name KeyParameter

## AWSSupport-ResetLinuxUserPassword

Beschreibung

Das `AWSSupport-ResetLinuxUserPassword` Runbook hilft Ihnen dabei, das Passwort eines lokalen Betriebssystembenutzers (OS) zurückzusetzen. Dieses Runbook ist besonders hilfreich für Benutzer, die über die serielle Konsole auf ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances zugreifen müssen. Das Runbook erstellt eine temporäre Amazon EC2 EC2-Instance in Ihrer AWS-Konto und einer AWS Identity and Access Management (IAM) -Rolle mit Berechtigungen zum Abrufen eines AWS Secrets Manager geheimen Werts, der das Passwort enthält.

Das Runbook stoppt Ihre Amazon EC2 EC2-Ziel-Instance, trennt das Amazon Elastic Block Store (Amazon EBS) -Stammvolume und fügt es der temporären Amazon EC2 EC2-Instance hinzu. Mithilfe

von Run Command wird auf der temporären Instance ein Skript ausgeführt, um das Passwort des von Ihnen angegebenen Betriebssystembenutzers festzulegen. Anschließend wird das Amazon EBS-Root-Volume wieder an Ihre Ziel-Instance angehängt. Das Runbook bietet auch die Möglichkeit, zu Beginn der Automatisierung einen Snapshot des Root-Volumes zu erstellen.

Bevor Sie beginnen

Erstellen Sie ein Secrets Manager Manager-Geheimnis mit dem Wert des Passworts, das Sie Ihrem Betriebssystembenutzer zuweisen möchten. Der Wert muss im Klartext angegeben werden. Weitere Informationen finden Sie unter Erstellen eines AWS Secrets Manager -Geheimnisses im AWS Secrets Manager -Benutzerhandbuch.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden. Erwägen Sie, den Wert des `CreateSnapshot` Parameters auf festzulegen. **`Yes`**
- Um das lokale Benutzerkennwort zu ändern, muss das Runbook Ihre Instance beenden. Wenn eine Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren. Außerdem werden alle automatisch zugewiesenen öffentlichen IPv4-Adressen freigegeben. Weitere Informationen darüber, was passiert, wenn Sie eine Instance beenden, finden Sie unter Stoppen und starten Sie Ihre Instance im Amazon EC2 EC2-Benutzerhandbuch.
- Wenn die Amazon EBS-Volumes, die an Ihre Amazon EC2 EC2-Zielinstanz angehängt sind, mit einem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel verschlüsselt sind, stellen Sie sicher, dass der AWS KMS Schlüssel nicht verschlüsselt ist, `deleted` da `disabled` sonst Ihre Instance nicht gestartet werden kann.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Linux-Instance, die das Betriebssystembenutzerkennwort enthält, das Sie zurücksetzen möchten.
- LinuxUserName

  Typ: Zeichenfolge

  Standard: ec2-user

  Beschreibung: (Optional) Das Betriebssystem-Benutzerkonto, dessen Passwort Sie zurücksetzen möchten.
- SecretArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN Ihres Secrets Manager Manager-Geheimnisses, das das neue Passwort enthält.
- SecurityGroupID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die an die temporäre Amazon EC2 EC2-Instance angehängt werden soll. Wenn Sie keinen Wert für diesen Parameter angeben, wird die Standardsicherheitsgruppe Amazon Virtual Private Cloud (Amazon VPC) verwendet.
- SubnetId

  Typ: Zeichenfolge

Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die temporäre Amazon EC2 EC2-Instance starten möchten. Standardmäßig wählt die Automatisierung dasselbe Subnetz wie Ihre Ziel-Instance aus. Wenn Sie sich dafür entscheiden, ein anderes Subnetz bereitzustellen, muss es sich in derselben Availability Zone wie die Ziel-Instance befinden und Zugriff auf Systems Manager Manager-Endpunkte haben.

- CreateSnapshot

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Ja

  Beschreibung: (Optional) Legt fest, ob ein Snapshot des Root-Volumes Ihrer Amazon EC2 EC2-Zielinstanz erstellt wird, bevor die Automatisierung ausgeführt wird.

- StopConsent

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Nein

  Beschreibung: Geben Sie ein, **`Yes`** um zu bestätigen, dass Ihre Amazon EC2 EC2-Zielinstanz während dieser Automatisierung gestoppt wird. Wenn die Amazon EC2 EC2-Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren und die automatische öffentliche IPv4-Adresse wird freigegeben. Weitere Informationen finden Sie unter Beenden und Starten Ihrer Instance im Amazon EC2 EC2-Benutzerhandbuch.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

## Dokumentschritte

1. `aws:branch`— Verzweigungen basierend darauf, ob Sie dem Stoppen der Amazon EC2 EC2-Zielinstanz zugestimmt haben.
2. `aws:assertAwsResourceProperty`Stellt sicher, dass sich der Status der Amazon EC2 EC2-Instance im `stopped` Status `running` oder befindet. Andernfalls endet die Automatisierung.
3. `aws:executeAwsApi`Ruft die Amazon EC2 EC2-Instance-Eigenschaften ab.
4. `aws:executeAwsApi`Ruft die Eigenschaften des Root-Volumes ab.
5. `aws:branch`Verzweigt die Automatisierung in Abhängigkeit davon, ob eine Subnetz-ID für die temporäre Amazon EC2 EC2-Instance bereitgestellt wurde.
6. `aws:assertAwsResourceProperty`Stellt sicher, dass sich das Subnetz, das Sie im `SubnetId` Parameter angeben, in derselben Availability Zone wie die Amazon EC2 EC2-Ziel-Instance befindet.
7. `aws:assertAwsResourceProperty`Stellt sicher, dass es sich bei dem Stammvolume der Amazon EC2 EC2-Instance um ein Amazon EBS-Volume handelt.
8. `aws:assertAwsResourceProperty`Stellt sicher, dass die Amazon EC2 EC2-Instance-Architektur `arm64` oder `x86_64` ist.
9. `aws:assertAwsResourceProperty`Stellt sicher, dass das Verhalten beim Herunterfahren der Amazon EC2 EC2-Instance stimmt `stop` und nicht`terminate`.
10. `aws:branch`Stellt sicher, dass die Amazon EC2 EC2-Instance keine Spot-Instance ist. Andernfalls endet die Automatisierung.
11. `aws:executeScript`Stellt sicher, dass die Amazon EC2 EC2-Instance nicht Teil einer Auto Scaling-Gruppe ist. Wenn die Instance Teil einer Auto Scaling-Gruppe ist, bestätigt die Automatisierung, dass sich die Amazon EC2 EC2-Instance in einem `Standby` Lebenszyklusstatus befindet.
12. `aws:createStack`Erstellt eine temporäre Amazon EC2 EC2-Instance, die verwendet wird, um das Passwort für den von Ihnen angegebenen Betriebssystembenutzer zurückzusetzen.
13. `aws:waitForAwsResourceProperty`Wartet, bis die neu gestartete temporäre Amazon EC2 EC2-Instance läuft.
14. `aws:executeAwsApi`Ruft die ID der temporären Amazon EC2 EC2-Instance ab.
15. `aws:waitForAwsResourceProperty`Wartet darauf, dass die temporäre Amazon EC2 EC2-Instance als von Systems Manager verwaltet gemeldet wird.
16. `aws:changeInstanceState`Stoppt die Amazon EC2 EC2-Zielinstanz.
17. `aws:changeInstanceState`Zwingt die Amazon EC2 EC2-Zielinstanz zum Beenden, falls sie in einem Stopp-Zustand hängen bleibt.

18. `aws:branch` Verzweigt die Automatisierung je nachdem, ob ein Snapshot des Root-Volumes der Amazon EC2 EC2-Zielinstanz angefordert wurde.
19. `aws:executeAwsApi` Erstellt einen Snapshot des Amazon EBS-Stammvolumes der Amazon EC2-Zielinstanz.
20. `aws:waitForAwsResourceProperty` Wartet darauf, dass sich der Snapshot in einem bestimmten Zustand befindet. `completed`
21. `aws:executeAwsApi` Trennt das Amazon EBS-Root-Volume von der Amazon EC2 EC2-Zielinstanz.
22. `aws:waitForAwsResourceProperty` Wartet darauf, dass das Amazon EBS-Root-Volume von der Amazon EC2 EC2-Zielinstanz getrennt wird.
23. `aws:executeAwsApi` Hängt das Amazon EBS-Stammvolume an die temporäre Amazon EC2 EC2-Instance an.
24. `aws:waitForAwsResourceProperty` Wartet darauf, dass das Amazon EBS-Root-Volume an die temporäre Amazon EC2 EC2-Instance angehängt wird.
25. `aws:runCommand` Setzt das Zielbenutzerkennwort zurück, indem ein Shell-Skript mit Run Command auf der temporären Amazon EC2 EC2-Instance ausgeführt wird.
26. `aws:executeAwsApi` Trennt das Amazon EBS-Root-Volume von der temporären Amazon EC2 EC2-Instance.
27. `aws:waitForAwsResourceProperty` Wartet darauf, dass das Amazon EBS-Root-Volume von der temporären Amazon EC2 EC2-Instance getrennt wird.
28. `aws:executeAwsApi` Trennt nach einem Fehler das Amazon EBS-Root-Volume von der temporären Amazon EC2 EC2-Instance.
29. `aws:waitForAwsResourceProperty` Wartet darauf, dass das Amazon EBS-Root-Volume nach einem Fehler von der temporären Amazon EC2 EC2-Instance getrennt wird.
30. `aws:branch` Verzweigt die Automatisierung je nachdem, ob ein Snapshot des Root-Volumes angefordert wurde, um den Wiederherstellungspfad für den Fall eines Fehlers zu ermitteln.
31. `aws:executeAwsApi` Hängt das Amazon EBS-Stammvolume erneut an die Amazon EC2 EC2-Zielinstanz an.
32. `aws:waitForAwsResourceProperty` Wartet darauf, dass das Amazon EBS-Root-Volume an die Amazon EC2 EC2-Instance angehängt wird.
33. `aws:executeAwsApi` Erstellt ein neues Amazon EBS-Volume aus dem Root-Volume-Snapshot der Amazon EC2 EC2-Instance.

34. `aws:waitForAwsResourceProperty` Wartet, bis sich das neue Amazon EBS-Volume in einem `available` Zustand befindet.
35. `aws:executeAwsApi` Hängt das neue Amazon EBS-Volume als Root-Volume an die Ziel-Instance an.
36. `aws:waitForAwsResourceProperty` Wartet darauf, dass sich das Amazon EBS-Volume in einem `attached` bestimmten Zustand befindet.
37. `aws:executeAwsApi` Beschreibt die AWS CloudFormation Stack-Ereignisse, wenn die Runbooks den Stack nicht erstellen oder aktualisieren können. AWS CloudFormation
38. `aws:branch` Verzweigt die Automatisierung in Abhängigkeit vom vorherigen Status der Amazon EC2 EC2-Instanz. Wenn der Status war `running`, wird die Instance gestartet. Wenn sie sich in einem `stopped` Status befand, wird die Automatisierung fortgesetzt.
39. `aws:changeInstanceState` Startet die Amazon EC2 EC2-Instance bei Bedarf.
40. `aws:waitForAwsResourceProperty` Wartet, bis sich der AWS CloudFormation Stack im Terminalstatus befindet, bevor er gelöscht wird.
41. `aws:executeAwsApi` Löscht den AWS CloudFormation Stack einschließlich der temporären Amazon EC2 EC2-Instance.

## AWSPremiumSupport-ResizeNitroInstance

Beschreibung

Das `AWSPremiumSupport-ResizeNitroInstance` Runbook bietet eine automatisierte Lösung für die Größenänderung von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die auf dem Nitro System basieren.

Um das potenzielle Risiko von Datenverlust und Ausfallzeiten zu reduzieren, überprüft das Runbook Folgendes:

- Stoppverhalten der Instanz.
- Wenn die Instance Teil einer Amazon EC2 Auto Scaling-Gruppe ist und sich im `standby` Modus befindet.
- Instanzstatus und Mietverhältnis.
- Der Instance-Typ, zu dem Sie wechseln möchten, unterstützt die Anzahl der Netzwerkschnittstellen, die derzeit an Ihre Instance angeschlossen sind.

- Die Prozessorarchitektur und der Virtualisierungstyp sind sowohl für den aktuellen Instance-Typ als auch für den Ziel-Instance-Typ identisch.
- Wenn die Instanz läuft, dass sie alle Statusprüfungen besteht.
- Der Instance-Typ, zu dem Sie wechseln möchten, ist in derselben Availability Zone verfügbar.

Wenn Amazon EC2 die Statusprüfungen nach der Änderung des Instance-Typs nicht besteht, kehrt das Runbook automatisch zum vorherigen Instance-Typ zurück.

Standardmäßig ändert dieses Runbook den Instance-Typ nicht, wenn es läuft und Instance-Store-Volumes angehängt sind. Das Runbook ändert den Instance-Typ auch nicht, wenn die Instanz Teil eines AWS CloudFormation Stacks ist. Wenn Sie eines dieser Verhaltensweisen ändern möchten, geben Sie `yes` für die `AllowCloudFormationInstances` Parameter `AllowInstanceStoreInstances` und an.

Das Runbook bietet zwei verschiedene Möglichkeiten, den Instanztyp anzugeben, zu dem Sie wechseln möchten:

- Geben Sie für einfache Automatisierungen, die auf eine einzelne Instanz abzielen, mithilfe des `TargetInstanceTypeFromParameter` Parameters den Instanztyp an, zu dem Sie wechseln möchten.
- Um Automatisierungen in großem Maßstab auszuführen, um den Instanztyp mehrerer Instanzen zu ändern, geben Sie den Instanztyp mithilfe des `TargetInstanceTypeFromTagValue` Parameters an. Informationen zur skalierbaren Ausführung von Automatisierungen finden Sie unter Ausführen von Automatisierungen in großem Maßstab.

Wenn Sie für keinen der Parameter einen Wert angeben, schlägt die Automatisierung fehl.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist entweder ein Enterprise- oder ein Business Support-Abonnement erforderlich. Weitere Informationen finden Sie unter AWS SupportTarife vergleichen.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden.

- Informationen zur Kompatibilität beim Ändern von Instanztypen finden Sie unter Kompatibilität beim Ändern des Instanztyps.
- Wenn die Automatisierung fehlschlägt und auf den ursprünglichen Instance-Typ zurückgesetzt wird, finden Sie weitere Informationen unter Problembehandlung beim Ändern des Instance-Typs.
- Wenn Sie den Instance-Typ ändern, muss das Runbook Ihre Instance stoppen. Wenn eine Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren. Außerdem werden alle automatisch zugewiesenen öffentlichen IPv4-Adressen veröffentlicht. Weitere Informationen darüber, was passiert, wenn Sie eine Instance beenden, finden Sie unter Stoppen und Starten Ihrer Instance.
- Mithilfe des `SkipInstancesWithTagKey` Parameters können Sie Instances überspringen, auf die ein bestimmter Amazon EC2-Tag-Schlüssel angewendet wurde.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Bestätigen

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Geben Sie ein, **`yes`** um zu bestätigen, dass Ihre Instance gestoppt wird, sofern sie gerade läuft.

- AllowInstanceStoreInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie dies angeben`yes`, erlauben Sie, dass das Runbook auf Instances ausgeführt wird, an die Instance-Speicher-Volumes angehängt sind.

- AllowCloudFormationInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie angeben`yes`, wird das Runbook auf Instanzen ausgeführt, die Teil eines AWS CloudFormation Stacks sind.

- DryRun

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie dies angeben`yes`, überprüft das Runbook die Anforderungen an die Größenänderung, ohne Änderungen am Instanztyp vorzunehmen.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, deren Typ Sie ändern möchten.

- SkipInstancesWithTagKey

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Automatisierung überspringt eine Zielinstanz, wenn der von Ihnen angegebene Tag-Schlüssel auf die Instanz angewendet wird.

- SleepTime

  Typ: Zeichenfolge

  Standard: 3

  Beschreibung: (Optional) Die Anzahl der Sekunden, für die dieses Runbook nach der Fertigstellung in den Ruhezustand versetzt werden soll.

- TagInstance

  Typ: Zeichenfolge

  Beschreibung: (Optional) Kennzeichnen Sie die Instanzen mit dem Schlüssel und Wert Ihrer Wahl und verwenden Sie dabei das folgende Format: *`Key=ChangingType, Value=True`*. Mit dieser Option können Sie Instances verfolgen, auf die dieses Runbook abzielt. Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.

- TargetInstanceTypeFromParameter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ, in den Sie Ihre Instance ändern möchten. Lassen Sie diesen Parameter leer, wenn Sie den Wert des im `TargetInstanceTypeFromTagValue` Parameter angegebenen Tag-Schlüssels verwenden möchten.

- TargetInstanceTypeFromTagValue

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der auf Ihre Ziel-Instances angewendete Tag-Schlüssel, dessen Wert den Instance-Typ enthält, zu dem Sie wechseln möchten. Wenn Sie einen Wert für den `TargetInstanceTypeFromParameter` Parameter angeben, überschreibt dieser jeden Wert, den Sie für diesen Parameter angeben.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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

Dokumentschritte

1. aws:assertAwsResourceProperty: Stellt sicher, dass die Amazon EC2-Instance nicht mit dem im SkipInstancesWithTagKey Parameter angegebenen Resourcen-Tag-Schlüssel gekennzeichnet ist. Wenn festgestellt wird, dass der Tag-Schlüssel auf die Instanz angewendet wurde, schlägt der Schritt fehl und die Automatisierung wird beendet.
2. aws:assertAwsResourceProperty: Bestätigt, dass der Status der Amazon EC2-Zielinstanzrunning, pendingstopped, oder stopping lautet. Andernfalls endet die Automatisierung.
3. aws:executeAwsApi: Ruft Eigenschaften aus der Amazon EC2-Instance ab.
4. aws:executeAwsApi: Sammelt Details über den aktuellen Amazon EC2-Instance-Typ.
5. aws:branch: Prüft, ob der aktuelle Instanztyp und der im TargetInstanceTypeFromParameter Parameter angegebene Instanztyp identisch sind. Wenn dies der Fall ist, endet die Automatisierung.
6. aws:assertAwsResourceProperty: Stellt sicher, dass die Instanz auf dem Nitro-System läuft.
7. aws:branch: Stellt sicher, dass der Root-Volume-Typ der Amazon EC2-Instance ein Amazon Elastic Block Store (Amazon EBS) -Volume ist.

8. `aws:assertAwsResourceProperty`: Bestätigt, dass das Verhalten beim Herunterfahren der Instanz ist `stop` und nicht`terminate`.
9. `aws:branch`: Stellt sicher, dass die Amazon EC2-Instance keine Spot-Instance ist.
10. `aws:branch`: Stellt sicher, dass es sich bei der Amazon EC2-Instance-Tenancy um eine Standardeinstellung handelt und nicht um einen dedizierten Host oder eine dedizierte Instance.
11. `aws:executeScript`: Bestätigt, dass es nur eine Automatisierung dieses Runbooks gibt, die auf die aktuelle Instanz-ID abzielt. Wenn bereits eine weitere Automatisierung läuft, die auf dieselbe Instanz abzielt, gibt die Automatisierung einen Fehler zurück und wird beendet.
12. `aws:branch`: Zweigt die Automatisierung auf der Grundlage des Status der Amazon EC2-Instance ab.
    a. Falls `stopped` oder`stopping`, wird die Automatisierung ausgeführt, `aws:waitForAwsResourceProperty` bis die Amazon EC2-Instance vollständig gestoppt ist.
    b. Falls `running` oder`pending`, wird die Automatisierung ausgeführt, `aws:waitForAwsResourceProperty` bis die Amazon EC2-Instance die Statusprüfungen bestanden hat.
13. `aws:assertAwsResourceProperty`: Bestätigt, dass die Amazon EC2-Instance nicht Teil einer Auto Scaling-Gruppe ist, indem der `DescribeAutoScalingInstances` API-Vorgang aufgerufen wird. Wenn die Instance Teil einer Auto Scaling-Gruppe ist, stellen Sie sicher, dass sich die Amazon EC2-Instance im `standby` Modus befindet.
14. `aws:branch`: Zweigt die Automatisierung ab, je nachdem, ob die Automatisierung überprüfen soll, ob die Amazon EC2-Instance Teil eines AWS CloudFormation Stacks ist:
    a. `aws:executeScript`Stellt sicher, dass die Amazon EC2-Instance nicht Teil eines AWS CloudFormation Stacks ist, indem der `DescribeStackResources` API-Vorgang aufgerufen wird.
15. `aws:executeAwsApi`: Gibt eine Liste von Instanztypen zurück, die denselben Prozessorarchitekturtyp und Virtualisierungstyp haben und die Anzahl der Netzwerkschnittstellen unterstützen, die derzeit an die Zielinstanz angeschlossen sind.
16. `aws:executeAwsApi`: Ruft den Wert des Zielinstanztyps aus dem im `TargetInstanceTypeFromTagValue` Parameter angegebenen Tag-Schlüssel ab.
17. `aws:executeScript`: Bestätigt, dass der aktuelle Instance-Typ und der Ziel-Instance-Typ kompatibel sind. Stellt sicher, dass der Ziel-Instance-Typ im selben Subnetz verfügbar ist. Überprüft, ob der Principal, der das Runbook gestartet hat, berechtigt ist, den Instanztyp zu ändern und die Instanz zu beenden und zu starten, falls sie ausgeführt wurde.

18. `aws:branch`: Zweigt die Automatisierung ab, je nachdem, ob der `DryRun` Parameterwert auf gesetzt ist`yes`. Wenn`yes`, endet die Automatisierung.
19. `aws:branch`: Prüft, ob der ursprüngliche Instance-Typ und der Ziel-Instance-Typ identisch sind. Wenn sie identisch sind, endet die Automatisierung.
20. `aws:executeAwsApi`: Ruft den aktuellen Instanzstatus ab.
21. `aws:changeInstanceState`: Stoppt die Amazon EC2-Instance.
22. `aws:changeInstanceState`: Zwingt die Instanz zum Stoppen, wenn sie im `stopping` Status feststeckt.
23. `aws:executeAwsApi`: Ändert den Instance-Typ in den Ziel-Instance-Typ.
24. `aws:sleep`: Wartet nach dem Ändern des Instanztyps 3 Sekunden, um die Konsistenz sicherzustellen.
25. `aws:branch`: Zweigt die Automatisierung auf der Grundlage des vorherigen Instanzstatus ab. Wenn ja`running`, wird die Instanz gestartet.
    a. `aws:changeInstanceState`: Startet die Amazon EC2-Instance, falls sie vor der Änderung des Instance-Typs ausgeführt wurde.
    b. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2-Instance die Statusprüfungen bestanden hat. Wenn die Instance die Statusprüfungen nicht besteht, wird die Instance wieder auf ihren ursprünglichen Instance-Typ zurückgesetzt.
        i. `aws:changeInstanceState`: Stoppt die Amazon EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird.
        ii. `aws:changeInstanceState`: Erzwingt das Stoppen der Amazon EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird, falls sie in einem Stopp-Zustand stecken bleibt.
        iii. `aws:executeAwsApi`: Ändert die Amazon EC2-Instance auf ihren ursprünglichen Typ.
        iv. `aws:sleep`: Wartet nach dem Ändern des Instanztyps 3 Sekunden, um die Konsistenz sicherzustellen.
        v. `aws:changeInstanceState`: Startet die Amazon EC2-Instance, falls sie vor der Änderung des Instance-Typs ausgeführt wurde.
        vi. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2-Instance die Statusprüfungen bestanden hat.
26. `aws:sleep`: Wartet, bevor das Runbook beendet wird.

# AWSSupport-RestoreEC2InstanceFromSnapshot

Beschreibung

Das `AWSSupport-RestoreEC2InstanceFromSnapshot` Runbook hilft Ihnen dabei, eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance aus einem funktionierenden Amazon Elastic Block Store (Amazon EBS) -Snapshot des Root-Volumes zu identifizieren und wiederherzustellen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EndDate

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das letzte Datum, an dem die Automatisierung nach einem Snapshot suchen soll.
- InplaceSwap

  Typ: Boolesch

Zulässige Werte: true | false

Beschreibung: (Optional) Wenn der Wert für diesen Parameter auf gesetzt ist`true`, ersetzt das neu erstellte Volume aus dem Snapshot das vorhandene Root-Volume, das an Ihre Instance angehängt ist.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, die Sie aus einem Snapshot wiederherstellen möchten.

- LookForInstanceStatusCheck

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn der Wert für diesen Parameter auf gesetzt ist, überprüft die Automatisierung`true`, ob Instanzstatusprüfungen bei den Testinstanzen, die über die Snapshots gestartet wurden, fehlschlagen.

- SkipSnapshotsBy

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Intervall, in dem Snapshots übersprungen werden, wenn nach Snapshots zur Wiederherstellung Ihrer Instance gesucht wird. Wenn beispielsweise 100 Snapshots verfügbar sind und Sie für diesen Parameter den Wert 2 angeben, wird jeder dritte Snapshot überprüft.

  Standard: 0

- SnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID eines Snapshots, aus dem Sie die Instanz wiederherstellen möchten.

- StartDate

Typ: Zeichenfolge

Beschreibung: (Optional) Das erste Datum, an dem die Automatisierung nach einem Snapshot suchen soll.

- TotalSnapshotsToLook

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Schnappschüsse, die von der Automatisierung überprüft werden.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:executeAwsApi`- Sammelt Details über die Zielinstanz.
2. `aws:assertAwsResourceProperty`- Überprüft, ob die Zielinstanz existiert.
3. `aws:assertAwsResourceProperty`— Überprüft, ob es sich bei dem Root-Volume um ein Amazon EBS-Volume handelt.
4. `aws:assertAwsResourceProperty`— Überprüft, ob nicht bereits eine andere Automatisierung ausgeführt wird, die auf diese Instanz abzielt.
5. `aws:executeAwsApi`- Markiert die Zielinstanz.
6. `aws:executeAwsApi`- Erzeugt eine AMI der Instanzen.
7. `aws:executeAwsApi`- Sammelt Details zu den im vorherigen Schritt AMI erstellten Objekten.
8. `aws:waitForAwsResourceProperty`- Wartet, bis der AMI Staat bereit ist, `available` bevor er weitermacht.
9. `aws:executeScript`- Startet eine neue Instanz von der neu erstellten ausAMI.
10. `aws:assertAwsResourceProperty`- Überprüft, ob der Instanzstatus lautet`available`.
11. `aws:executeAwsApi`- Sammelt Details über die neu gestartete Instanz.
12. `aws:branch`- Verzweigungen basierend darauf, ob Sie einen Wert für den `SnapshotId` Parameter angegeben haben.
13. `aws:executeScript`- Gibt eine Liste von Schnappschüssen innerhalb des angegebenen Zeitraums zurück.
14. `aws:executeAwsApi`- Stoppt die Instanz.
15. `aws:waitForAwsResourceProperty`- Wartet, bis der Lautstärkestatus erreicht ist. `available`
16. `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Instanzstatus erreicht ist. `stopped`
17. `aws:executeAwsApi`- Löst das Root-Volume.
18. `aws:waitForAwsResourceProperty`- Wartet, bis das Root-Volume abgetrennt wird.
19. `aws:executeAwsApi`- Hängt das neue Root-Volume an.

20. `aws:waitForAwsResourceProperty` - Wartet darauf, dass der neue Band angehängt wird.
21. `aws:executeAwsApi` - Startet die Instanz.
22. `aws:waitForAwsResourceProperty` - Wartet darauf, dass der Instanzstatus erreicht ist. `available`
23. `aws:waitForAwsResourceProperty` - Wartet darauf, dass die System- und Instanzstatusprüfungen für die Instanz bestanden haben.
24. `aws:executeScript` - Führt ein Skript aus, um einen Snapshot zu finden, mit dem erfolgreich ein Volume erstellt werden kann.
25. `aws:executeScript` - Führt ein Skript aus, um die Instanz mithilfe des neu erstellten Volumes aus dem von der Automatisierung identifizierten Snapshot oder mithilfe des Volumes wiederherzustellen, das aus dem Snapshot erstellt wurde, den Sie im `SnapshotId` Parameter angegeben haben.
26. `aws:executeScript` - Löscht Ressourcen, die durch die Automatisierung erstellt wurden.

Ausgaben

launchCloneInstance.InstanceIds

ListSnapshotByDate. Letzte Schnappschüsse

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot. Funktionierender Snapshot

InstanceRecovery.Ergebnis

## `AWSSupport-SendLogBundleToS3Bucket`

Beschreibung

Das `AWSSupport-SendLogBundleToS3Bucket` Runbook lädt ein vom EC2Rescue-Tool generiertes Log-Paket von der Zielinstanz in den angegebenen S3-Bucket hoch. Das Runbook installiert die plattformspezifische Version von ec2Rescue basierend auf der Plattform der Zielinstanz. EC2Rescue wird dann verwendet, um alle verfügbaren Betriebssystem-Protokolle zu erfassen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der von Windows oder Linux verwalteten Instance, von der Sie Protokolle erfassen möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket, in den die Protokolle hochgeladen werden sollen.

- S3Path

  Typ: Zeichenfolge

  Standard:`AWSSupport-SendLogBundleToS3Bucket/`

  Beschreibung: (Optional) S3-Pfad für die erfassten Protokolle.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Der Benutzer muss mindestens über ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instanz zu senden, sowie über ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können.

Dokumentschritte

1. `aws:runCommand`- Installieren Sie EC2Rescue über. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Führen Sie das PowerShell Skript aus, um Windows-Fehlerbehebungsprotokolle mit EC2Rescue zu sammeln.
3. `aws:runCommand`- Führen Sie das Bash-Skript aus, um mit EC2Rescue Protokolle zur Linux-Fehlerbehebung zu sammeln.

Ausgaben

collectAndUploadWindowsLogBundle.Ausgang

collectAndUploadLinuxLogBundle.Ausgang

## AWSSupport-StartEC2RescueWorkflow

Beschreibung

Das `AWSSupport-StartEC2RescueWorkflow` Runbook führt das bereitgestellte base64-codierte Skript (Bash oder Powershell) auf einer Hilfsinstanz aus, die erstellt wurde, um Ihre Instanz zu retten. Das Root-Volume Ihrer Instance ist der Helper-Instance (auch als EC2Rescue-Instance bezeichnet) angefügt und gemountet. Wenn Ihre Instance unter Windows läuft, geben Sie ein Powershell-Skript an. Verwenden Sie andernfalls Bash. Das Runbook legt einige Umgebungsvariablen fest, die Sie in Ihrem Skript verwenden können. Die Umgebungsvariablen enthalten Informationen über die Eingabe, die Sie bereitgestellt haben, sowie Informationen zu dem Offline-Root-Volume. Das Offline-Volume ist bereits gemountet und kann verwendet werden. Beispiel: Sie können eine Desired State Configuration-Datei zu einem Offline-Windows-Root-Volume oder chroot zu einem Offline-Linux-Root-Volume speichern und eine Offline-Wiederherstellung durchführen.

Diese Automatisierung ausführen (Konsole)

> **Important**
>
> Amazon EC2-Instances, die aus Marketplace Amazon Machine Images (AMIs) erstellt wurden, werden von dieser Automatisierung nicht unterstützt.

Zusätzliche Informationen

Um ein Skript mit base64 zu kodieren, können Sie PowerShell oder Bash verwenden. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::Rea
```

Bash:

```
base64 PATH_TO_FILE
```

Hier sehen Sie eine Liste der Umgebungsvariablen, die Sie in Ihren Offline-Skripts verwenden können, je nach Ziel-Betriebssystem.

Windows:

| Variable | Beschreibung | Beispielwert |
|---|---|---|
| $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 für Windows-Installationspfad | C:\Program Files\Amazon\EC2Rescue |
| $env:EC2RESCUE_EC2RW_DIR | EC2Rescue für Windows-Installationspfad | C:\Program Files\Amazon\EC2Rescue |
| $env:EC2RESCUE_EXECUTION_ID | {{ automation:EXECUTION_ID }} | 7ef8008e-219b-4aca-8bb5-65e2e898e20b |

| Variable | Beschreibung | Beispielwert |
| --- | --- | --- |
| $env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET | Offline Windows Current Control Set-Pfad | `HKLM:\AWSTempSystem\ControlSet001` |
| $env:EC2RESCUE_OFFLINE_DRIVE | Offline-Windows-Laufwerkbuchstabe | D:\ |
| $env:EC2RESCUE_OFFLINE_EBS_DEVICE | Offline-Root-Volume-EBS-Gerät | xvdf |
| $env:EC2RESCUE_OFFLINE_KERNEL_VER | Offline-Windows-Kernel-Version | 6.1.7601.24214 |
| $env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE | Offline-Windows-Architektur | AMD64 |
| $env:EC2RESCUE_OFFLINE_OS_CAPTION | Offline-Windows-Beschriftung | Windows Server 2008 R2 Datacenter |
| $env:EC2RESCUE_OFFLINE_OS_TYPE | Offline-Windows-Betriebssystemtyp | Server |
| $env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR | Offline-Windows-Programmdateien-Verzeichnispfad | D:\Program Files |
| $env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR | Offline-Windows-Programmdateien-x86-Verzeichnispfad | D:\Program Files (x86) |
| $env:EC2RESCUE_OFFLINE_REGISTRY_DIR | Offline-Windows-Registry-Verzeichnispfad | D:\Windows\System32\config |
| $env:EC2RESCUE_OFFLINE_SYSTEM_ROOT | Offline-Windows-Systemstamm-Verzeichnispfad | D:\Windows |
| $env:EC2RESCUE_REGION | {{ global:REGION }} | us-west-1 |

| Variable | Beschreibung | Beispielwert |
| --- | --- | --- |
| $env:EC2RESCUE_S3_BUCKET | {{S3BucketName}} | mybucket |
| $env:EC2RESCUE_S3_PREFIX | {{ S3Prefix }} | myprefix/ |
| $env:EC2RESCUE_SOURCE_INSTANCE | {{ InstanceId }} | i-abcdefgh123456789 |
| $script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL | Offline-Windows-Installations-Metadaten | Customer PowerShell-Objekt |

Linux:

| Variable | Beschreibung | Beispielwert |
| --- | --- | --- |
| 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 für Linux-Installationspfad | /usr/local/ec2rl-1.1.3 |
| EC2RESCUE_EXECUTION_ID | {{ automation:EXECUTION_ID }} | 7ef8008e-219b-4aca-8bb5-65e2e898e20b |
| EC2RESCUE_OFFLINE_DEVICE | Offline-Gerätename | /dev/xvdf1 |
| EC2RESCUE_OFFLINE_EBS_DEVICE | Offline-Root-Volume-EBS-Gerät | /dev/sdf |
| EC2RESCUE_OFFLINE_SYSTEM_ROOT | Offline-Root-Volume-Mounting-Punkt | /mnt/mount |

| Variable | Beschreibung | Beispielwert |
| --- | --- | --- |
| EC2RESCUE_PYTHON | Python-Version | 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 |

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AMIPrefix

  Typ: Zeichenfolge

  Standard: `AWSSupport-EC2Rescue`

  Beschreibung: (Optional) Ein Präfix für den Backup-AMI-Namen.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- CreatePostEC2 RescueBackup

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Setzen Sie es auf, `true` um ein AMI von zu erstellen, InstanceId nachdem Sie das Skript ausgeführt haben, bevor Sie es starten. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen.

- CreatePreEC2 RescueBackup

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Stellen Sie es auf ein, `true` um InstanceId vor der Ausführung des Skripts ein AMI von zu erstellen. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen.

- EC2 RescueInstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.small | t2.medium | t2.large

  Standard: t2.small

  Beschreibung: (Optional) Der EC2-Instance-Typ für die EC2Rescue-Instance.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer EC2-Instance. WICHTIG: Die AWS Systems Manager-Automatisierung stoppt diese Instance. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- OfflineScript

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Base64-kodiertes Skript zur Ausführung gegen die Helper-Instance. Verwenden Sie Bash, wenn Ihre Quellinstanz Linux ist und PowerShell wenn es Windows ist.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- S3Prefix

  Typ: Zeichenfolge

  Standard: `AWSSupport-EC2Rescue`

  Beschreibung: (Optional) Ein Präfix für die S3-Protokolle.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Die Subnetz-ID für die EC2Rescue-Instance. Standardmäßig wird dasselbe Subnetz verwendet, in dem sich die bereitgestellte Instance befindet. WICHTIG: Wenn Sie ein benutzerdefiniertes Subnetz bereitstellen, muss es sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpoints ermöglichen.

- UniqueId

  Typ: Zeichenfolge

  Standard: {{ automation:EXECUTION_ID }}

  Beschreibung: (Optional) Eine eindeutige Kennung für die Automatisierung.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass dem Benutzer, der die Automatisierung ausführt, die von AmazonSSM AutomationRole IAM verwaltete Richtlinie beigefügt wird. Zusätzlich zu dieser Richtlinie benötigt der Benutzer:

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

## Dokumentschritte

1. `aws:executeAwsApi` - Beschreiben Sie die bereitgestellte Instanz

2. `aws:executeAwsApi`- Beschreiben Sie das Root-Volume der bereitgestellten Instanz
3. `aws:assertAwsResourceProperty`- Überprüfen Sie, ob der Root-Volume-Gerätetyp EBS ist
4. `aws:assertAwsResourceProperty`- Überprüfen Sie, ob das Root-Volume nicht verschlüsselt ist
5. `aws:assertAwsResourceProperty`- Überprüfen Sie die angegebene Subnetz-ID
   a. (Aktuelles Instance-Subnetz verwenden) — Wenn * SubnetId = SelectedInstanceSubnet *, starten Sie den EC2Rescue-Stack, `aws:createStack` um den CloudFormation EC2Rescue-Stack bereitzustellen
   b. (Neue VPC erstellen) — Wenn * SubnetId = CreateNew VPC*, dann starten Sie, `aws:createStack` um den EC2Rescue-Stack bereitzustellen CloudFormation
   c. (Verwenden eines benutzerdefinierten Subnetzes) – In allen anderen Fällen:

      `aws:assertAwsResourceProperty`- Überprüfen Sie, ob sich das bereitgestellte Subnetz in derselben Availability Zone befindet wie die bereitgestellte Instance

      `aws:createStack`- Stellen Sie den CloudFormation EC2Rescue-Stack bereit
6. `aws:invokeLambdaFunction`- Führen Sie eine zusätzliche Eingabeüberprüfung durch
7. `aws:executeAwsApi`- Aktualisieren Sie den CloudFormation EC2Rescue-Stack, um die EC2Rescue-Helper-Instanz zu erstellen
8. `aws:waitForAwsResourceProperty`- Warten Sie, bis das CloudFormation EC2Rescue-Stack-Update abgeschlossen ist
9. `aws:executeAwsApi`- Beschreiben Sie die CloudFormation EC2Rescue-Stack-Ausgabe, um die EC2Rescue-Helper-Instance-ID zu erhalten
10. `aws:waitForAwsResourceProperty`- Warten Sie, bis die EC2Rescue-Helper-Instanz zu einer verwalteten Instanz wird
11. `aws:changeInstanceState`- Stoppt die bereitgestellte Instanz
12. `aws:changeInstanceState`- Stoppt die bereitgestellte Instanz
13. `aws:changeInstanceState`- Stopp der bereitgestellten Instanz erzwingen
14. `aws:assertAwsResourceProperty`- Überprüfen Sie den CreatePre RescueBackup EC2-Eingabewert
    a. (Pre-EC2Rescue-Backup erstellen) — Wenn * EC2 = wahr* CreatePre RescueBackup
    b. `aws:executeAwsApi`- Erstellen Sie ein AMI-Backup der bereitgestellten Instance
    c. `aws:createTags`- Taggen Sie das AMI-Backup

15. `aws:runCommand`- Installieren Sie ec2Rescue auf der EC2Rescue-Helper-Instanz
16. `aws:executeAwsApi`- Trennen Sie das Root-Volume von der bereitgestellten Instanz
17. `aws:assertAwsResourceProperty`- Überprüfen Sie die bereitgestellte Instanzplattform
    a. (Instance ist Windows):

       `aws:executeAwsApi`- Hängen Sie das Root-Volume als *xvdf* an die EC2Rescue-Helper-Instance an

       `aws:sleep`- Schlaf 10 Sekunden

       `aws:runCommand`- Führen Sie das bereitgestellte Offline-Skript in Powershell aus

    b. (Instance ist Linux):

       `aws:executeAwsApi`- Hängen Sie das Root-Volume als */dev/sdf* an die EC2Rescue-Helper-Instance an

       `aws:sleep`- Schlaf 10 Sekunden

       `aws:runCommand`- Führe das bereitgestellte Offline-Skript in Bash aus
18. `aws:changeInstanceState`- Stoppen Sie die EC2Rescue-Helper-Instanz
19. `aws:changeInstanceState`- Stopp der EC2Rescue-Helper-Instanz erzwingen
20. `aws:executeAwsApi`- Trennen Sie das Root-Volume von der EC2Rescue-Helper-Instance
21. `aws:executeAwsApi`- Hängen Sie das Root-Volume wieder an die bereitgestellte Instanz an
22. `aws:assertAwsResourceProperty`- Überprüfen Sie den CreatePost RescueBackup EC2-Eingabewert
    a. (Post-EC2Rescue-Backup erstellen) — Wenn * EC2 = wahr* CreatePost RescueBackup
    b. `aws:executeAwsApi`- Erstellen Sie ein AMI-Backup der bereitgestellten Instance
    c. `aws:createTags`- Taggen Sie das AMI-Backup
23. `aws:executeAwsApi`- Stellt den ursprünglichen Status „Löschen bei Beendigung“ für das Root-Volume der bereitgestellten Instance wieder her
24. `aws:changeInstanceState`- Stellt den Ausgangszustand der bereitgestellten Instanz wieder her (laufend/gestoppt)
25. `aws:deleteStack`- Lösche den CloudFormation EC2Rescue-Stack

Ausgaben

runScriptForLinux.Ausgabe

runScriptForWindows.Ausgabe

preScriptBackup.ImageId

postScriptBackup.ImageId

## AWSPremiumSupport-TroubleshootEC2DiskUsage

Beschreibung

Das `AWSPremiumSupport-TroubleshootEC2DiskUsage` Runbook hilft Ihnen bei der Untersuchung und potenziellen Behebung von Problemen mit der Nutzung von Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Root-Festplatten und anderen Festplatten. Wenn möglich, versucht das Runbook, Probleme zu beheben, indem es das Volume und sein Dateisystem erweitert. Um diese Aufgaben auszuführen, orchestriert dieses Runbook die Ausführung mehrerer Runbooks, die auf dem Betriebssystem der betroffenen Instanz basieren.

Das erste Runbook `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` oder bestimmt`AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, ob Festplattenprobleme durch eine Erweiterung des Volumes behoben werden können.

Das zweite Runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` oder`AWSPremiumSupport-ExtendVolumesOnLinux`, verwendet die Ausgabe des ersten Runbooks, um Python-Code auszuführen, der das Volumen ändert. Nachdem das Volume geändert wurde, erweitert das Runbook die Partition und das Dateisystem der betroffenen Volumes.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Enterprise- oder Business Support-Abonnement erforderlich. Weitere Informationen finden Sie unter AWS SupportTarife vergleichen.

Dieses Dokument wurde in Zusammenarbeit mit AWS Managed Services (AMS) erstellt. AMS hilft Ihnen, Ihre AWS Infrastruktur effizienter und sicherer zu verwalten. AMS bietet außerdem betriebliche Flexibilität, verbesserte Sicherheit und Einhaltung von Vorschriften, Kapazitätsoptimierung und Identifizierung von Kosteneinsparungen. Weitere Informationen finden Sie unter AWS Managed Services.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- InstanceId

  Typ: Zeichenfolge

  Erlaubte Werte: ^i- [a-z0-9] {8,17} $

  Beschreibung: (Erforderlich) ID Ihrer Amazon EC2-Instance.
- VolumeExpansionEnabled

  Typ: Boolesch

  Beschreibung: (Optional) Dieses Feld steuert, ob das Dokument die betroffenen Volumes und Partitionen erweitert.

  Standard: true
- VolumeExpansionUsageTrigger

  Typ: Zeichenfolge

  Beschreibung: (Optional) Minimale Nutzung des Partitionsspeichers, der erforderlich ist, um die Erweiterung auszulösen (in Prozent).

  Zulässige Werte: ^ [0-9] {1,2} $

  Standard: 85
- VolumeExpansionCapSize

Typ: Zeichenfolge

Beschreibung: (Optional) Maximale Größe, auf die das Amazon Elastic Block Store (Amazon EBS) -Volume erhöht wird (in GiB).

Zulässige Werte: ^ [0-9] {1,4} $

Standard: 2048

- VolumeExpansionGibIncrease

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erhöhung des Volumens in GiB. Der größte Nettozuwachs zwischen VolumeExpansionGibIncrease und VolumeExpansionPercentageIncrease wird verwendet.

  Zulässige Werte: ^ [0-9] {1,4} $

  Standard: 20

- VolumeExpansionPercentageIncrease

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erhöhung des Prozentsatzes der Lautstärke. Der größte Nettozuwachs zwischen VolumeExpansionGibIncrease und VolumeExpansionPercentageIncrease wird verwendet.

  Zulässige Werte: ^ [0-9] {1,2} $

  Standard: 20

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Prüfen Sie, ob die Instanz vom Systems Manager verwaltet wird
2. `aws:executeAwsApi`- Beschreibt die Instanz, um die Plattform abzurufen.
3. `aws:branch`- Filialautomatisierung basierend auf der Plattform der Instanz.
   a. Wenn es sich bei der Instanz um Windows handelt:
      i. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` Runbook aus, um Probleme mit der Festplattenauslastung auf der Instance zu diagnostizieren.

ii. `aws:executeAwsApi`- Ruft die Ausgabe der vorherigen Automatisierung ab.

iii. `aws:branch`- Abzweigungen auf der Grundlage der Ergebnisse der Diagnosen und ob Volumen vorhanden sind, die erweitert werden können, um die Warnung zu mildern.

A. Es gibt keine Volumina, die erweitert werden müssen: Beenden Sie die Automatisierung.

B. Es gibt Bände, die erweitert werden müssen:

I. `aws:executeAwsApi`- Erstellen Sie eine Amazon Machine Image (AMI) der Instanz.

II. `aws:waitForAwsResourceProperty`- Wartet darauf, dass der AMI Staat da ist. `available`

III. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-ExtendVolumesOnWindows` Runbook aus, um die Volumenänderung sowie die erforderlichen Schritte im Betriebssystem (OS) durchzuführen, um den neuen Speicherplatz verfügbar zu machen.

b. (Plattform ist nicht Windows) Wenn die Eingabeinstanz nicht Windows ist:

i. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` Runbook aus, um Probleme mit der Festplattenauslastung auf der Instance zu diagnostizieren.

ii. `aws:executeAwsApi`- Ruft die Ausgabe der vorherigen Automatisierung ab.

iii. `aws:branch`- Abzweigungen auf der Grundlage der Ergebnisse der Diagnosen und ob Volumen vorhanden sind, die erweitert werden können, um die Warnung zu mildern.

A. Es gibt keine Volumina, die erweitert werden müssen: Beenden Sie die Automatisierung.

B. Es gibt Bände, die erweitert werden müssen:

I. `aws:executeAwsApi`- Erstellen Sie eine AMI der Instanzen.

II. `aws:waitForAwsResourceProperty`- Wartet darauf, dass AMI der Staat da ist. `available`

III. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-ExtendVolumesOnLinux` Runbook aus, um die Volumenänderung sowie die erforderlichen Schritte im Betriebssystem durchzuführen, um den neuen Speicherplatz verfügbar zu machen.

Ausgaben

diagnoseDiskUsageAlertOnWindows.Ausgang

extendVolumesOnWindows.Ausgabe

diagnoseDiskUsageAlertOnLinux.Ausgang

extendVolumesOnLinux.Ausgabe

Erstellen Sie ein Backup unter Linux. ImageId

Sichern Sie AMI/Windows. ImageId

## AWSSupport-TroubleshootEC2InstanceConnect

Beschreibung

`AWSSupport-TroubleshootEC2InstanceConnect` Die -Automatisierung hilft bei der Analyse und Erkennung von Fehlern, die die Verbindung zu einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance mithilfe von Amazon EC2 Instance Connect verhindern. Es identifiziert Probleme, die durch ein nicht unterstütztes Amazon Machine Image (AMI), fehlende Installation oder Konfiguration von Paketen auf Betriebssystemebene, fehlende AWS Identity and Access Management (IAM)-Berechtigungen oder Netzwerkkonfigurationsprobleme verursacht werden.

Wie funktioniert es?

Das Runbook verwendet die Amazon EC2-Instance-ID, den Benutzernamen, den Verbindungsmodus, das Quell-IP-CIDR, den SSH-Port und den Amazon-Ressourcennamen (ARN) für die IAM-Rolle oder den Benutzer, bei der/dem Probleme mit Amazon EC2 Instance Connect auftreten. Anschließend werden die Voraussetzungen für die Verbindung mit einer Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect überprüft:

- Die Instance wird ausgeführt und befindet sich in einem fehlerfreien Zustand.
- Die Instance befindet sich in einer -AWSRegion, die von Amazon EC2 Instance Connect unterstützt wird.
- Das AMI der Instance wird von Amazon EC2 Instance Connect unterstützt.
- Die Instance kann den Instance Metadata Service (IMDSv2) erreichen.
- Das Amazon EC2 Instance Connect-Paket ist ordnungsgemäß installiert und auf Betriebssystemebene konfiguriert.
- Die Netzwerkkonfiguration (Sicherheitsgruppen, Netzwerk-ACL und Routing-Tabellenregeln) ermöglicht die Verbindung mit der Instance über Amazon EC2 Instance Connect.
- Die IAM-Rolle oder der IAM-Benutzer, die/der zur Nutzung von Amazon EC2 Instance Connect verwendet wird, hat Zugriff auf Push-Schlüssel zur Amazon EC2-Instance.

**Important**

- Um das Instance-AMI, die IMDSv2-Erreichbarkeit und die Installation des Amazon EC2 Instance Connect-Pakets zu überprüfen, muss die Instance SSM-verwaltet sein. Andernfalls werden diese Schritte übersprungen. Weitere Informationen finden Sie unter Warum wird meine Amazon EC2-Instance nicht als verwalteter Knoten angezeigt.
- Die Netzwerkprüfung erkennt nur, ob Sicherheitsgruppen- und Netzwerk-ACL-Regeln den Datenverkehr blockieren, wenn SourceIpCIDR als Eingabeparameter bereitgestellt wird. Andernfalls werden nur SSH-bezogene Regeln angezeigt.
- Verbindungen, die Amazon EC2 Instance Connect Endpoint verwenden, werden in diesem Runbook nicht validiert.
- Bei privaten Verbindungen überprüft die Automatisierung nicht, ob der SSH-Client auf dem Quellcomputer installiert ist und ob er die private IP-Adresse der Instance erreichen kann.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`

- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie zur `AWSSupport-TroubleshootEC2InstanceConnect` in der -AWS Systems ManagerKonsole.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId (Erforderlich):

     Die ID der Amazon EC2-Ziel-Instance, mit der Sie über Amazon EC2 Instance Connect keine Verbindung herstellen konnten.
   - AutomationAssumeRole (Optional):

     Der ARN der IAM-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - Benutzername (erforderlich):

     Der Benutzername, der für die Verbindung mit der Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect verwendet wird. Es wird verwendet, um zu bewerten, ob IAM-Zugriff für diesen bestimmten Benutzer gewährt wird.
   - EC2InstanceConnectRoleOrUser (erforderlich):

     Der ARN der IAM-Rolle oder des IAM-Benutzers, die Amazon EC2 Instance Connect verwendet, um Schlüssel an die Instance zu übertragen.
   - SSHPort (optional):

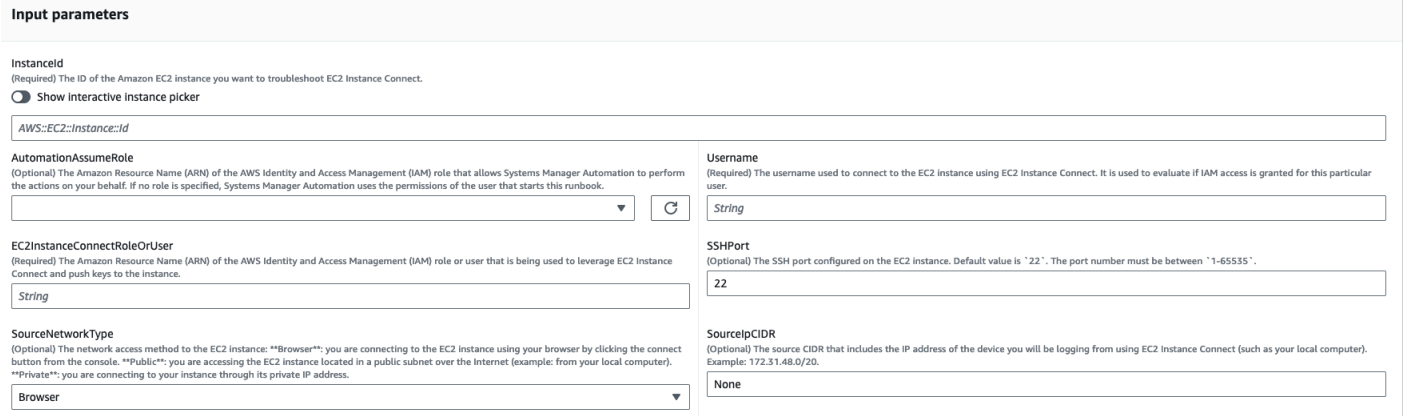
     Der auf der Amazon EC2 konfigurierte SSH-Port. Der Standardwert ist 22. Die Portnummer muss zwischen liegen`1-65535`.

- SourceNetworkType (Optional):

  Die Netzwerkzugriffsmethode für die Amazon EC2-Instance:

  - Browser: Sie stellen eine Verbindung über die -AWSManagementkonsole her.
  - Öffentlich: Sie stellen über das Internet eine Verbindung mit der Instance her, die sich in einem öffentlichen Subnetz befindet (z. B. auf Ihrem lokalen Computer).
  - Privat: Sie stellen eine Verbindung über die private IP-Adresse der Instance her.
- SourceIpCIDR (optional):

  Das Quell-CIDR, das die IP-Adresse des Geräts enthält (z. B. Ihren lokalen Computer), von dem Sie sich mit Amazon EC2 Instance Connect anmelden. Beispiel: 172.31.48.6/32. Wenn kein Wert mit dem öffentlichen oder privaten Zugriffsmodus bereitgestellt wird, bewertet das Runbook nicht, ob die Amazon EC2-Instance-Sicherheitsgruppe und Netzwerk-ACL-Regeln SSH-Datenverkehr zulassen. Stattdessen werden SSH-bezogene Regeln angezeigt.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - AssertInitialState:

     Stellt sicher, dass der Amazon EC2-Instance-Status ausgeführt wird. Andernfalls endet die Automatisierung.
   - GetInstanceProperties:

     Ruft die aktuellen Amazon EC2-Instance-Eigenschaften ab (PlatformDetails PublicIpAddress, VpcId SubnetId und MetadataHttpEndpoint).
   - GatherInstanceInformationFromSSM:

Ruft den Ping-Status der Systems Manager-Instance und die Betriebssystemdetails ab, wenn die Instance SSM-verwaltet ist.

- CheckIfAWSRegionSupported:

  Prüft, ob sich die Amazon EC2-Instance in einer von Amazon EC2 Instance Connect unterstützten AWS Region befindet.

- BranchOnIfAWSRegionSupported:

  Setzt die Ausführung fort, wenn die AWS Region von Amazon EC2 Instance Connect unterstützt wird. Andernfalls wird die Ausgabe erstellt und die Automatisierung wird beendet.

- CheckIfInstanceAMIIsSupported:

  Prüft, ob das mit der Instance verknüpfte AMI von Amazon EC2 Instance Connect unterstützt wird.

- BranchOnIfInstanceAMIIsSupported:

  Wenn das Instance-AMI unterstützt wird, führt es die Prüfungen auf Betriebssystemebene durch, z. B. die Erreichbarkeit von Metadaten und die Installation und Konfiguration des Amazon EC2 Instance Connect-Pakets. Andernfalls wird geprüft, ob HTTP-Metadaten über die AWS API aktiviert sind, und fährt dann mit dem Schritt Netzwerkprüfung fort.

- CheckIMDSReachabilityFromOs:

  Führt ein Bash-Skript auf der Amazon EC2-Linux-Ziel-Instance aus, um zu überprüfen, ob es die IMDSv2 erreichen kann.

- CheckEICPackageInstallation:

  Führt ein Bash-Skript auf der Amazon EC2 Linux-Ziel-Instance aus, um zu überprüfen, ob das Amazon EC2 Instance Connect-Paket ordnungsgemäß installiert und konfiguriert ist.

- CheckSSHConfigFromOs:

  Führt ein Bash-Skript auf der Amazon EC2 Linux-Ziel-Instance aus, um zu überprüfen, ob der konfigurierte SSH-Port mit dem Eingabeparameter „SSHPort.`

- CheckMetadataHTTPEndpointIsEnabled:

  Prüft, ob der HTTP-Endpunkt des Instance-Metadatenservice aktiviert ist.

- CheckEICNetworkAccess:

Prüft, ob die Netzwerkkonfiguration (Sicherheitsgruppen, Netzwerk-ACL und Routing-Tabellenregeln) eine Verbindung zur Instance über Amazon EC2 Instance Connect zulässt.

- CheckIAMRoleOrUserPermissions:

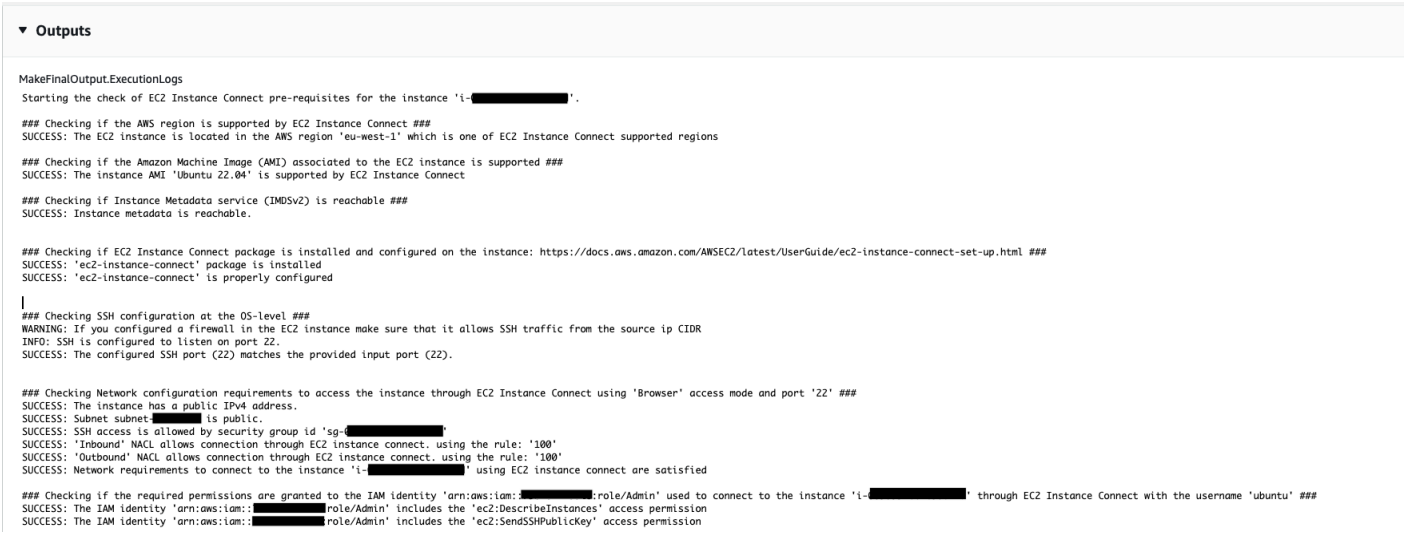
  Prüft, ob die IAM-Rolle oder der IAM-Benutzer, die/der zur Nutzung von Amazon EC2 Instance Connect verwendet wird, über den angegebenen Benutzernamen Zugriff auf Push-Schlüssel zur Amazon EC2-Instance hat.

- MakeFinalOutput:

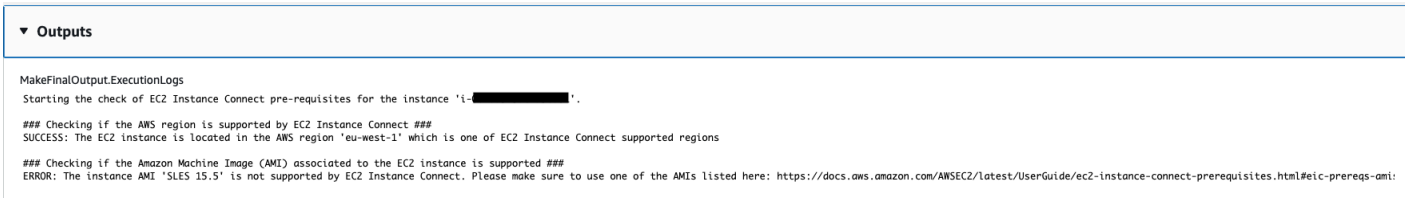
  Konsolidiert die Ausgabe aller vorherigen Schritte.

7. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten:

   Ausführung, bei der die Ziel-Instance alle erforderlichen Voraussetzungen erfüllt:




   Ausführung, bei der das AMI der Ziel-Instance nicht unterstützt wird:




## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

AWS -Servicedokumentation

- Wie behebe ich Probleme bei der Verbindung mit meiner Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect?

## AWSSupport-TroubleshootRDP

Beschreibung

Das `AWSSupport-TroubleshootRDP` Runbook ermöglicht es dem Benutzer, allgemeine Einstellungen auf der Zielinstanz zu überprüfen oder zu ändern, was sich auf RDP-Verbindungen (Remote Desktop Protocol) auswirken kann, wie den RDP-Port, Network Layer Authentication (NLA) und Windows-Firewall-Profile. Optional können Sie Änderungen offline anwenden, indem Sie die Instance anhalten und starten, wenn die Offline-Wiederherstellung von Benutzer ausdrücklich zugelassen wurde. Standardmäßig liest das Runbook die Werte der Einstellungen und gibt sie aus.

> **Important**
>
> Änderungen an den RDP-Einstellungen, dem RDP-Dienst und den Windows-Firewallprofilen sollten sorgfältig geprüft werden, bevor Sie dieses Runbook verwenden.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- Action

  Typ: Zeichenfolge

  Gültige Werte: CheckAll | FixAll | Benutzerdefiniert

  Standard: Custom

  Beschreibung: (Optional) [Benutzerdefiniert] Verwenden Sie die Werte von Firewall, RDPServiceStartupType, RDP ServiceActionPortAction, NLA SettingAction und RemoteConnections zur Verwaltung der Einstellungen. [CheckAll] Lesen Sie die Werte der Einstellungen, ohne sie zu ändern. [FixAll] Stellen Sie die RDP-Standardeinstellungen wieder her und deaktivieren Sie die Windows-Firewall.

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Fix only - Auf „True“ setzen, um eine Offline-RDP-Wiederherstellung zu erlauben, wenn die Online-Fehlerbehebung fehlschlägt, oder wenn die angegebene Instance keine verwaltete Instance ist. Hinweis: Für die Offline-Wiederherstellung hält SSM Automation die Instance an und erstellt ein AMI, bevor irgendwelche Operationen versucht werden.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Firewall

  Typ: Zeichenfolge

Gültige Werte: Prüfen | Deaktivieren

Standard: Check

Beschreibung: (Optional) Prüfen oder deaktivieren der Windows-Firewall (alle Profile).

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance, deren RDP-Einstellungen einer Fehlerbehebung unterzogen werden sollen.

- NLA SettingAction

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Deaktivieren

  Standard: Check

  Beschreibung: (Optional) Aktivieren oder Deaktivieren von Network Layer Authentication (NLA).

- RDP PortAction

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Ändern

  Standard: Check

  Beschreibung: (Optional) Prüfen des aktuell für RDP-Verbindungen verwendeten Ports oder Ändern des Ports zurück zu 3389 und Neustart des Service.

- RDP ServiceAction

  Typ: Zeichenfolge

  Gültige Werte: Check | Start | Restart | Force-Restart

  Standard: Check

  Beschreibung: (Optional) Überprüfen Sie den RDP-Dienst, starten Sie ihn neu oder erzwingen Sie einen Neustart (). TermService

- RDP ServiceStartupType

  Typ: Zeichenfolge

  Gültige Werte: Check | Auto

  Standard: Check

  Beschreibung: (Optional) Prüfen oder Einstellen des RDP-Service auf den automatischen Start beim Hochfahren von Windows.

- RemoteConnections

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren

  Standard: Check

  Beschreibung: (Optional) Eine Aktion zur Ausführung auf der Einstellung DenyTSConnections: Check, Aktivieren.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Nur Offline - Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline – Die Subnetz-ID für die EC2Rescue-Instance zum Ausführen der Offline-Fehlerbehebung. Wenn keine Subnetz-ID angegeben ist, erstellt AWS Systems Manager Automation eine neue VPC. WICHTIG: Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Für die Online-Problembehebung muss der Benutzer mindestens über ssm:DescribeInstanceInformation, ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instanz zu senden, sowie über ssm:, um die GetAutomationExecution Automatisierungsausgabe lesen zu können. Für die Offline-Korrektur muss der Benutzer mindestens über ssm:, ssm: DescribeInstanceInformation, ec2: StartAutomationExecution, plus ssm: verfügenDescribeInstances, um die Automatisierungsausgabe GetAutomationExecution lesen zu können. `AWSSupport-TroubleshootRDP`AufrufeAWS`Support-ExecuteEC2Rescue`, um die Offline-Korrektur durchzuführen. Bitte überprüfen Sie die Berechtigungen für, `AWSSupport-ExecuteEC2Rescue` um sicherzustellen, dass Sie die Automatisierung erfolgreich ausführen können.

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Prüfe, ob es sich bei der Instanz um eine Windows Server Instanz handelt
2. `aws:assertAwsResourceProperty`- Prüfen Sie, ob es sich bei der Instanz um eine verwaltete Instanz handelt
3. (Online-Fehlerbehebung) Wenn die Instance eine verwaltete Instance ist, dann:
   a. `aws:assertAwsResourceProperty`- Überprüfe den angegebenen Aktionswert
   b. (Online-Check) Wenn die Aktion = CheckAll, dann:

      `aws:runPowerShellScript`- Führt das PowerShell Skript aus, um den Status der Windows-Firewallprofile abzurufen.

      `aws:executeAutomation`- Ruft `AWSSupport-ManageWindowsService` auf, um den RDP-Dienststatus abzurufen.

      `aws:executeAutomation`- Ruft `AWSSupport-ManageRDPSettings` auf, um die RDP-Einstellungen abzurufen.
   c. (Online-Fix) Wenn die Aktion = FixAll, dann:

      `aws:runPowerShellScript`- Führt das PowerShell Skript aus, um alle Windows-Firewallprofile zu deaktivieren.

`aws:executeAutomation`- Ruft `AWSSupport-ManageWindowsService` auf, um den RDP-Dienst zu starten.

`aws:executeAutomation`- Ruft `AWSSupport-ManageRDPSettings` auf, um Remote-Verbindungen zu aktivieren und NLA zu deaktivieren.

d. (Online-Management) Wenn Action = Custom, dann:

`aws:runPowerShellScript`- Führt das PowerShell Skript zur Verwaltung der Windows-Firewallprofile aus.

`aws:executeAutomation`- Aufrufe `AWSSupport-ManageWindowsService` zur Verwaltung des RDP-Dienstes.

`aws:executeAutomation`- Aufrufe `AWSSupport-ManageRDPSettings` zur Verwaltung der RDP-Einstellungen.

4. (Offline-Wiederherstellung) Wenn die Instance keine verwaltete Instance ist:
   a. `aws:assertAwsResourceProperty`- Bestätigen AllowOffline= wahr
   b. `aws:assertAwsResourceProperty`- Aktion geltend machen = FixAll
   c. `aws:assertAwsResourceProperty`- Bestätigen Sie den Wert von SubnetId

      (Verwenden Sie das Subnetz der bereitgestellten Instanz) Wenn SubnetId SELECTED_INSTANCE_SUBNET

      `aws:executeAwsApi`- Ruft das Subnetz der aktuellen Instanz ab.

      `aws:executeAutomation`- `AWSSupport-ExecuteEC2Rescue` Mit dem Subnetz der bereitgestellten Instanz ausführen.
   d. (Verwenden Sie das angegebene benutzerdefinierte Subnetz) Wenn nicht SubnetId SELECTED_INSTANCE_SUBNET

      `aws:executeAutomation`- `AWSSupport-ExecuteEC2Rescue` Mit dem angegebenen SubnetId Wert ausführen.

Ausgaben

manageFirewallProfiles.Ausgang

ManagerDPServiceSettings. Ausgang

manageRDPSettings.Output

checkFirewallProfiles.Ausgang

Überprüfen Sie RDP. Output ServiceSettings

checkRDPSettings.Output

disableFirewallProfiles.Ausgang

Stellen Sie den standardmäßigen RDP wieder her. Output ServiceSettings

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

Problembehandlung bei RDPOfflineWithSubnetId. Output

## AWSSupport-TroubleshootSSH

Beschreibung

Das AWSSupport-TroubleshootSSH Runbook installiert das Amazon EC2Rescue-Tool für Linux und verwendet dann das EC2Rescue-Tool, um häufig auftretende Probleme zu überprüfen oder zu beheben, die eine Remote-Verbindung zum Linux-Computer über SSH verhindern. Optional können Sie Änderungen offline anwenden, indem Sie die Instance anhalten und starten, wenn die Offline-Wiederherstellung von Benutzer ausdrücklich zugelassen wurde. Standardmäßig arbeitet das Runbook im schreibgeschützten Modus.

Diese Automatisierung ausführen (Konsole)

Informationen zur Arbeit mit dem AWSSupport-TroubleshootSSH Runbook finden Sie in diesem Thema AWSSupport-TroubleshootSSH zur Fehlerbehebung vom AWS Premium Support.

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- Action

  Typ: Zeichenfolge

  Gültige Werte: CheckAll | FixAll

  Standard: CheckAll

  Beschreibung: (Erforderlich) Angabe, ob Probleme nur geprüft werden sollen, ohne sie zu beheben, oder ob nach der Prüfung alle erkannten Probleme automatisch behoben werden sollen.
- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Fix only - Auf „True“ setzen, um eine Offline-SSH-Wiederherstellung zu erlauben, wenn die Online-Fehlerbehebung fehlschlägt, oder wenn die angegebene Instance keine verwaltete Instance ist. Hinweis: Für die Offline-Wiederherstellung hält SSM Automation die Instance an und erstellt ein AMI, bevor irgendwelche Operationen versucht werden.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer EC2-Instance für Linux.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Nur Offline - Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline – Die Subnetz-ID für die EC2Rescue-Instance zum Ausführen der Offline-Fehlerbehebung. Wenn keine Subnetz-ID angegeben ist, erstellt AWS Systems Manager Automation eine neue VPC.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von ManagedInstanceCore Amazon verwaltete AmazonSSM-Richtlinie angehängt ist. Für die Online-Problembehebung muss der Benutzer mindestens über ssm:DescribeInstanceInformation, ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instanz zu senden, sowie über ssm:, um die GetAutomationExecution Automatisierungsausgabe lesen zu können. Für die Offline-Korrektur muss der Benutzer mindestens über ssm:, ssm: DescribeInstanceInformation, ec2: StartAutomationExecution, plus ssm: verfügenDescribeInstances, um die Automatisierungsausgabe GetAutomationExecution lesen zu können. `AWSSupport-TroubleshootSSH`AufrufeAWS`Support-ExecuteEC2Rescue`, um die Offline-Korrektur durchzuführen. Bitte überprüfen Sie die

Berechtigungen für, `AWSSupport-ExecuteEC2Rescue` um sicherzustellen, dass Sie die Automatisierung erfolgreich ausführen können.

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Prüfen Sie, ob es sich bei der Instanz um eine verwaltete Instanz handelt
   a. (Online-Wiederherstellung) Wenn die Instance verwaltete Instance ist:
      i. `aws:configurePackage`- Installieren Sie EC2Rescue für Linux über. `AWS-ConfigureAWSPackage`
      ii. `aws:runCommand`- Führen Sie das Bash-Skript aus, um EC2Rescue für Linux auszuführen.
   b. (Offline-Wiederherstellung) Wenn die Instance keine verwaltete Instance ist:
      i. `aws:assertAwsResourceProperty`- Bestätigen AllowOffline= wahr
      ii. `aws:assertAwsResourceProperty`- Aktion geltend machen = FixAll
      iii. `aws:assertAwsResourceProperty`- Bestätigen Sie den Wert von SubnetId
      iv. (Verwenden Sie das Subnetz der bereitgestellten Instanz) Wenn SubnetId SelectedInstanceSubnet wir `aws:executeAutomation` `AWSSupport-ExecuteEC2Rescue` mit dem Subnetz der bereitgestellten Instanz laufen sollen.
      v. (Verwenden Sie das angegebene benutzerdefinierte Subnetz) SubnetId Wird nicht für `aws:executeAutomation` die Ausführung `AWSSupport-ExecuteEC2Rescue` mit dem angegebenen SubnetId Wert SelectedInstanceSubnet verwendet.

Ausgaben

troubleshootSSH.Output

troubleshootSSHOffline.Output

Problembehebung SSHOfflineWithSubnetId. Output

## AWSSupport-TroubleshootSUSERegistration

Beschreibung

Das `AWSSupport-TroubleshootSUSERegistration` Runbook hilft Ihnen zu ermitteln, warum die Registrierung einer Amazon Elastic Compute Cloud (Amazon EC2) SUSE Linux Enterprise Server -Instance bei SUSE Update Infrastructure fehlgeschlagen ist. Die Automatisierungsausgabe

enthält Schritte zur Lösung des Problems oder hilft Ihnen bei der Behebung des Problems. Wenn die Instance während der Automatisierung alle Prüfungen besteht, wird sie bei SUSE Update Infrastructure registriert.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

-Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, die Sie beheben möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`

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

Dokumentschritte

- `aws:assertAwsResourceProperty`- Prüft, ob die Amazon EC2-Instance von AWS Systems Manager verwaltet wird.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance-Plattform vorhanden istSLES.
- `aws:runCommand`- Prüft, ob die `cloud-regionsrv-client` Paketversion größer oder gleich der erforderlichen Version 9.0.10 ist.
- `aws:runCommand`- Prüft, ob der symbolische Link für das Basisprodukt defekt ist, und repariert den Link, falls er defekt ist.
- `aws:runCommand`- Prüft, ob die Hosts-Datei (`/etc/hosts`) Datensätze für enthält`smt-ec2-suscloud.net`. Die Automatisierung entfernt alle doppelten Einträge.
- `aws:runCommand`- Prüft, ob der `curl` Befehl installiert ist.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance auf die Instance Metadata Service (IMDS) -Adresse 169.254.169.254 zugreifen kann.
- `aws:runCommand`- Prüft, ob die Amazon EC2-Instance über einen Rechnungscode oder AWS Marketplace Produktcode verfügt.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance mindestens einen regionalen Server über HTTPS erreichen kann.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance die Subscription Management Tool (SMT) -Server über HTTP erreichen kann.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance die Subscription Management Tool (SMT) -Server über HTTPS erreichen kann.
- `aws:runCommand`— Prüft, ob die Amazon EC2-Instance die `smt-ec2.susecloud.net` Adresse über HTTPS erreichen kann.
- `aws:runCommand`— Registriert die Amazon EC2-Instance bei SUSE Update Infrastructure.
- `aws:executeScript`- Erfasst die Ergebnisse aller vorherigen Schritte und gibt sie aus.

# AWSSupport-TroubleshootWindowsPerformance

Beschreibung

Das Runbook `AWSSupport-TroubleshootWindowsPerformance` hilft bei der Behebung laufender Leistungsprobleme auf der Windows-Instance Amazon Elastic Compute Cloud (Amazon EC2). Das Runbook erfasst Protokolle von der Ziel-Instance und analysiert CPU-, Arbeitsspeicher-, Festplatten- und Netzwerkleistungskennzahlen. Optional kann die Automatisierung einen Prozess-Dump erfassen, mit dessen Hilfe Sie die mögliche Ursache für Leistungseinbußen ermitteln können. Bei der Automatisierung werden auch die Ereignis- und Systemprotokolle mithilfe des neuesten `EC2Rescue`Tools erfasst, sofern Sie die Installation durch dieses Runbook zulassen.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Überprüft die Amazon EC2 EC2-Instance auf Voraussetzungen.
- Generiert Leistungsprotokolle auf der Root-Festplatte der Amazon EC2 EC2-Windows-Instance
- Speichert die erfassten Protokolle in einem Ordner `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Wenn ein Amazon Simple Storage Service (Amazon S3) -Bucket bereitgestellt wird und die Automation-Annahme-Rolle über die erforderlichen Berechtigungen verfügt, werden die erfassten Protokolle in den Amazon S3 S3-Bucket hochgeladen.
- Installiert das neueste `EC2Rescue` Tool auf der Amazon EC2 EC2-Windows-Instance, um Ereignisse und Systemprotokolle zu erfassen, falls Sie es installieren möchten. Es analysiert jedoch nicht den Prozess-Dump und die von erfassten Protokolle. `EC2Rescue`

> **Important**
>
> - Um dieses Runbook auszuführen, muss die Amazon EC2 EC2-Windows-Instance von verwaltet werden. AWS Systems Manager Weitere Informationen finden Sie unter Warum wird meine Amazon EC2 EC2-Instance nicht als verwalteter Knoten angezeigt?
> - Um dieses Runbook auszuführen, muss die Amazon EC2 EC2-Windows-Instance auf den Versionen Windows 8.1/Windows Server 2012 R2 (6.3) oder neuer mit PowerShell 4.0 oder höher ausgeführt werden. Weitere Informationen finden Sie unter Windows-Betriebssystemversion.

- Für die Generierung von Leistungsprotokollen sind mindestens 10 GB freier Speicherplatz auf dem Root-Gerät erforderlich. Wenn die Stammfestplatte größer als 100 GB ist, muss der freie Speicherplatz mehr als 10% der Festplattengröße betragen. Wenn Sie einen Prozess während der Ausführung sichern, muss der freie Speicherplatz größer als 10 GB sein, zuzüglich der gesamten Speichergröße, die der Prozess beansprucht, wenn der Prozess mehr als 10 GB Speicher verbraucht.
- Die auf dem Root-Gerät generierten Protokolle werden nicht automatisch gelöscht.
- Das Runbook deinstalliert das `EC2Rescue` Tool nicht. Weitere Informationen finden Sie unter Verwenden `EC2Rescue` für Windows Server.
- Es hat sich bewährt, diese Automatisierung bei Leistungseinbußen auszuführen. Sie können sie auch regelmäßig mithilfe einer AWS Systems Manager State Manager-Zuordnung oder durch die Planung von AWS Systems Manager Wartungsfenstern ausführen.

## Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

(Optional) Die dem Instance-Profil zugeordnete IAM-Rolle oder der auf der Instance konfigurierte IAM-Benutzer erfordert die folgenden Aktionen, um Logs in den für den Parameter angegebenen Amazon S3 S3-Bucket hochzuladen: *LogUploadBucketName*

- s3:PutObject
- s3:GetObject
- s3:ListBucket

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootWindowsPerformanceim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - InstanceId (Erforderlich):

Die ID der Amazon EC2 EC2-Windows-Zielinstanz, auf der Sie die Automatisierung ausführen möchten. Die Instanz muss von Systems Manager verwaltet werden, um die Automatisierung ausführen zu können.

- CaptureProcessDump (Optional):

  Der Typ des zu erfassenden Prozess-Dumps. Die Automatisierung kann einen Prozess-Dump für den Prozess erfassen, der zu Beginn der Automatisierung möglicherweise die Leistung beeinträchtigt. Das Instance-Root-Volume benötigt mindestens 10 GB freien Speicherplatz (mehr als 10% der Festplattengröße, wenn das Root-Volume größer als 100 GB ist, und 10 GB zuzüglich der gesamten vom Prozess verbrauchten Speichergröße, wenn der Prozess mehr als 10 GB Speicher verbraucht).

- LogCaptureDuration (Optional):

  Die Anzahl der Minuten zwischen `1` und`15`, für die diese Automatisierung Protokolle erfasst, solange das Problem noch besteht. Der Standardwert ist `5`.

- LogUploadBucketName (Fakultativ):

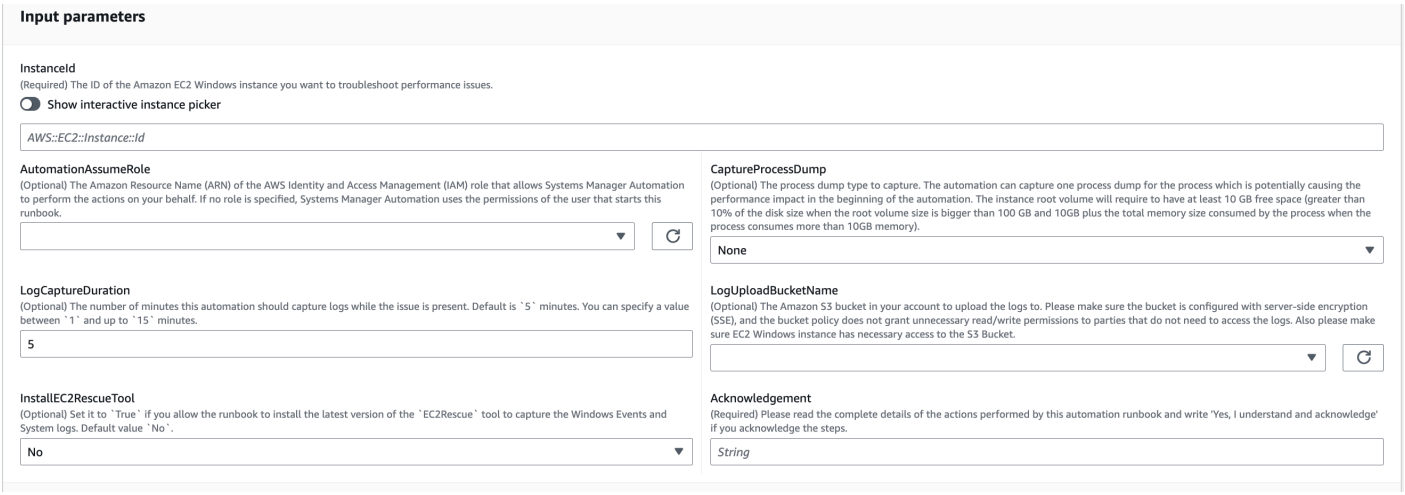
  Der Amazon S3 S3-Bucket in Ihrem Konto, in den Sie die Protokolle hochladen möchten. Der Bucket muss mit serverseitiger Verschlüsselung (SSE) konfiguriert sein, und die Bucket-Richtlinie darf Parteien, die keinen Zugriff auf die erfassten Protokolle benötigen, keine unnötigen Lese-/Schreibberechtigungen gewähren. Die Amazon EC2 EC2-Windows-Instance muss Zugriff auf den Amazon S3 S3-Bucket haben.

- Installieren Sie EC2 RescueTool (optional):

  Wird `Yes` auf gesetzt, damit das Runbook die neueste Version des `EC2Rescue` Tools zum Erfassen der Windows-Ereignisse und -Systemprotokolle installieren kann. Der Standardwert ist `No`.

- Bestätigung (erforderlich):

  Lesen Sie die vollständigen Details der Aktionen, die von diesem Automatisierungs-Runbook ausgeführt wurden, und geben Sie Folgendes ein, wenn Sie damit einverstanden sind. `Yes, I understand and acknowledge`




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - **`CheckConcurrency:`**

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die Instanz abzielt. Wenn das Runbook eine weitere Ausführung findet, die auf dieselbe Instance abzielt, gibt es einen Fehler zurück und wird beendet.
   - **`AssertInstanceIsWindows:`**

     Bestätigt, dass die Amazon EC2 EC2-Instance unter einem Windows-Betriebssystem läuft. Andernfalls endet die Automatisierung.
   - **`AssertInstanceIsManagedInstance:`**

     Bestätigt, dass die Amazon EC2 EC2-Instance von verwaltet wird. AWS Systems Manager Andernfalls endet die Automatisierung.
   - **`VerifyPrerequisites:`**

     Überprüft die PowerShell Version auf dem Instanz-Betriebssystem und stellt sicher, dass die Instanz über Systems Manager verbunden werden kann, um PowerShell Befehle auszuführen. Diese Automatisierung unterstützt PowerShell 4.0 und höher, die auf den Versionen Windows 8.1/Server 2012 R2 (6.3) oder neuer ausgeführt werden. Wenn die Version älter ist, schlägt die Automatisierung fehl. Wenn Sie sich dafür entscheiden, Protokolle in den Amazon S3 S3-Bucket hochzuladen, überprüft diese Automatisierung, ob das PowerShell Modul AWS Tools for verfügbar ist. Wenn nicht, endet die Automatisierung.
   - **`BranchOnProcessDump:`**

Verzweigt, je nachdem, ob Sie es so eingestellt haben, dass es den Dump von Prozessen erfasst, die sich auf die Leistung ausgewirkt haben.

- **`CaptureProcessDump:`**

  Prüft, ob die Instanz über genügend Speicherplatz verfügt, um diese Automatisierung auszuführen (wenn Sie „Höchste CPU/Arbeitsspeicher“ wählen).

- **`CapturePerformanceLogs:`**

  Überprüft erneut den Festplattenspeicher und führt das PowerShell Skript auf der Instanz aus, um Leistungsindikatoren zu erstellen und die Protokollierung von Systemmonitor und Windows Performance Recorder zu starten. Das Skript wird beendet, wenn der angegebene Wert erreicht `LogCaptureDuration` ist.

- **`SummarizePerformanceLogs:`**

  Fasst den im vorherigen Schritt generierten XML-Bericht zusammen`CapturePerformanceLogs`, um den verantwortlichen Prozess zu finden, der am meisten WorkingSet 64 (Arbeitsspeicher) und% Prozessorzeit (CPU) verbraucht und in der Ausgabe der Automatisierung angezeigt wird. Es generiert ähnliche Informationen für die Verwendung von LogicalDisk Netzwerkschnittstelle, Speicher, TCPv4, IPv4 und UDPv4 und speichert sie im Ausgabeordner. `analysis_output.log`

- **`BranchOnInstallEC2Rescue:`**

  Verzweigt, wenn Sie es so einstellen, dass das neueste `EC2Rescue` Tool in der Amazon EC2 EC2-Instance installiert wird.

- **`InstallEC2RescueTool:`**

  Installiert das `EC2Rescue` Tool im Instance-Betriebssystem zur Erfassung von `EC2Rescue` Protokollen mithilfe von`AWS-ConfigureAWSPackage`.

- **`RunEC2RescueTool:`**

  Führt das `EC2Rescue` Tool im Betriebssystem der Instanz aus, um alle benötigten Protokolle zu erfassen. `EC2Rescue`erfasst nur die erforderlichen Protokolle, um Speicherplatz zu sparen.

- **`BranchOnIfS3BucketProvided:`**

  Verzweigt auf der Grundlage von Benutzereingaben von`LogUploadBucketName`, um festzustellen, ob ein Bucket-Name zum Hochladen von Logs verfügbar ist.

- **`GetS3BucketPublicStatus:`**

  Ermittelt, ob ein Amazon S3 S3-Bucket bereitgestellt wird, und wenn ja, bestätigt es, dass der Amazon S3 S3-Bucket nicht öffentlich und mit SSE konfiguriert ist.

- **`UploadLogResult:`**

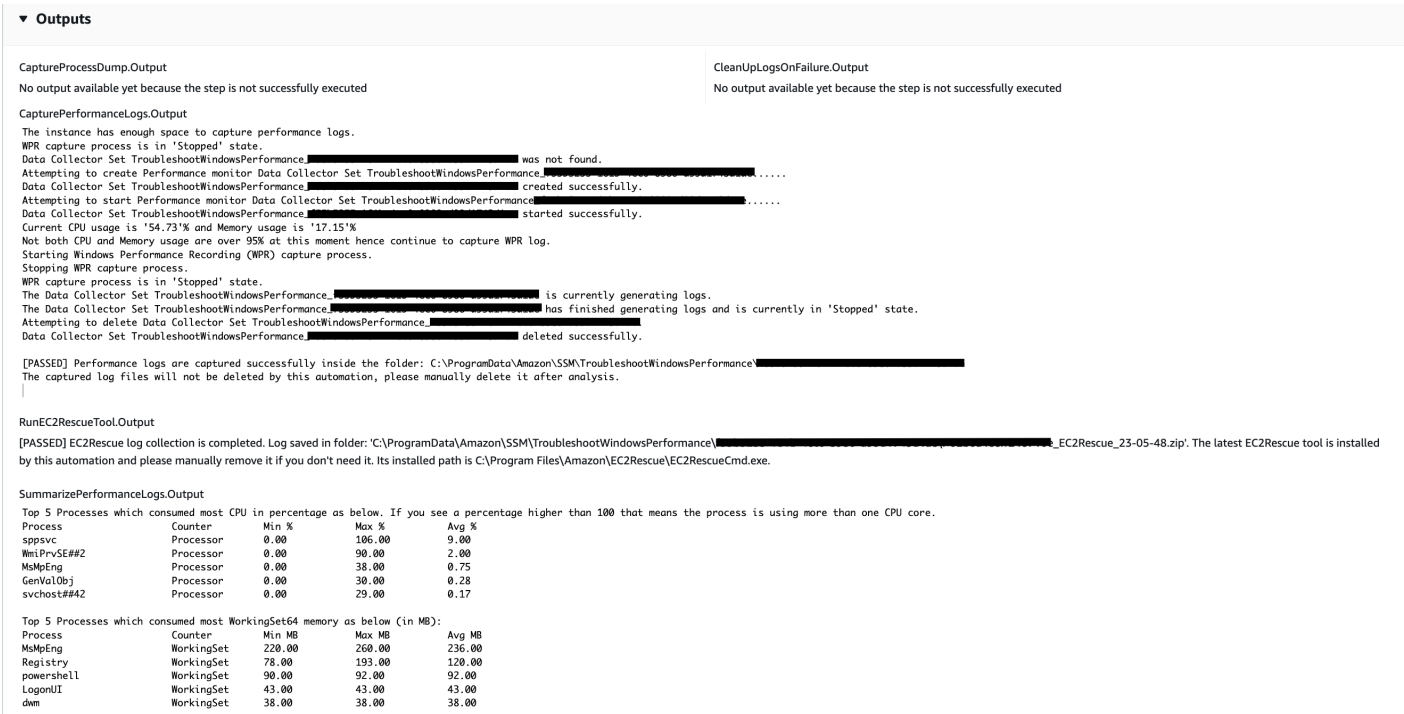
  Lädt die Protokolle in den bereitgestellten Amazon S3 S3-Bucket hoch. Wenn die PowerShell Version 5.0 oder höher ist, werden die Protokolle in ein ZIP-Archiv komprimiert und hochgeladen. Die ZIP-Datei wird nach Abschluss des Uploads gelöscht. Wenn die PowerShell Version unter 5.0 liegt, werden die Dateien direkt in einen Ordner hochgeladen.

- **`CleanUpLogsOnFailure:`**

  Löscht alle durch den `CapturePerformanceLogs` Schritt generierten Protokolle, wenn er fehlschlägt. Der `CleanUpLogsOnFailure` Schritt schlägt möglicherweise fehl oder es kommt zu einem Timeout, wenn der SSM-Agent nicht ordnungsgemäß funktioniert oder das Windows-System nicht reagiert.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   Ausführung, bei der die Zielinstanz alle erforderlichen Voraussetzungen erfüllt.



**Outputs**

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

```
The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance_[redacted] was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance_[redacted].....
Data Collector Set TroubleshootWindowsPerformance_[redacted] created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance[redacted].....
Data Collector Set TroubleshootWindowsPerformance_[redacted] started successfully.
Current CPU usage is '54.73'% and Memory usage is '17.15'%
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.
Starting Windows Performance Recording (WPR) capture process.
Stopping WPR capture process.
WPR capture process is in 'Stopped' state.
The Data Collector Set TroubleshootWindowsPerformance_[redacted] is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance_[redacted] has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance_[redacted]
Data Collector Set TroubleshootWindowsPerformance_[redacted] deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]
The captured log files will not be deleted by this automation, please manually delete it after analysis.
```

RunEC2RescueTool.Output

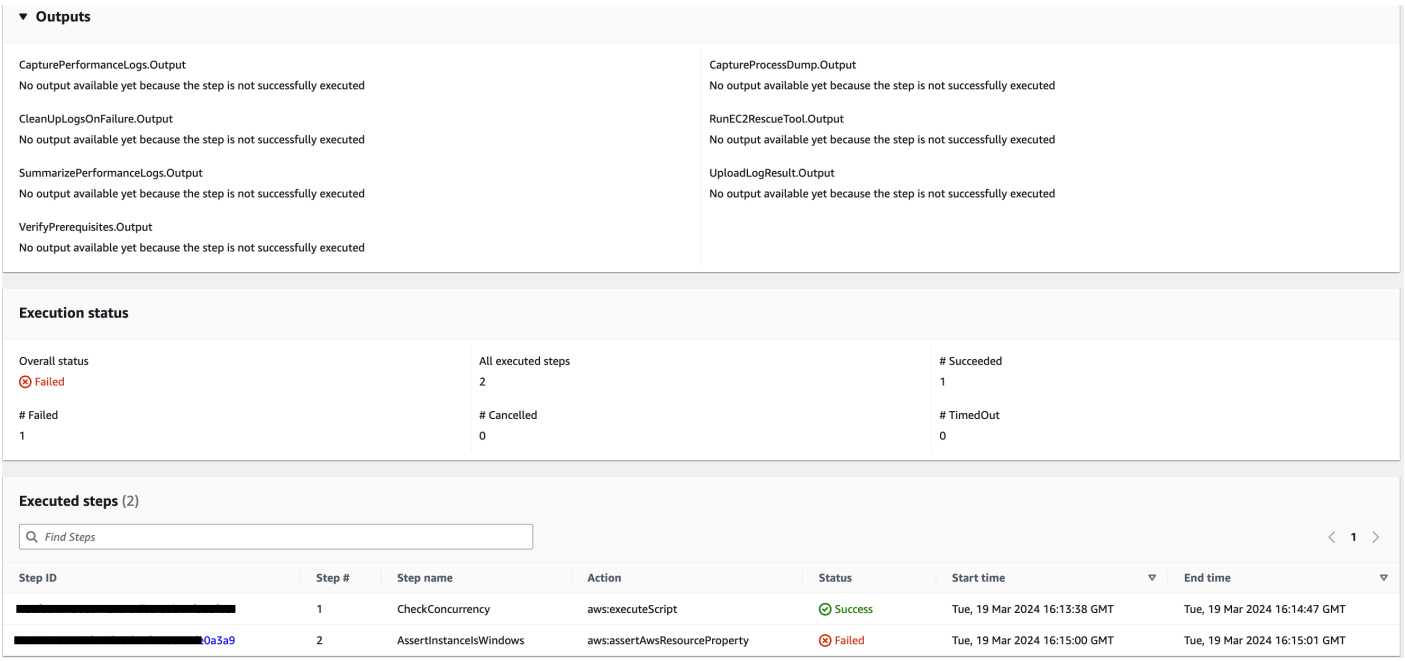
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]_EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

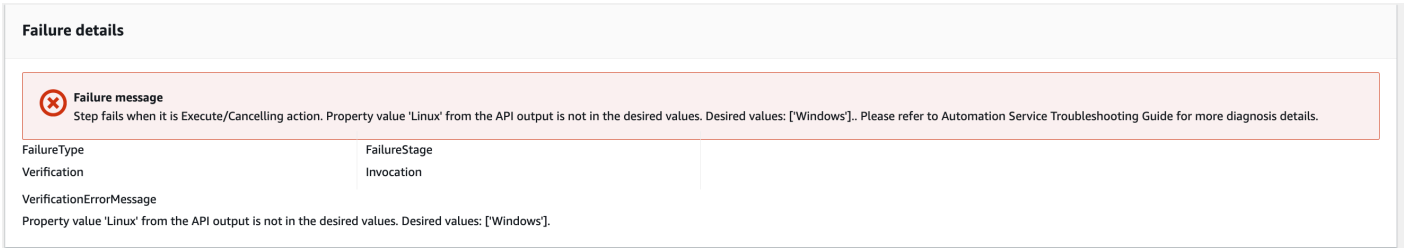
```
Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.
Process                 Counter         Min %           Max %           Avg %
sppsvc                  Processor       0.00            106.00          9.00
WmiPrvSE##2             Processor       0.00            90.00           2.00
MsMpEng                 Processor       0.00            38.00           0.75
GenValObj               Processor       0.00            30.00           0.28
svchost##42             Processor       0.00            29.00           0.17

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

Ausführung, bei der sich die Zielinstanz auf der Linux-Plattform befindet und die Ausführung fehlgeschlagen ist. Sie würden die Schritt-ID auswählen, um die Fehlerdetails zu sehen.




Die Fehlerdetails des Schritts`AssertInstanceIsWindows`.




## Referenzen

### Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

# `AWSSupport-TroubleshootWindowsUpdate`

## Beschreibung

Das `AWSSupport-TroubleshootWindowsUpdate` Runbook wird verwendet, um Probleme zu identifizieren, bei denen die Windows-Updates für Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instances fehlschlagen könnten.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Prüft, ob die Amazon EC2 EC2-Zielinstanz von AWS Systems Manager verwaltet wird.
- Überprüft, ob die Versionen AWS Systems Manager Agent (SSM Agent) und Windows Server für Systems Manager Manager-Patchvorgänge unterstützt werden.
- Prüft den für Windows-Updates empfohlenen verfügbaren Festplattenspeicher und ob ein Neustart aussteht. Ein ausstehender Neustart weist normalerweise darauf hin, dass Updates ausstehen, und ein Neustart ist erforderlich, bevor weitere Updates durchgeführt werden.
- Konfiguriert die Proxyeinstellungen auf Betriebssystemebene, was bei der Behebung von Verbindungsproblemen helfen kann.
- Führt einen Endpunkt-Konnektivitätstest von Amazon Simple Storage Service (Amazon S3) durch und ruft den `GetDeployablePatchSnapshotForInstance`API-Vorgang auf, um den aktuellen Snapshot für die Patch-Baseline abzurufen, die der verwaltete Knoten verwendet.
- Wenn die Verbindung fehlschlägt, bietet es die Möglichkeit, das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook auszuführen, um die Konnektivität der Instance mit Amazon S3 S3-Endpunkten zu analysieren.
- Validiert die Windows-Update-Konfiguration und testet Windows Server Update Services (WSUS) (falls zutreffend).

> **Important**
>
> - Active Directory-Domänencontroller werden nicht unterstützt.
> - Windows Server Version 2008 R2 oder frühere Versionen werden nicht unterstützt.
> - SSM Agent 1.2.371 oder frühere Versionen werden nicht unterstützt.
> - Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook wird verwendet `VPC Reachability Analyzer`, um die Netzwerkkonnektivität zwischen einer Quelle und einem Dienstendpunkt zu analysieren. Ihnen wird pro Analyselauf zwischen einer Quelle und einem Ziel berechnet. Weitere Informationen finden Sie unter Amazon VPC-Preise.

- Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook ist nicht in allen Regionen verfügbar, in denen Systems Manager unterstützt wird.

## Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Um das untergeordnete Runbook auszuführen`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, fügen Sie die in diesem Dokument aufgeführten Berechtigungen hinzu.

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

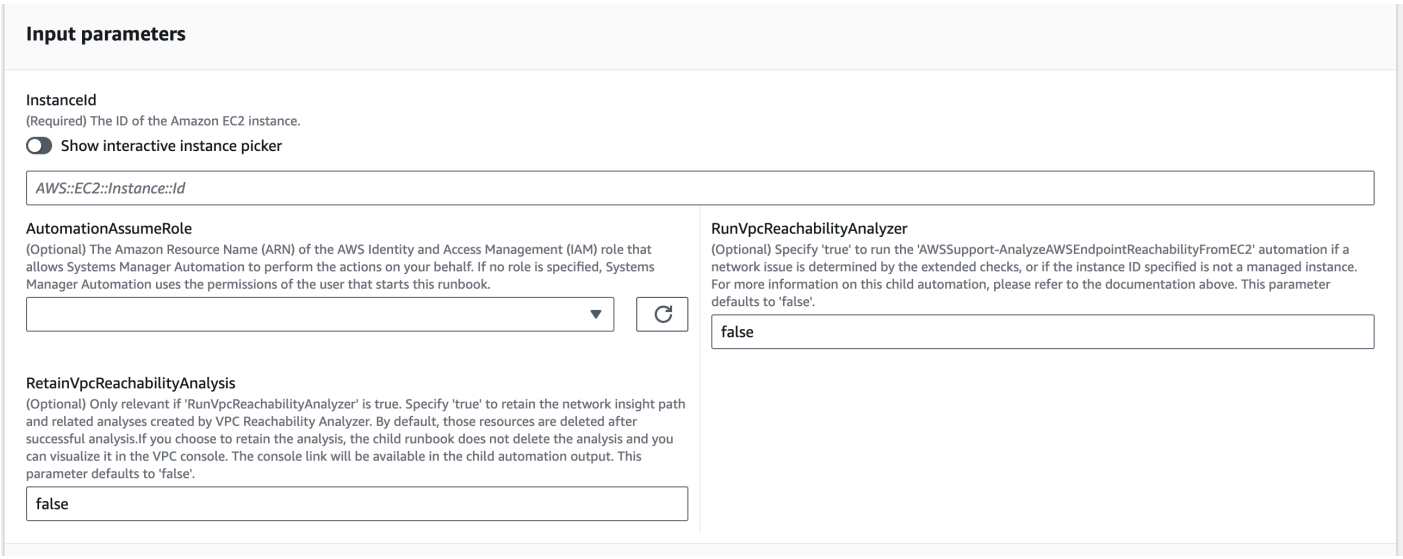
1. Navigieren Sie `AWSSupport-TroubleshootWindowsUpdate`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - InstanceId (Erforderlich):

     Geben Sie die ID der Amazon EC2 EC2-Instance ein, bei der das Windows-Update fehlgeschlagen ist.
   - RunVpcReachabilityAnalyzer(Optional):

     Geben Sie `true` an, ob die `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Automatisierung ausgeführt werden soll, wenn durch die erweiterten Prüfungen ein Netzwerkproblem festgestellt wurde oder wenn es sich bei der angegebenen Instanz-ID nicht um eine verwaltete Instanz handelt. Weitere Informationen zu dieser untergeordneten Automatisierung finden Sie in der Dokumentation. Der Standardwert ist `false`.
   - RetainVpcReachabilityAnalysis(Fakultativ):

     Nur relevant, wenn `RunVpcReachabilityAnalyzer` es ist`true`. Geben Sie `true` an, ob der Netzwerkerkenntpfad und die zugehörigen Analysen, die von erstellt wurden, beibehalten werden sollen`Reachability Analyzer`. Standardmäßig werden diese Ressourcen nach erfolgreicher Analyse gelöscht. Wenn Sie sich dafür entscheiden, die Analyse beizubehalten, löscht das untergeordnete Runbook die Analyse nicht und Sie können sie in der Amazon VPC-Konsole visualisieren. Der Konsolenlink wird in der Ausgabe der untergeordneten Automatisierung verfügbar sein. Der Standardwert`false`.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - **`getWindowsServerAndSSMAgentVersion:`**

     Überprüft, ob die Zielinstanz von der SSM-Agent-Version AWS Systems Manager und der Windows-Version verwaltet wird, und ruft Details dazu ab.
   - **`assertifInstanceIsSsmManaged:`**

     Stellt sicher, dass die Amazon EC2 EC2-Instance von AWS Systems Manager (SSM) verwaltet wird, andernfalls endet die Automatisierung.
   - **`CheckProxy:`**

     Sucht nach allen Proxytypen für die Windows-Instance.
   - **`CheckPrerequisites:`**

     Ruft die SSM-Agent-Version und die Windows-Version ab und ermittelt, ob es sich um einen Active Directory-Domänencontroller (DC) handelt. Wenn es sich bei der Instanz um einen DC handelt oder der SSM-Agent oder die Windows-Version nicht unterstützt wird, wird das Runbook beendet.
   - **`CheckDiskSpace:`**

     Ruft den verfügbaren Festplattenspeicher auf der Windows-Instanz ab und überprüft ihn, wenn er für die Durchführung des Windows-Updates ausreicht.

- **CheckPendingReboot:**

  Sucht nach ausstehenden Neustarts über die Windows-Instanz.

- **CheckS3Connectivity:**

  Prüft, ob die Instance die Amazon S3 S3-Endpunkte für `Patchbaseline` erreichen kann.

- **branchOnRunVpcReachabilityAnalyzer:**

  Wenn dies zutrifft, `RunVpcReachabilityAnalyzer` wird die Automatisierung verzweigt, um tiefere Analysen für das Debuggen der Amazon S3 S3-Konnektivität durchzuführen.

- **GenerateEndpoints:**

  Generiert einen Endpunkt für eine erweiterte Konnektivitätsprüfung für den Amazon S3 S3-Endpunkt.

- **analyzeAwsEndpointReachabilityFromEC2:**

  Ruft das Automatisierungs-Runbook,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. auf, um die Erreichbarkeit der ausgewählten Instance für die erforderlichen Endpunkte zu überprüfen.

- **CheckWindowsUpdateServices:**

  Überprüft den Status und den Starttyp des Windows Update-Dienstes.

- **CheckWindowsUpdateSettings:**

  Sucht nach Windows Update-Richtlinien, die über die Windows-Instanz konfiguriert wurden.

- **CheckWSUSSettings:**

  Überprüft, ob das Windows-Update mit WSUS oder Microsoft Update Catalog konfiguriert ist, und überprüft die Konnektivität.

- **CheckWUGlobalSettings:**

  Überprüft die globalen Windows Update-Einstellungen, die über die Windows-Instanz konfiguriert wurden.

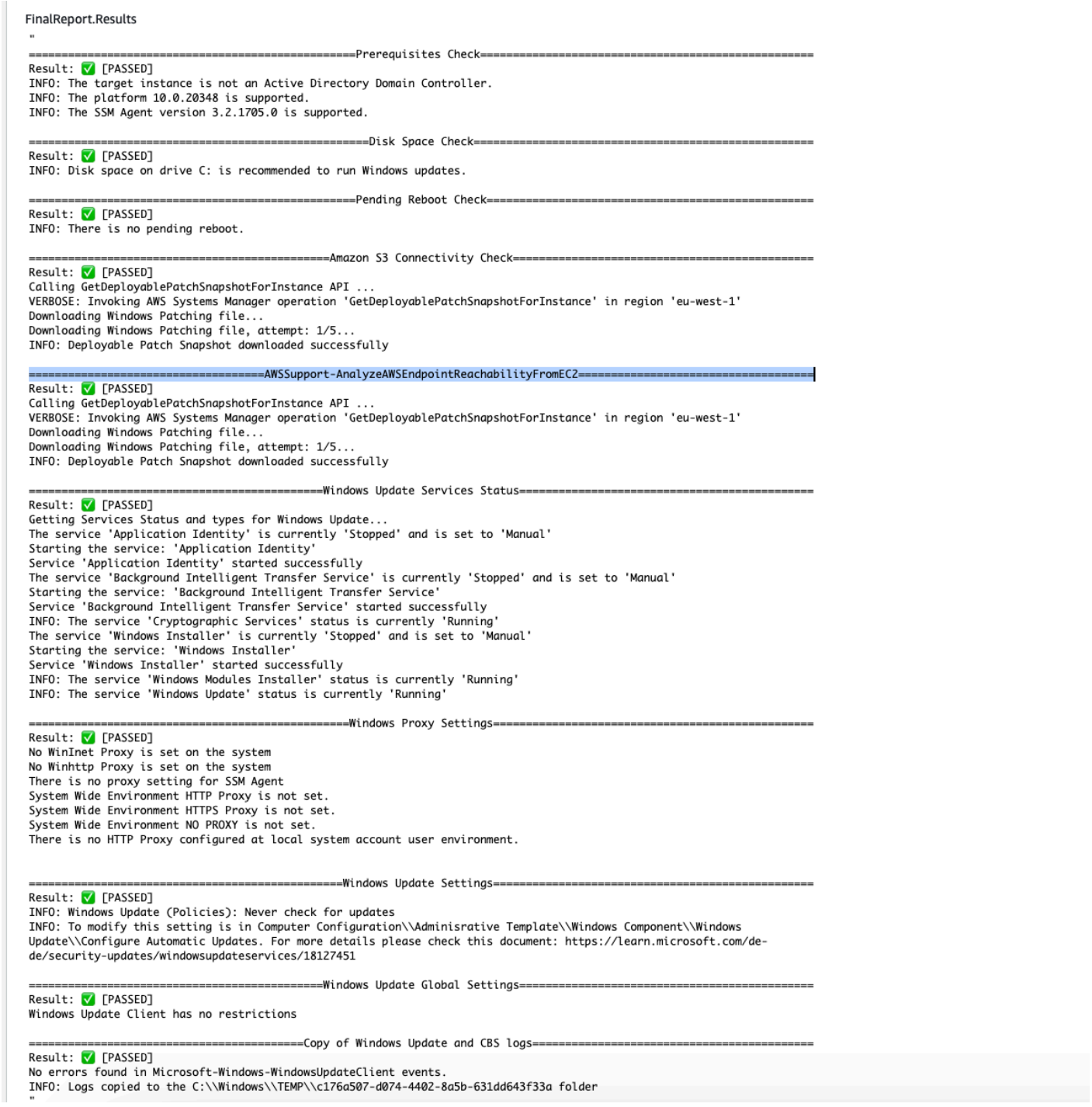
- **GenerateLogs:**

  Lädt Windows Update-Protokolle und CBS-Protokolle auf den Instanz-Desktop herunter und überprüft die Windows-Ereignisprotokolle auf Fehler.

- **`FinalReport:`**

  Generiert einen vollständigen Bericht über alle Schritte.

7. Wenn Sie fertig sind, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:



```
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
"
```

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

Dokumentation zum AWS Service

- Weitere Informationen finden Sie im Artikel TroubleShoot Windows Update.

## AWSSupport-UpgradeWindowsAWSDrivers

Beschreibung

Das `AWSSupport-UpgradeWindowsAWSDrivers` Runbook aktualisiert oder repariert Speicher- und AWS Netzwerktreiber auf der angegebenen EC2-Instance. Das Runbook versucht, die neuesten Treiberversionen AWS online zu installieren, indem es den SSM-Agent aufruft. Wenn SSM Agent nicht erreichbar ist, kann das Runbook eine Offline-Installation der AWS Treiber durchführen, wenn dies explizit angefordert wird.

> **Note**
>
> Sowohl das Online- als auch das Offline-Upgrade erstellen ein AMI, bevor sie versuchen, Vorgänge durchzuführen, die nach Abschluss der Automatisierung bestehen bleiben. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen. Die Online-Methode startet die Instance als Teil des Upgrade-Prozesses neu, während die Offline-Methode erfordert, dass die bereitgestellte EC2-Instance angehalten und dann gestartet wird.

> **Important**
>
> Wenn Ihre Instances AWS Systems Manager über VPC-Endpunkte eine Verbindung zu herstellen, schlägt dieses Runbook fehl, es sei denn, es wird in der Region us-east-1 verwendet. Dieses Runbook schlägt auch auf einem Domain-Controller fehl. Informationen

dazu, wie Sie AWS-PV-Treiber auf einem Domain-Controller aktualisieren, finden Sie unter Upgrade für einen Domain-Controller (AWS PV-Upgrade).

## Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Auf „true“ setzen, um eine Offline-Treiberaktualisierung zuzulassen, wenn die Online-Installation nicht durchgeführt werden kann. Hinweis: Die Offline-Methode erfordert, die bereitgestellte EC2-Instance anzuhalten und dann neu zu starten. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ForceUpgrade

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Nur Offline - Auf „true“ setzen, um zuzulassen, dass die Offline-Aktualisierung der Treiber fortgesetzt wird, auch wenn auf Ihrer Instance bereits die neuesten Treiber installiert sind.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer EC2-Instance für Windows Server.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline – Die Subnetz-ID für die EC2Rescue-Instance zum Ausführen der Offline-Treiberaktualisierung. Wenn keine Subnetz-ID angegeben ist, erstellt Systems Manager Automation eine neue VPC.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone wie befinden InstanceIdund den Zugriff auf die SSM-Endpunkte erlauben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die EC2-Instance, die den Befehl empfängt, muss mindestens über eine IAM-Rolle verfügen, die Berechtigungen für ssm:StartAutomationExecution und ssm:SendCommand enthält, um die Automatisierung auszuführen und den Befehl an die Instance zu senden, plus

ssm:GetAutomationExecution , um die Automatisierungsausgabe lesen zu können. Sie können die von `AmazonSSMManagedInstanceCore` Amazon verwaltete Richtlinie an Ihre IAM-Rolle anhängen, um diese Berechtigungen bereitzustellen. Wir empfehlen jedoch, die Automation-IAM-Rolle `AmazonSSMAutomationRole` zu diesem Zweck zu verwenden. Weitere Informationen finden Sie unter Verwenden von IAM zum Konfigurieren von Rollen für Automation.

Wenn Sie ein Offline-Upgrade durchführen, vgl. die für `AWSSupport-StartEC2RescueWorkflow` erforderlichen Berechtigungen.

Dokumentschritte

1. `aws:assertAwsResourceProperty` – Prüft, ob die Eingabe-Instance Windows ist.
2. `aws:assertAwsResourceProperty` – Prüft, ob die Eingabe-Instance eine verwaltete Instance ist. Wenn dies der Fall ist, beginnt das Online-Upgrade, oder das Offline-Upgrade wird evaluiert.
   a. (Online-Upgrade) Wenn die Input-Instance eine verwaltete Instance ist:
      i. `aws:createImage` – Erstellt ein AMI-Backup.
      ii. `aws:createTags` – Kennzeichnet das AMI-Backup.
      iii. `aws:runCommand` – Installiert den ENA-Netzwerktreiber über `AWS-ConfigureAWSPackage`.
      iv. `aws:runCommand` – Installiert den NVMe-Treiber über `AWS-ConfigureAWSPackage`.
      v. `aws:runCommand` – Installiert den AWS PV-Treiber über `AWS-ConfigureAWSPackage`.
   b. (Offline-Upgrade) Wenn die Input-Instance keine verwaltete Instance ist:
      i. `aws:assertAwsResourceProperty` – Prüft, ob das AllowOffline Flag auf gesetzt ist`true`. In diesem Fall wird das Offline-Upgrade gestartet, andernfalls endet die Automatisierung.
      ii. `aws:changeInstanceState` – Stoppen Sie die Quell-Instance.
      iii. `aws:changeInstanceState` – Stoppen der Quell-Instance erzwingen.
      iv. `aws:createImage` – Erstellen Sie ein AMI-Backup der Quell-Instance.
      v. `aws:createTags` – Markieren Sie das AMI-Backup der Quell-Instance.
      vi. `aws:executeAwsApi` – ENA für die Instance aktivieren
      vii. `aws:assertAwsResourceProperty` – Bestätigen Sie das -ForceUpgrade Flag.
      viii. Offline-Upgrade erzwingen) Wenn ForceUpgrade = „true“ ist, führen Sie aus`aws:executeAutomation`, um `AWSSupport-StartEC2RescueWorkflow` mit dem Treiber-Upgrade-Skript „erzwingen“ aufzurufen. Dadurch werden Treiber unabhängig von der aktuellen Version installiert.

ix. (Offline-Upgrade) Wenn ForceUpgrade = false, führen Sie aus`aws:executeAutomation`, um `AWSSupport-StartEC2RescueWorkflow` mit dem Treiber-Upgrade-Skript aufzurufen.

Ausgaben

preUpgradeBackup.ImageId

preOfflineUpgradeBackup.ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Ausgabe

forceUpgradeDriversOffline.Ausgabe

# Amazon ECS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Container Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

## `AWSSupport-CollectECSInstanceLogs`

Beschreibung

Das `AWSSupport-CollectECSInstanceLogs` Runbook sammelt Protokolldateien im Zusammenhang mit dem Betriebssystem und dem Amazon Elastic Container Service (Amazon ECS) von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um Sie bei der Behebung häufiger Amazon ECS-Probleme zu unterstützen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen am Dateisystem vorgenommen. Zu diesen Änderungen gehören die Erstellung temporärer Verzeichnisse und eines Protokollverzeichnisses, das Kopieren von Protokolldateien in diese Verzeichnisse und das Komprimieren der Protokolldateien in ein Archiv.

Wenn Sie einen Wert für den `LogDestination` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer Amazon EC2 EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Wenn der bereitgestellte Bucket in Ihrem Konto nicht verfügbar ist, werden die Protokolle außerdem nicht hochgeladen. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ECS InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, von der Sie Protokolle sammeln möchten. Die von Ihnen angegebene Instanz muss von Systems Manager verwaltet werden.

- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon S3 S3-Bucket in Ihrem AWS-Konto , in den Sie die archivierten Protokolle hochladen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Wir empfehlen, dass die Amazon EC2 EC2-Instance, die Sie im `ECSInstanceId` Parameter angeben, über eine IAM-Rolle verfügt, an die die von `AmazonSSMManagedInstanceCore` Amazon verwaltete Richtlinie angehängt ist. Um das Protokollarchiv in den Amazon S3 S3-Bucket hochzuladen, den Sie im `LogDestination` Parameter angeben, müssen Sie die folgenden Berechtigungen hinzufügen:

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

Dokumentschritte

- `assertInstanceIsManaged`- Überprüft, ob die Instanz, die Sie im `ECSInstanceId` Parameter angeben, von Systems Manager verwaltet wird.
- `getInstancePlatform`- Ruft Informationen über die Betriebssystemplattform (OS) der im `ECSInstanceId` Parameter angegebenen Instanz ab.
- `verifyInstancePlatform`— Verzweigt die Automatisierung auf der Grundlage der Betriebssystemplattform.
- `runLogCollectionScriptOnLinux`- Sammelt betriebssystem- und Amazon ECS-bezogene Protokolldateien auf Linux-Instances und erstellt eine Archivdatei im `/var/log/collectECSlogs` Verzeichnis.
- `runLogCollectionScriptOnWindows`- Sammelt betriebssystem- und Amazon ECS-bezogene Protokolldateien auf Windows-Instances und erstellt eine Archivdatei im `C:\ProgramData\collectECSlogs` Verzeichnis.
- `verifyIfS3BucketProvided`— Überprüft, ob ein Wert für den `LogDestination` Parameter angegeben wurde.
- `runUploadScript`- Verzweigt den Automatisierungsschritt auf der Grundlage der Betriebssystemplattform.
- `runUploadScriptOnLinux`- Lädt das Protokollarchiv in den im `LogDestination` Parameter angegebenen Amazon S3 S3-Bucket hoch und löscht die archivierte Protokolldatei aus dem Betriebssystem.
- `runUploadScriptOnWindows`- Lädt das Protokollarchiv in den im `LogDestination` Parameter angegebenen Amazon S3 S3-Bucket hoch und löscht die archivierte Protokolldatei aus dem Betriebssystem.

## `AWS-InstallAmazonECSAgent`

Beschreibung

Das `AWS-InstallAmazonECSAgent` Runbook installiert den Amazon Elastic Container Service (Amazon ECS) -Agenten auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt nur Amazon Linux- und Amazon Linux 2-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Amazon EC2 EC2-Instances, auf denen Sie den Amazon ECS-Agenten installieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Dokumentschritte

`aws:executeScript`- Installiert den Amazon ECS-Agenten auf den Amazon EC2 EC2-Instances, die Sie im `InstanceIds` Parameter angeben.

Ausgaben

InstallAmazonECSAgent. SuccessfulInstances — Die ID der Instance, bei der die Installation des Amazon ECS-Agenten erfolgreich war.

InstallAmazonECSAgent. FailedInstances — Die ID der Instance, bei der die Installation des Amazon ECS-Agenten fehlgeschlagen ist.

InstallAmazonECSAgent. InProgressInstances — Die ID der Instance, auf der der Amazon ECS-Agent installiert wird.

## AWS-ECSRunTask

Beschreibung

Das `AWS-ECSRunTask` Runbook führt die von Ihnen angegebene Amazon Elastic Container Service (Amazon ECS) -Aufgabe aus.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Kapazität ProviderStrategy

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Strategie des Kapazitätsanbieters, die für die Aufgabe verwendet werden soll.

- Cluster

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Kurzname oder der ARN des Clusters, auf dem Ihre Aufgabe ausgeführt werden soll. Wenn Sie keinen Cluster angeben, wird der Standardcluster verwendet.

- count

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Instanziierungen der angegebenen Aufgabe, die auf Ihrem Cluster platziert werden sollen. Sie können bis zu 10 Aufgaben für jede Anfrage angeben.

- Aktivieren Sie ECS ManagedTags

  Typ: Boolesch

  Beschreibung: (Optional) Gibt an, ob verwaltete Amazon ECS-Tags für die Aufgabe verwendet werden sollen. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-ECS-Ressourcen im Entwicklerhandbuch für Amazon Elastic Container Service.

- aktivieren ExecuteCommand

  Typ: Boolesch

  Beschreibung: (Optional) Legt fest, ob die Funktion zum Ausführen von Befehlen für die Container in dieser Aufgabe aktiviert werden soll. Wenn der Wert wahr ist, aktiviert dies die Funktion zum Ausführen von Befehlen für alle Container in der Aufgabe.

- Gruppe

Typ: Zeichenfolge

Beschreibung: (Optional) Der Name der Aufgabengruppe, die der Aufgabe zugeordnet werden soll. Der Standardwert ist der Familienname der Aufgabendefinition. z. B. `family:my-family-name`.

- LaunchType

  Typ: Zeichenfolge

  Gültige Werte: EC2 | FARGATE | EXTERNAL

  Beschreibung: (Optional) Die Infrastruktur, auf der Ihre eigenständige Aufgabe ausgeführt werden soll.

- networkConfiguration

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Netzwerkkonfiguration für die Aufgabe. Dieser Parameter ist für Aufgabendefinitionen erforderlich, die den `awsvpc` Netzwerkmodus verwenden, um ihre eigene elastic network interface zu erhalten, und er wird für andere Netzwerkmodi nicht unterstützt.

- überschreibt

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Liste von Container-Overrides im JSON-Format, die den Namen eines Containers in der angegebenen Aufgabendefinition und die Überschreibungen, die er erhalten soll, spezifiziert. Sie können den Standardbefehl für einen Container, der in der Aufgabendefinition oder im Docker-Image angegeben ist, mit einem Befehl override überschreiben. Sie können auch vorhandene Umgebungsvariablen überschreiben, die in der Aufgabendefinition oder im Docker-Image eines Containers angegeben sind. Darüber hinaus können Sie neue Umgebungsvariablen mit einer Umgebungsüberschreibung hinzufügen.

- Platzierungseinschränkungen

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Reihe von Platzierungsbeschränkungsobjekten, die für die Aufgabe verwendet werden sollen. Sie können bis zu 10 Einschränkungen für jede Aufgabe angeben, einschließlich Einschränkungen in der Aufgabendefinition und Einschränkungen, die zur Laufzeit angegeben wurden.

- Platzierungsstrategie

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Objekte der Platzierungsstrategie, die für die Aufgabe verwendet werden sollen. Sie können für jede Aufgabe maximal 5 Strategieregeln angeben.

- platformVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Plattformversion, die die Aufgabe verwendet. Eine Plattformversion ist nur für Aufgaben spezifiziert, die auf Fargate gehostet werden. Ist keine Plattformversion angegeben, wird die Plattformversion `LATEST` verwendet.

- propagateTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Legt fest, ob Tags von der Aufgabendefinition an die Aufgabe weitergegeben werden. Wenn kein Wert angegeben wird, werden die Tags nicht weitergegeben. Tags können nur während der Aufgabenerstellung an die Aufgaben übertragen werden.

- Referenz-ID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Referenz-ID, die für die Aufgabe verwendet werden soll. Die Referenz-ID kann eine maximale Länge von 1024 Zeichen haben.

- Gestartet von

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein optionales Tag, das beim Starten einer Aufgabe angegeben wird. Auf diese Weise können Sie identifizieren, welche Aufgaben zu einem bestimmten Job gehören, indem Sie die Ergebnisse eines `ListTasks` API-Vorgangs filtern. Bis zu 36 Buchstaben (Groß- und Kleinbuchstaben), Zahlen, Bindestriche (-) und Unterstriche (_) sind zulässig.

- tags

  Typ: Zeichenfolge

Beschreibung: (Optional) Metadaten, die Sie auf die Aufgabe anwenden möchten, um Aufgaben zu kategorisieren und zu organisieren. Jedes Tag besteht aus einem benutzerdefinierten Schlüssel und Wert.

- Aufgabendefinition

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der `family` und `revision` (`family:revision`) oder der vollständige ARN der auszuführenden Aufgabendefinition. Wenn keine Revision angegeben ist, wird die neueste `ACTIVE` Version verwendet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ecs:RunTask`

Dokumentschritte

`aws:executeScript`— Führt die Amazon ECS-Aufgabe auf der Grundlage der Werte aus, die Sie für die Runbook-Eingabeparameter angeben.

## AWSSupport-TroubleshootECSContainerInstance

Beschreibung

Das `AWSSupport-TroubleshootECSContainerInstance` Runbook hilft Ihnen bei der Fehlerbehebung bei einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die sich nicht bei einem Amazon ECS-Cluster registrieren kann. Diese Automatisierung überprüft, ob die Benutzerdaten für die Instance die richtigen Clusterinformationen enthalten, ob das Instance-Profil die erforderlichen Berechtigungen enthält und ob Probleme mit der Netzwerkkonfiguration auftreten.

> **Important**
>
> Um diese Automatisierung erfolgreich auszuführen, muss der Status Ihrer Amazon EC2 EC2-Instance und der Status des Amazon ECS-Clusters sein`ACTIVE`. `running`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon ECS-Clusters, bei dem sich die Instance nicht registrieren konnte.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, für die Sie eine Fehlerbehebung durchführen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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

Dokumentschritte

aws:ExecuteScript: Prüft, ob die Amazon EC2 EC2-Instance die Voraussetzungen erfüllt, die für die Registrierung bei einem Amazon ECS-Cluster erforderlich sind.

## AWSSupport-TroubleshootECSTaskFailedToStart

Beschreibung

Das AWSSupport-TroubleshootECSTaskFailedToStart Runbook hilft Ihnen bei der Fehlerbehebung, warum eine Amazon Elastic Container Service (Amazon ECS) -Aufgabe in einem Amazon ECS-Cluster nicht gestartet werden konnte. Sie müssen dieses Runbook genauso ausführen AWS-Region wie Ihre Aufgabe, die nicht gestartet werden konnte. Das Runbook analysiert die folgenden häufigen Probleme, die das Starten einer Aufgabe verhindern können:

- Netzwerkkonnektivität zur konfigurierten Container-Registry
- Fehlende IAM-Berechtigungen, die für die Aufgabenausführungsrolle erforderlich sind
- VPC-Endpunktkonnektivität
- Konfiguration der Regeln für Sicherheitsgruppen

- AWS Secrets Manager geheime Referenzen
- Konfiguration der Protokollierung

> **Note**
>
> Wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss, werden eine Lambda-Funktion und die erforderliche IAM-Rolle in Ihrem Konto erstellt. Diese Ressourcen werden verwendet, um die Netzwerkkonnektivität Ihrer fehlgeschlagenen Aufgabe zu simulieren. Die Automatisierung löscht diese Ressourcen, wenn sie nicht mehr benötigt werden. Wenn die Automatisierung die Ressourcen jedoch nicht löschen kann, müssen Sie dies manuell tun.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Amazon ECS-Clusters, in dem die Aufgabe nicht gestartet werden konnte.

- CloudwatchRetentionZeitraum

  Typ: Ganzzahl

  Beschreibung: (Optional) Der Aufbewahrungszeitraum in Tagen, für die Lambda-Funktionsprotokolle, die in Amazon CloudWatch Logs gespeichert werden sollen. Dies ist nur erforderlich, wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss.

  Gültige Werte: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Standard: 30

- TaskId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der fehlgeschlagenen Aufgabe. Verwenden Sie die zuletzt fehlgeschlagene Aufgabe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

## Dokumentschritte

- `aws:executeScript`- Überprüft, ob der Benutzer oder die Rolle, der die Automatisierung gestartet hat, über die erforderlichen IAM-Berechtigungen verfügt. Wenn Sie nicht über ausreichende Berechtigungen verfügen, um dieses Runbook zu verwenden, sind die fehlenden erforderlichen Berechtigungen in der Ausgabe der Automatisierung enthalten.
- `aws:branch`— Verzweigungen basieren darauf, ob Sie über Berechtigungen für alle erforderlichen Aktionen für das Runbook verfügen.
- `aws:executeScript`- Erstellt eine Lambda-Funktion in Ihrer VPC, wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss.
- `aws:branch`— Verzweigungen, die auf den Ergebnissen des vorherigen Schritts basieren.
- `aws:executeScript`- Analysiert mögliche Ursachen dafür, dass Ihre Aufgabe nicht gestartet werden konnte.
- `aws:executeScript`- Löscht Ressourcen, die durch diese Automatisierung erstellt wurden.
- `aws:executeScript`- Formatiert die Ausgabe der Automatisierung so, dass die Ergebnisse der Analyse an die Konsole zurückgegeben werden. Sie können die Analyse nach diesem Schritt überprüfen, bevor die Automatisierung abgeschlossen ist.
- `aws:branch`- Verzweigungen, die darauf basieren, ob die Lambda-Funktion und die zugehörigen Ressourcen erstellt wurden und gelöscht werden müssen.
- `aws:sleep`- Schläft 30 Minuten lang, sodass die elastic network interface für die Lambda-Funktion gelöscht werden kann.
- `aws:executeScript`- Löscht die Netzwerkschnittstelle der Lambda-Funktion.
- `aws:executeScript`— Formatiert die Ausgabe des Schritts zum Löschen der Netzwerkschnittstelle der Lambda-Funktion.

## AWS-UpdateAmazonECSAgent

Beschreibung

Das `AWS-UpdateAmazonECSAgent` Runbook aktualisiert den Amazon Elastic Container Service (Amazon ECS) -Agenten auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt nur Amazon Linux- und Amazon Linux 2-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterArn

  Typ: StringList

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Amazon ECS-Clusters, bei dem Ihre Container-Instances registriert sind.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Dokumentschritte

`aws:executeScript`- Aktualisiert den Amazon ECS-Agenten auf dem Amazon ECS-Cluster, den Sie in den `ClusterARN` Parametern angeben.

Ausgaben

UpdateAmazonECSAgent. UpdatedContainers — Die ID der Instance, bei der das Update des Amazon ECS-Agenten erfolgreich war.

UpdateAmazonECSAgent. FailedContainers - Die ID der Instance, bei der das Update des Amazon ECS-Agenten fehlgeschlagen ist.

UpdateAmazonECSAgent. InProgressContainers — Die ID der Instance, in der das Update des Amazon ECS-Agenten gerade läuft.

# Amazon EFS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic File System bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CheckAndMountEFS

## `AWSSupport-CheckAndMountEFS`

Beschreibung

Das `AWSSupport-CheckAndMountEFS` Runbook überprüft die Voraussetzungen für das Mounten Ihres Amazon Elastic File System (Amazon EFS) -Dateisystems und mountet das Dateisystem

auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt das Mounten Ihres Amazon EFS-Dateisystems mit dem DNS-Namen oder mithilfe der IP-Adresse des Mount-Ziels.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Aktion

  Typ: Zeichenfolge

  Gültige Werte: Prüfen Sie | CheckAndMount

  Beschreibung: (Erforderlich) Legt fest, ob das Runbook die Voraussetzungen oder die Voraussetzungen überprüft und das Dateisystem einhängt.
- EfsId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Dateisystems, das Sie mounten möchten.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, auf der Sie das Dateisystem mounten möchten.

- MountOptions

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die vom Amazon EFS-Mount-Helper unterstützten Optionen, die Sie beim Mounten des Dateisystems verwenden möchten. Wenn Sie die `tls` Option angeben, stellen Sie sicher, dass Stunnel auf der Ziel-Instance aktualisiert wurde.

- MountPoint

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Verzeichnis, in dem Sie das Dateisystem mounten möchten. Wenn Sie den `Check` Wert für den `Action` Parameter angeben, sollte dieser Parameter nicht angegeben werden.

- MountTargetIP

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die IP-Adresse des Mount-Ziels. Das Mounten nach IP-Adresse funktioniert in Umgebungen, in denen DNS deaktiviert ist, wie z. B. in virtuellen privaten Clouds (VPCs) mit deaktivierten DNS-Hostnamen. Sie können diese Option auch verwenden, wenn Ihre Umgebung einen anderen DNS-Anbieter als Amazon Route 53 (Route 53) verwendet.

- Region

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der AWS-Region Ort, an dem sich die Amazon EC2 EC2-Instance und das Dateisystem befinden.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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:*

Dokumentschritte

- aws:executeScript- Sammelt Details über die Amazon EC2 EC2-Instance, die Sie im InstanceId Parameter angeben.
- aws:executeScript- Sammelt Details über das Dateisystem, das Sie im Parameter angeben. EfsId
- aws:executeScript— Überprüft, ob die dem Dateisystem zugeordnete Sicherheitsgruppe Datenverkehr auf Port 2049 von der Amazon EC2 EC2-Instance zulässt, die Sie im Parameter angeben. InstanceId
- aws:assertAwsResourceProperty— Überprüft, ob die Amazon EC2 EC2-Instance, die Sie im InstanceId Parameter angeben, von Systems Manager verwaltet wird und ob der Status lautet. Online

- `aws:branch`— Verzweigt auf der Grundlage des Werts, den Sie für den `Action` Parameter angeben.
- `aws:runCommand`- Überprüft die Voraussetzungen für das Mounten des Dateisystems, das Sie im `EfsId` Parameter angeben.
- `aws:runCommand`- Überprüft die Voraussetzungen für das Mounten des Dateisystems, das Sie im `EfsId` Parameter angeben, und mountet das Dateisystem auf der Amazon EC2 EC2-Instance, die Sie im Parameter angeben. `InstanceId`

# Amazon EKS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Kubernetes Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups

## `AWSSupport-CollectEKSInstanceLogs`

Beschreibung

Das `AWSSupport-CollectEKSInstanceLogs` Runbook sammelt Protokolldateien im Zusammenhang mit dem Betriebssystem und Amazon Elastic Kubernetes Service (Amazon EKS) aus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um Ihnen bei der

Behebung häufig auftretender Probleme zu helfen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen an der Dateisystemstruktur vorgenommen, einschließlich der Erstellung temporärer Verzeichnisse, des Kopierens von Protokolldateien in die temporären Verzeichnisse und der Komprimierung der Protokolldateien in ein Archiv. Diese Aktivität kann zu einer erhöhten Auslastung `CPUUtilization` der EC2-Instance führen. Weitere Informationen zu finden Sie `CPUUtilization` unter Instance-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie einen Wert für den `LogDestination` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Diese Automatisierung erfordert mindestens 10 Prozent des verfügbaren Festplattenspeichers auf dem Amazon Elastic Block Store (Amazon EBS) -Stammvolume, das an Ihre EC2-Instance angehängt ist. Wenn auf dem Root-Volume nicht genügend Festplattenspeicher verfügbar ist, wird die Automatisierung gestoppt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EKS InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon EKS EC2-Instance, von der Sie Protokolle sammeln möchten.
- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der S3-Bucket in Ihrem Konto, in den die archivierten Protokolle hochgeladen werden sollen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Wir empfehlen, dass die EC2-Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, an die die von Amazon verwaltete AmazonSSM ManagedInstance Core-Richtlinie angehängt ist. Um das Protokollarchiv in den S3-Bucket hochzuladen, den Sie im `LogDestination` Parameter angeben, müssen Sie die Berechtigung hinzufügen. `s3:PutObject`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass das Betriebssystem des im `EKSInstanceId` Parameter angegebenen Werts Linux ist.

- `aws:runCommand`- Sammelt Protokolldateien zum Betriebssystem und zu Amazon EKS und komprimiert sie in ein Archiv im `/var/log` Verzeichnis.
- `aws:branch`— Bestätigt, ob ein Wert für den `LogDestination` Parameter angegeben wurde.
- `aws:runCommand`- Lädt das Log-Archiv in den S3-Bucket hoch, den Sie im `LogDestination` Parameter angeben.

## `AWS-CreateEKSClusterWithFargateProfile`

Beschreibung

Das `AWS-CreateEKSClusterWithFargateProfile` Runbook erstellt einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mithilfe eines. AWS Fargate

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Ein eindeutiger Name für den Cluster.

- ClusterRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, der Berechtigungen für die Kubernetes-Steuerebene bereitstellt, um AWS API-Operationen in Ihrem Namen aufzurufen.

- FargateProfileName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Fargate-Profils.

- FargateProfileRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle für die Ausführung von Amazon EKS Pod.

- FargateProfileSelektoren

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Selektoren, um Pods dem Fargate-Profil zuzuordnen.

- SubnetIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Subnetze, die Sie für Ihren Amazon EKS-Cluster verwenden möchten. Amazon EKS erstellt in diesen Subnetzen elastische Netzwerkschnittstellen für die Kommunikation zwischen Ihren Knoten und der Kubernetes-Steuerebene. Sie müssen mindestens zwei Subnetz-IDs angeben.

- EndpointPrivateEKS-Zugriff

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `True` um privaten Zugriff für den Kubernetes-API-Serverendpunkt Ihres Clusters zu ermöglichen. Wenn Sie den privaten Zugriff aktivieren, verwenden Kubernetes-API-Anfragen aus der VPC Ihres Clusters den privaten VPC-

Endpunkt. Wenn Sie den privaten Zugriff deaktivieren und Knoten oder AWS Fargate Pods im Cluster haben, stellen Sie sicher, dass die erforderlichen CIDR-Blöcke für die Kommunikation mit den Knoten oder Fargate-Pods `publicAccessCidrs` enthalten sind.

- EKS-Zugriff EndpointPublic

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `False` um den öffentlichen Zugriff auf den Kubernetes-API-Serverendpunkt Ihres Clusters zu deaktivieren. Wenn Sie den öffentlichen Zugriff deaktivieren, kann der Kubernetes-API-Server Ihres Clusters nur Anfragen von der VPC empfangen, in der er gestartet wurde.

- PublicAccessCIDRs

  Typ: StringList

  Beschreibung: (Optional) Die CIDR-Blöcke, denen Zugriff auf den öffentlichen Kubernetes-API-Serverendpunkt Ihres Clusters gewährt wird. Die Kommunikation mit dem Endpunkt über Adressen außerhalb der von Ihnen angegebenen CIDR-Blöcke wird verweigert. Wenn Sie den privaten Endpunktzugriff deaktiviert haben und Knoten oder Fargate-Pods im Cluster haben, stellen Sie sicher, dass Sie die erforderlichen CIDR-Blöcke angeben.

- SecurityGroupIDs

  Typ: StringList

  Beschreibung: (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die den von Amazon EKS in Ihrem Konto erstellten Elastic Network-Schnittstellen zugeordnet werden sollen.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- createEKSCluster (aws:executeAwsApi) — Erzeugt einen Amazon EKS-Cluster.
- verifyEKS ClusterIsActive (ForAwsResourcePropertyaws:wait) — Überprüft, ob der Cluster-Status lautet. `ACTIVE`
- CreateFargateProfile (aws:executeAwsApi) — Erzeugt ein Fargate für den Cluster.
- VerifyFargateProfileIsActive (aws:wait ForAwsResourceProperty) — Überprüft, ob der Status des Fargate-Profils lautet. `ACTIVE`

Ausgaben

`CreateEKSCluster.CreateClusterResponse`

Beschreibung: Die Antwort wurde vom API-Aufruf empfangen. `CreateCluster`

`CreateFargateProfile.CreateFargateProfileResponse`

Beschreibung: Die Antwort wurde vom `CreateFargateProfile` API-Aufruf empfangen.

## AWS-CreateEKSClusterWithNodegroup

Beschreibung

Das `AWS-CreateEKSClusterWithNodegroup` Runbook erstellt einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, der eine Knotengruppe für die Kapazität verwendet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein eindeutiger Name für den Cluster.
- ClusterRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, der Berechtigungen für die Kubernetes-Steuerebene bereitstellt, um AWS API-Operationen in Ihrem Namen aufzurufen.
- NodegroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein eindeutiger Name für die Knotengruppe.
- NodegroupRoleArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, die Ihrer Knotengruppe zugeordnet werden soll. Der Kubelet-Daemon von Amazon EKS Worker Node ruft in Ihrem Namen AWS APIs auf. Knoten erhalten über ein IAM-Instance-Profil und zugehörige Richtlinien Berechtigungen für diese API-Aufrufe. Bevor Sie Knoten starten und in einem Cluster registrieren können, müssen Sie eine IAM-Rolle erstellen, die diese Knoten beim Start verwenden können.

- SubnetIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Subnetze, die Sie für Ihren Amazon EKS-Cluster verwenden möchten. Amazon EKS erstellt in diesen Subnetzen elastische Netzwerkschnittstellen für die Kommunikation zwischen Ihren Knoten und der Kubernetes-Steuerebene. Sie müssen mindestens zwei Subnetz-IDs angeben.

- EndpointPrivateEKS-Zugriff

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `True` um privaten Zugriff für den Kubernetes-API-Serverendpunkt Ihres Clusters zu ermöglichen. Wenn Sie den privaten Zugriff aktivieren, verwenden Kubernetes-API-Anfragen aus der VPC Ihres Clusters den privaten VPC-Endpunkt. Wenn Sie den privaten Zugriff deaktivieren und Knoten oder AWS Fargate Pods im Cluster haben, stellen Sie sicher, dass die erforderlichen CIDR-Blöcke für die Kommunikation mit den Knoten oder Fargate-Pods `publicAccessCidrs` enthalten sind.

- EKS-Zugriff EndpointPublic

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `False` um den öffentlichen Zugriff auf den Kubernetes-API-Serverendpunkt Ihres Clusters zu deaktivieren. Wenn Sie den öffentlichen Zugriff deaktivieren, kann der Kubernetes-API-Server Ihres Clusters nur Anfragen von der VPC empfangen, in der er gestartet wurde.

- PublicAccessCIDRs

  Typ: StringList

Beschreibung: (Optional) Die CIDR-Blöcke, denen Zugriff auf den öffentlichen Kubernetes-API-Serverendpunkt Ihres Clusters gewährt wird. Die Kommunikation mit dem Endpunkt über Adressen außerhalb der von Ihnen angegebenen CIDR-Blöcke wird verweigert. Wenn Sie den privaten Endpunktzugriff deaktiviert haben und Knoten oder Fargate-Pods im Cluster haben, stellen Sie sicher, dass Sie die erforderlichen CIDR-Blöcke angeben.

- SecurityGroupIDs

  Typ: StringList

  Beschreibung: (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die den von Amazon EKS in Ihrem Konto erstellten Elastic Network-Schnittstellen zugeordnet werden sollen.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

### Dokumentschritte

- createEKSCluster (aws:executeAwsApi) — Erzeugt einen Amazon EKS-Cluster.
- verifyEKS ClusterIsActive (ForAwsResourcePropertyaws:wait) — Überprüft, ob der Cluster-Status lautet. `ACTIVE`

- CreateNodegroup (aws:executeAwsApi) — Erstellt eine Knotengruppe für den Cluster.
- VerifyNodegroupIsActive (aws:wait ForAwsResourceProperty) — Überprüft, ob der Status der Knotengruppe lautet. `ACTIVE`

Ausgaben

- `CreateEKSCluster.CreateClusterResponse`: Die Antwort wurde vom API-Aufruf empfangen. `CreateCluster`
- `CreateNodegroup.CreateNodegroupResponse`: Antwort vom `CreateNodegroup` API-Aufruf erhalten.

## AWS-DeleteEKSCluster

Beschreibung

Dieses Runbook löscht die mit einem Amazon EKS-Cluster verknüpften Ressourcen, einschließlich Knotengruppen und Fargate-Profilen. Optional können Sie alle selbstverwalteten Knoten, die AWS CloudFormation Stacks, die zum Erstellen der Knoten verwendet wurden, und den CloudFormation VPC-Stack für Ihren Cluster löschen. Weitere Informationen zum Löschen eines Clusters finden Sie unter Löschen eines Clusters im Amazon EKS-Benutzerhandbuch.

> **Note**
>
> Wenn Sie aktive Dienste in Ihrem Cluster haben, die einem Load Balancer zugeordnet sind, müssen Sie diese Dienste löschen, bevor Sie den Cluster löschen. Wenn Sie dies nicht tun, kann das System die Load Balancer nicht löschen. Gehen Sie wie folgt vor, um Dienste zu suchen und zu löschen, bevor Sie das `AWS-DeleteEKSCluster` Runbook ausführen.

So suchen und löschen Sie Dienste in Ihrem Cluster

1. Installieren Sie das Kubernetes-Befehlszeilenprogramm,. `kubectl` Weitere Informationen finden Sie unter Installation von kubectl im Amazon EKS-Benutzerhandbuch.
2. Führen Sie den folgenden Befehl aus, um alle Dienste aufzulisten, die in Ihrem Cluster ausgeführt werden.

```
kubectl get svc --all-namespaces
```

3. Führen Sie den folgenden Befehl aus, um alle Dienste zu löschen, denen ein EXTERNAL-IP-Wert zugeordnet ist. Diese Dienste werden von einem Load Balancer unterstützt, und Sie müssen sie in Kubernetes löschen, damit der Load Balancer und die zugehörigen Ressourcen ordnungsgemäß freigegeben werden können.

```
kubectl delete svc
service-name
```

Sie können das Runbook jetzt ausführen. `AWS-DeleteEKSCluster`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EKS ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters, der gelöscht werden soll.

- VPC-Stapel CloudFormation

  Typ: Zeichenfolge

  Beschreibung: (Optional) AWS CloudFormation Stack-Name für die VPC für den EKS-Cluster, der gelöscht wird. Dadurch werden der AWS CloudFormation Stack für VPC und alle vom Stack erstellten Ressourcen gelöscht.
- VPC CloudFormation StackRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN einer IAM-Rolle, die AWS CloudFormation davon ausgeht, den CloudFormation VPC-Stack zu löschen. AWS CloudFormation verwendet die Anmeldeinformationen der Rolle, um in Ihrem Namen Anrufe zu tätigen.
- SelfManagedNodeStacks

  Typ: Zeichenfolge

  Beschreibung: (Optional) Durch Kommas getrennte Liste von AWS CloudFormation Stack-Namen für selbstverwaltete Knoten. Dadurch werden die AWS CloudFormation Stacks für selbstverwaltete Knoten gelöscht.
- SelfManagedNodeStacksRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN einer IAM-Rolle, die AWS CloudFormation davon ausgeht, die selbstverwalteten Node Stacks zu löschen. AWS CloudFormation verwendet die Anmeldeinformationen der Rolle, um in Ihrem Namen Anrufe zu tätigen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

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

Dokumentschritte

- aws:executeScript- DeleteNodeGroups: Findet und löscht alle Knotengruppen im EKS-Cluster.
- aws:executeScript- DeleteFargateProfiles: Findet und löscht alle Fargate-Profile im EKS-Cluster.
- aws:executeScript- DeleteSelfManagedNodes: Löscht alle selbstverwalteten Knoten und die CloudFormation Stacks, die zur Erstellung der Knoten verwendet wurden.
- aws:executeScript- DeleteEksCluster: Löscht den EKS-Cluster.
- aws:executeScript- DeleteVPC CloudFormation Stack: Löscht den VPC-Stack. CloudFormation

## AWS-MigrateToNewEKSSelfManagedNodeGroup

Beschreibung

Das AWS-MigrateToNewEKSSelfManagedNodeGroup Runbook hilft Ihnen dabei, eine neue Linux-Knotengruppe von Amazon Elastic Kubernetes Service (Amazon EKS) zu erstellen, zu der Sie Ihre bestehende Anwendung migrieren können. Weitere Informationen finden Sie unter Migration zu einer neuen Knotengruppe im Amazon EKS-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- OldStackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder die Stack-ID Ihres vorhandenen AWS CloudFormation Stacks.

- NewStackName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des neuen AWS CloudFormation Stacks, der für Ihre neue Knotengruppe erstellt wird. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Stack-Name im folgenden Format erstellt:`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGruppe

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die Knoten für die Kommunikation mit der Amazon EKS-Steuerebene verwenden sollen. Wenn Sie keinen Wert für diesen Parameter angeben, wird die in Ihrem vorhandenen AWS CloudFormation Stack angegebene Sicherheitsgruppe verwendet.

- NodeInstanceGeben Sie ein

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instanztyp, den Sie für die neue Knotengruppe verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird der in Ihrem vorhandenen AWS CloudFormation Stack angegebene Instance-Typ verwendet.

- NodeGroupName

Typ: Zeichenfolge

Beschreibung: (Optional) Der Name Ihrer neuen Knotengruppe. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Name der Knotengruppe verwendet, der in Ihrem vorhandenen AWS CloudFormation Stack angegeben ist.

- NodeAutoScalingGroupDesiredCapacity

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die gewünschte Anzahl von Knoten, auf die skaliert werden soll, wenn Ihr neuer Stack erstellt wird. Diese Zahl muss größer oder gleich dem `NodeAutoScalingGroupMinSize` Wert und kleiner oder gleich dem Wert sein`NodeAutoScalingGroupMaxSize`. Wenn Sie keinen Wert für diesen Parameter angeben, wird die gewünschte Kapazität der Knotengruppe verwendet, die in Ihrem vorhandenen AWS CloudFormation Stack angegeben ist.

- NodeAutoScalingGroupMaxSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die Ihre Knotengruppe skaliert werden kann. Wenn Sie keinen Wert für diesen Parameter angeben, wird die maximale Größe der Knotengruppe verwendet, die in Ihrem vorhandenen AWS CloudFormation Stack angegeben ist.

- NodeAutoScalingGroupMinSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die Ihre Knotengruppe skaliert werden kann. Wenn Sie keinen Wert für diesen Parameter angeben, wird die Mindestgröße der Knotengruppe verwendet, die in Ihrem vorhandenen AWS CloudFormation Stack angegeben ist.

- NodeImageId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID von Amazon Machine Image (AMI), die die Knotengruppe verwenden soll.

- NodeImageidssmParam

  Typ: Zeichenfolge

Beschreibung: (Optional) Der öffentliche Systems Manager Manager-Parameter für denAMI, den die Knotengruppe verwenden soll.

- NodeVolumeGröße

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Größe des Root-Volumes für Ihre Knoten in GiB. Wenn Sie keinen Wert für diesen Parameter angeben, wird die in Ihrem vorhandenen AWS CloudFormation Stack angegebene Knoten-Volume-Größe verwendet.

- NodeVolumeGeben Sie ein

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Typ des Amazon EBS-Volumes, das Sie für das Root-Volume Ihrer Knoten verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird der in Ihrem vorhandenen AWS CloudFormation Stack angegebene Volume-Typ verwendet.

- KeyName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das key pair, das Sie Ihren Knoten zuweisen möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird das in Ihrem vorhandenen AWS CloudFormation Stack angegebene key pair verwendet.

- Subnetze

  Typ: StringList

  Beschreibung: (Optional) Eine durch Kommas getrennte Liste der Subnetz-IDs, die Sie für Ihre neue Knotengruppe verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, werden die in Ihrem vorhandenen AWS CloudFormation Stack angegebenen Subnetze verwendet.

- Deaktivieren Sie IMDSV1

  Typ: Boolesch

  Beschreibung: (Optional) Geben Sie an, ob der Instanz-Metadatendienst Version 1 (IMDSv1) deaktiviert werden `true` soll. Standardmäßig unterstützen Knoten IMDSv1 und IMDSv2.

- BootstrapArguments

Typ: Zeichenfolge

Beschreibung: (Optional) Zusätzliche Argumente, die Sie an das Node-Bootstrap-Skript übergeben möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- DetermineParameterValuesForNewNodeGroup (aws:ExecuteScript) — Sammelt die Parameterwerte, die für die neue Knotengruppe verwendet werden sollen.

- CreateStack (aws:CreateStack) — Erstellt den Stack für die neue Knotengruppe. AWS CloudFormation
- GetNewStackNodeInstanceRole (aws:executeAwsApi) — Ruft die Rolle der Knoteninstanz ab.
- GetNewStackSecurityGroup (aws:executeAwsApi) — Der Schritt ruft die Knotensicherheitsgruppe ab.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) — Fügt der neu erstellten Sicherheitsgruppe Eingangsregeln hinzu, sodass sie Datenverkehr von der Gruppe akzeptieren kann, die Ihrer vorherigen Knotengruppe zugewiesen wurde.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) — Fügt der vorherigen Sicherheitsgruppe Eingangsregeln hinzu, sodass sie Datenverkehr von der Sicherheitsgruppe akzeptieren kann, die Ihrer neu erstellten Knotengruppe zugewiesen ist.
- VerifyStackComplete (aws:assert AwsResource Property) — Überprüft, ob der neue Stack-Status lautet. `CREATE_COMPLETE`

Ausgaben

DetermineParameterValuesForNewNodeGroup. NewStackParameters - Die Parameter, die zum Erstellen des neuen Stacks verwendet wurden.

GetNewStackNodeInstanceRole. NewNodeInstanceRole — Die Knoteninstanzrolle für die neue Knotengruppe.

GetNewStackSecurityGruppe. NewNodeSecurityGroup — Die ID der Sicherheitsgruppe für die neue Knotengruppe.

DetermineParameterValuesForNewNodeGroup. NewStackName - Der AWS CloudFormation Stack-Name für die neue Knotengruppe.

CreateStack. StackId - Die AWS CloudFormation Stack-ID für die neue Knotengruppe.

## AWSPremiumSupport-TroubleshootEKSCluster

Beschreibung

Das `AWSPremiumSupport-TroubleshootEKSCluster` Runbook diagnostiziert häufig auftretende Probleme mit einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster und der zugrunde liegenden Infrastruktur und bietet empfohlene Schritte zur Behebung.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist entweder ein Enterprise- oder ein Business Support-Abonnement erforderlich. Weitere Informationen finden Sie unter AWS Supportpläne vergleichen.

Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters, für den Sie eine Fehlerbehebung durchführen möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des privaten Amazon S3 S3-Buckets, in den der vom Runbook generierte Bericht hochgeladen werden soll.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Darüber hinaus muss die AWS Identity and Access Management (IAM-) Richtlinie, die dem Benutzer oder der Rolle zugewiesen ist, die die Automatisierung startet, den ssm:GetParameter Vorgang mit den folgenden öffentlichen AWS Systems Manager Parametern zulassen, um das neueste empfohlene Amazon EKS Amazon Machine Image (AMI) für die Worker-Knoten abzurufen.

- 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

Um den vom Runbook generierten Bericht in einen Amazon S3 S3-Bucket hochzuladen, sind die folgenden Berechtigungen für den angegebenen Amazon S3 S3-Bucket erforderlich.

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

Dokumentschritte

- aws:executeAwsApi- Sammelt Details für den angegebenen Amazon EKS-Cluster.
- aws:executeScript- Sammelt Details zu den Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Auto Scaling Scaling-Gruppen, AMI s und Amazon EC2-GPU-Grafikinstanztypen.
- aws:executeScript- Sammelt Details zur Virtual Private Cloud (VPC), Subnetze, Network Address Translation (NAT) -Gateways, Subnetzrouten, Sicherheitsgruppen und Network Access Control Lists (ACLs) des Amazon EKS-Clusters.
- aws:executeScript— Sammelt Details zu den angehängten IAM-Instance-Profilen und Rollenrichtlinien.

- `aws:executeScript`- Sammelt Details des Amazon S3 S3-Buckets, den Sie im `S3BucketName` Parameter angeben.
- `aws:executeScript`- Klassifiziert die Amazon VPC-Subnetze als öffentlich oder privat.
- `aws:executeScript`- Überprüft die Amazon VPC-Subnetze auf Tags, die als Teil eines Amazon EKS-Clusters erforderlich sind.
- `aws:executeScript`- Überprüft die Amazon VPC-Subnetze auf die Tags, die für Elastic Load Balancing Balancing-Subnetze erforderlich sind.
- `aws:executeScript`- Prüft, ob die Worker-Node-Amazon-EC2-Instances die neuesten für Amazon EKS optimierten AMI s verwenden
- `aws:executeScript`- Überprüft, ob die Amazon VPC-Sicherheitsgruppen den Worker-Knoten die erforderlichen Tags zugewiesen haben.
- `aws:executeScript`- Überprüft die Amazon VPC-Sicherheitsgruppenregeln für Amazon EKS-Cluster und Worker-Nodes auf die empfohlenen Eingangsregeln für den Amazon EKS-Cluster.
- `aws:executeScript`- Überprüft die Amazon VPC-Sicherheitsgruppenregeln für Amazon EKS-Cluster und Worker-Nodes auf die empfohlenen Ausgangsregeln aus dem Amazon EKS-Cluster.
- `aws:executeScript`- Überprüft die Netzwerk-ACL-Konfiguration der Amazon VPC-Subnetze.
- `aws:executeScript`— Prüft, ob die Amazon EC2 EC2-Instances des Worker-Nodes über die erforderlichen verwalteten Richtlinien verfügen.
- `aws:executeScript`- Prüft, ob die Auto Scaling Scaling-Gruppen über die erforderlichen Tags für Cluster-Autoscaling verfügen.
- `aws:executeScript`— Prüft, ob die Amazon EC2 EC2-Instances des Worker-Nodes mit dem Internet verbunden sind.
- `aws:executeScript`- Generiert einen Bericht auf der Grundlage der Ergebnisse der vorherigen Schritte. Wenn ein Wert für den `S3BucketName` Parameter angegeben wird, wird der generierte Bericht in den Amazon S3 S3-Bucket hochgeladen.

## AWSSupport-TroubleshootEKSWorkerNode

Beschreibung

Das `AWSSupport-TroubleshootEKSWorkerNode` Runbook analysiert einen Amazon Elastic Compute Cloud (Amazon EC2) -Worker-Knoten und einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, um Sie bei der Identifizierung und Behebung häufiger Ursachen zu

unterstützen, die verhindern, dass Worker-Knoten einem Cluster beitreten können. Das Runbook enthält Anleitungen, die Ihnen bei der Lösung aller identifizierten Probleme helfen sollen.

> **Important**
>
> Um diese Automatisierung erfolgreich auszuführen, muss der Status Ihres Amazon EC2 `running` EC2-Worker-Knotens und der Amazon EKS-Cluster-Status sein`ACTIVE`.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters.
- Worker-ID

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des Amazon EC2 EC2-Worker-Knotens, der dem Cluster nicht beitreten konnte.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

### Dokumentschritte

- `aws:assertAwsResourceProperty`— Bestätigt, dass der Amazon EKS-Cluster, den Sie im `ClusterName` Parameter angeben, existiert und sich in einem `ACTIVE` Zustand befindet.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der Amazon EC2 EC2-Worker-Knoten, den Sie im `WorkerID` Parameter angeben, existiert und sich in einem `running` Status befindet.
- `aws:executeScript`- Führt ein Python-Skript aus, das dabei hilft, mögliche Ursachen dafür zu identifizieren, dass der Worker-Knoten dem Cluster nicht beitreten kann.

## AWS-UpdateEKSCluster

Beschreibung

Das `AWS-UpdateEKSCluster` Runbook hilft Ihnen dabei, Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf die Kubernetes-Version zu aktualisieren, die Sie verwenden möchten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name Ihres Amazon EKS-Clusters.

- Version

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Kubernetes-Version, auf die Sie Ihren Cluster aktualisieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktualisiert die Kubernetes-Version, die von Ihrem Amazon EKS-Cluster verwendet wird.
- `aws:waitForAwsResourceProperty`- Wartet auf den Aktualisierungsstatus. `Successful`

## AWS-UpdateEKSManagedNodeGroup

Beschreibung

Das `AWS-UpdateEKSManagedNodeGroup` Runbook hilft Ihnen bei der Aktualisierung einer von Amazon Elastic Kubernetes Service (Amazon EKS) verwalteten Knotengruppe. Sie können entweder eine oder eine `Version` Aktualisierung auswählen. `Configuration`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Clusters, dessen Knotengruppe Sie aktualisieren möchten.
- NodeGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der zu aktualisierenden Knotengruppe.
- UpdateType

  Typ: Zeichenfolge

  Gültige Werte: Knotengruppenversion aktualisieren | Knotengruppenkonfigurationen aktualisieren

  Standard: Version der Knotengruppe aktualisieren

  Beschreibung: (Erforderlich) Die Art des Updates, das Sie für die Knotengruppe durchführen möchten.

Die folgenden Parameter gelten nur für den `Version` Aktualisierungstyp:

- AMI ReleaseVersion

  Typ: Zeichenfolge

Beschreibung: (Optional) Die optimierte Version von Amazon EKSAMI, die Sie verwenden möchten. Standardmäßig wird die neueste Version verwendet.

- ForceUpgrade

  Typ: Boolesch

  Beschreibung: (Optional) Wenn dieser Wert zutrifft, schlägt das Update nicht fehl, wenn das Budget bei einer Pod-Unterbrechung überschritten wurde.

- KubernetesVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Kubernetes-Version, auf die die Knotengruppe aktualisiert werden soll.

- LaunchTemplateID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Startvorlage.

- LaunchTemplateName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Startvorlage.

- LaunchTemplateVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Version der Startvorlage für Amazon Elastic Compute Cloud (Amazon EC2). Dieser Parameter ist nur gültig, wenn eine Knotengruppe anhand einer Startvorlage erstellt wurde.

Die folgenden Parameter gelten nur für den `Configuration` Aktualisierungstyp:

- AddOrUpdateNodeGroupLabels

  Typ: StringMap

  Beschreibung: (Optional) Kubernetes-Labels, die Sie hinzufügen oder aktualisieren möchten.

- AddOrUpdateKubernetesTaintsEffect

  Typ: StringList

  Beschreibung: (Optional) Die Kubernetes-Taints, die Sie hinzufügen oder aktualisieren möchten.
- MaxUnavailableNodeGroups

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, die während eines Versionsupdates gleichzeitig nicht verfügbar sind.
- MaxUnavailablePercentageNodeGruppe

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Der Prozentsatz der Knoten, die während eines Versionsupdates nicht verfügbar sind.
- NodeGroupDesiredSize

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der Knoten, die die verwaltete Knotengruppe verwalten soll.
- NodeGroupMaxSize

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die die verwaltete Knotengruppe skaliert werden kann.
- NodeGroupMinSize

  Typ: Ganzzahl

  Standard: 0

Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die die verwaltete Knotengruppe skaliert werden kann.

- RemoveKubernetesTaintsEffect

  Typ: StringList

  Beschreibung: (Optional) Die Kubernetes-Taints, die Sie entfernen möchten.

- RemoveNodeGroupLabels

  Typ: StringList

  Beschreibung: (Optional) Eine durch Kommas getrennte Liste von Bezeichnungen, die Sie entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Dokumentschritte

- `aws:executeScript`— Aktualisiert eine Amazon EKS-Cluster-Knotengruppe entsprechend den Werten, die Sie für die Runbook-Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet, bis der Cluster-Aktualisierungsstatus erreicht ist. `Successful`

## AWS-UpdateEKSSelfManagedLinuxNodeGroups

Beschreibung

Das `AWS-UpdateEKSSelfManagedLinuxNodeGroups` Runbook aktualisiert selbstverwaltete verwaltete Knotengruppen in Ihrem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mithilfe eines Stacks. AWS CloudFormation

Wenn Ihr Cluster Auto Scaling verwendet, empfehlen wir, die Bereitstellung auf zwei Replikate herunterzuskalieren, bevor Sie dieses Runbook verwenden.

Um eine Bereitstellung auf zwei Replikate zu skalieren

1. Installieren Sie das Kubernetes-Befehlszeilenprogramm,. `kubectl` Weitere Informationen finden Sie unter Installieren von kubectl im Amazon-EKS-Benutzerhandbuch.
2. Führen Sie den folgenden Befehl aus.

   ```
   kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
   ```
3. Führen Sie das Runbook aus. `AWS-UpdateEKSSelfManagedLinuxNodeGroups`
4. Skalieren Sie die Bereitstellung wieder auf die gewünschte Anzahl von Replikaten, indem Sie den folgenden Befehl ausführen.

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

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters.

- NodeGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der verwalteten Knotengruppe.

- ClusterControlPlaneSecurityGruppe

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe auf der Kontrollebene.

- Deaktivieren Sie IMDSv1

  Typ: Boolesch

  Beschreibung: (Optional) Legt fest, ob Sie Instance Metadata Service Version 1 (IMDSv1) und IMDSv2 zulassen möchten.

- KeyName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Schlüsselname für die Instanzen.

- NodeAutoScalingGroupDesiredCapacity

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Knoten, die die Knotengruppe verwalten soll.

- NodeAutoScalingGroupMaxSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die die Knotengruppe skaliert werden kann.

- NodeAutoScalingGroupMinSize

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die die Knotengruppe skaliert werden kann.

- NodeInstanceGeben Sie ein

  Typ: Zeichenfolge

  Standard: t3.large

  Beschreibung: (Optional) Der Instanztyp, den Sie für die Knotengruppe verwenden möchten.

- NodeImageID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID von Amazon Machine Image (AMI), die die Knotengruppe verwenden soll.

- NodeImageidssmParam

  Typ: Zeichenfolge

  Standard: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Beschreibung: (Optional) Der öffentliche Systems Manager Manager-Parameter für denAMI, den die Knotengruppe verwenden soll.

- StackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des AWS CloudFormation Stacks, der zur Aktualisierung der Knotengruppe verwendet wird.

- Subnetze

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs für die Subnetze, die Ihr Cluster verwenden soll.

- VpcId

  Typ: Zeichenfolge

Standard: Standard

Beschreibung: (Erforderlich) Die Virtual Private Cloud (VPC), in der Ihr Cluster bereitgestellt wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Dokumentschritte

- `aws:executeScript`— Aktualisiert eine Amazon EKS-Cluster-Knotengruppe entsprechend den Werten, die Sie für die Runbook-Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet auf die Rückgabe des AWS CloudFormation Stack-Aktualisierungsstatus.

# Elastic Beanstalk

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Elastic Beanstalk Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

## AWSSupport-CollectElasticBeanstalkLogs

Beschreibung

Das `AWSSupport-CollectElasticBeanstalkLogs` Runbook sammelt AWS Elastic Beanstalk zugehörige Protokolldateien aus einer Amazon Elastic Compute Cloud (Amazon EC2) Windows Server -Instance, die von Elastic Beanstalk gestartet wurde, um Sie bei der Behebung häufiger Probleme zu unterstützen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen an der Dateisystemstruktur vorgenommen, einschließlich der Erstellung temporärer Verzeichnisse, des Kopierens von Protokolldateien in die temporären Verzeichnisse und der Komprimierung der Protokolldateien in ein Archiv. Diese Aktivität kann zu einer erhöhten Auslastung der `CPUUtilization` Amazon EC2 EC2-Instance führen. Weitere Informationen zu finden Sie `CPUUtilization` unter Instance-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer Amazon EC2 EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn Sie keinen Wert für den `S3BucketName` Parameter angeben, lädt die Automatisierung das Log-Bundle in den standardmäßigen Elastic Beanstalk Amazon S3 S3-Bucket hoch, in AWS-Region dem Sie die Automatisierung ausführen. Das Verzeichnis ist nach der folgenden Struktur benannt:. `elasticbeanstalk-` *`region`* `-` *`accountID`* Die Werte für *`Region`* und *`accountID`* unterscheiden sich je nach Region, in der AWS-Konto Sie die Automatisierung ausführen. Das Protokollpaket wird im `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* Verzeichnis gespeichert. Die Werte für *`EnvironmentID`* und *`InstanceID`* unterscheiden sich je nach Ihrer Elastic Beanstalk Beanstalk-Umgebung und der Amazon EC2 EC2-Instance, von der Sie Logs sammeln.

Standardmäßig verfügt das AWS Identity and Access Management (IAM-) Instance-Profil, das an die Amazon EC2 EC2-Instances der Elastic Beanstalk-Umgebung angehängt ist, über die erforderlichen Berechtigungen, um das Bundle in den standardmäßigen Elastic Beanstalk Amazon S3 S3-Bucket für Ihre Umgebung hochzuladen. Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, muss das der Amazon EC2 EC2-Instance zugeordnete Instance-Profil die `s3:PutObject` Aktionen`s3:GetBucketAcl`, `s3:GetBucketPolicys3:GetBucketPolicyStatus`, und für den angegebenen Amazon S3 S3-Bucket und -Pfad zulassen.

> **Note**
>
> Für diese Automatisierung sind mindestens 500 MB verfügbarer Festplattenspeicher auf dem Amazon Elastic Block Store (Amazon EBS) -Stammvolume erforderlich, das an Ihre Amazon EC2 EC2-Instance angehängt ist. Wenn auf dem Root-Volume nicht genügend Festplattenspeicher verfügbar ist, wird die Automatisierung gestoppt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EnvironmentId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID Ihrer Elastic Beanstalk Beanstalk-Umgebung, aus der Sie das Log-Bundle sammeln möchten.

- InstanceId

  Typ: Zeichenfolge

  (Erforderlich) Die ID der Amazon EC2 EC2-Instance in Ihrer Elastic Beanstalk Beanstalk-Umgebung, aus der Sie das Protokollpaket abrufen möchten.

- S3 BucketName

  Typ: Zeichenfolge

  (Optional) Der Amazon S3 S3-Bucket, in den Sie die archivierten Protokolle hochladen möchten.

- S3 BucketPath

  Typ: Zeichenfolge

  (Optional) Der Amazon S3 S3-Bucket-Pfad, in den Sie das Log-Bundle hochladen möchten. Dieser Parameter wird ignoriert, wenn Sie keinen Wert für den `S3BucketName` Parameter angeben.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

### Dokumentschritte

- `aws:assertAwsResourceProperty`— Bestätigt, dass die Amazon EC2 EC2-Instance, die Sie im `InstanceId` Parameter angeben, von AWS Systems Manager verwaltet wird.

- `aws:assertAwsResourceProperty`— Bestätigt, dass es sich bei der Amazon EC2-Instance, die Sie im `InstanceId` Parameter angeben, um eine Windows Server Instance handelt.
- `aws:runCommand`— Prüft, ob die Instance Teil einer Elastic Beanstalk Beanstalk-Umgebung ist, ob ausreichend Speicherplatz vorhanden ist, um die Protokolle zu bündeln, und ob der Amazon S3 S3-Bucket, in den die Logs hochgeladen werden sollen, öffentlich ist.
- `aws:runCommand`- Sammelt die Protokolldateien und lädt das Archiv in den im `S3BucketName` Parameter angegebenen Amazon S3 S3-Bucket oder in den Standard-Bucket für Ihre Elastic Beanstalk Beanstalk-Umgebung hoch, falls kein Wert angegeben ist.

## AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Beschreibung

Das `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` Runbook ermöglicht die Protokollierung in der von Ihnen angegebenen Umgebung AWS Elastic Beanstalk (Elastic Beanstalk).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- EnvironmentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Elastic Beanstalk Beanstalk-Umgebung, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Protokollierung in der Elastic Beanstalk Beanstalk-Umgebung, die Sie im `EnvironmentId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status der Umgebung ändert. `Ready`
- `aws:executeScript`— Überprüft, ob die Protokollierung in der Elastic Beanstalk Beanstalk-Umgebung aktiviert wurde.

## AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Beschreibung

Das `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` Runbook aktiviert Benachrichtigungen für die von Ihnen angegebene AWS Elastic Beanstalk (Elastic Beanstalk-) Umgebung.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EnvironmentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Elastic Beanstalk Beanstalk-Umgebung, für die Sie Benachrichtigungen aktivieren möchten.
- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon Simple Notification Service (Amazon SNS) -Themas, an das Sie Benachrichtigungen senden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

Dokumentschritte

- aws:executeAwsApi— Aktiviert Benachrichtigungen für die Elastic Beanstalk Beanstalk-Umgebung, die Sie im EnvironmentId Parameter angeben.
- aws:waitForAwsResourceProperty- Wartet darauf, dass sich der Status der Umgebung ändert. Ready
- aws:executeScript— Überprüft, ob Benachrichtigungen für die Elastic Beanstalk Beanstalk-Umgebung aktiviert wurden.

## AWSSupport-TroubleshootElasticBeanstalk

Beschreibung

Das AWSSupport-TroubleshootElasticBeanstalk Runbook hilft Ihnen bei der Behebung der möglichen Gründe, warum sich Ihre AWS Elastic Beanstalk Umgebung im Status „oder“ befindet. Degraded Severe Diese Automatisierung überprüft die folgenden AWS Ressourcen, die mit Ihrer Elastic Beanstalk Beanstalk-Umgebung verknüpft sind:

- Konfigurationsdetails für einen Load Balancer, einen AWS CloudFormation Stack, eine Amazon EC2 Auto Scaling Scaling-Gruppe, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und eine Virtual Private Cloud (VPC).
- Probleme mit der Netzwerkkonfiguration mit den zugehörigen Sicherheitsgruppenregeln, Routing-Tabellen und Netzwerkzugriffskontrolllisten (ACLs), die Ihren Subnetzen zugeordnet sind.
- Überprüft die Konnektivität zu den Elastic Beanstalk Beanstalk-Endpunkten und zum öffentlichen Internetzugang.
- Überprüft den Status des Load Balancers.
- Überprüft den Status der Amazon EC2 EC2-Instances.
- Ruft ein Protokollpaket aus Ihrer Elastic Beanstalk Beanstalk-Umgebung ab und lädt die Dateien optional in. AWS Support

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ApplicationName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name Ihrer Elastic Beanstalk Beanstalk-Anwendung.
- EnvironmentName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name Ihrer Elastic Beanstalk Beanstalk-Umgebung.
- AWSS3UploaderLink

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine URL, die Ihnen zur Verfügung gestellt wurde, AWS Support um das Log-Bundle aus Ihrer Elastic Beanstalk Beanstalk-Umgebung hochzuladen. Diese Option ist nur für Kunden verfügbar, die einen AWS Support Plan erworben und einen Support-Fall eröffnet haben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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*`

Dokumentschritte

- `aws:executeScript`— Überprüft, ob der AWS Identity and Access Management (IAM-) Principal, der die Automatisierung gestartet hat, über die erforderlichen Berechtigungen verfügt, um alle im Runbook definierten Aktionen auszuführen.
- `aws:branch`— Verzweigt den Workflow auf der Grundlage der Ergebnisse des vorherigen Schritts.

- `aws:executeScript`- Sammelt Informationen über die Elastic Beanstalk Beanstalk-Umgebung, einschließlich Load Balancer, AWS CloudFormation Stack, Auto Scaling Scaling-Gruppe, Amazon EC2 EC2-Instances und VPC-Konfiguration.
- `aws:executeScript`- Überprüft die Routentabellen und ACLs, die den Subnetzen in Ihrer VPC zugeordnet sind, auf Probleme mit der Netzwerkkonnektivität.
- `aws:executeScript`- Überprüft die mit Ihren Amazon EC2-Instances verknüpften Sicherheitsgruppenregeln auf Probleme mit der Netzwerkkonnektivität.
- `aws:executeScript`- Überprüft die Statuschecks für die Amazon EC2 EC2-Instances.
- `aws:executeScript`- Generiert einen Link für ein Log-Bundle Ihrer Elastic Beanstalk Beanstalk-Umgebung.
- `aws:executeScript`— Lädt das Protokollpaket hoch in. AWS Support
- `aws:executeScript`- Gibt einen Bericht mit Aktionspunkten aus, der Sie bei der Behebung von Problemen unterstützt, die sich auf den Status Ihrer Elastic Beanstalk Beanstalk-Umgebung auswirken könnten.

# Elastic Load Balancing

AWS Systems Manager Automation stellt vordefinierte Runbooks für Elastic Load Balancing bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- AWS-UpdateAlb-Modus DesyncMitigation
- AWS-UpdateCLB-Modus DesyncMitigation

# AWSConfigRemediation-DropInvalidHeadersForALB

Beschreibung

Das AWSConfigRemediation-DropInvalidHeadersForALB Runbook ermöglicht es dem von Ihnen angegebenen Application Load Balancer, HTTP-Header mit ungültigen Headern zu entfernen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Load Balancers, für den Sie ungültige Header löschen möchten.

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Einstellung „Ungültige Header löschen“ für den Load Balancer, den Sie im Parameter angeben. `LoadBalancerArn`
- `aws:executeScript`— Überprüft, ob die Einstellung „ungültige Header löschen“ auf dem Load Balancer aktiviert wurde, den Sie im Parameter angeben. `LoadBalancerArn`

## AWS-EnableCLBAccessLogs

Beschreibung

Das `AWS-EnableCLBAccessLogs` Runbook ermöglicht Zugriffsprotokolle für einen Classic Load Balancer.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- EmitInterval

  Typ: Ganzzahl

  Gültige Werte: 5 | 60

  Standard: 60

  Beschreibung: (Optional) Das Intervall für die Veröffentlichung der Zugriffsprotokolle in Minuten.

- LoadBalancerNamen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste von Classic Load Balancers, für die Sie Zugriffsprotokolle aktivieren möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3) -Buckets, in dem die Zugriffsprotokolle gespeichert werden.

- S3 BucketPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die logische Hierarchie, die Sie beispielsweise für Ihren Amazon S3 S3-Bucket erstellt haben`my-bucket-prefix/prod`. Wenn das Präfix nicht angegeben wird, wird das Protokoll auf der Bucket-Stammebene platziert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert Zugriffsprotokolle für die Classic Load Balancers, die Sie im `LoadBalancerNames` Parameter angeben.

Ausgaben

Aktiviert CLBAccessLogs. SuccessesLoadBalancers — Liste der Load Balancer-Namen, für die die Zugriffsprotokolle erfolgreich aktiviert wurden.

Aktivieren Sie CLBAccessLogs. FailedLoadBalancers — MapList die Namen der Load Balancer, bei denen die Aktivierung der Zugriffsprotokolle fehlgeschlagen ist, und der Grund für den Fehler.

## `AWS-EnableCLBConnectionDraining`

Beschreibung

Das `AWS-EnableCLBConnectionDraining` Runbook ermöglicht den Verbindungsabbau auf einem Classic Load Balancer (CLB) bis zum angegebenen Timeout-Wert. Connection Drainings ermöglichen es der CLB, Anfragen während der Übertragung zu bearbeiten, die an Instances gestellt werden, deren Registrierung aufgehoben wird oder deren Status nicht korrekt ist. Der angegebene Timeout ist die Zeit, in der Verbindungen aufrechterhalten werden, bevor die Instance als deregistriert gemeldet wird. Weitere Informationen zum Verbindungsabbau auf CLBs finden Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren im Benutzerhandbuch für Classic Load Balancers.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Load Balancers, für den Sie den Verbindungsabbau aktivieren möchten.
- ConnectionTimeout

  Typ: Ganzzahl

  Gültige Werte: 1—3600

  Standard: 300

  Beschreibung: (Erforderlich) Der Wert für das Verbindungs-Timeout für den Load Balancer. Der Timeout-Wert kann zwischen 1 und 3600 Sekunden festgelegt werden.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Dokumentschritte

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): Aktiviert den Verbindungsabbau und legt den angegebenen Timeout-Wert für den von Ihnen angegebenen Load Balancer fest.

- VerifyLoadBalancerConnectionDrainingEnabled(AwsResourceaws:assert-Eigenschaft): Überprüft, ob der Verbindungsabbau für den Load Balancer aktiviert ist.
- VerifyLoadBalancerConnectionDrainingTimeout(AwsResourceaws:assert-Eigenschaft): Überprüft, ob der Wert für das Verbindungstimeout für den Load Balancer dem von Ihnen angegebenen Wert entspricht.

## AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Beschreibung

Das `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` Runbook ermöglicht zonenübergreifendes Load Balancing für den von Ihnen angegebenen Classic Load Balancer (CLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB, für den Sie den zonenübergreifenden Load Balancing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert den zonenübergreifenden Lastenausgleich für den CLB, den Sie im Parameter angeben. `LoadBalancerName`
- `aws:assertAwsResourceProperty`- Überprüft, ob der zonenübergreifende Load Balancing auf dem CLB aktiviert wurde.

## AWSConfigRemediation-EnableELBDeletionProtection

Beschreibung

Das `AWSConfigRemediation-EnableELBDeletionProtection` Runbook aktiviert den Löschschutz für den von Ihnen angegebenen Elastic Load Balancer (ELB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des ELB, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeScript`- Aktiviert den Löschschutz auf dem ELB, den Sie im `LoadBalancerArn` Parameter angeben.

## AWSConfigRemediation-EnableLoggingForALBAndCLB

Beschreibung

Das `AWSConfigRemediation-EnableLoggingForALBAndCLB` Runbook ermöglicht die Protokollierung für den angegebenen AWS Application Load Balancer oder einen Classic Load Balancer (CLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Classic Load Balancer Balancer-Name oder der Application Load Balancer Balancer-ARN.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket-Name.
- S3 BucketPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die logische Hierarchie, die Sie beispielsweise für Ihren Amazon Simple Storage Service (Amazon S3) -Bucket erstellt haben`my-bucket-prefix/prod`. Wenn das Präfix nicht angegeben wird, wird das Protokoll auf der Bucket-Stammebene platziert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeScript`- Aktiviert und überprüft die Protokollierung für den Classic Load Balancer oder den Application Load Balancer.

## AWSSupport-TroubleshootCLBConnectivity

Beschreibung

Das `AWSSupport-TroubleshootCLBConnectivity` Runbook hilft Ihnen bei der Behebung von Verbindungsproblemen zwischen Classic Load Balancer (CLB) und Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Außerdem werden Verbindungsprobleme zwischen einem Client und der CLB überprüft. In diesem Runbook werden auch die Integritätsprüfungen für das CLB überprüft, es wird überprüft, ob die bewährten Methoden befolgt werden, und es wird ein Dashboard zur Problembehebung für Sie erstellt. Optional können Sie die Automatisierungsausgabe in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochladen. Dieses Runbook unterstützt jedoch nicht das Hochladen von Ausgaben in öffentlich zugängliche S3-Buckets. Wir empfehlen, für diese Automatisierung einen temporären S3-Bucket zu erstellen.

> **Important**
>
> Bei der Verwendung dieses Runbooks können Gebühren für das erstellte Dashboard anfallen. Weitere Informationen finden Sie unter CloudWatchAmazon-Preise

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InvestigationType

  Typ: Zeichenfolge

  Gültige Werte: Bewährte Methoden | Verbindungsprobleme | Dashboard zur Fehlerbehebung

  Beschreibung: (Erforderlich) Die Operationen, die das Runbook ausführen soll.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB.
- S3Location

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des S3-Buckets, an den Sie die Automatisierungsergebnisse senden möchten. Öffentlich zugängliche Buckets werden nicht unterstützt. Wenn Ihr S3-Bucket serverseitige Verschlüsselung verwendet, muss der Benutzer oder die Rolle, die diese Automatisierung ausführt, über `kms:GenerateDataKey` Berechtigungen für den AWS KMS Schlüssel verfügen.

- S3 LocationPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie die Automatisierungsausgabe hochladen möchten. *Die Formatausgabe wird im folgenden Format gespeichert: DOC-EXAMPLE-BUCKET/ S3 LocationPrefix/{{}} _ {{automation: InvestigationTypeEXECUTION_ID}} .txt.*

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Überprüft, ob der CLB, den Sie im Parameter angeben, existiert. LoadBalancerName
- aws:branch- Verzweigt auf der Grundlage des für den Parameter angegebenen Werts. InvestigationType
- aws:executeScript- Führt Konnektivitätsprüfungen zum CLB durch.
- aws:executeScript— Überprüft, ob die CLB-Konfiguration den Best Practices von Elastic Load Balancing entspricht.
- aws:executeScript- Erstellt ein CloudWatch Amazon-Dashboard für Ihr CLB.
- aws:executeScript- Erstellt eine Textdatei mit den Ergebnissen der Automatisierung und lädt sie in den Amazon S3 S3-Bucket hoch, den Sie im S3Location Parameter angeben.

Ausgaben

RunBestPraktiken. Zusammenfassung

RunConnectivityPrüfungen. Zusammenfassung

CreateTroubleshootingDashboard.Ausgabe

UploadOutputTOS3. Ausgabe

## AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Beschreibung

Das `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` Runbook aktiviert den zonenübergreifenden Load Balancing für den von Ihnen angegebenen Network Load Balancer (NLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des NLB, für den Sie zonenübergreifendes Load Balancing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert zonenübergreifendes Load Balancing für den NLB, den `LoadBalancerArn` Sie im Parameter angeben.
- `aws:executeScript`- Überprüft, ob der zonenübergreifende Load Balancing auf dem NLB aktiviert wurde.

## AWS-UpdateAlb-Modus DesyncMitigation

Beschreibung

Das `AWS-UpdateALBDesyncMitigationMode` Runbook aktualisiert den Desync-Minimierungsmodus auf einem Application Load Balancer (ALB) auf den angegebenen Mitigationsmodus. Der Desync-Minimationsmodus bestimmt, wie der Load Balancer Anfragen verarbeitet, die ein Sicherheitsrisiko für Ihre Anwendung darstellen könnten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des ALB, dessen Desync-Minderungsmodus Sie ändern möchten.

- DesyncMitigationModus

  Typ: Zeichenfolge

  Gültige Werte: überwachen | defensiv | striktesten

  Beschreibung: (Erforderlich) Der Schadensbegrenzungsmodus, den die ALB verwenden soll. Informationen zu Desync-Minimationsmodi finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- VerifyLoadBalancerType (AwsResourceaws:assert-Eigenschaft) — Überprüft, ob der für den `LoadBalancerArn` Eingabeparameter angegebene Wert für einen Application Load Balancer bestimmt ist, bevor mit dem nächsten Schritt fortgefahren wird.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) — Aktualisiert den ALB, sodass er den angegebenen Wert verwendet. `DesyncMitigationMode`

- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) — Überprüft, ob der Desync-Minderungsmodus für das Ziel-ALB aktualisiert wurde.

Ausgaben

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Nachrichten-Payload des Skripts, das die Änderung an Ihrem ALB verifiziert.

## AWS-UpdateCLB-Modus DesyncMitigation

Beschreibung

Das `AWS-UpdateCLBDesyncMitigationMode` Runbook aktualisiert den Desync-Minimierungsmodus auf einem Classic Load Balancer (CLB) auf den angegebenen Mitigationsmodus. Der Desync-Minimationsmodus bestimmt, wie der Load Balancer Anfragen verarbeitet, die ein Sicherheitsrisiko für Ihre Anwendung darstellen könnten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB, für den Sie den Desync-Minimierungsmodus ändern möchten.

- DesyncMitigationModus

  Typ: Zeichenfolge

  Gültige Werte: überwachen | defensiv | striktesten

  Beschreibung: (Erforderlich) Der Schadensbegrenzungsmodus, den die CLB verwenden soll. Informationen zu Desync-Minimationsmodi finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Dokumentschritte

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) — Aktualisiert den CLB so, dass er den angegebenen Wert verwendet. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) — Überprüft, ob der Desync-Minderungsmodus für die Ziel-CLB aktualisiert wurde.

### Ausgaben

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Payload der Nachricht des Skripts, das die Änderung an Ihrem CLB verifiziert.

# Amazon EMR

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon EMR bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## `AWSSupport-AnalyzeEMRLogs`

Beschreibung

Dieses Runbook hilft bei der Identifizierung von Fehlern bei der Ausführung eines Jobs auf einem Amazon EMR-Cluster. Das Runbook analysiert eine Liste definierter Protokolle im Dateisystem und sucht nach einer Liste mit vordefinierten Schlüsselwörtern. Diese Protokolleinträge werden verwendet, um Amazon CloudWatch Events-Ereignisse zu erstellen, sodass Sie auf der Grundlage der Ereignisse alle erforderlichen Maßnahmen ergreifen können. Optional veröffentlicht das Runbook Protokolleinträge in der Amazon CloudWatch Logs-Protokollgruppe Ihrer Wahl. Dieses Runbook sucht derzeit in Protokolldateien nach den folgenden Fehlern und Mustern:

- container_out_of_memory — Der YARN-Container hat nicht mehr genügend Speicher, die Ausführung des Jobs kann fehlschlagen.
- yarn_nodemanager_health: Der CORE- oder TASK-Knoten hat nur noch wenig Speicherplatz zur Verfügung und er kann keine Aufgaben ausführen.
- node_state_change: Der CORE- oder TASK-Knoten ist vom MASTER-Knoten nicht erreichbar.
- step_failure: Ein EMR-Schritt ist fehlgeschlagen.
- no_core_nodes_running: Derzeit laufen keine CORE-Knoten, der Cluster ist fehlerhaft.
- hdfs_missing_blocks: Es fehlen HDFS-Blöcke, was zu Datenverlust führen könnte.
- hdfs_high_util: Die HDFS-Auslastung ist hoch, was sich auf Jobs und die Clusterintegrität auswirken kann.
- instance_controller_restart: Der Instance-Controller-Prozess wurde neu gestartet. Dieser Prozess ist für die Clusterintegrität unerlässlich.

- instance_controller_restart_legacy: Der Instance-Controller-Prozess wurde neu gestartet. Dieser Prozess ist für die Clusterintegrität unerlässlich.
- high_load: Es wurde ein hoher Lastdurchschnitt erkannt. Dies kann sich auf die Berichterstattung über den Knotenstatus auswirken oder zu Timeouts oder Verlangsamungen führen.
- yarn_node_blacklisted: Der CORE- oder TASK-Knoten wurde von YARN für die Ausführung von Aufgaben gesperrt.
- yarn_node_lost: Der CORE- oder TASK-Knoten wurde von YARN als LOST markiert, mögliche Verbindungsprobleme.

Instanzen, die mit dem von Ihnen angegebenen verknüpft sind`ClusterID`, müssen von verwaltet werden. AWS Systems Manager Sie können diese Automatisierung einmal ausführen, die Automatisierung so planen, dass sie in einem bestimmten Zeitintervall ausgeführt wird, oder einen zuvor durch eine Automatisierung erstellten Zeitplan entfernen. Dieses Runbook unterstützt die Amazon EMR-Release-Versionen 5.20 bis 6.30.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterID

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des Clusters, dessen Knotenprotokolle Sie analysieren möchten.

- Operation

  Typ: Zeichenfolge

  Gültige Werte: Einmal ausführen | Zeitplan | Zeitplan entfernen

  Beschreibung: (Erforderlich) Der Vorgang, der auf dem Cluster ausgeführt werden soll.

- IntervalTime

  Typ: Zeichenfolge

  Gültige Werte: 5 Minuten | 10 Minuten | 15 Minuten

  Beschreibung: (Optional) Die Zeitspanne zwischen der Ausführung der Automatisierung. Dieser Parameter ist nur anwendbar, wenn Sie ihn `Schedule` für den `Operation` Parameter angeben.

- LogToCloudWatchLogs

  Typ: Zeichenfolge

  Gültige Werte: ja | nein

  Beschreibung: (Optional) Wenn Sie `yes` für den Wert dieses Parameters einen Wert angeben, erstellt die Automatisierung eine CloudWatch Logs-Protokollgruppe mit dem im `CloudWatchLogGroup` Parameter angegebenen Namen, in der alle übereinstimmenden Protokolleinträge gespeichert werden.

- CloudWatchLogGroup

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der CloudWatch Logs-Log-Gruppe, in der Sie alle passenden Logeinträge speichern möchten. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

- CreateLogInsightsDashboard

  Typ: Zeichenfolge

Gültige Werte: ja | nein

Beschreibung: (Optional) Wenn Sie dies angebenyes, wird das CloudWatch Dashboard erstellt, sofern es noch nicht vorhanden ist. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

- CreateMetricFiltert

  Typ: Zeichenfolge

  Gültige Werte: ja | nein

  Beschreibung: (Optional) Geben Sie an, `yes` ob Sie Metrikfilter für die Protokollgruppe CloudWatch Logs erstellen möchten. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeAwsApi- Sammelt Informationen über den im Parameter angegebenen Amazon EMR-Cluster. ClusterID
- aws:branch— Verzweigungen auf der Grundlage von Eingaben.
  - Wenn die angegebene Operation Run Once oder istSchedule:
    - aws:assertAwsResourceProperty- Überprüft, ob der Cluster verfügbar ist.
    - aws:executeAwsApi- Sammelt die IDs aller Instanzen, die im Cluster ausgeführt werden.
    - aws:assertAwsResourceProperty- Überprüft, ob der SSM-Agent auf allen Instanzen im Cluster ausgeführt wird.
    - aws:branch- Verzweigt je nachdem, ob Sie angegeben haben, dass die Automatisierung einmal oder nach einem Zeitplan ausgeführt werden soll.
      - Wenn der bereitgestellte Vorgang wie folgt lautetRun Once:
        - aws:branch- Verzweigt auf der Grundlage des im LogToCloudWatchLogs Parameter angegebenen Werts.

- Wenn `LogToCloudWatchLogs` der Wert ist`yes`:
  - `aws:executeScript`- Prüft, ob eine CloudWatch Logs-Log-Gruppe mit dem im Parameter angegebenen Namen `CloudWatchLogGroup` bereits existiert. Wenn nicht, wird die Gruppe mit dem angegebenen Namen erstellt.
  - `aws:branch`- Verzweigt auf der Grundlage des im `CreateMetricFilters` Parameter angegebenen Werts.
    - Wenn `CreateMetricFilters` der Wert ist`yes`:
      - `aws:executeAwsApi`- Für jeden metrischen Filter werden 12 Schritte ausgeführt
      - `aws:branch`- Verzweigungen, die auf dem im `CreateLogInsightsDashboard` Parameter angegebenen Wert basieren.
        - Wenn `CreateLogInsightsDashboard` der Wert ist`yes`:
          - `aws:executeAwsApi`- Erstellt ein CloudWatch Dashboard mit demselben Namen, der im `CloudWatchLogGroup` Parameter angegeben ist, falls es noch nicht existiert.
        - Wenn `CreateLogInsightsDashboard` der Wert ist`no`:
          - `aws:runCommand`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
    - Wenn `CreateMetricFilters` der Wert ist`no`:
      - `aws:branch`- Verzweigt auf der Grundlage des im `CreateLogInsightsDashboard` Parameter angegebenen Werts.
        - Wenn `CreateLogInsightsDashboard` der Wert ist`yes`:
          - `aws:executeAwsApi`- Erstellt ein CloudWatch Dashboard mit demselben Namen, der im `CloudWatchLogGroup` Parameter angegeben ist, falls es noch nicht existiert.
        - Wenn `CreateLogInsightsDashboard` der Wert ist`no`:
          - `aws:runCommand`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
- Wenn `LogToCloudWatchLogs` der Wert ist`no`:
  - `aws:executeAwsApi`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
- Wenn die bereitgestellte Operation wie folgt lautet`Schedule`:

    - `aws:createStack`— Erstellt ein EventBridge Amazon-Ereignis, das auf dieses Runbook abzielt.
- Wenn die angegebene Operation wie folgt lautet`Remove Schedule`:
    - `aws:executeAwsApi`- Überprüft, ob ein Zeitplan für den Cluster existiert.
    - `aws:deleteStack`- Löscht den Zeitplan.

Ausgaben

GetClusterInformationen. ClusterName

GetClusterInformationen. ClusterState

ListingClusterinstanzen.instanceIds

CreatingScheduleCloudFormationStapel. StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExistiert.Ausgabe

FindLogPatternOnEMR-Knoten. CommandId

## `AWSSupport-DiagnoseEMRLogsWithAthena`

Beschreibung

Das `AWSSupport-DiagnoseEMRLogsWithAthena` Runbook hilft bei der Diagnose von Amazon EMR-Protokollen mithilfe von Amazon Athena in Integration mit AWS Glue Data Catalog. Amazon Athena wird verwendet, um die Amazon EMR-Protokolldateien nach Containern, Knotenprotokollen oder beidem abzufragen, mit optionalen Parametern für bestimmte Datumsbereiche oder schlüsselwortbasierte Suchen.

Das Runbook kann automatisch den Amazon EMR-Protokollspeicherort für einen vorhandenen Cluster abrufen, oder Sie können den Amazon S3 S3-Protokollspeicherort angeben. Um die Protokolle zu analysieren, geht das Runbook wie folgt vor:

- Erstellt eine AWS Glue Datenbank und führt Amazon Athena Data Definition Language (DDL) - Abfragen am Amazon S3-Protokollspeicherort von Amazon EMR aus, um Tabellen für Cluster-Protokolle und eine Liste bekannter Probleme zu erstellen.

- Führt DML-Abfragen (Data Manipulation Language) aus, um in den Amazon EMR-Protokollen nach bekannten Problemmustern zu suchen. Die Abfragen geben eine Liste der erkannten Probleme, deren Anzahl und die Anzahl der übereinstimmenden Keywords pro Amazon S3 S3-Dateipfad zurück.
- Die Ergebnisse werden in einen Amazon S3 S3-Bucket hochgeladen, den Sie unter dem Präfix angeben`saw_diagnose_EMR_known_issues`.
- Das Runbook gibt die Amazon Athena Athena-Abfrageergebnisse zurück und hebt Ergebnisse, Empfehlungen und Verweise auf Artikel aus dem Amazon Knowledge Center (KC) hervor, die aus einer vordefinierten Untergruppe stammen.
- Nach Abschluss oder Fehlschlag werden die AWS Glue Datenbank und die Dateien mit bekannten Problemen, die in den Amazon S3 S3-Bucket hochgeladen wurden, gelöscht.

Wie funktioniert das?

`AWSSupport-DiagnoseEMRLogsWithAthena`Sie führen mithilfe von Amazon Athena Analysen von Amazon EMR-Protokollen durch, um Fehler zu erkennen und Ergebnisse, Empfehlungen und relevante Knowledge Center-Artikel hervorzuheben.

Das Runbook führt die folgenden Schritte aus:

- Rufen Sie den Amazon EMR-Cluster-Protokollstandort mithilfe der Cluster-ID ab oder geben Sie den Amazon S3 S3-Standort ein, um den Speicherort und die Größe des Protokolls abzurufen.
- Geben Sie eine Schätzung der Athena-Kosten auf der Grundlage der Größe des Protokollstandorts an.
- Holen Sie sich die Genehmigung zum Fortfahren, indem Sie die Genehmigung von den zuständigen IAM-Prinzipalen einholen, bevor Sie Athena-Abfragen ausführen und mit den nächsten Schritten fortfahren.
- Laden Sie bekannte Probleme in den angegebenen Amazon S3 S3-Bucket hoch, erstellt eine AWS Glue Datenbank und Tabellen.
- Führen Sie Athena-Abfragen an den Amazon EMR-Protokolldaten aus. Abfragen können nach Datumsbereich, Schlüsselwörtern oder beiden Kriterien suchen oder auf der Grundlage der bereitgestellten Eingaben ohne Filter ausgeführt werden.
- Analysieren Sie die Ergebnisse, um Ergebnisse, Empfehlungen und relevante KC-Artikel hervorzuheben.
- Ausgabelinks für Amazon Athena DML-Abfrageergebnisse.

- Bereinigen Sie die Umgebung, indem Sie erstellte Datenbanken, Tabellen und hochgeladene bekannte Probleme entfernen.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

- Athena: Ausführung GetQuery
- Athena: Hinrichtung StartQuery
- Athena: Aussage GetPrepared
- athena: Aussage CreatePrepared
- Kleber: GetDatabase
- kleben: CreateDatabase
- kleben: DeleteDatabase
- kleben: CreateTable
- kleben: GetTable
- kleben: DeleteTable
- elastisches MapReduce: DescribeCluster
- s3: ListBucket
- s3: GetBucket Versionierung
- s3: Versionen ListBucket
- s3: GetBucket PublicAccess Blockieren
- s3: GetBucket PolicyStatus
- s3: GetObject
- s3: GetBucket Standort

- Preisgestaltung: GetProducts
- Preisgestaltung: GetAttribute Werte
- Preisgestaltung: DescribeServices
- Preisgestaltung: ListPrice Listen

> **Important**
>
> Um den Zugriff nur auf die Ressourcen zu beschränken, die für diese Automatisierung benötigt werden, fügen Sie der IAM-Rolle, die dem SSM-Dienst vertraut, die folgende Richtlinie hinzu. Ersetzen Sie Partition, Region und Konto durch die entsprechenden Werte für die Partition, Region und Kontonummer, auf der das Runbook ausgeführt wird.

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie im AWS Systems Manager Bereich Dokumente zu LogsWith -DiagnoseMr Athena. AWSSupport
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - ClusterID (erforderlich):

     Die Amazon EMR-Cluster-ID.
   - S3 LogLocation (fakultativ):

     Der Amazon S3 S3-Speicherort für Amazon EMR-Protokolle. Geben Sie die URL des Amazon S3 S3-Speicherorts im Path-Stil ein, zum Beispiel:. `s3://mybucket/myfolder/j-1K48XXXXXXHCB/` Geben Sie diesen Parameter an, wenn der Amazon EMR-Cluster für mehr als `30` Tage beendet wurde.
   - S3 BucketName (erforderlich):

Der Amazon S3 S3-Bucket-Name zum Hochladen einer Liste bekannter Probleme und der Ausgabe von Amazon Athena Athena-Abfragen. Für den Bucket sollte Block Public Access aktiviert sein und sich in derselben AWS Region und demselben Konto wie der Amazon EMR-Cluster befinden.

- Genehmiger (erforderlich):

  Die Liste der AWS authentifizierten Principals, die die Aktion entweder genehmigen oder ablehnen können. Sie können Prinzipale angeben, indem Sie eines der folgenden Formate verwenden: Benutzername, Benutzer-ARN, IAM-Rollen-ARN oder IAM Assume Role ARN. Die maximale Anzahl an Genehmigern ist 10.

- FetchNodeLogsOnly (Optional):

  Wenn auf gesetzt`true`, diagnostiziert die Automatisierung die Protokolle des Amazon EMR-Anwendungscontainers. Der Standardwert ist `false`.

- FetchContainersLogsOnly (Fakultativ):

  Wenn auf gesetzt`true`, diagnostiziert die Automatisierung die Amazon EMR-Container-Protokolle. Der Standardwert ist `false`.

- EndSearchDate (Fakultativ):

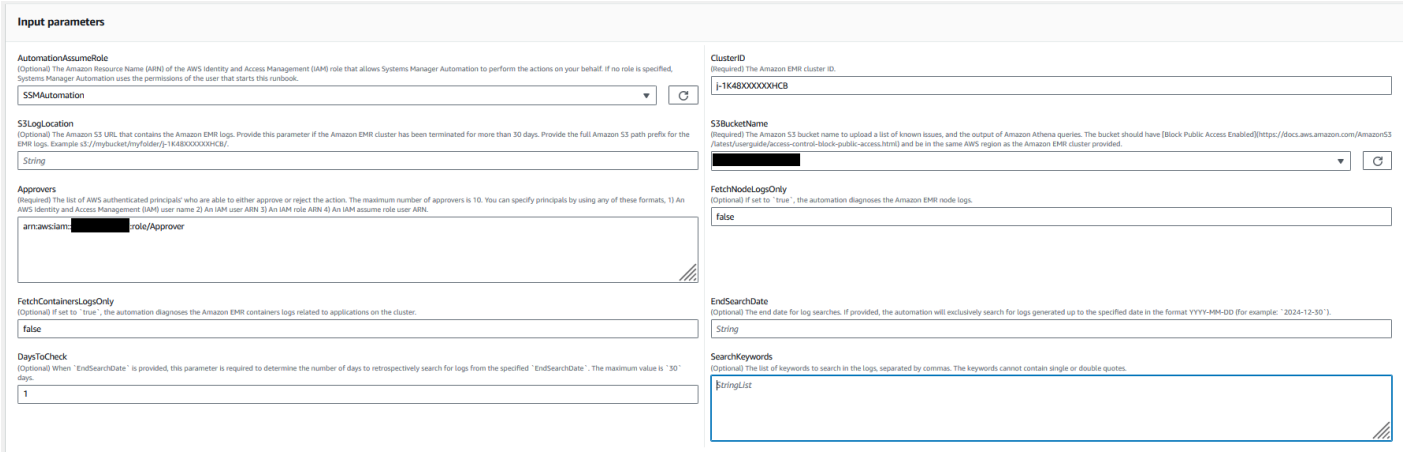
  Das Enddatum für Protokollsuchen. Falls angegeben, sucht die Automatisierung ausschließlich nach Protokollen, die bis zum angegebenen Datum im Format YYYY-MM-DD generiert wurden (zum Beispiel:). `2024-12-30`

- DaysToCheck (Fakultativ):

  Wenn angegeben, `EndSearchDate` ist dieser Parameter erforderlich, um die Anzahl der Tage zu bestimmen, für die rückwirkend nach Protokollen aus den angegebenen Daten gesucht werden soll. `EndSearchDate` Der Höchstwert beträgt `30` Tage. Der Standardwert ist `1`.

- SearchKeywords (Fakultativ):

  Die Liste der Schlüsselwörter, nach denen in den Protokollen gesucht werden soll, getrennt durch Kommas. Die Schlüsselwörter dürfen keine einfachen oder doppelten Anführungszeichen enthalten.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - erhaltenLogLocation:

     Ruft den Amazon S3 S3-Protokollspeicherort ab, indem die angegebene Amazon EMR-Cluster-ID abgefragt wird. Wenn die Automatisierung den Protokollspeicherort nicht anhand der Amazon EMR-Cluster-ID abfragen kann, verwendet das Runbook den `S3LogLocation` Eingabeparameter.
   - ZweigprotokollOnValid:

     Überprüft den Speicherort der Amazon EMR-Protokolle. Wenn der Standort gültig ist, fahren Sie mit der Schätzung der potenziellen Kosten von Amazon Athena bei der Ausführung von Abfragen in den Amazon EMR-Protokollen fort.
   - Schätzung: AthenaCosts

     Ermittelt die Größe der Amazon EMR-Protokolle und bietet eine Kostenschätzung für die Ausführung von Athena-Scans für den Protokolldatensatz. Für nicht kommerzielle Regionen (keine AWS Partitionen) wird in diesem Schritt lediglich die Protokollgröße angegeben, ohne die Kosten zu schätzen. Die Kosten können anhand der Athena-Preisdokumentation in der angegebenen Region berechnet werden.
   - Automatisierung genehmigen:

     Wartet auf die Genehmigung durch die designierten IAM-Prinzipale, um mit den nächsten Schritten der Automatisierung fortzufahren. Die Genehmigungsbenachrichtigung enthält die geschätzten Kosten für den Amazon Athena Athena-Scan in den Amazon EMR-Protokollen sowie Einzelheiten zu den Ressourcen, die durch die Automatisierung bereitgestellt werden.

- Anfragen hochladen: KnownIssues ExecuteAthena

  Lädt die vordefinierten bekannten Probleme in den im `S3BucketName` Parameter angegebenen Amazon S3 S3-Bucket hoch. Erstellt eine AWS Glue Datenbank und Tabellen. Führt Amazon Athena Athena-Abfragen in der AWS Glue Datenbank auf der Grundlage der Eingabeparameter aus.

- Status abrufenQueryExecution:

  Wartet, bis die Ausführung der Amazon Athena Athena-Abfrage im `SUCCEEDED` Status ist. Die Amazon Athena DML-Abfrage sucht nach Fehlern und Ausnahmen in Amazon EMR-Clusterprotokollen.

- analysieren: AthenaResults

  Analysiert die Amazon Athena Athena-Ergebnisse, um Ergebnisse, Empfehlungen und Knowledge Center-Artikel (KC) bereitzustellen, die aus einem vordefinierten Satz von Zuordnungen stammen.

- Holen Sie sich Query1: AnalyzeResults ExecutionStatus

  Wartet, bis die Abfrageausführung im Status ist. `SUCCEEDED` Die Amazon Athena DML-Abfrage analysiert die Ergebnisse der vorherigen DML-Abfrage. Diese Analyseabfrage gibt übereinstimmende Ausnahmen mit Lösungen und KC-Artikeln zurück

- Holen Sie sich AnalyzeResults Query2ExecutionStatus:

  Wartet, bis die Abfrageausführung im Status ist. `SUCCEEDED` Die Amazon Athena DML-Abfrage analysiert die Ergebnisse der vorherigen DML-Abfrage. Diese Analyseabfrage gibt eine Liste der Ausnahmen/Fehler zurück, die in jedem Amazon S3 S3-Protokollpfad erkannt wurden.

- Nachricht drucken: AthenaQueries

  Druckt Links für die Ergebnisse der Amazon Athena DML-Abfragen.

- Ressourcen bereinigen:

  Bereinigt Ressourcen, indem die erstellte AWS Glue Datenbank und Dateien mit bekannten Problemen gelöscht werden, die im Amazon EMR-Protokoll-Bucket erstellt wurden.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt „Ausgaben“ die detaillierten Ergebnisse der Ausführung:

   Output bietet drei Links für Athena-Abfrageergebnisse:

- Liste aller Fehler und häufig aufgetretenen Ausnahmen, die in den Amazon EMR-Clusterprotokollen gefunden wurden, zusammen mit den entsprechenden Protokollspeicherorten (Amazon S3 S3-Präfix).
- Zusammenfassung der eindeutigen bekannten Ausnahmen, die in den Amazon EMR-Protokollen abgeglichen wurden, zusammen mit empfohlenen Lösungen und KC-Artikeln zur Unterstützung bei der Fehlerbehebung.
- Details darüber, wo bestimmte Fehler und Ausnahmen in den Amazon S3 S3-Protokollpfaden auftreten, um weitere Diagnosen zu unterstützen.


Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Weitere Informationen finden Sie unter Problembehandlung bei Amazon EMR-Clustern

# OpenSearch Amazon-Dienst

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon OpenSearch Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

## AWSConfigRemediation-DeleteOpenSearchDomain

Beschreibung

Das `AWSConfigRemediation-DeleteOpenSearchDomain` Runbook löscht die angegebene Amazon OpenSearch Service-Domain mithilfe der DeleteDomainAPI.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- DomainName

  Typ: Zeichenfolge

  Zulässige Werte: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

  Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie löschen möchten.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Dokumentschritte

- `aws:executeScript`- Akzeptiert den Amazon OpenSearch Service-Domainnamen als Eingabe, löscht ihn und verifiziert den Löschvorgang.

## AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Beschreibung

Das `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` Runbook wird `EnforceHTTPS` auf einer bestimmten Amazon OpenSearch Service-Domain mithilfe der UpdateDomainConfig-API aktiviert.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- DomainName

Typ: Zeichenfolge

Zulässige Werte: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie verwenden möchten, um HTTPS durchzusetzen.

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Dokumentschritte

- `aws:executeScript`— Aktiviert die `EnforceHTTPS` Endpunktoption auf der Amazon OpenSearch Service-Domain, die Sie im `DomainName` Parameter angeben.

## AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Beschreibung

Das `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` Runbook aktualisiert die Sicherheitsgruppenkonfiguration auf einer bestimmten Amazon OpenSearch Service-Domain mithilfe der UpdateDomainConfig-API.

> **Note**
>
> AWS Sicherheitsgruppen können nur auf Amazon OpenSearch Service-Domains angewendet werden, die für Amazon Virtual Private Cloud (VPC) Access konfiguriert sind, und nicht auf Amazon OpenSearch Service-Domains, die für Public Access konfiguriert sind.

## Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- DomainName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie zur Aktualisierung von Sicherheitsgruppen verwenden möchten.
- SecurityGroupListe

  Typ: StringList

  Beschreibung: (Erforderlich) Die Sicherheitsgruppen-IDs, die Sie der Amazon OpenSearch Service-Domain zuweisen möchten.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Dokumentschritte

- `aws:executeScript`- Aktualisiert die Sicherheitsgruppenkonfiguration auf der Amazon OpenSearch Service-Domain, die Sie im `DomainName` Parameter angeben.

## `AWSSupport-TroubleshootOpenSearchRedYellowCluster`

Beschreibung

`AWSSupport-TroubleshootOpenSearchRedYellowCluster` Automation Runbook wird verwendet, um die Ursache für den Zustand roter oder gelber Cluster zu identifizieren und Sie durch das Zurücksetzen des Clusters auf Grün zu führen.

Wie funktioniert es?

Das Runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` hilft Ihnen bei der Behebung der Ursache eines roten oder gelben Clusters und bietet die nächsten Schritte zur Behebung dieses Problems, indem es die Cluster-Konfiguration und die Ressourcenauslastung analysiert.

Das Runbook führt die folgenden Schritte aus:

- Ruft die DescribeDomain API für die Zieldomäne auf, um die Cluster-Konfiguration abzurufen.
- Prüft, ob die OpenSearch Service-Domain internetbasiert (öffentlich) oder Amazon Virtual Private Cloud (VPC) ist.
- Erstellt je nach Clusterkonfiguration eine öffentliche oder Amazon-VPC-basierte AWS Lambda Funktion. Hinweis: Die Lambda-Funktion enthält den Fehlerbehebungscode, der die OpenSearch

Service-APIs für den Cluster ausführt, um festzustellen, warum sich der Cluster im roten oder gelben Zustand befindet.
- Löscht die Lambda-Funktion.
- Zeigt die durchgeführten Prüfungen und die nächsten empfohlenen Schritte zur Behebung des roten oder gelben Clusterproblems an.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Der `LambdaExecutionRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

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

Übersicht über die `LambdaExecutionRole` Richtlinie:

Im Folgenden finden Sie ein Beispiel für die Ausführungsrolle (AWS Identity and Access Management (IAM)-Rolle einer Lambda-Funktion, die der Funktion die Berechtigung erteilt, auf die für dieses Runbook erforderlichen AWS Services und Ressourcen zuzugreifen. Weitere Informationen finden Sie unter Lambda-Ausführungsrolle.

> **Note**
>
> Die `ec2:DescribeNetworkInterfaces`, und `ec2:DeleteNetworkInterface` sind nur erforderlich`ec2:CreateNetworkInterface`, wenn Ihr OpenSearch Service-Cluster Amazon-VPC-basiert ist, damit die Lambda-Funktion die Amazon-VPC-Netzwerkschnittstellen erstellen und verwalten kann. Weitere Informationen finden Sie unter Verbinden ausgehender Netzwerke mit Ressourcen in einer Amazon VPC und Lambda-Ausführungsrolle.

```
        {
            "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"
                }

            ]
        }
```

## Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

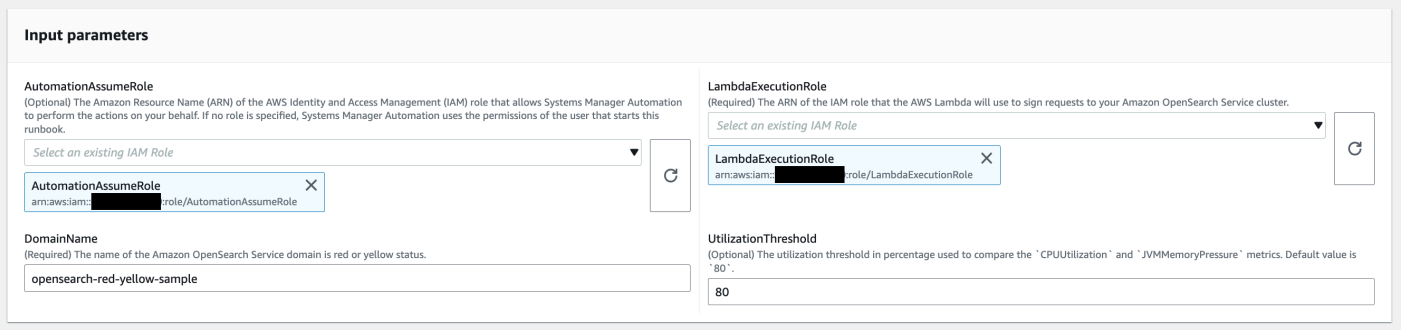
1. Navigieren Sie in der AWSSupport-TroubleshootOpenSearchRedYellowCluster AWS Systems Manager Konsole zur -.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - LambdaExecutionRole (Erforderlich):

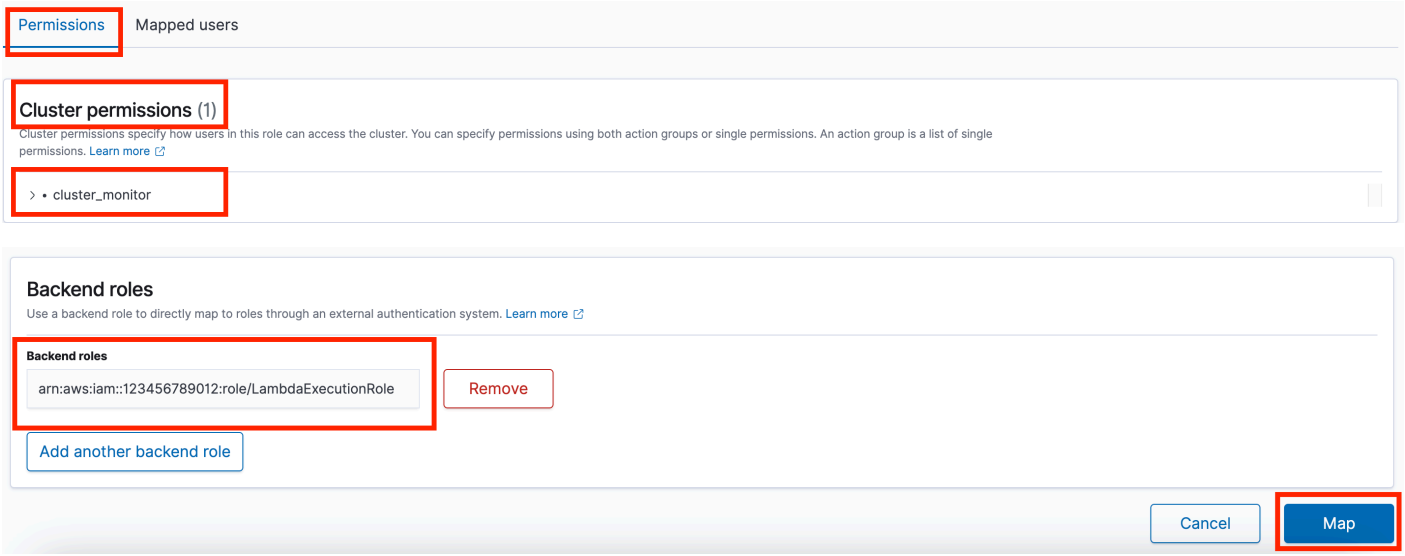
     Der ARN der IAM-Rolle, die Lambda zum Signieren von Anforderungen an Ihren Amazon-OpenSearch Service-Cluster verwendet.
   - DomainName (Erforderlich):

     Der Name der OpenSearch Service-Domain mit dem Zustandsstatus eines roten oder gelben Clusters.
   - UtilizationThreshold (Optional):

     Der Prozentsatz des Auslastungsschwellenwerts, der zum Vergleichen der CPUUtilization- und JVM-MemoryPressure Metriken verwendet wird. Der Standardwert ist 80.




4. Wenn Sie die differenzierte Zugriffskontrolle auf einem - OpenSearch Service-Cluster aktiviert haben, stellen Sie sicher, dass der `LambdaExecutionRole` Rollen-ARN einer Rolle mit mindestens -`cluster_monitor`Berechtigung zugeordnet ist.




5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - GetClusterConfiguration:

     Ruft die OpenSearch Service-Cluster-Konfiguration ab.
   - Erstellen von AWSLambdaFunctionStack:

     Erstellt eine temporäre Lambda-Funktion in Ihrem Konto mit AWS CloudFormation. Die Lambda-Funktion wird verwendet, um die OpenSearch Service-APIs auszuführen.
   - WaitForAWSLambdaFunctionStack:

     Wartet, bis der CloudFormation Stack abgeschlossen ist.
   - GetClusterMetricsFromCloudWatch:

     Ruft die Cluster-bezogenen Metriken von Amazon , CloudWatch ClusterStatus CPUUtilization und JVM MemoryPressure OpenSearch Service und das Erstellungsdatum ab.
   - RunOpenSearchAPIs:

     Verwendet die Lambda-Funktion, um die OpenSearch Service-APIs aufzurufen und die Cluster-Metrikdaten zu analysieren, um die Ursache für den roten oder gelben Clusterstatus zu diagnostizieren.
   - Löschen von AWSLambdaFunctionStack:

     Löscht die durch diese Automatisierung in Ihrem Konto erstellte Lambda-Funktion.

8. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten.
   - RootCause:

     Bietet einen Überblick über die identifizierte Ursache für den Clusterzustand im roten oder gelben Zustand.
   - IssueDescription:

     Enthält Details dazu, warum sich der Cluster im roten oder gelben Zustand befindet, und mögliche Schritte, um den Cluster wieder in den grünen Zustand zu versetzen.

Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

AWS -Servicedokumentation

- Weitere Informationen finden Sie unterFehlerbehebung bei Amazon OpenSearch Service

## AWSSupport-TroubleshootOpenSearchHighCPU

Beschreibung

Das -`AWSSupport-TroubleshootOpenSearchHighCPU`Runbook bietet eine automatisierte Lösung zum Sammeln von Diagnosedaten aus einer Amazon- OpenSearch Service-Domain zur Behebung hoher CPU-Probleme.

Wie funktioniert es?

Das `AWSSupport-TroubleshootOpenSearchHighCPU` Runbook hilft bei der Behebung einer hohen CPU-Auslastung in der Amazon- OpenSearch Service-Domain.

Das Runbook führt die folgenden Schritte aus:

- Führt die DescribeDomain API für die bereitgestellte Amazon- OpenSearch Service-Domain aus, um die Cluster-Metadaten abzurufen.
- Prüft AWS CloudFormation, ob die Amazon- OpenSearch Service-Domain öffentlich oder Amazon-VPC-basiert ist und mithilfe von eine öffentliche oder Amazon-VPC-basierte AWS Lambda Funktion erstellt.
- Die Lambda-Funktion ruft Diagnosedaten aus den Amazon- OpenSearch Service-Domains ab.
- Verwendet einen - AWS Step Functions Zustandsautomaten, um mehrere Lambda-Funktionsausführungen zu orchestrieren und umfassendere Daten zu sammeln.
- Speichert die gesammelten Daten standardmäßig 24 Stunden lang in einer Amazon- CloudWatch Protokollgruppe.
- Löscht die erstellten Ressourcen mit Ausnahme der CloudWatch Protokollgruppe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Der LambdaExecutionRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

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

- `logs:PutLogEvents`

Die Lambda-Ausführungsrolle gewährt der Funktion die Berechtigung, auf die für dieses Runbook erforderlichen AWS Services und Ressourcen zuzugreifen. Weitere Informationen finden Sie unter Lambda-Ausführungsrolle.

> **Note**
>
> Die `ec2:DescribeNetworkInterfaces`, und `ec2:DeleteNetworkInterface` sind nur erforderlich`ec2:CreateNetworkInterface`, wenn Ihr OpenSearch Service-Cluster Amazon-VPC-basiert ist, damit die Lambda-Funktion die Amazon-VPC-Netzwerkschnittstellen erstellen und verwalten kann. Weitere Informationen finden Sie unter Verbinden ausgehender Netzwerke mit Ressourcen in einer Amazon VPC und Lambda-Ausführungsrolle.

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie in der - AWS Systems Manager Konsole zur AWSSupport-TroubleshootOpenSearchHighCPU.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - DomainName (Erforderlich):

     Der Name der Amazon- OpenSearch Service-Domäne, die Sie bei hohen CPU-Problemen beheben möchten.
   - LambdaExecutionRoleForOpenSearch (Erforderlich):

     Der ARN der IAM-Rolle, die an die Lambda-Funktion angehängt werden soll. Die Lambda-Funktion verwendet die Anmeldeinformationen dieser Rolle, um Anforderungen an die Amazon-

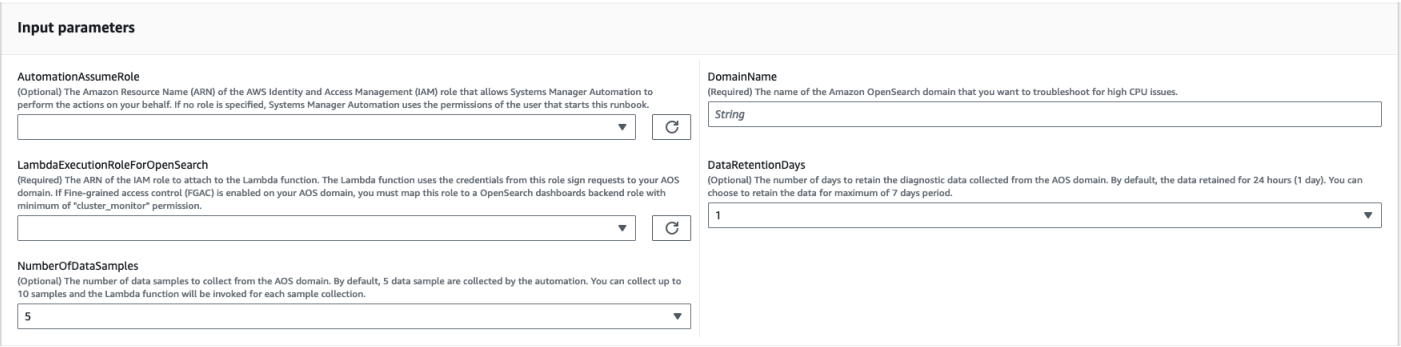
OpenSearch Service-Domain zu signieren. Wenn die differenzierte Zugriffskontrolle in der Amazon- OpenSearch Service-Domain aktiviert ist, müssen Sie diese Rolle einer OpenSearch Service-Dashboards-Backend-Rolle mit mindestens der Berechtigung „cluster_monitor“ zuordnen.

- DataRetentionDays (Optional):

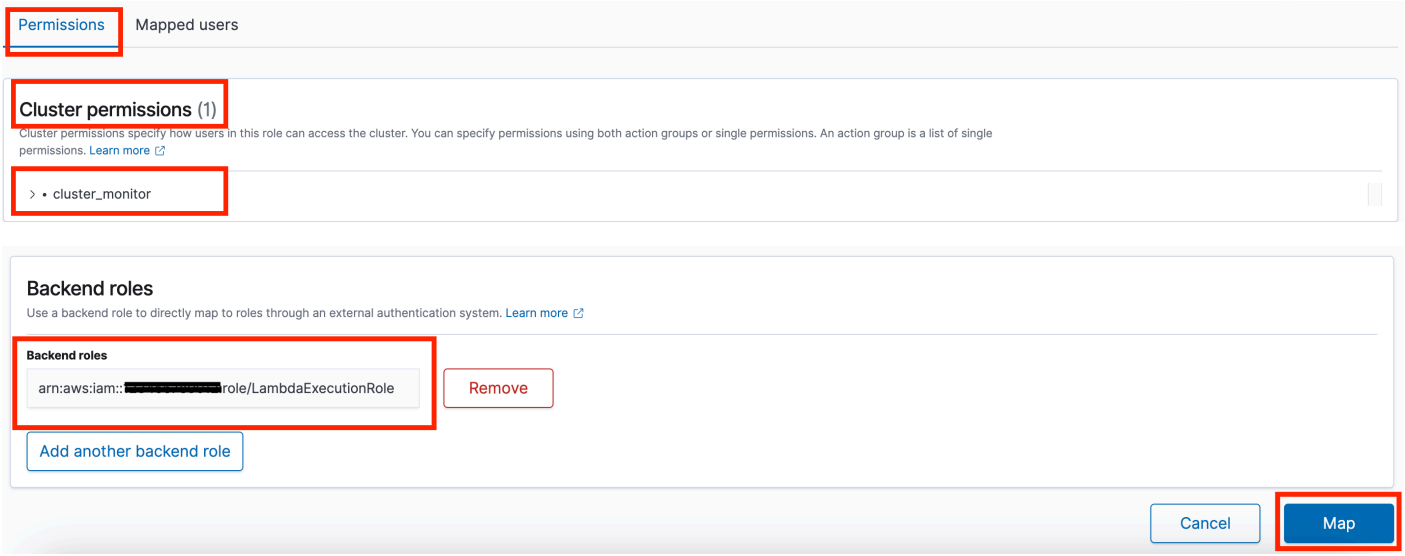
  Die Anzahl der Tage für die Aufbewahrung der von der Amazon- OpenSearch Service-Domain gesammelten Diagnosedaten. Standardmäßig werden die Daten 24 Stunden (ein Tag) lang aufbewahrt. Sie können die Daten maximal 30 Tage lang aufbewahren.

- NumberOfDataSamples (Optional):

  Die Anzahl der Datenbeispiele, die von der Amazon- OpenSearch Service-Domain gesammelt werden sollen. Standardmäßig werden 5 Datenstichproben gesammelt. Sie können bis zu 10 Stichproben sammeln und die Lambda-Funktion wird für jede Stichprobensammlung aufgerufen.




4. Wenn Sie die differenzierte Zugriffskontrolle auf einem - OpenSearch Service-Cluster aktiviert haben, stellen Sie sicher, dass der `LambdaExecutionRole` Rollen-ARN einer Rolle mit mindestens -`cluster_monitor`Berechtigung zugeordnet ist.



5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - checkConcurrency

     Stellt sicher, dass es nur eine Ausführung dieses Runbooks gibt, die auf die angegebene Amazon- OpenSearch Service-Domain ausgerichtet ist. Wenn das Runbook eine andere Ausführung findet, die auf denselben Domänennamen abzielt, gibt es einen Fehler zurück und endet.
   - getDomainConfig:

     Ruft die Konfigurationsdetails für die Ziel- OpenSearch Service-Domain ab.
   - provisionResources:

     Stellt die Ressourcen für die Datenerfassung mithilfe von bereit AWS CloudFormation.
   - waitForStackErstellung:

     Wartet, bis der AWS CloudFormation Stack abgeschlossen ist.
   - describeStackResources:

     Beschreibt den AWS CloudFormation Stack und ruft den ARN des Zustandsautomaten ab.
   - runStateMachine:

     Ruft die Lambda-Funktion des Datenkollektors einmal oder mehrmals auf, indem ein Step-Functions-Zustandsautomat ausgeführt wird.
   - describeErrorsFromStackEvents:

     Beschreibt Fehler aus dem AWS CloudFormation Stack auf Fehler.
   - unstageOpenSearchHighCPUAutomation:

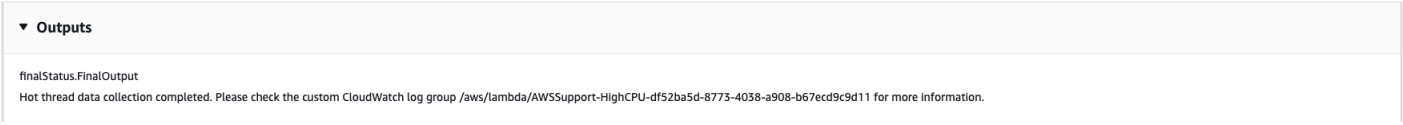
     Löscht den `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation Stack.
   - describeErrorsFromStackDeletion:

     Beschreibt Fehler, die beim Löschen des AWS CloudFormation Stacks aufgetreten sind.
   - finalStatus:

Gibt die endgültige Ausgabe des `AWSSupport-TroubleshootOpenSearchHighCPU` Runbooks zurück.

8. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten.
   - finalStatus .FinalOutput:

     Stellt die CloudWatch Protokollgruppe bereit, in der die Diagnosedaten gespeichert sind.




Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

AWS -Servicedokumentation

- Weitere Informationen finden Sie unterFehlerbehebung bei Amazon OpenSearch Service

# EventBridge

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon EventBridge bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

# AWS-AddOpsItemDedupStringToEventBridgeRule

Beschreibung

Das `AWS-AddOpsItemDedupStringToEventBridgeRule` Runbook fügt eine Deduplizierungszeichenfolge für alle hinzu, die mit einer AWS Systems Manager OpsItems Amazon-Regel verknüpft sind. EventBridge Das Runbook fügt der Regel keine Deduplizierungszeichenfolge hinzu, wenn bereits eine angewendet wurde. Weitere Informationen zu Deduplizierungszeichenfolgen und OpsItems finden Sie unter Reduzieren von Duplikaten OpsItems im Benutzerhandbuch.AWS Systems Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DedupString

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Deduplizierungszeichenfolge, die Sie der Regel hinzufügen möchten.
- RuleName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der Regel, zu der Sie die Deduplizierungszeichenfolge hinzufügen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Dokumentschritte

- `aws:executeScript`- Fügt der EventBridge Regel, die Sie im Parameter angeben, eine Deduplizierungszeichenfolge hinzu. `RuleName`

## AWS-DisableEventBridgeRule

Beschreibung

Das *AWS-DisableEventBridgeRule* Runbook deaktiviert die von Ihnen angegebene EventBridge Amazon-Regel. Weitere Informationen zu Regeln finden Sie unter EventBridge EventBridge Amazon-Regeln im Amazon-Benutzerhandbuch. EventBridge

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EventBusName

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Optional) Der Event-Bus, der der Regel zugeordnet ist, die Sie deaktivieren möchten.
- RuleName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Regel, die Sie deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Dokumentschritte

- `aws:executeAwsApi`- Deaktiviert die EventBridge Regel, die Sie im `RuleName` Parameter angeben.

# GuardDuty

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon GuardDuty bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWSConfigRemediation-CreateGuardDutyDetector

Beschreibung

Das `AWSConfigRemediation-CreateGuardDutyDetector` Runbook erstellt einen Amazon GuardDuty (GuardDuty) -Detektor in dem Bereich, in AWS-Region dem Sie die Automatisierung ausführen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Dokumentschritte

- `aws:executeAwsApi`- Erzeugt einen GuardDuty Detektor.
- `aws:assertAwsResourceProperty`- Überprüft, ob `Status` der Detektor aktiviert ist`ENABLED`.

# IAM

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Identity and Access Management Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Ordnen Sie einer verwalteten Instanz eine AWS Identity and Access Management (IAM-) Rolle zu.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ForceReplace

  Typ: Boolesch

  Beschreibung: (Optional) Markierung, um anzugeben, ob das vorhandene IAM-Profil ersetzt werden soll oder nicht.

  Standard: true
- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Instance, der Sie eine IAM-Rolle zuweisen möchten.

- RoleName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der IAM-Rolle, die der verwalteten Instanz hinzugefügt werden soll.

Dokumentschritte

1. `aws:executeAwsApi`- DescribeInstanceProfile - Suchen Sie das IAM-Instanzprofil, das der EC2-Instance zugeordnet ist.
2. `aws:branch`- CheckInstanceProfileAssociations - Überprüfen Sie das mit der EC2-Instance verknüpfte IAM-Instanzprofil.
   a. Wenn ein IAM-Instanzprofil angehängt und auf Folgendes eingestellt `ForceReplace` ist: `true`
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Trennen Sie das IAM-Instanzprofil von der EC2-Instance.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Listet die Instanzprofile für die angegebene IAM-Rolle auf.
   c. `aws:branch`- CheckInstanceProfileCreated - Prüfen Sie, ob der angegebenen IAM-Rolle ein zugeordnetes Instanzprofil zugeordnet ist.
      i. Wenn der IAM-Rolle ein zugeordnetes Instanzprofil zugeordnet ist:
         A. `aws:executeAwsApi`- AttachIAM ProfileToInstance — Hängen Sie die IAM-Instance-Profilrolle an die EC2-Instance an.
      i. Wenn der IAM-Rolle kein Instanzprofil zugeordnet ist:
         A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Erstellen Sie eine Instanzprofilrolle für die angegebene IAM-Rolle.
         B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Ordnen Sie die Instanzprofilrolle der angegebenen IAM-Rolle zu.
         C. `aws:executeAwsApi`- GetInstanceProfile - Ruft die Instanzprofildaten für die angegebene IAM-Rolle ab.

D. `aws:executeAwsApi`- AttachIAM ProfileToInstanceWithRetry — Hängt die IAM-Instanzprofilrolle an die EC2-Instance an.

Ausgaben

ProfileToInstanceWithAttachIAM wiederholen. AssociationId

GetInstanceSteckbrief. InstanceProfileName

GetInstanceProfil. InstanceProfileArn

IAM-Instanz anhängenProfileTo. AssociationId

ListInstanceProfilesForRolle. InstanceProfileName

ListInstanceProfilesForRolle. InstanceProfileArn

## `AWS-DeleteIAMInlinePolicy`

Beschreibung

Das `AWS-DeleteIAMInlinePolicy` Runbook löscht alle AWS Identity and Access Management (IAM-) Inline-Richtlinien, die mit den von Ihnen angegebenen IAM-Identitäten verknüpft sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- IamArns

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste von ARNs für die IAM-Identitäten, aus denen Sie Inline-Richtlinien löschen möchten. Diese Liste kann IAM-Benutzer, -Gruppen oder -Rollen enthalten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Dokumentschritte

- `aws:executeScript`— Löscht die IAM-Inline-Richtlinien, die den Ziel-IAM-Identitäten zugeordnet sind.

## AWSConfigRemediation-DeleteIAMRole

Beschreibung

Das `AWSConfigRemediation-DeleteIAMRole` Runbook löscht die von Ihnen angegebene AWS Identity and Access Management (IAM-) Rolle. Durch diese Automatisierung werden keine Instanzprofile gelöscht, die der IAM-Rolle zugeordnet sind, oder dienstverknüpfte Rollen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Ich bin die Rollen-ID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Rolle, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`

- iam:ListInstanceProfilesForRole
- iam:ListRolePolicies
- iam:ListRoles
- iam:RemoveRoleFromInstanceProfile

Dokumentschritte

- aws:executeScript- Erfasst den Namen der IAM-Rolle, die Sie im Parameter angeben. IAMRoleID
- aws:executeScript- Sammelt Richtlinien und Instanzprofile, die der IAM-Rolle zugeordnet sind.
- aws:executeScript- Löscht die angehängten Richtlinien.
- aws:executeScript— Löscht die IAM-Rolle und überprüft, ob die Rolle gelöscht wurde.

## AWSConfigRemediation-DeleteIAMUser

Beschreibung

Das AWSConfigRemediation-DeleteIAMUser Runbook löscht den von Ihnen angegebenen AWS Identity and Access Management (IAM-) Benutzer. Durch diese Automatisierung werden die folgenden Ressourcen, die dem IAM-Benutzer zugeordnet sind, gelöscht oder getrennt:

- Access keys (Zugriffsschlüssel)
- Angehängte verwaltete Richtlinien
- Git-Anmeldeinformationen
- Mitgliedschaften in IAM-Gruppen
- IAM-Benutzerpasswort
- Eingebundene Richtlinien
- Geräte mit Multi-Faktor-Authentifizierung (MFA)
- Zertifikate signieren
- Öffentliche SSH-Schlüssel

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAM UserId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des IAM-Benutzers, den Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Erfasst den Benutzernamen des IAM-Benutzers, den Sie im Parameter angeben. IAMUserId
- aws:executeScript- Sammelt Zugriffsschlüssel, Zertifikate, Anmeldeinformationen, MFA-Geräte und SSH-Schlüssel, die dem IAM-Benutzer zugeordnet sind.
- aws:executeScript— Sammelt Gruppenmitgliedschaften und Richtlinien für den IAM-Benutzer.
- aws:executeScript- Löscht Zugriffsschlüssel, Zertifikate, Anmeldeinformationen, MFA-Geräte und SSH-Schlüssel, die dem IAM-Benutzer zugeordnet sind.
- aws:executeScript— Löscht Gruppenmitgliedschaften und Richtlinien für den IAM-Benutzer.
- aws:executeScript- Löscht den IAM-Benutzer und überprüft, ob der Benutzer gelöscht wurde.

## AWSConfigRemediation-DeleteUnusedIAMGroup

Beschreibung

Das AWSConfigRemediation-DeleteUnusedIAMGroup Runbook löscht eine IAM-Gruppe, die keine Benutzer enthält.

Das `AWSConfigRemediation-DeleteUnusedIAMGroup` Runbook löscht eine IAM-Gruppe, die keine Benutzer enthält.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der IAM-Gruppe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`

- `iam:DetachGroupPolicy`

Dokumentschritte

- `aws:executeScript`— Entfernt verwaltete IAM-Richtlinien und Inline-IAM-Richtlinien, die der IAM-Zielgruppe zugeordnet sind, und löscht dann die IAM-Gruppe.

## `AWSConfigRemediation-DeleteUnusedIAMPolicy`

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedIAMPolicy` Runbook löscht eine AWS Identity and Access Management (IAM-) Richtlinie, die keinen Benutzern, Gruppen oder Rollen zugeordnet ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAM ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID der IAM-Richtlinie, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DeletePolicy`
- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Dokumentschritte

- `aws:executeScript`- Löscht die Richtlinie, die Sie im `IAMResourceId` Parameter angeben, und überprüft, ob die Richtlinie gelöscht wurde.

## `AWSConfigRemediation-DetachIAMPolicy`

Beschreibung

Das `AWSConfigRemediation-DetachIAMPolicy` Runbook trennt die von Ihnen angegebene AWS Identity and Access Management (IAM-) Richtlinie.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAM ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Richtlinie, die Sie trennen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Dokumentschritte

- `aws:executeScript`— Trennt die IAM-Richtlinie von allen Ressourcen.

# AWSConfigRemediation-EnableAccountAccessAnalyzer

Beschreibung

Das `AWSConfigRemediation-EnableAccountAccessAnalyzer` Runbook erstellt einen AWS Identity and Access Management (IAM) Access Analyzer in Ihrem. AWS-Konto Informationen zu Access Analyzer finden Sie unter Using AWS IAM Access Analyzer im IAM-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AnalyzerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des zu erstellenden Analyzers.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt einen Access Analyzer für Ihr Konto.
- `aws:waitForAwsResourceProperty`- Wartet auf den Status des Access Analyzers. `ACTIVE`
- `aws:assertAwsResourceProperty`- Bestätigt, dass der Status des Access Analyzers lautet`ACTIVE`.

## `AWSSupport-GrantPermissionsToIAMUser`

Beschreibung

Dieses Runbook gewährt einer IAM-Gruppe (neu oder bereits vorhanden) die angegebenen Berechtigungen und fügt der Gruppe den vorhandenen IAM-Benutzer hinzu. Zur Auswahl stehende Richtlinien: Fakturierung oder Support. Denken Sie zur Aktivierung des Fakturierungszugriffs für IAM auch an die Aktivierung des Zugriffs von IAM-Benutzern und verbundenen Benutzern auf die Fakturierungs- und Kostenmanagement-Seiten.

> **Important**
>
> Wenn Sie eine vorhandene IAM-Gruppe bereitstellen, erhalten alle aktuellen IAM-Benutzer in der Gruppe die neuen Berechtigungen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ICH BIN GroupName

  Typ: Zeichenfolge

  Standard: ExampleSupportAndBillingGroup

  Beschreibung: (Erforderlich). Dabei kann es sich um eine neue oder vorhandene Gruppe handeln. Muss mit Einschränkungen für IAM-Entitätsnamen übereinstimmen.
- ICH BIN UserName

  Typ: Zeichenfolge

  Standard: ExampleUser

  Beschreibung: (Erforderlich) Es muss sich um einen vorhandenen Benutzer handeln.
- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die Lambda annimmt.
- Berechtigungen

  Typ: Zeichenfolge

  Gültige Werte: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  Standard: SupportAndBillingFullAccess

Beschreibung: (Erforderlich) Wählen Sie eine der folgenden Optionen: `SupportFullAccess` Gewährt vollen Zugriff auf das Support Center. `BillingFullAccess`gewährt vollen Zugriff auf das Abrechnungs-Dashboard. `SupportAndBillingFullAccess`gewährt vollen Zugriff auf das Support Center und das Abrechnungs-Dashboard. Weitere Informationen zu den Richtlinien finden Sie unter „Dokumentdetails“.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die erforderlichen Berechtigungen hängen davon ab, wie `AWSSupport-GrantPermissionsToIAMUser` das Programm ausgeführt wird.

Wird als der aktuell angemeldete Benutzer oder die aktuell angemeldete Rolle ausgeführt

Es wird empfohlen, die von `AmazonSSMAutomationRole` Amazon verwaltete Richtlinie und die folgenden zusätzlichen Berechtigungen beizufügen, um die Lambda-Funktion und die IAM-Rolle für die Übergabe an Lambda erstellen zu können:

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

Verwenden von und AutomationAssumeRole LambdaAssumeRole

Der Benutzer muss über die Berechtigungen ssm: StartAutomation Execution für das Runbook und PassRoleiam: für die IAM-Rollen verfügen, die als AutomationAssume Rolle und Rolle übergeben wurden. LambdaAssume Hier finden Sie die Berechtigungen, die die einzelnen IAM-Rollen benötigen:

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

Dokumentschritte

1. `aws:createStack`- Führen Sie AWS CloudFormation Template aus, um eine Lambda-Funktion zu erstellen.
2. `aws:invokeLambdaFunction`- Führen Sie Lambda aus, um IAM-Berechtigungen festzulegen.
3. `aws:deleteStack`- Vorlage löschen CloudFormation .

Ausgaben

configureIAM.Payload

## AWSConfigRemediation-RemoveUserPolicies

Beschreibung

Das `AWSConfigRemediation-RemoveUserPolicies` Runbook löscht die AWS Identity and Access Management (IAM-) Inline-Richtlinien und trennt alle verwalteten Richtlinien, die dem von Ihnen angegebenen Benutzer zugewiesen sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAM-Benutzer-ID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Benutzers, für den Sie Richtlinien entfernen möchten.
- PolicyType

  Typ: Zeichenfolge

  Gültige Werte: Alle | Inline | Verwaltet

  Standard: Alle

  Beschreibung: (Erforderlich) Der Typ der IAM-Richtlinien, die Sie aus dem Benutzer entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Dokumentschritte

- `aws:executeScript`- Löscht und trennt IAM-Richtlinien von dem Benutzer, den Sie im Parameter angeben. `IAMUserID`

## AWSConfigRemediation-ReplaceIAMInlinePolicy

Beschreibung

Das `AWSConfigRemediation-ReplaceIAMInlinePolicy` Runbook ersetzt eine Inline-Richtlinie AWS Identity and Access Management (IAM) durch eine replizierte verwaltete IAM-Richtlinie. Bei einer Inline-Richtlinie, die einem Benutzer, einer Gruppe oder einer Rolle zugewiesen ist, werden die Inline-Richtlinienberechtigungen in eine verwaltete IAM-Richtlinie geklont. Die verwaltete IAM-Richtlinie wird der Ressource hinzugefügt und die Inline-Richtlinie wird entfernt. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- InlinePolicyName

  Typ: StringList

  Beschreibung: (Erforderlich) Die Inline-IAM-Richtlinie, die Sie ersetzen möchten.
- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des IAM-Benutzers, der Gruppe oder der Rolle, deren Inline-Richtlinie Sie ersetzen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Ersetzen Sie die Inline-IAM-Richtlinie durch eine AWS replizierte Richtlinie für die von Ihnen angegebene Ressource.

## AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Beschreibung

Das AWSConfigRemediation-RevokeUnusedIAMUserCredentials Runbook widerruft unbenutzte AWS Identity and Access Management (IAM-) Passwörter und aktive Zugriffsschlüssel. Dieses Runbook deaktiviert auch abgelaufene Zugriffsschlüssel und löscht abgelaufene Anmeldeprofile. AWS Config muss an dem Ort aktiviert sein, AWS-Region an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- IAM ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Ressource, für die Sie ungenutzte Anmeldeinformationen sperren möchten.

- MaxCredentialUsageAge

  Typ: Zeichenfolge

  Standard: 90

  Beschreibung: (Erforderlich) Die Anzahl der Tage, innerhalb derer die Anmeldeinformationen verwendet worden sein müssen.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

## Dokumentschritte

- `aws:executeScript`- Widerruft die IAM-Anmeldeinformationen für den im Parameter angegebenen Benutzer. `IAMResourceId` Abgelaufene Zugriffsschlüssel werden deaktiviert und abgelaufene Anmeldeprofile werden gelöscht.

> **Note**
>
> Stellen Sie sicher, dass der `MaxCredentialUsageAge` Parameter dieser Behebungsaktion so konfiguriert ist, dass er dem `maxAccessKeyAge` Parameter der AWS Config Regel entspricht, die Sie zum Auslösen dieser Aktion verwenden: access-keys-rotated.

## `AWSConfigRemediation-SetIAMPasswordPolicy`

Beschreibung

Das `AWSConfigRemediation-SetIAMPasswordPolicy` Runbook legt die AWS Identity and Access Management (IAM-) Benutzerkennwortrichtlinie für Ihre fest. AWS-Konto

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- AllowUsersToChangePasswort

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, AWS-Konto können alle IAM-Benutzer in Ihrem Konto das verwenden AWS Management Console , um ihre Passwörter zu ändern.
- HardExpiry

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, können IAM-Benutzer ihre Passwörter nach Ablauf des Kennworts nicht zurücksetzen.
- MaxPasswordAlter

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der Tage, an denen das Passwort eines IAM-Benutzers gültig ist.
- MinimumPasswordLänge

  Typ: Ganzzahl

  Standard: 6

  Beschreibung: (Optional) Die Mindestanzahl von Zeichen, die ein IAM-Benutzerkennwort haben darf.
- PasswordReusePrävention

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der vorherigen Passwörter, die ein IAM-Benutzer nicht wiederverwenden darf.

- RequireLowercaseCharaktere

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers einen Kleinbuchstaben aus dem lateinischen ISO-Grundalphabet (a bis z) enthalten.
- RequireNumbers

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers ein numerisches Zeichen (0-9) enthalten.
- RequireSymbols

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers ein nicht-alphanumerisches Zeichen enthalten (! @ # $% ^ * () _ + - = [] {} | ').
- RequireUppercaseCharaktere

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers einen Großbuchstaben aus dem lateinischen ISO-Alphabet (A bis Z) enthalten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Dokumentschritte

- `aws:executeScript`- Legt die IAM-Benutzerkennwortrichtlinie auf der Grundlage der Werte fest, die Sie für die Runbook-Parameter für Ihren angeben. AWS-Konto

# Amazon-Kinesis-Data-Streams

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Kinesis Data Streams bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableKinesisStreamEncryption

## `AWS-EnableKinesisStreamEncryption`

Beschreibung

Das `AWS-EnableKinesisStreamEncryption` Runbook ermöglicht die Verschlüsselung auf einem Amazon Kinesis Data Streams (Kinesis Data Streams). Bei Produzentenanwendungen, die in einen verschlüsselten Stream schreiben, treten Fehler auf, wenn sie keinen Zugriff auf den AWS Key Management Service (AWS KMS)-Schlüssel haben.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- KinesisStreamName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Streams, für den Sie die Verschlüsselung aktivieren möchten.

- KeyId

  Typ: Zeichenfolge

  Standard: alias/aws/kinesis

  Beschreibung: (Erforderlich) Der vom Kunden verwaltete AWS KMS Schlüssel, den Sie für die Verschlüsselung verwenden möchten. Dieser Wert kann eine global eindeutige Kennung, ein ARN für einen Alias oder einen Schlüssel oder ein Aliasname mit dem Präfix „alias/“ sein. Sie können den AWS verwalteten Schlüssel auch verwenden, indem Sie den Standardwert für den -Parameter verwenden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Dokumentschritte

- VerifyKinesisStreamStatus (aws:waitforAwsResourceProperty) – Prüft den Status der Kinesis Data Streams.
- EnableKinesisStreamEncryption (aws:executeAwsApi) – Aktiviert die Verschlüsselung für die Kinesis Data Streams.
- VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty) – Wartet, bis der Status von Kinesis Data Streams zu zurückkehrt`ACTIVE`.
- VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty) – Prüft, ob die Verschlüsselung für die Kinesis Data Streams aktiviert ist.

# AWS KMS

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Key Management Service Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

## `AWSConfigRemediation-CancelKeyDeletion`

Beschreibung

Das `AWSConfigRemediation-CancelKeyDeletion` Runbook storniert das Löschen des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Sie angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des vom Kunden verwalteten Schlüssels, für den Sie den Löschvorgang abbrechen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Dokumentschritte

- `aws:executeAwsApi`- Bricht das Löschen des vom Kunden verwalteten Schlüssels ab, den `KeyId` Sie im Parameter angeben.
- `aws:assertAwsResourceProperty`- Bestätigt, dass das Löschen von Schlüsseln für Ihren vom Kunden verwalteten Schlüssel deaktiviert ist.

## AWSConfigRemediation-EnableKeyRotation

Beschreibung

Das `AWSConfigRemediation-EnableKeyRotation` Runbook ermöglicht die automatische Schlüsselrotation für den symmetrischen AWS Key Management Service (AWS KMS), vom Kunden verwalteten Schlüssel.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des vom Kunden verwalteten Schlüssels, für den Sie die automatische Schlüsselrotation aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die automatische Schlüsselrotation für den vom Kunden verwalteten Schlüssel, den Sie im `KeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die automatische Schlüsselrotation für Ihren vom Kunden verwalteten Schlüssel aktiviert ist.

# Lambda

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Lambda Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

## `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing`

Beschreibung

Das `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` Runbook aktiviert AWS X-Ray Live-Tracing für die AWS Lambda Funktion, die Sie im Parameter angeben. `FunctionName`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder der ARN der Lambda-Funktion, für die die Ablaufverfolgung aktiviert werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Röntgenverfolgung für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben.

- `aws:assertAwsResourceProperty`- Überprüft, ob die Röntgenverfolgung für die Lambda-Funktion aktiviert wurde.

Ausgaben

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Antwort auf den `UpdateFunctionConfiguration` API-Aufruf.

## `AWSConfigRemediation-DeleteLambdaFunction`

Beschreibung

Das `AWSConfigRemediation-DeleteLambdaFunction` Runbook löscht die von Ihnen AWS Lambda angegebene Funktion.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LambdaFunctionName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die im Parameter angegebene Lambda-Funktion. `LambdaFunctionName`
- `aws:executeScript`— Überprüft, ob die Lambda-Funktion gelöscht wurde.

## AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Beschreibung

Das `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` Runbook verschlüsselt im Ruhezustand die Umgebungsvariablen für die AWS Lambda (Lambda-) Funktion, die Sie mit einem AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel angeben. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass die Umgebungsvariablen Ihrer Lambda-Funktion gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Funktionen mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder der ARN der Lambda-Funktion, deren Umgebungsvariablen Sie verschlüsseln möchten.
- KMS KeyArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung der Umgebungsvariablen Ihrer Lambda-Funktion verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die `LastUpdateStatus` Eigenschaft aktiviert ist. `Successful`
- `aws:executeAwsApi`- Verschlüsselt die Umgebungsvariablen für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben, mithilfe des vom AWS KMS Kunden verwalteten Schlüssels, den `KMSKeyArn` Sie im Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die Verschlüsselung für die Umgebungsvariablen für Ihre Lambda-Funktion aktiviert ist.

## AWSConfigRemediation-MoveLambdaToVPC

Beschreibung

Das `AWSConfigRemediation-MoveLambdaToVPC` Runbook verschiebt eine AWS Lambda (Lambda-) Funktion in eine Amazon Virtual Private Cloud (Amazon VPC).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, die zu einer Amazon VPC verschoben werden soll.

- SecurityGroupIDs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Sicherheitsgruppen-IDs, die Sie den Elastic Network Interfaces (ENIs) zuweisen möchten, die mit Ihrer Lambda-Funktion verknüpft sind.

- SubnetIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Subnetz-IDs, für die Sie die Elastic Network Interfaces (ENIs) erstellen möchten, die Ihrer Lambda-Funktion zugeordnet sind.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

### Dokumentschritte

- `aws:executeAwsApi`- Aktualisiert die Amazon VPC-Konfiguration für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die Lambda-Funktion aktiviert `LastUpdateStatus` ist. `successful`
- `aws:executeScript`— Überprüft, ob die Amazon VPC-Konfiguration der Lambda-Funktion erfolgreich aktualisiert wurde.

# AWSSupport-RemediateLambdaS3Event

Beschreibung

Das `AWSSupport-TroubleshootLambdaS3Event` Runbook bietet eine automatisierte Lösung für die in den AWS Knowledge Center-Artikeln beschriebenen Verfahren Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung nicht meine Lambda-Funktion aus? und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Mit diesem Runbook können Sie ermitteln und beheben, warum eine Amazon Simple Storage Service (Amazon S3) -Ereignisbenachrichtigung die von Ihnen angegebene AWS Lambda Funktion nicht ausgelöst hat. Wenn in der Runbook-Ausgabe vorgeschlagen wird, die Parallelität Ihrer Lambda-Funktion zu validieren und zu konfigurieren, finden Sie weitere Informationen unter Asynchroner Aufruf und Funktionsskalierung.AWS Lambda

> **Note**
>
> Fehler „Die folgenden Zielkonfigurationen konnten nicht überprüft werden“ können auch aufgrund falscher Amazon S3-Ereigniskonfigurationen von Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Queue Service (Amazon SQS) auftreten. Dieses Runbook überprüft nur Lambda-Funktionskonfigurationen. Wenn Sie nach der Verwendung des Runbooks immer noch die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“ angezeigt wird, überprüfen Sie bitte alle vorhandenen Amazon SNS- und Amazon SQS Amazon S3 S3-Eventkonfigurationen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaFunctionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Lambda-Funktion.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Ereignisbenachrichtigungen die Lambda-Funktion auslösen.
- Aktion

  Typ: Zeichenfolge

  Gültige Werte: Troubleshooting | Remediate

  Beschreibung: (Erforderlich) Die Aktion, die das Runbook ausführen soll. `Troubleshoot`Diese Option hilft bei der Identifizierung von Problemen, führt jedoch keine Mutationsaktionen durch, um das Problem zu lösen. `Remediate`Diese Option hilft bei der Identifizierung von Problemen und versucht, sie für Sie zu lösen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`

- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Dokumentschritte

- `aws:branch`- Verzweigungen, die auf der für den `Action` Parameter angegebenen Eingabe basieren.

  Wenn der angegebene Wert wie folgt lautet`Troubleshoot`:

  - `aws:executeAutomation`- Führt das `AWSSupport-TroubleshootLambdaS3Event` Runbook aus.
  - `aws:executeAwsApi`- Überprüft die Ausgabe des `AWSSupport-TroubleshootLambdaS3Event` Runbooks, das im vorherigen Schritt ausgeführt wurde.

  Wenn der angegebene Wert wie folgt lautet`Remediate`:

  - `aws:executeScript`— Führt ein Skript aus, um die im Abschnitt Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung meine Lambda-Funktion nicht aus? beschriebenen Probleme zu beheben und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Artikel im Knowledge Center.

Ausgaben

CheckOutput.Output

Korrigieren Sie das Lambdas3-Ereignis. Ausgabe

## `AWSSupport-TroubleshootLambdaInternetAccess`

Beschreibung

Das `AWSSupport-TroubleshootLambdaInternetAccess` Runbook hilft Ihnen bei der Behebung von Internetzugriffsproblemen für eine AWS Lambda Funktion, die in Amazon Virtual Private Cloud (Amazon VPC) gestartet wurde. Ressourcen wie Subnetzrouten, Sicherheitsgruppenregeln und

ACL-Regeln (Network Access Control List) werden überprüft, um sicherzustellen, dass ausgehender Internetzugang zulässig ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, für die Sie Probleme mit dem Internetzugang beheben möchten.
- destinationIp

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ziel-IP-Adresse, zu der Sie eine ausgehende Verbindung herstellen möchten.
- destinationPort

  Typ: Zeichenfolge

Standard: 443

Beschreibung: (Optional) Der Zielport, über den Sie eine ausgehende Verbindung herstellen möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

### Dokumentschritte

- `aws:executeScript`- Überprüft die Konfiguration verschiedener Ressourcen in Ihrer VPC, in der die Lambda-Funktion gestartet wurde.
- `aws:branch`— Verzweigungen, die darauf basieren, ob sich die angegebene Lambda-Funktion in einer VPC befindet oder nicht.
- `aws:executeScript`- Überprüft die Routentabellenrouten für das Subnetz, in dem die Lambda-Funktion gestartet wurde, und stellt sicher, dass Routen zu einem NAT-Gateway (Network Address Translation) und einem Internet-Gateway vorhanden sind. Bestätigt, dass sich die Lambda-Funktion nicht in einem öffentlichen Subnetz befindet.
- `aws:executeScript`- Überprüft, ob die der Lambda-Funktion zugeordnete Sicherheitsgruppe ausgehenden Internetzugang auf der Grundlage der für die `destinationIp` Parameter und angegebenen Werte zulässt. `destinationPort`
- `aws:executeScript`- Überprüft die ACL-Regeln, die den Subnetzen der Lambda-Funktion zugeordnet sind, und das NAT-Gateway ermöglicht ausgehenden Internetzugang auf der Grundlage der für die Parameter und angegebenen Werte. `destinationIp` `destinationPort`

### Ausgaben

checkVPC.vpc — Die ID der VPC, auf der Ihre Lambda-Funktion gestartet wurde.

checkVPC.subnet — Die IDs der Subnetze, in denen Ihre Lambda-Funktion gestartet wurde.

CheckVPC.SecurityGroups — Sicherheitsgruppen, die der Lambda-Funktion zugeordnet sind.

checkNACL.nacl — Analysenachricht mit Ressourcennamen. `LambdaIp`bezieht sich auf die private IP-Adresse der elastic network interface für Ihre Lambda-Funktion. Das `LambdaIpRules` Objekt wird nur für Subnetze generiert, die eine Route zu einem NAT-Gateway haben. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

```
{
   "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"
   }
}
```

check SecurityGroups .secgrps — Analyse für die Sicherheitsgruppe, die mit Ihrer Lambda-Funktion verknüpft ist. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

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

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

CheckSubnet.Subnets — Analyse für die Subnetze in Ihrer VPC, die Ihrer Lambda-Funktion zugeordnet sind. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

```
{
   "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

Beschreibung

Das `AWSSupport-TroubleshootLambdaS3Event` Runbook bietet eine automatisierte Lösung für die in den AWS Knowledge Center-Artikeln beschriebenen Verfahren Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung nicht meine Lambda-Funktion aus? und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Mit diesem Runbook können Sie ermitteln, warum eine Amazon Simple Storage Service (Amazon S3) -Ereignisbenachrichtigung die von Ihnen angegebene AWS Lambda Funktion nicht ausgelöst hat. Wenn in der Runbook-Ausgabe vorgeschlagen wird, die Parallelität Ihrer Lambda-Funktion zu validieren und zu konfigurieren, finden Sie weitere Informationen unter Asynchroner Aufruf und Funktionsskalierung.AWS Lambda

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaFunctionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Lambda-Funktion, die die Amazon S3 S3-Ereignisbenachrichtigung auslöst.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Ereignisbenachrichtigungen die Lambda-Funktion auslösen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Dokumentschritte

- `aws:executeScript`- Führt das Skript aus, um die Konfigurationseinstellungen für die Amazon S3 S3-Ereignisbenachrichtigung zu überprüfen. Validiert die ressourcenbasierte IAM-Richtlinie für Ihre Lambda-Funktion und generiert einen AWS Command Line Interface (AWS CLI) -Befehl, um die erforderlichen Berechtigungen hinzuzufügen, falls die erforderlichen Berechtigungen in der Richtlinie fehlen. Validiert die Ressourcenrichtlinien anderer Lambda-Funktionen, die Teil von Ereignisbenachrichtigungen für denselben S3-Bucket sind, und generiert einen AWS CLI Befehl als Ausgabe, wenn die erforderlichen Berechtigungen fehlen.

Ausgaben

Lambdas3Event.OUTPUT

# Amazon Managed Workflows für Apache Airflow

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon Managed Workflows für Apache Airflow. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootMWAAEnvironmentCreation

## `AWSSupport-TroubleshootMWAAEnvironmentCreation`

Beschreibung

Das -`AWSSupport-TroubleshootMWAAEnvironmentCreation`Runbook enthält Informationen zum Debuggen von Problemen bei der Umgebungserstellung von Amazon Managed Workflows for Apache Airflow (Amazon MWAA) und zum Durchführen von Prüfungen zusammen mit den dokumentierten Gründen nach bestem Bemühen, um den Fehler zu identifizieren.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Ruft die Details der Amazon MWAA-Umgebung ab.
- Überprüft die Berechtigungen der Ausführungsrolle.

- Prüft, ob die Umgebung über Berechtigungen zur Verwendung des bereitgestellten AWS KMS Schlüssels für die Protokollierung verfügt und ob die erforderliche CloudWatch Protokollgruppe vorhanden ist.
- Parst die Protokolle in der bereitgestellten Protokollgruppe, um Fehler zu finden.
- Prüft die Netzwerkkonfiguration, um zu überprüfen, ob die Amazon MWAA-Umgebung Zugriff auf die erforderlichen Endpunkte hat.
- Generiert einen Bericht mit den Erkenntnissen.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

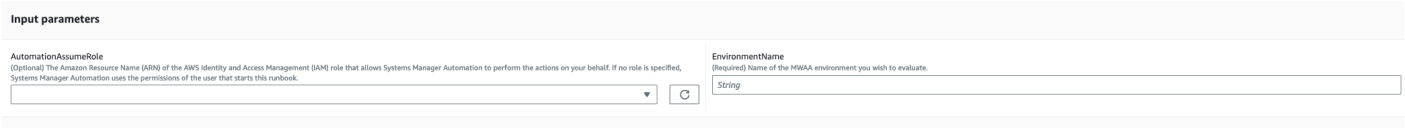
Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie zu AWSSupport-TroubleshootMWAAEnvironmentCreation in Systems Manager unter Dokumente.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - EnvironmentName (Erforderlich):

     Name der Amazon MWAA-Umgebung, die Sie auswerten möchten.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - **`GetMWAAEnvironmentDetails:`**

     Ruft die Details der Amazon MWAA-Umgebung ab. Wenn dieser Schritt fehlschlägt, wird der Automatisierungsprozess angehalten und als angezeigt`Failed`.
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Überprüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3- CloudWatch, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn ein vom Kunden verwalteter AWS Key Management Service (AWS KMS) Schlüssel erkannt wird, validiert die Automatisierung die erforderlichen Berechtigungen des Schlüssels. In diesem Schritt wird die `iam:SimulateCustomPolicy`-API verwendet, um zu überprüfen, ob die Automatisierungsausführungsrolle alle erforderlichen Berechtigungen erfüllt.
   - **`CheckKMSPolicyOnKMSKey:`**

     Prüft, ob die AWS KMS Schlüsselrichtlinie der Amazon MWAA-Umgebung die Verwendung des Schlüssels zum Verschlüsseln von CloudWatch Protokollen erlaubt. Wenn der AWS KMS Schlüssel AWS-verwaltet ist, überspringt die Automatisierung diese Prüfung.
   - **`CheckIfRequiredLogGroupsExists:`**

     Prüft, ob die erforderlichen CloudWatch Protokollgruppen für die Amazon MWAA-Umgebung vorhanden sind. Andernfalls prüft die Automatisierung CloudTrail auf - `CreateLogGroup` und -`DeleteLogGroup`Ereignisse. Dieser Schritt prüft auch auf `CreateLogGroup` Ereignisse.
   - **`BranchOnLogGroupsFindings:`**

     Verzweigungen, die auf dem Vorhandensein von CloudWatch Protokollgruppen im Zusammenhang mit der Amazon MWAA-Umgebung basieren. Wenn mindestens eine Protokollgruppe vorhanden ist, analysiert die Automatisierung sie, um Fehler zu finden. Wenn keine Protokollgruppen vorhanden sind, überspringt die Automatisierung den nächsten Schritt.
   - **`CheckForErrorsInLogGroups:`**

Parst die CloudWatch Protokollgruppen, um Fehler zu finden.

- **GetRequiredEndPointsDetails:**

  Ruft die von der Amazon MWAA-Umgebung verwendeten Service-Endpunkte ab.

- **CheckNetworkConfiguration:**

  Überprüft, ob die Netzwerkkonfiguration der Amazon MWAA-Umgebung die Anforderungen erfüllt, einschließlich Prüfungen von Sicherheitsgruppen, Netzwerk-ACLs, Subnetzen und Routing-Tabellenkonfigurationen.

- **CheckEndpointsConnectivity:**

  Ruft die `AWSSupport-ConnectivityTroubleshooter` untergeordnete Automatisierung auf, um die Konnektivität der Amazon MWAA zu den erforderlichen Endpunkten zu überprüfen.

- **CheckS3BlockPublicAccess:**

  Prüft, ob der Amazon S3-Bucket der Amazon-MWAA-Umgebung `Block Public Access` aktiviert ist, und überprüft auch die allgemeinen Amazon S3-Block-Public-Access-Einstellungen des Kontos.

- **GenerateReport:**

  Sammelt Informationen aus der Automatisierung und gibt das Ergebnis oder die Ausgabe jedes Schritts aus.

7. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten:

   - Überprüfen der Berechtigungen für die Amazon MWAA-Umgebungsausführungsrolle:

     Prüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3 CloudWatch-, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn ein vom Kunden verwalteter AWS KMS Schlüssel erkannt wird, validiert die Automatisierung die erforderlichen Berechtigungen des Schlüssels.

   - Überprüfen der Amazon MWAA- AWS KMS Umgebungsschlüsselrichtlinie:

     Prüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3 CloudWatch-, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn ein kundenverwalteter AWS KMS Schlüssel erkannt wird, prüft die Automatisierung außerdem, ob der Schlüssel die erforderlichen Berechtigungen hat.

- Überprüfen der Amazon MWAA- CloudWatch Umgebungsprotokollgruppen:

  Prüft, ob die erforderlichen CloudWatch Protokollgruppen für die Amazon MWAA-Umgebung vorhanden sind. Wenn dies nicht der Fall ist, prüft die Automatisierung CloudTrail , ob die `DeleteLogGroup` Ereignisse `CreateLogGroup` und gefunden werden.

- Überprüfen der Routing-Tabellen der Amazon MWAA-Umgebung:

  Prüft, ob die Amazon-VPC-Routing-Tabellen in der Amazon-MWAA-Umgebung ordnungsgemäß konfiguriert sind.

- Überprüfen der Sicherheitsgruppen der Amazon MWAA-Umgebung:

  Prüft, ob die Amazon MWAA-Umgebung Amazon VPC-Sicherheitsgruppen ordnungsgemäß konfiguriert sind.

- Überprüfen der Netzwerk-ACLs der Amazon MWAA-Umgebung:

  Prüft, ob die Amazon-VPC-Sicherheitsgruppen in der Amazon-MWAA-Umgebung ordnungsgemäß konfiguriert sind.

- Überprüfen der Amazon MWAA-Umgebungssubnetze:

  Prüft, ob die Subnetze der Amazon MWAA-Umgebung privat sind.

- Überprüfung der Konnektivität der für die Amazon MWAA-Umgebung erforderlichen Endpunkte:

  Prüft, ob die Amazon MWAA-Umgebung auf die erforderlichen Endpunkte zugreifen kann. Zu diesem Zweck ruft die Automatisierung die `AWSSupport-ConnectivityTroubleshooter` Automatisierung auf.

- Überprüfen des Amazon-SAmazon S3Buckets der Amazon-MWAA-Umgebung:

  Prüft, ob der Amazon S3-Bucket der Amazon-MWAA-Umgebung `Block Public Access` aktiviert ist, und überprüft auch die Amazon-SAmazon S3-Einstellungen zum Blockieren des öffentlichen Zugriffs des Kontos.

- Beim Überprüfen der Amazon MWAA- CloudWatch Umgebungsprotokolle werden Fehler gruppiert:

  Parst die vorhandenen CloudWatch Protokollgruppen der Amazon MWAA-Umgebung, um Fehler zu finden.


## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

# Neptune

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Neptune bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWS-EnableNeptuneDbAuditLogsToCloudWatch

Beschreibung

Das -`AWS-EnableNeptuneDbAuditLogsToCloudWatch`Runbook hilft Ihnen, Audit-Protokolle für einen Amazon Neptune-DB-Cluster an Amazon CloudWatch Logs zu senden.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem

Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID des Neptune-DB-Clusters, für den Sie Prüfungsprotokolle aktivieren möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

### Dokumentschritte

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) – Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) – Prüft, ob der Neptune-DB-Engine-Typ ist`neptune`.
- EnableNeptuneDbAuditLogs (aws:executeAwsApi) – Aktiviert Prüfungsprotokolle für den zu sendenden Neptune-DB-Cluster CloudWatch .
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) – Überprüft, ob der Status des Neptune-DB-Clusters lautet`available`.
- VerifyNeptuneDbAuditLogs (aws:executeScript ) – Prüft, ob Prüfungsprotokolle erfolgreich für das Senden an - CloudWatch Protokolle konfiguriert wurden.

# AWS-EnableNeptuneDbBackupRetentionPeriod

Beschreibung

Das AWS-EnableNeptuneDbBackupRetentionPeriod Runbook hilft Ihnen, automatisierte Backups mit einem Aufbewahrungszeitraum zwischen 7 und 35 Tagen für einen Amazon Neptune-DB-Cluster zu aktivieren.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der (IAM)-Rolle, mit der AWS Identity and Access Management Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID des Neptune-DB-Clusters, für den Sie Backups aktivieren möchten.
- BackupRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 7–35

Beschreibung: (Erforderlich) Die Anzahl der Tage, für die Backups aufbewahrt werden.

- PreferredBackupWindow

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein täglicher Zeitraum von mindestens 30 Minuten, wenn Sicherungen erstellt werden. Der Wert muss in UTC (Universal Time Coordinated) angegeben sein und das folgende Format verwenden: `hh24:mm-hh24:mm`. Der Aufbewahrungszeitraum für Backups kann nicht mit dem bevorzugten Wartungsfenster in Konflikt geraten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) – Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) – Prüft, ob der Neptune-DB-Engine-Typ ist`neptune`.
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) – Überprüft, ob der Status des Neptune-DB-Clusters lautet`available`.
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) – Legt den Aufbewahrungszeitraum für den Neptune-DB-Cluster fest.
- VerifyNeptuneDbBackupsEnabled (aws:executeScript ) – Prüft, ob Aufbewahrungszeitraum und Backup-Fenster erfolgreich festgelegt wurden.

# AWS-EnableNeptuneClusterDeletionProtection

Beschreibung

Das AWS-EnableNeptuneClusterDeletionProtection Runbook aktiviert den Löschschutz für den von Ihnen angegebenen Amazon Neptune-Cluster.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Neptune-Clusters, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ssm:GetAutomationExecution

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) – Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) – Überprüft, ob der Engine-Typ des angegebenen DB-Clusters ist`neptune`.
- VerifyNeptuneStatus (aws:waitForAwsResourceProperty) – Prüft, ob der Status des Clusters laute`available`.
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi) – Aktiviert den Löschschutz auf dem Neptune-DB-Cluster.
- VerifyNeptuneDbDeletionProtection (aws:assertAwsResourceProperty) – Prüft, ob der Löschschutz auf dem DB-Cluster aktiviert ist.

Ausgaben

- EnableNeptuneDbDeletionProtection.EnableNeptuneDbDeletionProtectionResponse - Die Ausgabe der API-Operation.

# Amazon RDS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Relational Database Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Das `AWS-CreateEncryptedRdsSnapshot` Runbook erstellt einen verschlüsselten Snapshot aus einer unverschlüsselten Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DB InstanceIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon RDS-Instance, von der Sie einen Snapshot erstellen möchten.
- DB SnapshotIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Namensvorlage für den Amazon RDS-Snapshot. Die Standard-Namensvorlage ist *`DB InstanceIdentifier -yyyymmddhhmmss`*.
- Verschlüsselte DB SnapshotIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name für den verschlüsselten Snapshot. Der Standardname ist der Wert, den Sie für den `DBSnapshotIdentifier` angehängten Parameter angeben. `-encrypted`

- InstanceTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, die der DB-Instance hinzugefügt werden sollen. (Beispiel: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '
- KmsKeyID

  Typ: Zeichenfolge

  Standard: `alias/aws/rds`

  Beschreibung: (Optional) Der ARN, die Schlüssel-ID oder der Schlüsselalias des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln des Snapshots verwenden möchten.
- SnapshotTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, die dem Snapshot hinzugefügt werden sollen. (Beispiel: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Dokumentschritte

- `aws:executeScript`- Erstellt einen Snapshot der DB-Instance, die Sie im `DBInstanceIdentifier` Parameter angeben.
- `aws:executeScript`- Überprüft, ob der im vorherigen Schritt erstellte Snapshot existiert und existiert`available`.

- `aws:executeScript`- Kopiert den zuvor erstellten Snapshot in einen verschlüsselten Snapshot.
- `aws:executeScript`- Überprüft, ob der im vorherigen Schritt erstellte verschlüsselte Snapshot existiert.

Ausgaben

CopyRdsSnapshotToEncryptedRdsSchnappschuss. EncryptedSnapshotId - Die ID des verschlüsselten Amazon RDS-Snapshots.

## AWS-CreateRdsSnapshot

Beschreibung

Erstellen Sie einen Amazon Relational Database Service (Amazon RDS) -Snapshot für eine Amazon RDS-Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DB InstanceIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die InstanceId DB-ID der RDS-Instance, aus der ein Snapshot erstellt werden soll.
- DB SnapshotIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die SnapshotIdentifier DB-ID des zu erstellenden RDS-Snapshots.
- InstanceTags

  Typ: Zeichenfolge

  Beschreibung (optional): Tags, die für eine Instance erstellt werden sollen.
- SnapshotTags

  Typ: Zeichenfolge

  Beschreibung (optional): Tags, die für Snapshots erstellt werden sollen.

Dokumentschritte

createRDSSnapshot — Erstellt den RDS-Snapshot und gibt die Snapshot-ID zurück.

verifyRDSSnapshot — Überprüft, ob der im vorherigen Schritt erstellte Snapshot existiert.

Ausgaben

RSSnapshot createRDSSnapshot. SnapshotId — Die ID des erstellten Snapshots.

## `AWSConfigRemediation-DeleteRDSCluster`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSCluster` Runbook löscht den von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. AWS Config muss an dem Ort aktiviert sein, AWS-Region an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DB ClusterId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

Dokumentschritte

- `aws:executeScript`- Löscht den DB-Cluster, den Sie im `DBClusterId` Parameter angeben.

## `AWSConfigRemediation-DeleteRDSClusterSnapshot`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSClusterSnapshot` Runbook löscht den angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster-Snapshot.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DB-ID ClusterSnapshot

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Amazon RDS-Cluster-Snapshot-ID, die gelöscht werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Dokumentschritte

- `aws:branch`- Überprüft, ob sich der Cluster-Snapshot im `available` Status befindet. Wenn es nicht verfügbar ist, endet der Flow.
- `aws:executeAwsApi`— Löscht den angegebenen Amazon RDS-Cluster-Snapshot unter Verwendung der Cluster-Snapshot-ID der Datenbank (DB).
- `aws:executeScript`— Überprüft, ob der angegebene Amazon RDS-Cluster-Snapshot gelöscht wurde.

## `AWSConfigRemediation-DeleteRDSInstance`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSInstance` Runbook löscht die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Instance. Wenn Sie eine Datenbank-Instance (DB) löschen, werden alle automatisierten Backups für diese Instance gelöscht und können nicht wiederhergestellt werden. Manuelle DB-Snapshots werden nicht gelöscht. Wenn sich die DB-Instance, die Sie löschen möchten`failed`, im `incompatible-restore` Status`incompatible-network`, oder befindet, müssen Sie den `SkipFinalSnapshot` Parameter auf `true` setzen.

> **Note**
>
> Wenn sich die DB-Instance, die Sie löschen möchten, in einem Amazon Aurora Aurora-DB-Cluster befindet, löscht das Runbook die DB-Instance nicht, wenn es sich um eine Read Replica und die einzige Instance im DB-Cluster handelt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, die Sie löschen möchten.
- SkipFinalSchnappschuss

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird kein letzter Snapshot erstellt, bevor die DB-Instance gelöscht wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt den Namen der DB-Instance aus dem Wert, den Sie im `DbiResourceId` Parameter angeben.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie im `SkipFinalSnapshot` Parameter angeben.
- `aws:executeAwsApi`- Löscht die DB-Instance, die Sie im `DbiResourceId` Parameter angeben.
- `aws:executeAwsApi`- Löscht die DB-Instance, die Sie im `DbiResourceId` Parameter angeben, nachdem der endgültige Snapshot erstellt wurde.
- `aws:assertAwsResourceProperty`— Überprüft, ob die DB-Instance gelöscht wurde.

## `AWSConfigRemediation-DeleteRDSInstanceSnapshot`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSInstanceSnapshot` Runbook löscht den von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Instance-Snapshot. Nur Snapshots im Status werden gelöscht. `available` Dieses Runbook unterstützt nicht das Löschen von Snapshots aus Amazon Aurora Aurora-Datenbank-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbSnapshotID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Snapshots, den Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst den Status des im Parameter angegebenen Snapshots. `DbSnapshotId`
- `aws:assertAwsResourceProperty`- Bestätigt, dass der Status des Snapshots lautet`available`.
- `aws:executeAwsApi`- Löscht den im `DbSnapshotId` Parameter angegebenen Snapshot.
- `aws:executeScript`- Überprüft, ob der Snapshot gelöscht wurde.

## AWSConfigRemediation-DisablePublicAccessToRDSInstance

Beschreibung

Das `AWSConfigRemediation-DisablePublicAccessToRDSInstance` Runbook deaktiviert den öffentlichen Zugriff für die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance (DB).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie den öffentlichen Zugriff deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Überprüft, ob sich die DB-Instances in einem `AVAILABLE` bestimmten Zustand befinden.
- `aws:executeAwsApi`— Deaktiviert den öffentlichen Zugriff auf Ihre DB-Instance.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die DB-Instance in einen `MODIFYING` Status wechselt.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die DB-Instance in einen `AVAILABLE` Status wechselt.
- `aws:assertAwsResourceProperty`- Bestätigt, dass der öffentliche Zugriff auf der DB-Instance deaktiviert ist.

## AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Beschreibung

Das `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` Runbook aktiviert die `CopyTagsToSnapshot` Einstellung auf dem von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. Wenn Sie diese Einstellung aktivieren, werden alle Tags aus dem DB-Cluster in Snapshots des DB-Clusters kopiert. Standardmäßig werden sie nicht kopiert. AWS Config muss dort aktiviert sein AWS-Region , wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für den DB-Cluster so schnell wie möglich asynchron angewendet.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie die `CopyTagsToSnapshot` Einstellung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`

- `rds:ModifyDBCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt die DB-Cluster-ID aus der DB-Cluster-Ressourcen-ID.
- `aws:assertAwsResourceProperty`- Bestätigt, dass sich der DB-Cluster in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`- Aktiviert die `CopyTagsToSnapshot` Einstellung in Ihrem DB-Cluster.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `CopyTagsToSnapshot` Einstellung in Ihrem DB-Cluster aktiviert ist.

## AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Beschreibung

Das `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` Runbook aktiviert die `CopyTagsToSnapshot` Einstellung auf der Amazon Relational Database Service (Amazon RDS) -Instance, die Sie angeben. Wenn Sie diese Einstellung aktivieren, werden alle Tags aus der DB-Instance in Snapshots der DB-Instance kopiert. Standardmäßig werden sie nicht kopiert. AWS Config muss dort aktiviert sein AWS-Region , wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie die `CopyTagsToSnapshot` Einstellung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.

- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die `CopyTagsToSnapshot` Einstellung auf Ihrer DB-Instance.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `CopyTagsToSnapshot` Einstellung auf Ihrer DB-Instance aktiviert ist.

## AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Beschreibung

Das `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` Runbook aktiviert Enhanced Monitoring auf der von Ihnen angegebenen Amazon RDS-Datenbank-Instance. Informationen zu Enhanced Monitoring finden Sie unter Enhanced Monitoring im Amazon RDS-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- MonitoringInterval

  Typ: Ganzzahl

  Gültige Werte: 1 | 5 | 10 | 15 | 30 | 60

  Beschreibung: (Erforderlich) Das Intervall in Sekunden, in dem Enhanced Monitoring-Metriken von der DB-Instance erfasst werden.
- MonitoringRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die es Amazon RDS ermöglicht, Enhanced Monitoring-Metriken an Amazon CloudWatch Logs zu senden.
- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Enhanced Monitoring aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die erweiterte Überwachung Ihrer DB-Instance.
- `aws:executeScript`— Bestätigt, dass Enhanced Monitoring auf Ihrer DB-Instance aktiviert ist.

# AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Beschreibung

Das `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` Runbook aktiviert die `AutoMinorVersionUpgrade` Einstellung auf der von Ihnen angegebenen Amazon RDS-Datenbank-Instance. Wenn Sie diese Einstellung aktivieren, werden kleinere Versions-Upgrades während des Wartungsfensters automatisch auf die DB-Instance angewendet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie die `AutoMinorVersionUpgrade` Einstellung verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die `AutoMinorVersionUpgrade` Einstellung auf Ihrer DB-Instance.
- `aws:executeScript`— Bestätigt, dass die `AutoMinorVersionUpgrade` Einstellung auf Ihrer DB-Instance aktiviert ist.

## AWSConfigRemediation-EnableMultiAZOnRDSInstance

Beschreibung

Das `AWSConfigRemediation-EnableMultiAZOnRDSInstance` Runbook ändert Ihre Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance (DB) in eine Multi-AZ-Bereitstellung. Das Ändern dieser Einstellung führt nicht zu einem Nutzungsausfall. Die Änderung wird im nächsten Wartungsfenster übernommen, sofern Sie den Parameter nicht auf setzen. `ApplyImmediately` `true`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- ApplyImmediately

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der AWS-Region eindeutige, unveränderliche Bezeichner für die DB-Instance, um die `MultiAZ` Einstellung zu aktivieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Dokumentschritte

- `aws:executeAwsApi`- Ruft den DB-Instance-Namen unter Verwendung des im Parameter angegebenen Werts ab. `DBInstanceId`
- `aws:executeAwsApi`- Überprüft, ob das ist`DBInstanceStatus`. `available`
- `aws:branch`- Prüft, ob `true` auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, bereits auf eingestellt `MultiAZ` ist.
- `aws:executeAwsApi`- Ändert die `MultiAZ` Einstellung `true` auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, auf.
- `aws:assertAwsResourceProperty`- Überprüft, ob `true` auf `MultiAZ` der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, auf gesetzt ist.

## `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance`

Beschreibung

Das `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` Runbook aktiviert Performance Insights auf der von Ihnen angegebenen Amazon RDS-DB-Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Performance Insights aktivieren möchten.

- PerformanceInsightsKMS KeyId

  Typ: Zeichenfolge

  Standard: `alias/aws/rds`

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Performance Insights zur Verschlüsselung aller potenziell sensiblen Daten verwenden soll. Wenn Sie den Schlüsselalias für diesen Parameter eingeben, stellen Sie dem Wert ein Präfix voran. **`alias/`** Wenn Sie keinen Wert für diesen Parameter angeben, Von AWS verwalteter Schlüssel wird der verwendet.

- PerformanceInsightsRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 7, 731

  Standard: 7

  Beschreibung: (Optional) Die Anzahl der Tage, an denen Sie Performance Insights Insights-Daten aufbewahren möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der DB-Instance-Status lautet`available`.
- `aws:executeAwsApi`- Sammelt den ARN des vom AWS KMS Kunden verwalteten Schlüssels, der im `PerformanceInsightsKMSKeyId` Parameter angegeben ist.
- `aws:branch`— Prüft, ob der `PerformanceInsightsKMSKeyId` Eigenschaft der DB-Instance bereits ein Wert zugewiesen ist.
- `aws:executeAwsApi`— Aktiviert Performance Insights auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der für den `PerformanceInsightsKMSKeyId` Parameter angegebene Wert verwendet wurde, um die Verschlüsselung für Performance Insights auf der DB-Instance zu aktivieren.
- `aws:assertAwsResourceProperty`— Bestätigt, dass Performance Insights auf der DB-Instance aktiviert ist.

## `AWSConfigRemediation-EnableRDSClusterDeletionProtection`

Beschreibung

Das `AWSConfigRemediation-EnableRDSClusterDeletionProtection` Runbook aktiviert den Löschschutz auf dem von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt den DB-Clusternamen aus der DB-Cluster-Ressourcen-ID.

- `aws:assertAwsResourceProperty`— Überprüft, ob der DB-Cluster-Status lautet. `available`
- `aws:executeAwsApi`— Aktiviert den Löschschutz auf dem DB-Cluster, den Sie im `ClusterId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob der Löschschutz auf dem DB-Cluster aktiviert wurde.

## AWSConfigRemediation-EnableRDSInstanceBackup

Beschreibung

Das `AWSConfigRemediation-EnableRDSInstanceBackup` Runbook ermöglicht Backups für die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance. Dieses Runbook unterstützt nicht die Aktivierung von Backups für Amazon Aurora Aurora-Datenbank-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BackupRetentionZeitraum

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die Backups aufbewahrt werden.
- DbiResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Backups aktivieren möchten.
- PreferredBackupFenster

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der tägliche Zeitraum (in UTC), in dem Backups erstellt werden.

  Einschränkungen:
  - Muss im folgenden Format vorliegen `hh24:mi-hh24:mi`
  - Muss in koordinierter Weltzeit (UTC) angegeben werden
  - Darf nicht mit dem bevorzugten Wartungsfenster in Konflikt treten.
  - Muss mindestens 30 Minuten betragen.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeScript`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID. Aktiviert Backups für Ihre DB-Instance. Bestätigt, dass Backups auf der DB-Instance aktiviert sind.

## AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Beschreibung

Das `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` Runbook aktiviert den Löschschutz für die von Ihnen angegebene Amazon RDS-Datenbank-Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbInstanceResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:executeAwsApi`— Aktiviert den Löschschutz für Ihre DB-Instance.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der Löschschutz auf der DB-Instance aktiviert ist.

## AWSConfigRemediation-ModifyRDSInstancePortNumber

Beschreibung

Das `AWSConfigRemediation-ModifyRDSInstancePortNumber` Runbook ändert die Portnummer, auf der die Amazon Relational Database Service (Amazon RDS) -Instance

Verbindungen akzeptiert. Wenn Sie diese Automatisierung ausführen, wird die Datenbank neu gestartet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- PortNumber

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Portnummer, über die die DB-Instance Verbindungen annehmen soll.
- RDSDB-ID InstanceResource

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, deren eingehende Portnummer Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Ändert die Nummer des eingehenden Ports, über den Ihre DB-Instance Verbindungen akzeptiert.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich die DB-Instance in einem bestimmten Zustand befindet. `MODIFYING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich die DB-Instance in einem `AVAILABLE` bestimmten Zustand befindet.

## `AWSSupport-ModifyRDSSnapshotPermission`

Beschreibung

Mit dem `AWSSupport-ModifyRDSSnapshotPermission` Runbook können Sie die Berechtigungen für mehrere Amazon Relational Database Service (Amazon RDS) -Snapshots ändern. Mit diesem Runbook können Sie Schnappschüsse erstellen `Public` oder `Private` diese mit anderen teilen. AWS-Konten Mit einem Standard-KMS-Schlüssel verschlüsselte Snapshots können nicht mit anderen Konten geteilt werden, die dieses Runbook verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- AccountIds

  Typ: StringList

  Standard: keiner

  Beschreibung: (Optional) Die IDs der Konten, mit denen Sie Snapshots teilen möchten. Dieser Parameter ist erforderlich, wenn Sie `No` den Wert des `Private` Parameters eingeben.

- AccountPermissionBetrieb

  Typ: Zeichenfolge

  Gültige Werte: hinzufügen | entfernen

  Standard: keiner

  Beschreibung: (Optional) Die Art des auszuführenden Vorgangs.

- Privat

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Geben Sie `No` den Wert ein, wenn Sie Snapshots mit bestimmten Konten teilen möchten.

- SnapshotIdentifiers

Typ: StringList

Beschreibung: (Erforderlich) Die Namen der Amazon RDS-Snapshots, deren Berechtigungen Sie ändern möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

### Dokumentschritte

1. `aws:executeScript`- Überprüft die IDs der im Parameter angegebenen Snapshots. `SnapshotIdentifiers` Nach der Überprüfung der IDs sucht das Skript nach verschlüsselten Snapshots und gibt eine Liste aus, falls welche gefunden wurden.
2. `aws:branch`- Verzweigt die Automatisierung auf der Grundlage des Werts, den Sie für den `Private` Parameter eingeben.
3. `aws:executeScript`- Ändert die Berechtigungen der angegebenen Snapshots, um sie für die angegebenen Konten freizugeben.
4. `aws:executeScript`- Ändert die Berechtigungen der Snapshots, um sie von zu zu ändern. `Public` `Private`

### Ausgaben

ValidateSnapshots.EncryptedSnapshots

SharewithOtherKonten. Ergebnis

MakePrivate. Ergebnis

MakePrivate. Befehle

# AWSPremiumSupport-PostgreSQLWorkloadReview

Beschreibung

Das `AWSPremiumSupport-PostgreSQLWorkloadReview` Runbook erfasst mehrere Schnappschüsse Ihrer Amazon Relational Database Service (Amazon RDS) PostgreSQL-Datenbanknutzungsstatistiken. Die erfassten Statistiken sind erforderlich, damit ein Experte von AWS Support Proactive Services eine Betriebsprüfung durchführen kann. Die Statistiken werden mithilfe einer Reihe von benutzerdefinierten SQL- und Shell-Skripten gesammelt. Diese Skripts werden auf eine temporäre Amazon Elastic Compute Cloud (Amazon EC2) -Instance in Ihrer heruntergeladen AWS-Konto , die mit diesem Runbook erstellt wurde. Für das Runbook müssen Sie Anmeldeinformationen mit einem AWS Secrets Manager geheimen Schlüssel angeben, der ein Schlüssel-Wert-Paar aus Benutzername und Passwort enthält. Der Benutzername muss über Berechtigungen verfügen, um die standardmäßigen PostgreSQL-Statistikansichten und -funktionen abzufragen.

Dieses Runbook erstellt AWS-Konto mithilfe eines Stacks automatisch die folgenden AWS Ressourcen in Ihrem System. AWS CloudFormation Sie können die Stack-Erstellung mithilfe der AWS CloudFormation Konsole überwachen.

- Eine Virtual Private Cloud (VPC) und eine Amazon EC2 EC2-Instance wurden in einem privaten Subnetz der VPC mit optionaler Konnektivität zum Internet über ein NAT-Gateway gestartet.
- Eine AWS Identity and Access Management (IAM-) Rolle, die der temporären Amazon EC2 EC2-Instance mit Berechtigungen zum Abrufen des geheimen Secrets Manager Manager-Werts zugewiesen ist. Die Rolle bietet auch Berechtigungen zum Hochladen von Dateien in einen Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl und optional in einen AWS Support Fall.
- Eine VPC-Peering-Verbindung, um Konnektivität zwischen Ihrer DB-Instance und der temporären Amazon EC2 EC2-Instance zu ermöglichen.
- Systems Manager-, Secrets Manager- und Amazon S3 S3-VPC-Endpoints, die an die temporäre VPC angeschlossen sind.
- Ein Wartungsfenster mit registrierten Aufgaben, die die temporäre Amazon EC2 EC2-Instance regelmäßig starten und stoppen, Datenerfassungsskripten ausführen und Dateien in einen Amazon S3 S3-Bucket hochladen. Für das Wartungsfenster wird auch eine IAM-Rolle erstellt, die Berechtigungen zur Ausführung der registrierten Aufgaben bereitstellt.

Wenn das Runbook abgeschlossen ist, wird der AWS CloudFormation Stack, der zum Erstellen der erforderlichen AWS Ressourcen verwendet wird, gelöscht und der Bericht wird in den Amazon S3 S3-Bucket Ihrer Wahl hochgeladen, und optional wird ein AWS Support Fall erstellt.

> **Note**
>
> Standardmäßig wird das Amazon EBS-Root-Volume der temporären Amazon EC2 EC2-Instance beibehalten. Sie können diese Option überschreiben, indem Sie den `EbsVolumeDeleteOnTermination` Parameter auf setzen. `true`

Voraussetzungen

- Enterprise Support-Abonnement Für dieses Runbook und die Proactive Services Workload Diagnostics and Reviews ist ein Enterprise Support-Abonnement erforderlich. Bevor Sie dieses Runbook verwenden, wenden Sie sich an Ihren Technical Account Manager (TAM) oder Specialist TAM (STAM), um weitere Anweisungen zu erhalten. Weitere Informationen finden Sie unter Proactive Services.AWS Support
- Konto und AWS-Region Kontingente Stellen Sie sicher, dass Sie die maximale Anzahl von Amazon EC2 EC2-Instances oder VPCs, die Sie in Ihrem Konto und Ihrer Region, in der Sie dieses Runbook verwenden, erstellen können, nicht erreicht haben. Wenn Sie eine Erhöhung des Limits beantragen müssen, sehen Sie sich das Formular zur Erhöhung des Service-Limits an.
- Konfiguration der Datenbank
  1. Für die Datenbank, die Sie im `DatabaseName` Parameter angeben, sollte die `pg_stat_statements` Erweiterung konfiguriert sein. Wenn Sie die Konfiguration `pg_stat_statements` nicht vorgenommen habens`hared_preload_libraries`, müssen Sie den Wert in der DB-Parametergruppe bearbeiten und die Änderungen übernehmen. Bei Änderungen am Parameter `shared_preload_libraries` müssen Sie Ihre DB-Instance neu starten. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen. Wenn Sie `pg_stat_statements` mehr hinzufügen, `shared_preload_libraries` wird dies zu einem gewissen Leistungsaufwand führen. Dies ist jedoch nützlich, um die Leistung einzelner Kontoauszüge zu verfolgen. Weitere Informationen zur `pg_stat_statements` Erweiterung finden Sie in der PostgreSQL-Dokumentation. Wenn Sie die Erweiterung nicht konfigurieren oder wenn die `pg_stat_statements` Erweiterung nicht in der Datenbank vorhanden ist, die für die Statistikerfassung verwendet wird, wird die Analyse auf Abrechnungsebene nicht im Operational Review dargestellt.

2. Stellen Sie sicher, dass die `track_activities` Parameter `track_counts` und nicht ausgeschaltet sind. Wenn diese Parameter in der DB-Parametergruppe deaktiviert sind, sind keine aussagekräftigen Statistiken verfügbar. Wenn Sie diese Parameter ändern, müssen Sie Ihre DB-Instance neu starten. Weitere Informationen finden Sie unter Arbeiten mit Parametern auf Ihrer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.
3. Wenn der `track_io_timing` Parameter ausgeschaltet ist, werden die Statistiken auf I/O-Ebene nicht in die Betriebsüberprüfung einbezogen. Bei Änderungen `track_io_timing` müssen Sie Ihre DB-Instance neu starten, was je nach Arbeitslast der DB-Instance zu zusätzlichem Leistungsaufwand führt. Trotz des Leistungsaufwands für kritische Workloads bietet dieser Parameter nützliche Informationen zur I/O-Zeit pro Abfrage.

Abrechnung und Gebühren AWS-Konto Ihnen werden die Kosten für die temporäre Amazon EC2 EC2-Instance, das zugehörige Amazon EBS-Volume, das NAT-Gateway und die während der Ausführung dieser Automatisierung übertragenen Daten in Rechnung gestellt. Standardmäßig erstellt dieses Runbook eine `t3.micro` Amazon Linux 2-Instance, um die Statistiken zu sammeln. Das Runbook startet und stoppt die Instance zwischen den Schritten, um die Kosten zu senken.

Datensicherheit und Verwaltung Dieses Runbook sammelt Statistiken, indem es die PostgreSQL-Statistikansichten und -funktionen abfragt. Stellen Sie sicher, dass die im `SecretId` Parameter angegebenen Anmeldeinformationen nur Leseberechtigungen für die Statistikansichten und -funktionen zulassen. Im Rahmen der Automatisierung werden die Sammelskripte in Ihren Amazon S3 S3-Bucket hochgeladen und befinden sich dorts3://*DOC-EXAMPLE-BUCKET*/*automation execution id*/queries/.

Diese Skripts sammeln Daten, die von einem AWS Spezialisten verwendet werden, um wichtige Leistungsindikatoren auf Objektebene zu überprüfen. Das Skript sammelt Informationen wie Tabellenname, Schemaname und Indexname. Wenn eine dieser Informationen vertrauliche Informationen wie Umsatzindikatoren, Benutzername, E-Mail-Adresse oder andere persönlich identifizierbare Informationen enthält, empfehlen wir, dass Sie diese Workload-Prüfung beenden. Wenden Sie sich an Ihren AWS TAM, um einen alternativen Ansatz für die Überprüfung der Arbeitslast zu besprechen.

Stellen Sie sicher, dass Sie über die erforderliche Genehmigung und Freigabe verfügen, um die im Rahmen dieser Automatisierung gesammelten Statistiken und Metadaten mit AWS anderen zu teilen.

Sicherheitsüberlegungen Wenn Sie den `UpdateRdsSecurityGroup` Parameter auf setzen`yes`, aktualisiert das Runbook die Ihrer DB-Instance zugeordnete Sicherheitsgruppe, um eingehenden Datenverkehr von der privaten IP-Adresse der temporären Amazon EC2 EC2-Instance zuzulassen.

Wenn Sie den `UpdateRdsRouteTable` Parameter auf setzen`yes`, aktualisiert das Runbook die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem Ihre DB-Instance läuft, um Traffic zur temporären Amazon EC2 EC2-Instance über die VPC-Peering-Verbindung zuzulassen.

Benutzererstellung Damit das Sammelskript eine Verbindung zu Ihrer Amazon RDS-Datenbank herstellen kann, müssen Sie einen Benutzer einrichten, der berechtigt ist, die Statistikansichten zu lesen. Dann müssen Sie die Anmeldeinformationen in Secrets Manager speichern. Wir empfehlen, einen neuen dedizierten Benutzer für diese Automatisierung zu erstellen. Wenn Sie einen separaten Benutzer erstellen, können Sie die im Rahmen dieser Automatisierung ausgeführten Aktivitäten prüfen und nachverfolgen.

1. Erstellen Sie einen neuen Benutzer.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "CREATE USER <user_name> PASSWORD '<password>';"
   ```

2. Stellen Sie sicher, dass dieser Benutzer nur schreibgeschützte Verbindungen herstellen kann.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET default_transaction_read_only=true;"
   ```

3. Legen Sie Grenzwerte auf Benutzerebene fest.

   ```
   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. Erteilen Sie dem neuen Benutzer `pg_monitor` Berechtigungen, damit er auf die DB-Statistiken zugreifen kann. (Die `pg_monitor` Rolle ist Mitglied von `pg_read_all_settings`pg_read_all_stats, und`pg_stat_scan_table`.)

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "GRANT pg_monitor to <user_name>;"
   ```

Berechtigungen, die dem temporären Amazon EC2 EC2-Instance-Profil durch diese Systems Manager Manager-Automatisierung hinzugefügt wurden Die folgenden Berechtigungen werden der IAM-Rolle hinzugefügt, die der temporären Amazon EC2 EC2-Instance zugeordnet ist. Die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie ist auch mit der IAM-Rolle verknüpft, sodass die Amazon EC2 EC2-Instance von Systems Manager verwaltet werden kann.

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

Durch diese Systems Manager Manager-Automatisierung zum temporären Wartungsfenster hinzugefügte Berechtigungen Die folgenden Berechtigungen werden automatisch der IAM-Rolle hinzugefügt, die den Windows-Wartungsaufgaben zugeordnet ist. Die Windows-Wartungsaufgaben starten, stoppen und senden Befehle an die temporäre Amazon EC2 EC2-Instance.

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

[Führen Sie diese Automatisierung aus (Konsole)]

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DB InstanceIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID Ihrer DB-Instance.
- DatabaseName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Datenbankname, der auf Ihrer DB-Instance gehostet wird.

- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN Ihres Secrets Manager Manager-Secrets, der das Schlüsselwertpaar aus Benutzername und Passwort enthält. Der AWS CloudFormation Stack erstellt eine IAM-Richtlinie mit Berechtigungen für den `GetSecretValue` Vorgang mit diesem ARN. Die Anmeldeinformationen werden verwendet, damit die temporäre Instanz die Datenbankstatistiken sammeln kann. Wenden Sie sich an Ihren TAM oder STAM, um die erforderlichen Mindestberechtigungen zu besprechen.

- Bestätigen Sie

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Geben Sie ein, **`yes`** ob Sie bestätigen, dass dieses Runbook temporäre Ressourcen in Ihrem Konto erstellt, um Statistiken von Ihrer DB-Instance zu sammeln. Wir empfehlen, sich mit Ihrem TAM oder STAM in Verbindung zu setzen, bevor Sie diese Automatisierung ausführen.

- SupportCase

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die AWS Support Fallnummer, die Sie von Ihrem TAM oder STAM erhalten haben. Falls angegeben, aktualisiert das Runbook den Fall und fügt die gesammelten Daten an. Für diese Option muss die temporäre Amazon EC2 EC2-Instance über eine Internetverbindung verfügen, um auf den AWS Support API-Endpunkt zugreifen zu können. Sie müssen den `AllowVpcInternetAccess` Parameter auf setzen. `true` Der Betreff der Groß- und Kleinschreibung muss den Ausdruck enthaltenAWSPremiumSupport-PostgreSQLWorkloadReview.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket-Name in Ihrem Konto, in das Sie die von der Automatisierung gesammelten Daten hochladen möchten. Stellen Sie sicher, dass die Bucket-

Richtlinie Prinzipalen, die keinen Zugriff auf den Inhalt des Buckets benötigen, keine unnötigen Lese- oder Schreibberechtigungen gewährt. Wir empfehlen, für diese Automatisierung einen neuen temporären Amazon S3 S3-Bucket zu erstellen. Das Runbook gewährt der IAM-Rolle, die der temporären Amazon EC2 EC2-Instance zugeordnet ist, Berechtigungen für den `s3:PutObject` API-Vorgang. Die hochgeladenen Dateien befinden sich in. `s3://`*`bucket name`*`/`*`automation execution id`*`/`

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Typ der temporären Amazon EC2 EC2-Instance, die die benutzerdefinierten SQL- und Shell-Skripts ausführt.

  Gültige Werte: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Standard: t3.micro

- VpcCidr

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IP-Adressbereich in CIDR-Notation für die neue VPC (z. B.`172.31.0.0/16`). Stellen Sie sicher, dass Sie ein CIDR auswählen, das sich nicht mit einer vorhandenen VPC mit Konnektivität zu Ihrer DB-Instance überschneidet oder mit dieser übereinstimmt. Die kleinste VPC, die Sie erstellen können, verwendet eine /28-Subnetzmaske, und die größte VPC verwendet eine /16-Subnetzmaske.

  Standard: 172.31.0.0/16

- StackResourcesNamePrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Namenspräfix und das Tag für den Namen der AWS CloudFormation Stack-Ressourcen. Das Runbook erstellt die AWS CloudFormation Stack-Ressourcen unter Verwendung dieses Präfixes als Teil des Namens und des Tags, die auf die Ressourcen angewendet werden. Die Struktur für das Schlüssel-Wert-Paar des Tags lautet. *`StackResourcesNamePrefix`*`:{{automation:EXECUTION_ID}}`

  Standard: AWSPostgreSQLWorkloadReview

- Plan

Typ: Zeichenfolge

Beschreibung: (Optional) Der Zeitplan für das Wartungsfenster. Gibt an, wie oft die Aufgaben im Wartungsfenster ausgeführt werden. Der Standardwert ist jeder`1 hour`.

Gültige Werte: 15 Minuten | 30 Minuten | 1 Stunde | 2 Stunden | 4 Stunden | 6 Stunden | 12 Stunden | 1 Tag | 2 Tage | 4 Tage

Standard: 1 Stunde

- Dauer

  Typ: Ganzzahl

  Beschreibung: (Optional) Die maximale Dauer in Minuten, für die die Automatisierung ausgeführt werden soll. Die maximal unterstützte Dauer beträgt 8.640 Minuten (6 Tage). Der Standardwert ist 4.320 Minuten (3 Tage).

  Gültige Werte: 30-8640

  Standard: 4320

- UpdateRdsRouteTable

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, aktualisiert das Runbook die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem Ihre DB-Instance ausgeführt wird. Eine IPv4-Route wird hinzugefügt, um den Datenverkehr über die neu erstellte VPC-Peering-Verbindung an die private IPv4-Adresse der temporären Amazon EC2 EC2-Instance weiterzuleiten.

  Zulässige Werte: true | false

  Standard: false

- AllowVpcInternetAccess

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, erstellt das Runbook ein NAT-Gateway, um Internetkonnektivität für die temporäre Amazon EC2 EC2-Instance zur Kommunikation mit dem AWS Support API-Endpunkt bereitzustellen. Sie können diesen Parameter

so belassen, als `false` ob das Runbook nur die Ausgabe in Ihren Amazon S3 S3-Bucket hochladen soll.

Zulässige Werte: true | false

Standard: false

- UpdateRdsSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, aktualisiert das Runbook die Ihrer DB-Instance zugeordnete Sicherheitsgruppe, um Datenverkehr von der privaten IP-Adresse der temporären Instance aus zuzulassen.

  Gültige Werte: false | true

  Standard: false

- EbsVolumeDeleteOnKündigung

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird das Root-Volume der temporären Amazon EC2 EC2-Instance gelöscht, nachdem das Runbook abgeschlossen und der Stack gelöscht wurde. AWS CloudFormation

  Gültige Werte: false | true

  Standard: false

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:assertAwsResourceProperty- Bestätigt, dass sich die DB-Instance im available Status befindet.
2. aws:executeAwsApi- Sammelt Details über die DB-Instance.
3. aws:executeScript- Prüft, ob der im angegebene Amazon S3 S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen S3BucketName zulässt.
4. aws:executeScript- Ruft den AWS CloudFormation Vorlageninhalt aus dem Automation-Runbook-Anhang ab, der verwendet wird, um die temporären AWS Ressourcen in Ihrem AWS-Konto zu erstellen.
5. aws:createStack- Erstellt die AWS CloudFormation Stack-Ressourcen.
6. aws:waitForAwsResourceProperty- Wartet, bis die von der AWS CloudFormation Vorlage erstellte Amazon EC2 EC2-Instance läuft.
7. aws:executeAwsApi— Ruft die IDs für die temporäre Amazon EC2 EC2-Instance und die VPC-Peering-Verbindung ab, die von erstellt wurden. AWS CloudFormation
8. aws:executeAwsApi— Ruft die IP-Adresse für die temporäre Amazon EC2 EC2-Instance ab, um die Konnektivität mit Ihrer DB-Instance zu konfigurieren.
9. aws:executeAwsApi— Kennzeichnet das Amazon EBS-Volume, das an die temporäre Amazon EC2 EC2-Instance angehängt ist.

10. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.
11. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance von Systems Manager verwaltet wird. Wenn bei diesem Schritt eine Zeitüberschreitung eintritt oder ein Fehler auftritt, startet das Runbook die Instance neu.
    a. `aws:executeAwsApi`— Startet die temporäre Amazon EC2 EC2-Instance neu, falls der vorherige Schritt fehlgeschlagen ist oder das Zeitlimit überschritten wurde.
    b. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance nach dem Neustart von Systems Manager verwaltet wird.
12. `aws:runCommand`- Installiert die Anwendungsanforderungen für den Metadatensammler auf der temporären Amazon EC2 EC2-Instance.
13. `aws:runCommand`- Konfiguriert den Zugriff auf Ihre DB-Instance, indem eine Konfigurationsdatei auf der temporären Amazon EC2 EC2-Instance erstellt wird.
14. `aws:executeAwsApi`— Erstellt ein Wartungsfenster, in dem die Metadatensammler-Anwendung regelmäßig mithilfe von Run Command ausgeführt werden kann. Das Wartungsfenster startet und stoppt die Instanz zwischen den Befehlen.
15. `aws:waitForAwsResourceProperty`- Wartet, bis das von der AWS CloudFormation Vorlage erstellte Wartungsfenster bereit ist.
16. `aws:executeAwsApi`- Ruft die IDs für das Wartungsfenster und den Änderungskalender ab, die von AWS CloudFormation erstellt wurden.
17. `aws:sleep`- Wartet bis zum Enddatum des Wartungsfensters.
18. `aws:executeAwsApi`- Schaltet das Wartungsfenster aus.
19. `aws:executeScript`- Ruft die Ergebnisse der Aufgaben ab, die während des Wartungsfensters ausgeführt wurden.
20. `aws:waitForAwsResourceProperty`- Wartet, bis das Wartungsfenster die letzte Aufgabe abgeschlossen hat, bevor der Vorgang fortgesetzt wird.
21. `aws:branch`- Verzweigt den Workflow je nachdem, ob Sie einen Wert für den `SupportCase` Parameter angegeben haben.
    a. `aws:changeInstanceState`- Startet die temporäre Amazon EC2 EC2-Instance und wartet, bis die Statusprüfungen bestanden sind, bevor der Bericht hochgeladen wird.
    b. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance von Systems Manager verwaltet wird. Wenn dieser Schritt das Timeout überschreitet oder fehlschlägt, startet das Runbook die Instance neu.

i. `aws:executeAwsApi`— Startet die temporäre Amazon EC2 EC2-Instance neu, falls der vorherige Schritt fehlgeschlagen ist oder das Zeitlimit überschritten wurde.

ii. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance nach dem Neustart von Systems Manager verwaltet wird.

c. `aws:runCommand`- Hängt den Metadatenbericht an den AWS Support Fall an, wenn Sie einen Wert für den Parameter angegeben haben. `SupportCase` Das Skript komprimiert den Bericht und teilt ihn in 5 MB-Dateien auf. Die maximale Anzahl von Dateien, die das Skript an einen AWS Support Fall anhängt, beträgt 12.

22. `aws:changeInstanceState`- Stoppt die temporäre Amazon EC2 EC2-Instance für den Fall, dass der AWS CloudFormation Stack nicht gelöscht werden kann.

23. `aws:executeAwsApi`— Beschreibt die AWS CloudFormation Stack-Ereignisse, falls die Runbooks den Stack nicht erstellen oder aktualisieren können. AWS CloudFormation

24. `aws:waitForAwsResourceProperty`- Wartet, bis sich der AWS CloudFormation Stack im Terminalstatus befindet, bevor er gelöscht wird.

25. `aws:executeAwsApi`- Löscht den AWS CloudFormation Stapel mit Ausnahme des Wartungsfensters. Das Amazon EBS-Stammvolume, das der temporären Amazon EC2 EC2-Instance zugeordnet ist, wird beibehalten, wenn der `EbsVolumeDeleteOnTermination` Parameterwert auf gesetzt wurde. `false`

## AWS-RebootRdsInstance

Beschreibung

Das `AWS-RebootRdsInstance` Runbook startet eine Amazon Relational Database Service (Amazon RDS) -DB-Instance neu, sofern sie nicht bereits neu gestartet wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon RDS-DB-Instance, die Sie neu starten möchten.

Dokumentschritte

RebootInstance - Startet die DB-Instance neu, falls sie nicht bereits neu gestartet wird.

WaitForAvailableState - Wartet darauf, dass die DB-Instance den Neustartvorgang abgeschlossen hat.

Ausgaben

Diese Automatisierung hat keine Ausgaben.

## AWSSupport-ShareRDSSnapshot

Beschreibung

Das `AWSSupport-ShareRDSSnapshot` Runbook bietet eine automatisierte Lösung für das Verfahren, das im Knowledge Center-Artikel Wie kann ich einen verschlüsselten Amazon RDS-DB-Snapshot mit einem anderen Konto teilen? beschrieben wird. Wenn Ihr Amazon Relational Database Service (Amazon RDS) -Snapshot mit der Standardeinstellung verschlüsselt wurde Von AWS verwalteter Schlüssel, können Sie den Snapshot nicht teilen. In diesem Fall müssen Sie den Snapshot mit einem vom Kunden verwalteten Schlüssel kopieren und den Snapshot dann mit dem Zielkonto teilen. Diese Automatisierung führt diese Schritte mit dem Wert aus, den Sie im

`SnapshotName` Parameter angeben, oder anhand des letzten Snapshots, der für die ausgewählte Amazon RDS-DB-Instance oder den ausgewählten Amazon RDS-DB-Cluster gefunden wurde.

> **Note**
>
> Wenn Sie keinen Wert für den `KMSKey` Parameter angeben, erstellt die Automatisierung einen neuen, vom AWS KMS Kunden verwalteten Schlüssel in Ihrem Konto, der zur Verschlüsselung des Snapshots verwendet wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AccountIds

  Typ: StringList

  Beschreibung: (Erforderlich) Durch Kommas getrennte Liste von Konto-IDs, mit denen der Snapshot geteilt werden soll.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Datenbank

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der Amazon RDS-DB-Instance oder des Clusters, dessen Snapshot Sie teilen möchten. Dieser Parameter ist optional, wenn Sie einen Wert für den `SnapshotName` Parameter angeben.

- KMS-Schlüssel

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der vollständige Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, der zur Verschlüsselung des Snapshots verwendet wurde.

- SnapshotName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des DB-Clusters oder Instance-Snapshots, den Sie verwenden möchten.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

`AutomationAssumeRole`Für den erfolgreichen Start des Runbooks für einen DB-Cluster sind die folgenden Aktionen erforderlich.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`

- `rds:ModifyDBClusterSnapshotAttribute`

Die zur Ausführung der Automatisierung verwendete IAM-Rolle muss als Schlüsselbenutzer hinzugefügt werden, um den im Parameter angegebenen KMS-Schlüssel verwenden zu können. `ARNKmsKey` Informationen zum Hinzufügen von Schlüsselbenutzern zu einem KMS-Schlüssel finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch.

Das `AutomationAssumeRole` erfordert die folgenden zusätzlichen Aktionen, um das Runbook erfolgreich zu starten, wenn Sie keinen Wert für den `KMSKey` Parameter angeben.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`
- `kms:DescribeKey`

Dokumentschritte

1. `aws:executeScript`- Überprüft, ob ein Wert für den `KMSKey` Parameter angegeben wurde, und erstellt einen vom AWS KMS Kunden verwalteten Schlüssel, falls kein Wert gefunden wird.
2. `aws:branch`- Überprüft, ob ein Wert für den `SnapshotName` Parameter angegeben wurde, und verzweigt entsprechend.
3. `aws:executeAwsApi`- Prüft, ob der bereitgestellte Snapshot von einer DB-Instance stammt.
4. `aws:executeScript`- Formatiert den `SnapshotName` Parameter und ersetzt Doppelpunkte durch einen Bindestrich.
5. `aws:executeAwsApi`- Kopiert den Snapshot mit dem angegebenen Wert. `KMSKey`
6. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
7. `aws:executeAwsApi`- Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
8. `aws:executeAwsApi`- Prüft, ob der bereitgestellte Snapshot aus einem DB-Cluster stammt.
9. `aws:executeScript`- Formatiert den `SnapshotName` Parameter und ersetzt Doppelpunkte durch einen Bindestrich.
10. `aws:executeAwsApi`- Kopiert den Snapshot mit dem angegebenen Wert. `KMSKey`
11. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.

12. `aws:executeAwsApi` - Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
13. `aws:executeAwsApi` - Prüft, ob der für den `Database` Parameter angegebene Wert eine DB-Instance ist.
14. `aws:executeAwsApi` - Prüft, ob der für den `Database` Parameter angegebene Wert ein DB-Cluster ist.
15. `aws:executeAwsApi` - Ruft eine Liste von Snapshots für die angegebenen Daten ab. `Database`
16. `aws:executeScript` - Ermittelt den neuesten verfügbaren Snapshot aus der Liste, die im vorherigen Schritt zusammengestellt wurde.
17. `aws:executeAwsApi` - Kopiert den DB-Instance-Snapshot mit dem angegebenen Wert`KMSKey`.
18. `aws:waitForAwsResourceProperty` - Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
19. `aws:executeAwsApi` - Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
20. `aws:executeAwsApi` - Ruft eine Liste von Snapshots für den angegebenen ab. `Database`
21. `aws:executeScript` - Ermittelt den neuesten verfügbaren Snapshot aus der Liste, die im vorherigen Schritt zusammengestellt wurde.
22. `aws:executeAwsApi` - Kopiert den DB-Instance-Snapshot mit dem angegebenen Wert`KMSKey`.
23. `aws:waitForAwsResourceProperty` - Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
24. `aws:executeAwsApi` - Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
25. `aws:executeScript` - Löscht den vom AWS KMS Kunden verwalteten Schlüssel, der durch die Automatisierung erstellt wurde, wenn Sie keinen Wert für den `KMSKey` Parameter angegeben haben und die Automatisierung fehlschlägt.

## `AWS-StartRdsInstance`

Beschreibung

Starten Sie eine Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon RDS-Instance, die gestartet werden soll.

## AWS-StartStopAuroraCluster

Beschreibung

Dieses Runbook startet oder stoppt einen Amazon Aurora Aurora-Cluster.

> **Note**
>
> Um einen Cluster zu starten, muss er sich in einem `stopped` Status befinden. Um einen Cluster zu stoppen, muss er sich in einem `available` Status befinden. Dieses Runbook kann nicht verwendet werden, um einen Cluster zu starten oder zu stoppen, der ein Aurora Serverless-Cluster, ein Aurora-Multimaster-Cluster, Teil einer globalen Aurora-Datenbank oder ein Cluster ist, der Aurora-Parallelabfrage verwendet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Aurora-Clusters, den Sie beenden oder starten möchten.
- Aktion

  Typ: Zeichenfolge

  Gültige Werte: Start | Stop

  Standard: Start

  Beschreibung: (Erforderlich) Der Name des Aurora-Clusters, den Sie beenden oder starten möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

Dokumentschritte

- `aws:executeScript`- Startet oder stoppt den Cluster auf der Grundlage der Werte, die Sie für die angeben.

Ausgaben

StartStopAuroraCluster. ClusterName - Der Name des Aurora-Clusters

StartStopAuroraCluster. CurrentStatus - Der aktuelle Status des Aurora-Clusters

StartStopAuroraCluster.Message — Einzelheiten der Automatisierung

## AWS-StopRdsInstance

Beschreibung

Stoppen Sie eine Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon RDS-Instance, die gestoppt werden soll.

## AWSSupport-TroubleshootConnectivityToRDS

Beschreibung

Das `AWSSupport-TroubleshootConnectivityToRDS` Runbook diagnostiziert Verbindungsprobleme zwischen einer EC2-Instance und einer Amazon Relational Database Service Service-Instance. Die Automatisierung stellt sicher, dass die DB-Instance verfügbar ist, und überprüft dann die zugehörigen Sicherheitsgruppenregeln, Netzwerkzugriffskontrolllisten (Network Access Control Lists, Netzwerk-ACLs) und Routing-Tabellen auf potenzielle Verbindungsprobleme.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DB InstanceIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die DB-Instance-ID, mit der die Konnektivität getestet werden soll.

- SourceInstance

  Typ: Zeichenfolge

  Zulässiges Muster: ^i-[a-z0-9]{8,17}$

  Beschreibung: (Erforderlich) Die ID der EC2-Instance, von der die Konnektivität getestet werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass der DB-Instance-Status lautet`available`.
- `aws:executeAwsApi`— Ruft Informationen über die DB-Instance ab.

- `aws:executeAwsApi`— Ruft Informationen über die Netzwerk-ACLs der DB-Instance ab.
- `aws:executeAwsApi`— Ruft das CIDR des DB-Instance-Subnetzes ab.
- `aws:executeAwsApi`— Ruft Informationen über die EC2-Instance ab.
- `aws:executeAwsApi`— Ruft Informationen über die Netzwerk-ACLs der EC2-Instanz ab.
- `aws:executeAwsApi`— Ruft Informationen über die Sicherheitsgruppen ab, die der EC2-Instance zugeordnet sind.
- `aws:executeAwsApi`— Ruft Informationen über die Sicherheitsgruppen ab, die der DB-Instance zugeordnet sind.
- `aws:executeAwsApi`- Ruft Informationen über die Routing-Tabellen ab, die der EC2-Instance zugeordnet sind.
- `aws:executeAwsApi`— Ruft Informationen über die Haupt-Routing-Tabelle ab, die der Amazon VPC für die EC2-Instance zugeordnet ist.
- `aws:executeAwsApi`— Ruft Informationen über die Routing-Tabellen ab, die der DB-Instance zugeordnet sind.
- `aws:executeAwsApi`— Ruft Informationen über die Haupt-Routing-Tabelle ab, die der Amazon VPC für die DB-Instance zugeordnet ist.
- `aws:executeScript`— Wertet Sicherheitsgruppenregeln aus.
- `aws:executeScript`- Wertet Netzwerk-ACLs aus.
- `aws:executeScript`- Wertet Routentabellen aus.
- `aws:sleep`- Beendet die Automatisierung.

Ausgaben

getRDS InstanceProperties .DB InstanceIdentifier — Die in der Automatisierung verwendete DB-Instance.

getRDS InstanceProperties .DB InstanceStatus — Der aktuelle Status der DbInstance.

evalSecurityGroupRegeln. SecurityGroupEvaluation — Ergebnisse des Vergleichs der `SourceInstance` Sicherheitsgruppenregeln mit den Sicherheitsgruppenregeln der DB-Instance.

evalNetworkAclRegeln. NetworkAclEvaluation — Ergebnisse des Vergleichs der `SourceInstance` Netzwerk-ACLs mit den Netzwerk-ACLs der DB-Instance.

evalRouteTableEinträge. RouteTableEvaluation - Ergebnisse aus dem Vergleich der `SourceInstance` Routentabelle mit den DB-Instance-Routen.

# AWSSupport-TroubleshootRDSIAMAuthentication

Beschreibung

Die AWSSupport-TroubleshootRDSIAMAuthentication hilft bei der Fehlerbehebung AWS Identity and Access Management (IAM) für Amazon-RDS-for-PostgreSQL-, Amazon-RDS-for-MySQL-, Amazon RDS for MariaDB, Amazon-Aurora-PostgreSQL- und Amazon-Aurora-MySQL-Instances. Verwenden Sie dieses Runbook, um die Konfiguration zu überprüfen, die für die IAM-Authentifizierung mit einer Amazon-RDS-Instance oder einem Aurora-Cluster erforderlich ist. Es enthält auch Schritte zur Behebung der Verbindungsprobleme mit der Amazon-RDS-Instance oder dem Aurora-Cluster.

> **Important**
>
> Dieses Runbook unterstützt nicht Amazon RDS für Oracle oder Amazon RDS für Microsoft SQL Server.

> **Important**
>
> Wenn eine Amazon EC2-Quell-Instance bereitgestellt wird und die Zieldatenbank Amazon RDS ist, AWSSupport-TroubleshootConnectivityToRDS wird eine untergeordnete Automatisierung zur Fehlerbehebung bei der TCP-Konnektivität aufgerufen. Die Ausgabe enthält auch Befehle, die Sie auf Ihrer Amazon EC2-Instance oder Ihrem Quellcomputer ausführen können, um mithilfe der IAM-Authentifizierung eine Verbindung zu den Amazon-RDS-Instances herzustellen.

Wie funktioniert es?

Dieses Runbook besteht aus sechs Schritten:

- Schritt 1: validateInputs :Validiert die Eingaben für die Automatisierung.
- Schritt 2: branchOnSourceEC2Provided :Prüft, ob in den Eingabeparametern eine Quell-Amazon EC2-Instance-ID angegeben ist.
- Schritt 3: validateRDSConnectivity :Validiert die Amazon-RDS-Konnektivität von der Amazon EC2Quell-Instance, falls angegeben.

- Schritt 4: validateRDSIAMAuthentication :Überprüft, ob die IAM-Authentifizierungsfunktion aktiviert ist.
- Schritt 5: validateIAMPolicies :Prüft, ob die erforderlichen IAM-Berechtigungen in dem bereitgestellten IAM-Benutzer/der IAM-Rolle vorhanden sind.
- Schritt 6: generateReport :Generiert einen Bericht über die Ergebnisse der zuvor ausgeführten Schritte.

## Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- RDSType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich): Wählen Sie den Typ der relationalen Datenbank aus, mit der Sie eine Verbindung herstellen und sich authentifizieren möchten.

  Zulässige Werte: `Amazon RDS` oder `Amazon Aurora Cluster.`
- DBInstanceIdentifier

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Kennung der Amazon RDS-Zieldatenbank-Instance oder des Aurora-Datenbank-Clusters.

Zulässiges Muster: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

Maximale Zeichenanzahl: 63

- SourceEc2InstanceIdentifier

  Typ: `AWS::EC2::Instance::Id`

  Beschreibung: (Optional) Die Amazon EC2-Instance-ID, wenn Sie von einer Amazon EC2-Instance, die im selben Konto und in derselben Region ausgeführt wird, eine Verbindung zur Amazon-RDS-Datenbank-Instance herstellen. Geben Sie diesen Parameter nicht an, wenn die Quelle keine Amazon EC2-Instance ist oder wenn der Ziel-Amazon-RDS-Typ ein Aurora-Datenbank-Cluster ist.

  Standard: ""

- DBIAMRoleName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IAM-Rollenname, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn der Parameter nicht angegeben `DBIAMUserName` ist. Andernfalls lassen Sie ihn leer. Entweder `DBIAMRoleName` oder `DBIAMUserName` muss angegeben werden.

  Zulässiges Muster: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Maximale Zeichenanzahl: 64

  Standard: ""

- DBIAMUserName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IAM-Benutzername, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn der `DBIAMRoleName` Parameter nicht angegeben

ist. Andernfalls lassen Sie ihn leer. Entweder `DBIAMRoleName` oder `DBIAMUserName` muss angegeben werden.

Zulässiges Muster: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

Maximale Zeichenanzahl: 64

Standard: `""`

- DBUserName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Datenbankbenutzername, der einer IAM-Rolle/einem IAM-Benutzer für die IAM-basierte Authentifizierung innerhalb der Datenbank zugeordnet ist. Die Standardoption `*` prüft, ob die `rds-db:connect` Berechtigung für alle Benutzer in der Datenbank zulässig ist.

  Zulässiges Muster: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Maximale Zeichenanzahl: 64

  Standard: `*`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Anweisungen

1. Navigieren Sie in der -AWS Systems ManagerKonsole zu AWSSupport-TroubleshootRDSIAMAuthentication.
2. Wählen Sie Automatisierung ausführen aus
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - RDSType (erforderlich):

     Wählen Sie den Typ von Amazon RDS aus, mit dem Sie eine Verbindung herstellen und sich authentifizieren möchten. Wählen Sie aus den beiden zulässigen Werten aus: `Amazon RDS` oder `Amazon Aurora Cluster.`
   - DB InstanceIdentifier (erforderlich):

     Geben Sie die ID der Amazon RDS-Zieldatenbank-Instance oder des Aurora-Clusters ein, mit dem Sie eine Verbindung herstellen möchten, und verwenden Sie IAM-Anmeldeinformationen für die Authentifizierung.
   - SourceEc2 InstanceIdentifier (optional):

     Geben Sie die Amazon EC2-Instance-ID an, wenn Sie von einer Amazon EC2-Instance, die sich im selben Konto und in derselben Region befindet, eine Verbindung zur Amazon-RDS-

Datenbank-Instance herstellen. Lassen Sie das Feld leer, wenn die Quelle nicht Amazon EC2 ist oder wenn der Ziel-Amazon-RDS-Typ ein Aurora-Cluster ist.

- DBIAM RoleName (optional):

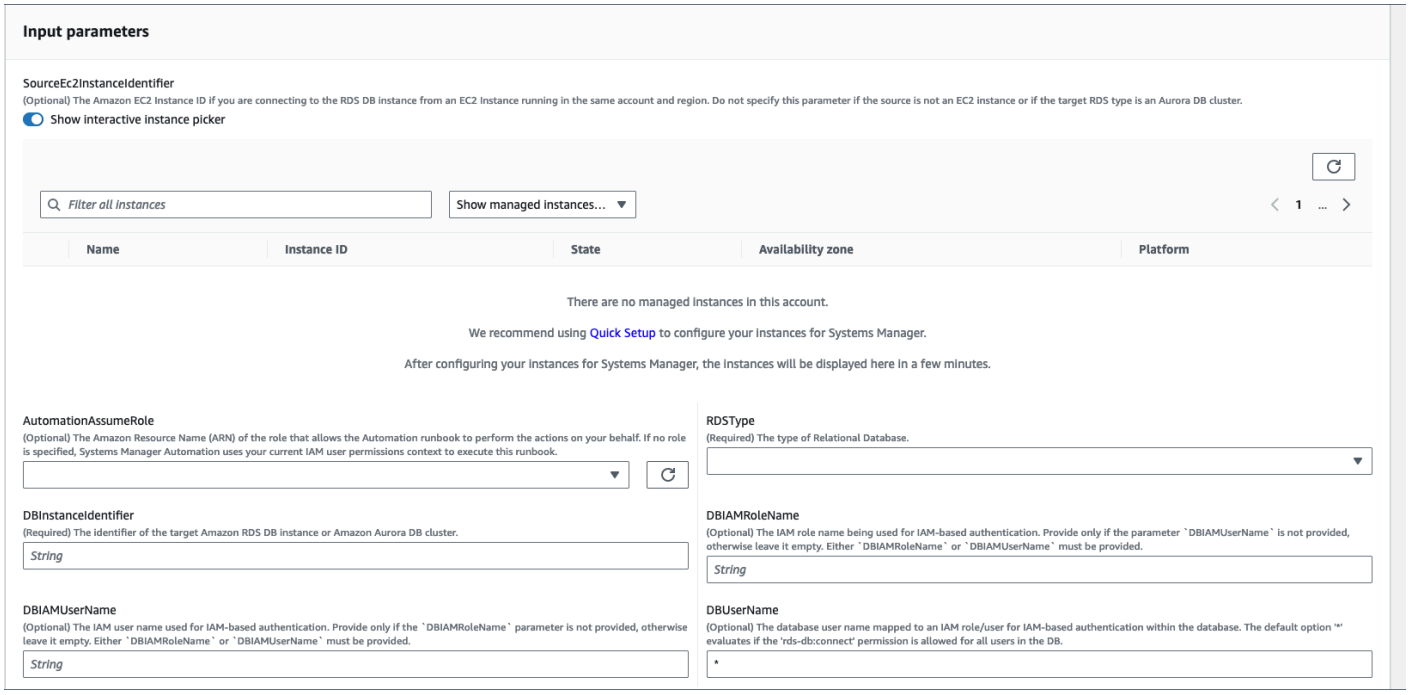
  Geben Sie den Namen der IAM-Rolle ein, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn nicht angegeben `DBIAMUserName` ist. Lassen Sie andernfalls das Feld leer. Entweder `DBIAMRoleName` oder `DBIAMUserName` muss angegeben werden.

- DBIAM UserName (optional):

  Geben Sie den IAM-Benutzer ein, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn nicht angegeben `DBIAMRoleName` ist, andernfalls lassen Sie das Feld leer. Entweder `DBIAMRoleName` oder `DBIAMUserName` muss angegeben werden.

- DB UserName (optional):

  Geben Sie den Datenbankbenutzer ein, der einer IAM-Rolle/einem IAM-Benutzer für die IAM-basierte Authentifizierung innerhalb der Datenbank zugeordnet ist. Die Standardoption * wird zur Auswertung verwendet. In diesem Feld wird nichts angegeben.




4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:

   - Schritt 1: validateInputs:

Validiert die Eingaben für die Automatisierung – `SourceEC2InstanceIdentifier` (optional), `DBInstanceIdentifier` oder `ClusterIDund` `DBIAMRoleName` oder `DBIAMUserName`. Es überprüft, ob die eingegebenen Eingabeparameter in Ihrem Konto und Ihrer Region vorhanden sind. Außerdem wird überprüft, ob der Benutzer einen der IAM-Parameter eingegeben hat (z. B. `DBIAMRoleName` oder `DBIAMUserName`). Darüber hinaus werden weitere Überprüfungen durchgeführt, z. B. wenn sich die erwähnte Datenbank im Status Verfügbar befindet.

- Schritt 2: branchOnSourceEC2Provided

  Prüft, ob die Quelle Amazon EC2 in den Eingabeparametern bereitgestellt wird und die Datenbank Amazon RDS ist. Wenn ja, wird mit Schritt 3 fortgefahren. Wenn nicht, wird Schritt 3 übersprungen, bei dem es sich um die AmazonAmazon EC2-Amazon-RDS-Konnektivitätsvalidierung handelt, und mit Schritt 4 fortgefahren.

- Schritt 3: validateRDSConnectivity

  Wenn die Quelle Amazon EC2 in den Eingabeparametern bereitgestellt wird und die Datenbank Amazon RDS ist, initiiert Schritt 2 Schritt 3. In diesem Schritt `AWSSupport-TroubleshootConnectivityToRDS` wird die untergeordnete Automatisierung aufgerufen, um die Amazon-RDS-Konnektivität von Amazon EC2-Quelle zu überprüfen. Das untergeordnete Automatisierungs-Runbook `AWSSupport-TroubleshootConnectivityToRDS` überprüft, ob die erforderlichen Netzwerkkonfigurationen (Amazon Virtual Private Cloud [Amazon VPC], Sicherheitsgruppen, Network Access Control List [NACL], Amazon-RDS-Verfügbarkeit) vorhanden sind, damit Sie eine Verbindung von der Amazon EC2-Instance zur Amazon-RDS-Instance herstellen können.

- Schritt 4: validateRDSIAMAuthentication:

  Überprüft, ob die IAM-Authentifizierungsfunktion auf der Amazon-RDS-Instance oder dem Aurora-Cluster aktiviert ist.

- Schritt 5: validateIAMPolicies:

  Prüft, ob die erforderlichen IAM-Berechtigungen in dem IAM-Benutzer/der IAM-Rolle vorhanden sind, der/die übergeben wurde, damit sich die IAM-Anmeldeinformationen bei der Amazon-RDS-Instance für den angegebenen Datenbankbenutzer authentifizieren können (falls vorhanden).

- Schritt 6: generateReport:

  Ruft alle Informationen aus den vorherigen Schritten ab und gibt das Ergebnis oder die Ausgabe jedes Schritts aus. Außerdem werden die Schritte aufgeführt, auf die verwiesen und die

ausgeführt werden sollen, um mithilfe der IAM-Anmeldeinformationen eine Verbindung mit der Amazon-RDS-Instance herzustellen.

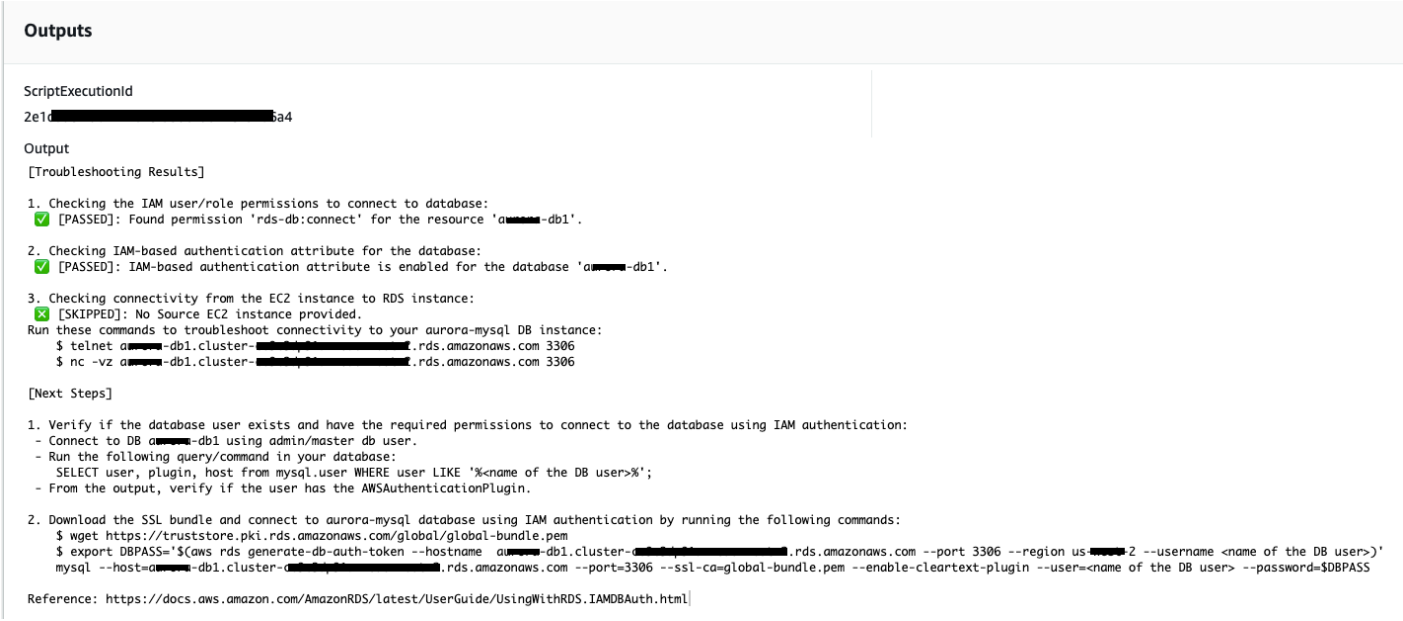
7. Wenn die Automatisierung abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse:
   - Überprüfen der IAM-Benutzer-/Rollenberechtigung zum Herstellen einer Verbindung mit der Datenbank:

     Prüft, ob die erforderlichen IAM-Berechtigungen in dem IAM-Benutzer/der IAM-Rolle vorhanden sind, der/die übergeben wurde, damit sich die IAM-Anmeldeinformationen bei der Amazon-RDS-Instance für den angegebenen Datenbankbenutzer authentifizieren können (falls vorhanden).
   - Überprüfen des IAM-basierten Authentifizierungsattributs für die Datenbank:

     Prüft, ob die Funktion der IAM-Authentifizierung für den angegebenen Amazon-RDS-Datenbank-/Aurora-Cluster aktiviert ist.
   - Überprüfen der Konnektivität von Amazon EC2-Instance zur Amazon-RDS-Instance:

     Prüft, ob die erforderlichen Netzwerkkonfigurationen (Amazon VPC, Sicherheitsgruppen, NACL, Amazon-RDS-Verfügbarkeit) vorhanden sind, damit Sie eine Verbindung von der Amazon EC2-Instance zur Amazon-RDS-Instance herstellen können.
   - Nächste Schritte:

     Listet die Befehle und Schritte auf, auf die verwiesen und die ausgeführt werden sollen, um mithilfe der IAM-Anmeldeinformationen eine Verbindung mit der Amazon-RDS-Instance herzustellen.




Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

## AWSSupport-ValidateRdsNetworkConfiguration

Beschreibung

`AWSSupport-ValidateRdsNetworkConfiguration` Die -Automatisierung hilft, den Status inkompatibler Netzwerke für Ihre vorhandene Amazon Relational Database Service (Amazon RDS)/ Amazon Aurora/Amazon DocumentDB-Instance zu vermeiden, bevor Sie `ModifyDBInstance` oder ausführen`StartDBInstance`. Wenn sich die Instance bereits im Status „Inkompatibles Netzwerk“ befindet, gibt das Runbook den Grund an.

Wie funktioniert es?

Dieses Runbook bestimmt, ob Ihre Amazon-RDS-Datenbank-Instance in den Status „inkompatibles Netzwerk“ übergeht oder ob sie sich im Status „inkompatibles Netzwerk“ befindet.

Das Runbook führt die folgenden Prüfungen für Ihre Amazon-RDS-Datenbank-Instance durch:

- Amazon Elastic Network Interface (ENI)-Kontingent pro Region.
- Alle Subnetze in der Datenbank-Subnetzgruppe sind vorhanden.
- Für das/die Subnetz(e) sind ausreichend freie IP-Adressen verfügbar.
- (Für öffentlich zugängliche Amazon-RDS-Instances) Einstellungen von VPC-Attributen (`enableDnsSupport` und `enableDnsHostnames`).

> **Important**
>
> Wenn Sie dieses Dokument für Amazon-Aurora-/Amazon DocumentDB-Cluster verwenden, stellen Sie sicher, dass Sie `DBInstanceIdentifier` anstelle von verwenden`ClusterIdentifier`. Andernfalls schlägt das Dokument im ersten Schritt fehl.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `ec2:DescribeSubnets`

Beispielrichtlinie:

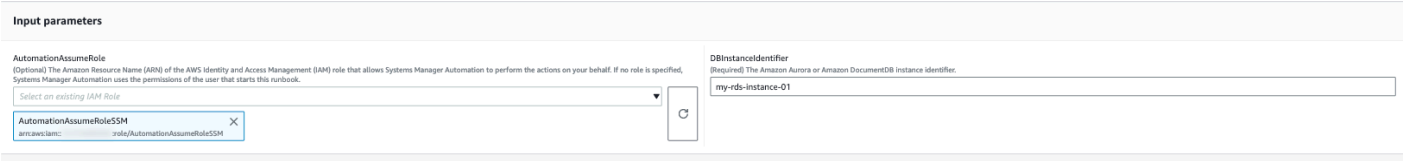
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateRdsNetwork",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "servicequotas:GetServiceQuota",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
            ]
        }
    ]
}
```

Anweisungen

1. Navigieren Sie in der -AWS Systems ManagerKonsole zur [AWSSupport-ValidateRdsNetworkConfiguration].
2. Wählen Sie Automatisierung ausführen aus
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - DB InstanceIdentifier (erforderlich):

Geben Sie die Instance-ID des Amazon Relational Database Service ein.




4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:
   - Schritt 1: assertRdsState:

     Prüft, ob die angegebene Instance-ID vorhanden ist und einen der folgenden Status hat: `available`, `stopped`, oder `incompatible-network`.
   - Schritt 2: gatherRdsInformation:

     Sammelt die erforderlichen Informationen über die Amazon-RDS-Instance, die später in der Automatisierung verwendet werden sollen.
   - Schritt 3: checkEniQuota:

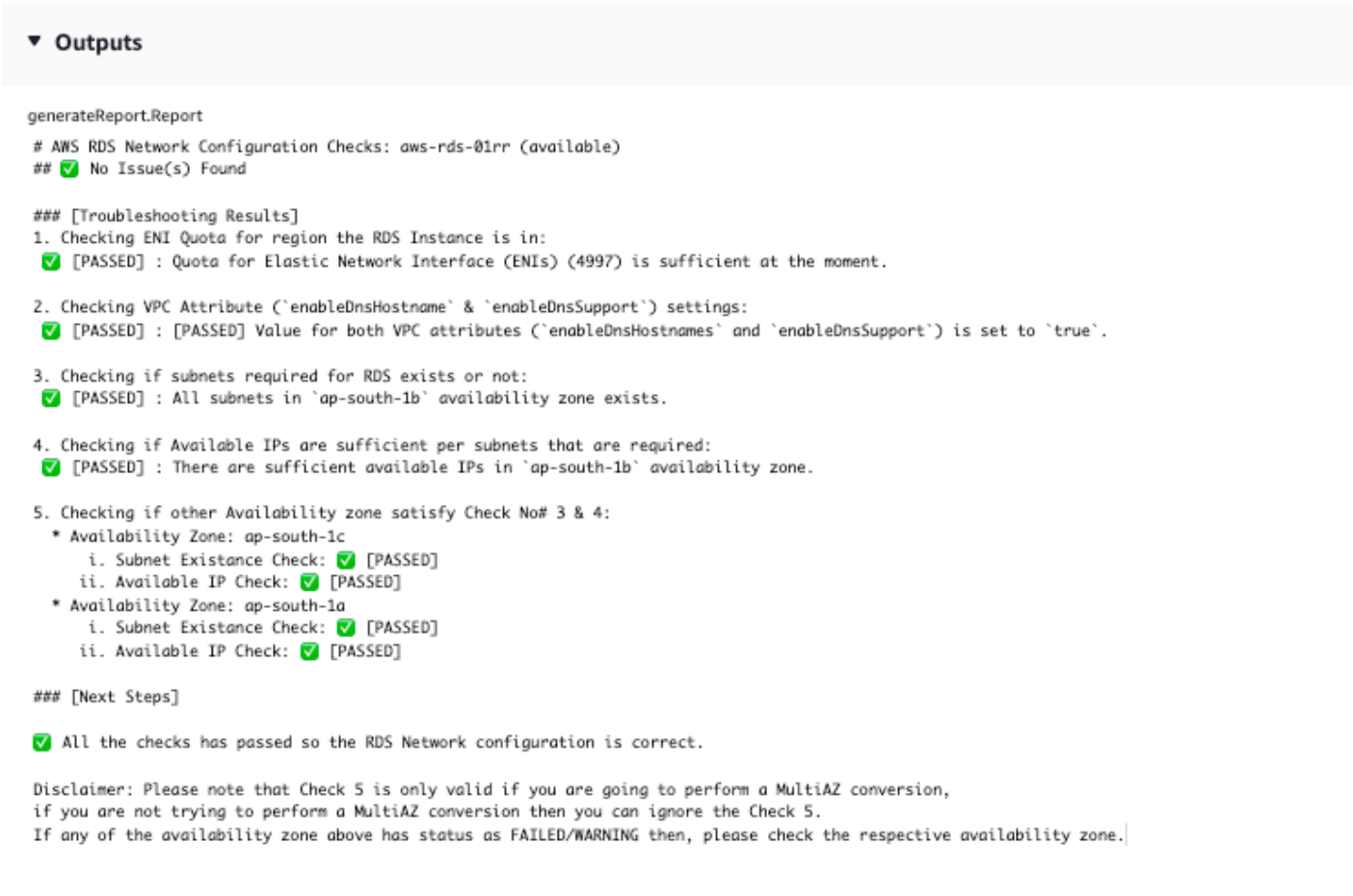
     Prüft auf das aktuell verfügbare Kontingent von Amazon ENI für die Region.
   - Schritt 4: validateVpcAttributes:

     Überprüft, ob die DNS-Parameter (`enableDnsSupport` und `enableDnsHostnames`) der Amazon VPC auf „true“ gesetzt sind (oder nicht, wenn die Amazon-RDS-Instance ist`PubliclyAccessible`).
   - Schritt 5: validateSubnetAttributes:

     Validiert das Vorhandensein von Subnetzen in der `DBSubnetGroup` und prüft, ob für jedes Subnetz verfügbare IPs vorhanden sind.
   - Schritt 6: generateReport:

     Ruft alle Informationen aus den vorherigen Schritten ab und gibt das Ergebnis oder die Ausgabe jedes Schritts aus. Außerdem werden die Schritte aufgeführt, auf die verwiesen werden soll und die ausgeführt werden sollen, um mithilfe der IAM-Anmeldeinformationen eine Verbindung mit der Amazon-RDS-Instance herzustellen.
7. Wenn die Automatisierung abgeschlossen ist, lesen Sie den Abschnitt Outputs für die detaillierten Ergebnisse:

Amazon RDS-Instance mit gültiger Netzwerkkonfiguration:



**Outputs**

generateReport.Report

```
# AWS RDS Network Configuration Checks: aws-rds-01rr (available)
## ✅ No Issue(s) Found

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
 ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4997) is sufficient at the moment.

2. Checking VPC Attribute (`enableDnsHostname` & `enableDnsSupport`) settings:
 ✅ [PASSED] : [PASSED] Value for both VPC attributes (`enableDnsHostnames` and `enableDnsSupport`) is set to `true`.

3. Checking if subnets required for RDS exists or not:
 ✅ [PASSED] : All subnets in `ap-south-1b` availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
 ✅ [PASSED] : There are sufficient available IPs in `ap-south-1b` availability zone.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1c
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]
  * Availability Zone: ap-south-1a
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]

### [Next Steps]

✅ All the checks has passed so the RDS Network configuration is correct.

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

Amazon-RDS-Instance mit falscher Netzwerkkonfiguration (VPC-Attribut enableDnsHostnames ist auf „false“ gesetzt):

**Outputs**

generateReport.Report

```
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattrs (stopped)
### ⛔ Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
 ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute (`enableDnsHostname` & `enableDnsSupport`) settings:
 ❌ [FAILED] : Value for `enableDnsHostnames` VPC Attribute is `false`.

3. Checking if subnets required for RDS exists or not:
 ✅ [PASSED] : All subnets in `ap-south-1b` availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
 ! [WARNING] : There are sufficient available IPs in `ap-south-1b` availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1a
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ! [WARNING]

### [Next Steps]
o Please set the value of `enableDnsHostnames` VPC attribute to `true`.
   [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop opeartion on the instance.
   [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

### AWS -Servicedokumentation

- Wie behebe ich Probleme mit einer Amazon-RDS-Datenbank, die sich in einem inkompatiblen Netzwerkstatus befindet?
- Wie behebe ich Probleme mit einer Amazon DocumentDB-Instance, die sich in einem inkompatiblen Netzwerkstatus befindet?

# Amazon-Redshift

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Redshift bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## `AWSConfigRemediation-DeleteRedshiftCluster`

Beschreibung

Das `AWSConfigRemediation-DeleteRedshiftCluster` Runbook löscht den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon Redshift Redshift-Clusters, den Sie löschen möchten.
- SkipFinalClusterSnapshot

  Typ: Boolesch

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt, erstellt die Automatisierung einen Snapshot`false`, bevor der Amazon Redshift Redshift-Cluster gelöscht wird. Wenn auf gesetzt`true`, wird kein endgültiger Cluster-Snapshot erstellt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Dokumentschritte

- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `SkipFinalClusterSnapshot` Parameter angeben.

- `aws:executeAwsApi`— Löscht den im Parameter angegebenen Amazon Redshift Redshift-Cluster. `ClusterIdentifier`
- `aws:assertAwsResourceProperty`— Überprüft, ob der Amazon Redshift Redshift-Cluster gelöscht wurde.

## AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Beschreibung

Das `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` Runbook deaktiviert den öffentlichen Zugriff für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie den öffentlichen Zugriff deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`- Deaktiviert den öffentlichen Zugriff für den im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status des Clusters ändert. `available`
- `aws:assertAwsResourceProperty`- Bestätigt, dass die Einstellung für öffentlichen Zugriff auf dem Cluster deaktiviert ist.

## AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` Runbook aktiviert die Auditprotokollierung für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3) -Buckets, in den Sie Protokolle hochladen möchten.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie die Audit-Protokollierung aktivieren möchten.
- S3 KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie Protokolle hochladen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`

- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Dokumentschritte

- `aws:branch`- Verzweigt basierend darauf, ob ein Wert für den `S3KeyPrefix` Parameter angegeben wurde.
- `aws:executeAwsApi`- Aktiviert die Auditprotokollierung auf dem im `ClusterIdentifier` Parameter angegebenen Cluster.
- `aws:assertAwsResourceProperty`— Überprüft, ob die Auditprotokollierung auf dem Cluster aktiviert wurde.

## AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` Runbook ermöglicht automatisierte Snapshots für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- AutomatedSnapshotRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die automatische Snapshots aufbewahrt werden.

- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie automatische Snapshots aktivieren möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

## Dokumentschritte

- `aws:executeAwsApi`— Aktiviert Automatisierungs-Snapshots auf dem im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status des Clusters ändert. `available`
- `aws:executeScript`- Bestätigt, dass automatische Snapshots auf dem Cluster aktiviert wurden.

# AWSConfigRemediation-EnableRedshiftClusterEncryption

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterEncryption` Runbook ermöglicht die Verschlüsselung auf dem von Ihnen angegebenen Amazon Redshift Redshift-Cluster mithilfe eines AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre Amazon Redshift Redshift-Cluster gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Cluster mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln. Dieses Runbook kann den vom AWS KMS Kunden verwalteten Schlüssel, der auf einem bereits verschlüsselten Cluster verwendet wird, nicht ändern. Um den vom AWS KMS Kunden verwalteten Schlüssel zu ändern, der zur Verschlüsselung eines Clusters verwendet wird, müssen Sie zuerst die Verschlüsselung auf dem Cluster deaktivieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie die Verschlüsselung aktivieren möchten.

- KMSKeyarn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung der Clusterdaten verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Verschlüsselung auf dem im `ClusterIdentifier` Parameter angegebenen Amazon Redshift Redshift-Cluster.
- `aws:assertAwsResourceProperty`— Überprüft, ob die Verschlüsselung auf dem Cluster aktiviert wurde.

## AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` Runbook ermöglicht erweitertes Virtual Private Cloud (VPC) -Routing für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster. Informationen zu erweitertem VPC-Routing finden Sie unter Amazon Redshift Enhanced VPC Routing im Amazon Redshift Management Guide.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert erweitertes VPC-Routing auf dem im `ClusterIdentifier` Parameter angegebenen Cluster.
- `assertAwsResourceProperty`- Bestätigt, dass erweitertes VPC-Routing auf dem Cluster aktiviert wurde.

## AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Beschreibung

Das `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` Runbook erfordert, dass eingehende Verbindungen SSL für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Dokumentschritte

- `aws:executeAwsApi`- Ruft Parameterdetails aus dem im Parameter angegebenen Cluster ab. `ClusterIdentifier`
- `aws:executeAwsApi`- Aktiviert die `require_ssl` Einstellung für den im `ClusterIdentifier` Parameter angegebenen Cluster.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `require_ssl` Einstellung auf dem Cluster aktiviert wurde.
- `aws:executeScript`- Überprüft die `require_ssl` Einstellung für den Cluster.

## AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Beschreibung

Das `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` Runbook ändert die Wartungseinstellungen für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AllowVersionUpgraden

  Typ: Boolesch

  Beschreibung: (Erforderlich) Wenn diese Option auf gesetzt ist`true`, werden Hauptversions-Upgrades während des Wartungsfensters automatisch auf den Cluster angewendet.
- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- AutomatedSnapshotRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, an denen automatische Snapshots aufbewahrt werden.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

- PreferredMaintenanceFenster

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der wöchentliche Zeitraum (in UTC), in dem Systemwartungen durchgeführt werden können.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ändert die Wartungseinstellungen für den im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:assertAwsResourceProperty`- Bestätigt, dass die geänderten Wartungseinstellungen für den Cluster konfiguriert wurden.

## AWSConfigRemediation-ModifyRedshiftClusterNodeType

Beschreibung

Das `AWSConfigRemediation-ModifyRedshiftClusterNodeType` Runbook ändert den Knotentyp und die Anzahl der Knoten für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Classic

  Typ: Boolesch

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird für die Größenänderung der klassische Größenänderungsprozess verwendet.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, dessen Knotentyp Sie ändern möchten.
- ClusterType

  Typ: Zeichenfolge

  Gültige Werte: Einzelknoten | Mehrknoten

  Beschreibung: (Erforderlich) Der Clustertyp, den Sie Ihrem Cluster zuweisen möchten.
- NodeType

  Typ: Zeichenfolge

  Gültige Werte: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

Beschreibung: (Erforderlich) Der Knotentyp, den Sie Ihrem Cluster zuweisen möchten.

- NumberOfKnoten

  Typ: Ganzzahl

  Gültige Werte: 2-100

  Beschreibung: (Optional) Die Anzahl der Knoten, die Sie Ihrem Cluster zuweisen möchten. Wenn es sich bei Ihrem Cluster um einen `single-node` Typ handelt, geben Sie keinen Wert für diesen Parameter an.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Dokumentschritte

- `aws:executeScript`- Ändert den Knotentyp und die Anzahl der Knoten für den `ClusterIdentifier` im Parameter angegebenen Cluster.

# Amazon S3

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Storage Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Das `AWS-ArchiveS3BucketToIntelligentTiering` Runbook erstellt oder ersetzt eine intelligente Tiering-Konfiguration für den von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, für den Sie eine intelligente Tiering-Konfiguration erstellen möchten.

- ConfigurationId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die intelligente Tiering-Konfiguration. Dies kann eine neue Konfigurations-ID oder die ID einer vorhandenen Konfiguration sein.

- NumberOfDaysToArchivieren

  Typ: Zeichenfolge

  Gültige Werte: 90-730

  Beschreibung: (Erforderlich) Die Anzahl der aufeinanderfolgenden Tage, nachdem ein Objekt in Ihrem Bucket für die Stufe Archive Access in Frage kommt.

- NumberOfDaysToDeepArchive

  Typ: Zeichenfolge

  Gültige Werte: 180-730

  Beschreibung: (Erforderlich) Die Anzahl der aufeinanderfolgenden Tage, nachdem ein Objekt in Ihrem Bucket für den Übergang in die Stufe Deep Archive Access in Frage kommt.

- S3Prefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, auf die Sie die Konfiguration anwenden möchten.

- Tags

Typ: MapList

Beschreibung: (Optional) Metadaten, die den Objekten zugewiesen sind, auf die Sie die Konfiguration anwenden möchten. Tags bestehen aus einem benutzerdefinierten Schlüssel und Wert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Dokumentschritte

- PutsBucketIntelligentTieringConfiguration (aws:ExecuteScript) — Erstellt oder aktualisiert eine Amazon S3 Intelligent-Tiering-Konfiguration für den angegebenen Bucket.
- VerifyBucketIntelligentTieringConfiguration (aws:assert AwsResource Property) — Überprüft, ob die intelligente S3-Bucket-Konfiguration auf den angegebenen Bucket angewendet wurde.

## AWS-ConfigureS3BucketLogging

Beschreibung

Aktivieren Sie die Protokollierung in einem Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, für den Sie die Protokollierung konfigurieren möchten.
- GrantedPermission

  Typ: Zeichenfolge

  Gültige Werte: FULL_CONTROL | READ | WRITE

  Beschreibung: (Erforderlich) Die dem Berechtigungsempfänger zugewiesenen Berechtigungen für den Bucket.
- GranteeEmailAdresse

  Typ: Zeichenfolge

  (Optional) E-Mail-Adresse des Berechtigungsempfängers
- GranteeId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die kanonische Benutzer-ID des Berechtigungsempfängers.
- GranteeType

Typ: Zeichenfolge

Gültige Werte: CanonicalUser | AmazonCustomerByEmail | Gruppe

Beschreibung: (Erforderlich) Typ des Berechtigungsempfängers.

- GranteeUri

  Typ: Zeichenfolge

  Beschreibung: (Optional) URI der Berechtigungsempfängergruppe.

- TargetBucket

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Gibt den Bucket an, in dem Amazon S3 Serverzugriffsprotokolle speichern soll. In jedem Bucket, den Sie besitzen, können vier Protokolle sein. Sie können auch mehrere Buckets konfigurieren, um ihre Protokolle zu demselben Ziel-Bucket zu senden. In diesem Fall sollten Sie TargetPrefix für jeden Quell-Bucket einen anderen auswählen, damit die bereitgestellten Protokolldateien anhand des Schlüssels unterschieden werden können.

- TargetPrefix

  Typ: Zeichenfolge

  Standard: /

  Beschreibung: (Optional) Gibt ein Präfix für die Schlüssel an, unter denen die Protokolldateien gespeichert werden.

## AWS-ConfigureS3BucketVersioning

Beschreibung

Konfigurieren Sie die Versionierung für einen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, für den Sie die Versionierung konfigurieren möchten.
- VersioningState

  Typ: Zeichenfolge

  Gültige Werte: Aktiviert | Suspendiert

  Standard: Aktiviert

  Beschreibung: (Optional) Wird auf den VersioningConfiguration .Status angewendet. Bei der Einstellung „Aktiviert“ aktiviert dieser Prozess das Versioning für die Objekte in dem Bucket; alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Versions-ID. Wenn dieser Prozess auf gesetzt ist`Suspended`, deaktiviert er die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten die Versions-ID. `null`

## AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Beschreibung

Das `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` Runbook konfiguriert die Einstellungen für den öffentlichen Zugriffsblock von Amazon Simple Storage Service (Amazon S3) für einen Amazon S3-Bucket auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BlockPublicAcls

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Zugriffskontrolllisten (ACLs) für den S3-Bucket und Objekte, die in dem S3-Bucket gespeichert sind, den Sie im `BucketName` Parameter angeben.
- BlockPublicRichtlinie

  Typ: Boolesch

  Standard: true

Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Bucket-Richtlinien für den S3-Bucket, den Sie im `BucketName` Parameter angeben.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie konfigurieren möchten.

- IgnorePublicAcls

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, ignoriert Amazon S3 alle öffentlichen ACLs für den S3-Bucket, den Sie im Parameter angeben. `BucketName`

- RestrictPublicBuckets

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, schränkt Amazon S3 die Richtlinien für öffentliche Buckets für den S3-Bucket ein, den Sie im `BucketName` Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt oder ändert die `PublicAccessBlock` Konfiguration für den im Parameter angegebenen S3-Bucket. `BucketName`
- `aws:executeScript`- Gibt die `PublicAccessBlock` Konfiguration für den im `BucketName` Parameter angegebenen S3-Bucket zurück und überprüft anhand der in den Runbook-Parametern angegebenen Werte, ob die Änderungen erfolgreich vorgenommen wurden.

## `AWSConfigRemediation-ConfigureS3PublicAccessBlock`

Beschreibung

Das `AWSConfigRemediation-ConfigureS3PublicAccessBlock` Runbook konfiguriert die Einstellungen für den öffentlichen Zugriff AWS-Konto von Amazon Simple Storage Service (Amazon S3) auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AccountId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Besitzers des S3-Buckets AWS-Konto , den Sie konfigurieren.
- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- BlockPublicAcls

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, blockiert Amazon S3 öffentliche Zugriffskontrolllisten (ACLs) für S3-Buckets, deren Eigentümer die von AWS-Konto Ihnen im Parameter angegebenen sind. `AccountId`

- BlockPublicRichtlinie

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Bucket-Richtlinien für S3-Buckets, deren Eigentümer die sind, die AWS-Konto Sie im `AccountId` Parameter angeben.

- IgnorePublicAcls

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, ignoriert Amazon S3 alle öffentlichen ACLs für S3-Buckets, die den gehören, die AWS-Konto Sie im Parameter angeben. `AccountId`

- RestrictPublicBuckets

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, schränkt Amazon S3 öffentliche Bucket-Richtlinien für S3-Buckets ein, deren Eigentümer die sind, die AWS-Konto Sie im Parameter angeben. `AccountId`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt oder ändert die `PublicAccessBlock` Konfiguration für den im Parameter AWS-Konto angegebenen `AccountId` Wert.
- `aws:executeScript`- Gibt die `PublicAccessBlock` Konfiguration für den im `AccountId` Parameter AWS-Konto angegebenen Wert zurück und überprüft anhand der in den Runbook-Parametern angegebenen Werte, ob die Änderungen erfolgreich vorgenommen wurden.

## `AWS-CreateS3PolicyToExpireMultipartUploads`

Beschreibung

Das `AWS-CreateS3PolicyToExpireMultipartUploads` Runbook erstellt eine Lebenszyklusrichtlinie für einen bestimmten Bucket, die bei unvollständigen, laufenden, mehrteiligen Uploads nach einer bestimmten Anzahl von Tagen abläuft. Dieses Runbook führt die neue Lebenszyklus-Richtlinie mit allen vorhandenen Lifecycle-Bucket-Richtlinien zusammen, die bereits existieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie konfigurieren möchten.
- DaysUntilLäuft ab

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Anzahl der Tage, die Amazon S3 wartet, bevor alle Teile des Uploads dauerhaft entfernt werden.
- RuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID, die zur Identifizierung der Lifecycle-Bucket-Regel verwendet wurde. Dies muss ein eindeutiger Wert sein.
- S3Prefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, auf die Sie die Konfiguration anwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Dokumentschritte

- ConfigureExpireMultipartUploads (aws:ExecuteScript) — Konfiguriert die Lebenszyklusrichtlinie für den Bucket.
- VerifyExpireMultipartUploads (aws:ExecuteScript) — Überprüft, ob die Lebenszyklusrichtlinie für den Bucket konfiguriert wurde.

Ausgaben

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

## AWS-DisableS3BucketPublicReadWrite

Beschreibung

Verwenden Sie Amazon Simple Storage Service (Amazon S3)`Block Public Access`, um den Lese- und Schreibzugriff für einen öffentlichen S3-Bucket zu deaktivieren. Weitere Informationen finden Sie unter Verwenden von Amazon S3 Block Public Access im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket, zu dem Sie den Zugriff einschränken möchten.

## AWS-EnableS3BucketEncryption

Beschreibung

Konfiguriert die Standardverschlüsselung für einen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, in dem Sie den Inhalt verschlüsseln möchten.

- SSEAlgorithm

  Typ: Zeichenfolge

  Standard: AES256

  Beschreibung: (Optional) Der serverseitige Verschlüsselungsalgorithmus für die Standard-Verschlüsselung.

## AWS-EnableS3BucketKeys

Beschreibung

Das `AWS-EnableS3BucketKeys` Runbook aktiviert Bucket Keys auf dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Dieser Schlüssel auf Bucket-Ebene erstellt während seines Lebenszyklus Datenschlüssel für neue Objekte. Wenn Sie keinen Wert für den `KmsKeyId` Parameter angeben, wird die serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) für die Standardverschlüsselungskonfiguration verwendet.

> **Note**
>
> Amazon S3 Bucket Keys werden für die duale serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln (DSSE-KMS) nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, für den Sie Bucket Keys aktivieren möchten.
- KMS KeyId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Sie für die serverseitige Verschlüsselung verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Dokumentschritte

- ChooseEncryptionType (aws:branch) — Wertet den für den `KmsKeyId` Parameter angegebenen Wert aus, um festzustellen, ob SSE-S3 (AES256) oder SSE-KMS verwendet werden.
- PutBucketkeysKMS (aws:executeAwsApi) — Setzt die Eigenschaft für den angegebenen S3-Bucket unter Verwendung der angegebenen Werte auf. `BucketKeyEnabled` `true` `KmsKeyId`
- PutBucketkeySaes256 (aws:executeAwsApi) — Setzt die `BucketKeyEnabled` Eigenschaft für den angegebenen S3-Bucket mit AES256-Verschlüsselung auf`true`.
- verifyS3 BucketKeysEnabled (aws:assert AwsResource Property) — Überprüft, ob die Bucket Keys im Ziel-S3-Bucket aktiviert sind.

## `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy`

Beschreibung

Das `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` Runbook entfernt grundlegende Richtlinienanweisungen, die Platzhalter (`Principal: *`oder`Principal: "AWS": *`) für `Allow` Aktionen enthalten, aus Ihrer Amazon Simple Storage Service (Amazon S3) -Bucket-Richtlinie. Richtlinienerklärungen mit Bedingungen werden ebenfalls entfernt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Richtlinie Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Dokumentschritte

- `aws:executeScript`- Ändert die Bucket-Richtlinie und überprüft, ob die wichtigsten Richtlinienanweisungen mit Platzhaltern aus dem Amazon S3 S3-Bucket entfernt wurden, den Sie im Parameter angeben. `BucketName`

## AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Beschreibung

Das `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` Runbook erstellt eine Bucket-Richtlinienanweisung für Amazon Simple Storage Service (Amazon S3), die HTTP-Anfragen an den von Ihnen angegebenen Amazon S3-Bucket ausdrücklich ablehnt.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie HTTP-Anfragen ablehnen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Dokumentschritte

- `aws:executeScript`— Erstellt eine Bucket-Richtlinie für den im `BucketName` Parameter angegebenen S3-Bucket, die HTTP-Anfragen explizit ablehnt.

## AWSSupport-TroubleshootS3PublicRead

Beschreibung

Das `AWSSupport-TroubleshootS3PublicRead` Runbook diagnostiziert Probleme beim Lesen von Objekten aus dem öffentlichen Amazon Simple Storage Service (Amazon S3) -Bucket, den `S3BucketName` Sie im Parameter angeben. Eine Teilmenge der Einstellungen wird auch für Objekte im S3-Bucket analysiert.

Führen Sie diese Automatisierung aus (Konsole)

Einschränkungen

- Diese Automatisierung sucht nicht nach Zugriffspunkten, die öffentlichen Zugriff auf Objekte ermöglichen.
- Diese Automatisierung wertet keine Bedingungsschlüssel in der S3-Bucket-Richtlinie aus.
- Wenn Sie verwenden AWS Organizations, bewertet diese Automatisierung keine Richtlinien zur Servicekontrolle, um zu bestätigen, dass der Zugriff auf Amazon S3 zulässig ist.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- CloudWatchLogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Amazon CloudWatch Logs-Protokollgruppe, in die Sie die Automatisierungsausgabe senden möchten. Wenn keine Protokollgruppe gefunden wird, die dem von Ihnen angegebenen Wert entspricht, erstellt die Automatisierung anhand dieses Parameterwerts eine Protokollgruppe. Die Aufbewahrungsfrist für die durch diese Automatisierung erstellte Protokollgruppe beträgt 14 Tage.

- CloudWatchLogStreamName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der CloudWatch Log-Log-Stream, in den Sie die Automatisierungsausgabe senden möchten. Wenn kein Log-Stream gefunden wird, der dem von Ihnen angegebenen Wert entspricht, erstellt die Automatisierung einen Log-Stream mit diesem Parameterwert. Wenn Sie keinen Wert für diesen Parameter angeben, verwendet die Automatisierung den `ExecutionId` als Namen des Log-Streams.

- HttpGet

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

Beschreibung: (Optional) Wenn dieser Parameter auf gesetzt ist`true`, sendet die Automatisierung eine teilweise HTTP-Anfrage an die Objekte in der von `S3BucketName` Ihnen angegebenen Liste. Nur das erste Byte des Objekts wird mithilfe des Range-HTTP-Headers zurückgegeben.

- IgnoreBlockPublicAccess

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Wenn dieser Parameter auf gesetzt ist`true`, ignoriert die Automatisierung die Einstellungen für den öffentlichen Zugriff des S3-Buckets, den Sie im `S3BucketName` Parameter angeben. Es wird nicht empfohlen, diesen Parameter gegenüber dem Standardwert zu ändern.

- MaxObjects

  Typ: Ganzzahl

  Gültige Werte: 1—25

  Standard: 5

  Beschreibung: (Optional) Die Anzahl der zu analysierenden Objekte im S3-Bucket, die Sie im `S3BucketName` Parameter angeben.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets für die Fehlerbehebung.

- S3 PrefixName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, die Sie in Ihrem S3-Bucket analysieren möchten. Weitere Informationen finden Sie unter Objektschlüssel im Amazon Simple Storage Service-Benutzerhandbuch.

- StartAfter

Typ: Zeichenfolge

Beschreibung: (Optional) Der Name des Objektschlüssels, bei dem die Automatisierung mit der Analyse von Objekten in Ihrem S3-Bucket beginnen soll.

- ResourcePartition

  Typ: Zeichenfolge

  Zulässige Werte: `aws` | `aws-us-gov` | `aws-cn`

  Standard: `aws`

  Beschreibung: (Erforderlich) Die Partition, auf der sich Ihr S3-Bucket befindet.

- Verbose

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Um während der Automatisierung detailliertere Informationen zurückzugeben, setzen Sie diesen Parameter auf`true`. Es werden nur Warn- und Fehlermeldungen zurückgegeben, wenn der Parameter auf gesetzt ist`false`.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die `logs:PutLogEvents` Berechtigungen `logs:CreateLogGrouplogs:CreateLogStream`, und sind nur erforderlich, wenn Sie möchten, dass die Automatisierung Protokolldaten an CloudWatch Logs sendet.

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

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass der S3-Bucket existiert und zugänglich ist.
- `aws:executeScript`- Gibt den Standort des S3-Buckets und Ihre kanonische Benutzer-ID zurück.

- `aws:executeScript`- Gibt die Einstellungen für die Sperrung des öffentlichen Zugriffs für Ihr Konto und den S3-Bucket zurück.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der S3-Bucket-Payer auf `BucketOwner` eingestellt ist. Wenn im S3-Bucket aktiviert `Requester Pays` ist, endet die Automatisierung.
- `aws:executeScript`- Gibt den Status der S3-Bucket-Richtlinie zurück und bestimmt, ob sie als öffentlich betrachtet wird. Weitere Informationen zu öffentlichen S3-Buckets finden Sie unter Die Bedeutung von „öffentlich“ im Amazon Simple Storage Service-Benutzerhandbuch.
- `aws:executeAwsApi`— Gibt die S3-Bucket-Richtlinie zurück.
- `aws:executeAwsApi`- Gibt alle Kontextschlüssel zurück, die in der S3-Bucket-Richtlinie gefunden wurden.
- `aws:assertAwsResourceProperty`— Bestätigt, ob die `GetObject` API-Aktion in der S3-Bucket-Richtlinie ausdrücklich abgelehnt wurde.
- `aws:executeAwsApi`— Gibt die Zugriffskontrollliste (ACL) für den S3-Bucket zurück.
- `aws:executeScript`- Erstellt eine CloudWatch Logs-Log-Gruppe und einen Log-Stream, wenn Sie einen Wert für den `CloudWatchLogGroupName` Parameter angeben.
- `aws:executeScript`- Basierend auf den Werten, die Sie in den Runbook-Eingabeparametern angeben, bewertet es, ob irgendwelche der während der Automatisierung gesammelten S3-Bucket-Einstellungen verhindern, dass Objekte von der Öffentlichkeit abgerufen werden. Dieses Skript führt die folgenden Funktionen aus:
  - Wertet die Einstellungen für öffentliche Zugangssperren aus
  - Gibt Objekte aus Ihrem S3-Bucket auf der Grundlage der Werte zurück, die Sie in den `StartAfter` Parametern `MaxObjects`S3`PrefixName`, und angeben.
  - Gibt die S3-Bucket-Richtlinie zurück, um eine benutzerdefinierte IAM-Richtlinie für die von Ihrem S3-Bucket zurückgegebenen Objekte zu simulieren.
  - Führt eine teilweise HTTP-Anfrage an die zurückgegebenen Objekte aus, wenn der `HttpGet` Parameter auf `true` gesetzt ist. Nur das erste Byte des Objekts wird mithilfe des Range-HTTP-Headers zurückgegeben.
  - Überprüft den Schlüsselnamen des zurückgegebenen Objekts, um zu bestätigen, ob er mit einem oder zwei Punkten endet. Objektschlüsselnamen, die mit Punkten enden, können nicht von der Amazon S3 S3-Konsole heruntergeladen werden.
  - Prüft, ob der Besitzer des zurückgegebenen Objekts mit dem Besitzer des S3-Buckets übereinstimmt.

- Prüft, ob die ACL des Objekts anonymen Benutzern `FULL_CONTROL` Berechtigungen gewährt `READ` oder gewährt.
- Gibt Tags zurück, die dem Objekt zugeordnet sind.
- Verwendet die simulierte IAM-Richtlinie, um zu bestätigen, ob es in der S3-Bucket-Richtlinie für die `GetObject` API-Aktion eine ausdrückliche Ablehnung für dieses Objekt gibt.
- Gibt die Metadaten des Objekts zurück, um zu bestätigen, dass die Speicherklasse unterstützt wird.
- Überprüft die serverseitigen Verschlüsselungseinstellungen des Objekts, um zu bestätigen, ob das Objekt mit einem AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel verschlüsselt ist.

Ausgaben

AnalyzeObjects.bucket

AnalyzeObjects.objekt

# SageMaker

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon SageMaker bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-DisableSageMakerNotebookRootAccess

## `AWS-DisableSageMakerNotebookRootAccess`

Beschreibung

Das `AWS-DisableSageMakerNotebookRootAccess` Runbook deaktiviert den Root-Zugriff auf eine SageMaker Amazon-Notebook-Instance. Während der Automatisierung wird die Notebook-Instance gestoppt, um die erforderlichen Änderungen vorzunehmen. SageMaker Studio-Notebook-Instanzen werden nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- NotebookInstanceName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der SageMaker Notebook-Instanz, auf der der Root-Zugriff deaktiviert werden soll.
- StartInstanceAfterUpdate

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Legt fest, ob die Notebook-Instanz nach dem Deaktivieren des Root-Zugriffs gestartet wird. Die Standardeinstellung für diesen Parameter ist`true`. Wenn auf gesetzt`true`, wird die Instanz gestartet, nachdem der Root-Zugriff deaktiviert wurde. Wenn auf gesetzt`false`, verbleibt die Instanz in dem `stopped` Zustand, in dem der Root-Zugriff deaktiviert wurde.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Dokumentschritte

- CheckNotebookInstanceStatus (aws:executeAwsApi): Prüft den aktuellen Status der Notebook-Instanz.
- StopOrUpdateNotebookInstance (aws:branch): Verzweigt basierend auf dem Status der Notebook-Instanz.
- StopNotebookInstance (aws:executeAwsApi): Startet die Instanz, wenn der Status lautet. `stopped`
- WaitForInstanceToStop (aws:wait ForAwsResourceProperty): Überprüft, ob die Instanz `stopped`
- UpdateNotebookInstance (aws:executeAwsApi): Deaktiviert den Root-Zugriff auf die Notebook-Instanz.
- WaitForNotebookUpdate (aws:wait ForAwsResourceProperty): Überprüft, ob der Root-Zugriff deaktiviert wurde und die Instanz einen Status hat. `stopped`
- ChooseInstanceStart (aws:branch): Verzweigung, die darauf basiert, ob die Instanz gestartet werden soll.
- StartNotebookInstance (aws:executeAwsApi): Startet die Notebook-Instanz.
- VerifyNotebookInstanceStatus (aws:wait ForAwsResourceProperty): Überprüft, ob die Instanz aktiv ist, bevor der Root-Zugriff deaktiviert wird`available`.
- VerifyNotebookInstanceRootAccess (AwsResourceaws:assert-Eigenschaft): Überprüft, ob die Einstellung für den Root-Zugriff auf die Notebook-Instanz erfolgreich deaktiviert wurde.

# Secrets Manager

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Secrets Manager Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## `AWSConfigRemediation-DeleteSecret`

Beschreibung

Das `AWSConfigRemediation-DeleteSecret` Runbook löscht ein Geheimnis und alle darin gespeicherten Versionen. AWS Secrets Manager Sie können optional das Wiederherstellungsfenster angeben, in dem Sie das Geheimnis wiederherstellen können. Wenn Sie keinen Wert für den `RecoveryWindowInDays` Parameter angeben, wird der Vorgang standardmäßig auf 30 Tage eingestellt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- RecoveryWindowInDays

  Typ: Ganzzahl

  Gültige Werte: 7-30

  Standard: 30

  Beschreibung: (Optional) Die Anzahl der Tage, an denen Sie das Geheimnis wiederherstellen können.

- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Geheimnisses, das Sie löschen möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

## Dokumentschritte

- `aws:executeAwsApi`- Löscht das Geheimnis, das Sie im `SecretId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob das Löschen des Geheimnisses geplant wurde.

# AWSConfigRemediation-RotateSecret

Beschreibung

Das `AWSConfigRemediation-RotateSecret` Runbook rotiert ein in gespeichertes Geheimnis. AWS Secrets Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- RotationInterval

  Typ: Intervall

  Gültige Werte: 1—365

  Beschreibung: (Erforderlich) Die Anzahl der Tage zwischen den Rotationen des Geheimnisses.
- RotationLambdaArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Lambda Funktion, die das Geheimnis rotieren kann.

- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Geheimnisses, das Sie rotieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Dokumentschritte

- `aws:executeAwsApi`- Dreht das Geheimnis, das Sie im `SecretId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob die Rotation für das Geheimnis aktiviert wurde.

# Security Hub

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Security Hub Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-EnableSecurityHub

## `AWSConfigRemediation-EnableSecurityHub`

Beschreibung

Das `AWSConfigRemediation-EnableSecurityHub` Runbook aktiviert AWS Security Hub (Security Hub) für die AWS-Konto und AWS-Region wo Sie die Automatisierung ausführen. Informationen zu Security Hub finden Sie unter Was ist AWS Security Hub? im AWS Security Hub Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EnableDefaultStandards

  Typ: Boolesch

  Standard: true

  Beschreibung: (Erforderlich) Wenn auf gesetzt`true`, sind die von Security Hub festgelegten Standardsicherheitsstandards aktiviert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert Security Hub im Girokonto und in der Region.
- `aws:executeAwsApi`- Überprüft, ob Security Hub aktiviert wurde.

# AWS Shield

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS Shield Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSPremiumSupport-DDoSResiliencyAssessment

## `AWSPremiumSupport-DDoSResiliencyAssessment`

Beschreibung

Das Automatisierungs-AWS Systems ManagerRunbook von hilft Ihnen`AWSPremiumSupport-DDoSResiliencyAssessment`, DDoS-Schwachstellen und die Konfiguration von -Ressourcen gemäß dem AWS Shield Advanced Schutz für Ihr zu überprüfenAWS-Konto. Es bietet einen Bericht über Konfigurationseinstellungen für Ressourcen, die anfällig für DDoSDDoSAngriffe (Distributed Denial of Service). Es wird verwendet, um die folgenden Ressourcen zu erfassen, zu analysieren und zu bewerten: Amazon Route 53, Amazon Load Balancer, Amazon- CloudFront Verteilungen AWS Global Accelerator und AWS Elastic IPs für ihre Konfigurationseinstellungen gemäß den empfohlenen bewährten Methoden für AWS Shield Advanced Protection. Der endgültige Konfigurationsbericht ist in einem Amazon S3-Bucket Ihrer Wahl als HTML-Datei verfügbar.

Wie funktioniert es?

Dieses Runbook enthält eine Reihe von Prüfungen für die verschiedenen Arten von Ressourcen, die für den öffentlichen Zugriff aktiviert sind, und ob für sie Schutzmaßnahmen gemäß den

Empfehlungen im AWS Whitepaper zu bewährten Methoden für DDoS konfiguriert sind. Das Runbook führt Folgendes aus:

- Prüft, ob ein Abonnement für aktiviert AWS Shield Advanced ist.
- Wenn diese Option aktiviert ist, wird festgestellt, ob es geschützte Shield-Advanced-Ressourcen gibt.
- Es findet alle globalen und regionalen Ressourcen in der AWS-Konto und prüft, ob diese Shield-geschützt sind.
- Sie benötigt die Ressourcentypparameter für die Bewertung, den Amazon S3-Bucket-Namen und die Amazon S3-BucketAWS-Konto-ID (S3BucketOwner).
- Es gibt die Ergebnisse als HTML-Bericht zurück, der im bereitgestellten Amazon S3-Bucket gespeichert ist.

Die Eingabeparameter `AssessmentType` entscheiden, ob die Prüfungen für alle Ressourcen durchgeführt werden. Standardmäßig prüft das Runbook auf alle Arten von Ressourcen. Wenn nur der `RegionalResources` Parameter `GlobalResources` oder ausgewählt ist, führt das Runbook nur Prüfungen für die ausgewählten Ressourcentypen durch.

> **Important**
>
> - Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Enterprise- oder Business-Support-Abonnement erforderlich. Weitere Informationen finden Sie unter Vergleichen von - AWS SupportPlänen.
> - Für dieses Runbook ist ein -`ACTIVE`AWS Shield AdvancedAbonnement erforderlich.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- AssessmentType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Bestimmt die Art der Ressourcen, die für die DDoSDDoSAusfallsicherheit bewertet werden sollen. Standardmäßig wertet das Runbook sowohl globale als auch regionale Ressourcen aus. Für regionale Ressourcen beschreibt das Runbook alle Application (ALB)- und Network (NLB)-Load Balancer sowie alle Auto Scaling-Gruppen in IhremAWS-Konto/Ihrer Region.

  Zulässige Werte: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  Standard: Globale und regionale Ressourcen

- S3BucketName

  Typ: `AWS::S3::Bucket::Name`

  Beschreibung: (Erforderlich) Der Name des Amazon S3-Buckets, in den der Bericht hochgeladen wird.

  Zulässiges Muster: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3BucketOwnerAccount

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das AWS-Konto, dem der Amazon S3-Bucket gehört. Bitte geben Sie diesen Parameter an, wenn der Amazon S3-Bucket zu einem anderen gehörtAWS-Konto. Andernfalls können Sie diesen Parameter leer lassen.

Zulässiges Muster: `^$|^[0-9]{12,13}$`

- S3BucketOwnerRoleArn

  Typ: `AWS::IAM::Role::Arn`

  Beschreibung: (Optional) Der ARN einer IAM-Rolle mit Berechtigungen zum Beschreiben des Amazon S3-Buckets und zum AWS-Konto Blockieren der Konfiguration des öffentlichen Zugriffs, wenn sich der Bucket in einem anderen befindetAWS-Konto. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook die `AutomationAssumeRole` oder den IAM-Benutzer, der dieses Runbook startet (wenn nicht angegeben `AutomationAssumeRole` ist). Bitte sehen Sie sich den Abschnitt mit den erforderlichen Berechtigungen in der Runbook-Beschreibung an.

  Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3BucketPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Präfix für den Pfad in Amazon S3 zum Speichern der Ergebnisse.

  Zulässiges Muster: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine IAM-Richtlinie für die Automation Assume-Rolle

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

Anweisungen

1. Navigieren Sie in der -AWS Systems ManagerKonsole zum AWSPremiumSupport-DDoSResiliencyAssessment.
2. Wählen Sie Automatisierung ausführen aus
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - AssessmentType (Optional):

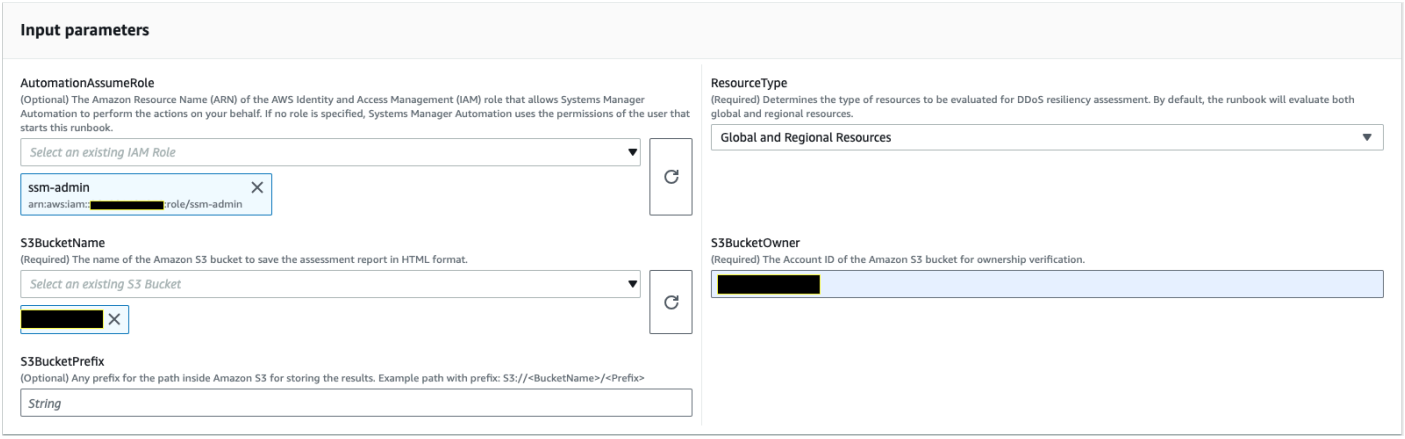
     Bestimmt die Art der Ressourcen, die für die DDoSDDoSAusfallsicherheit bewertet werden sollen. Standardmäßig wertet das Runbook sowohl globale als auch regionale Ressourcen aus.
   - S3BucketName (erforderlich):

     Der Name des Amazon S3-Buckets, in dem der Bewertungsbericht im HTML-Format gespeichert werden soll.
   - S3BucketOwner (optional):

Die AWS-Konto ID des Amazon S3-Buckets für die Eigentumsüberprüfung. Die AWS-Konto ID ist erforderlich, wenn der Bericht in einem kontoübergreifenden Amazon S3-Bucket veröffentlicht werden muss, und optional, wenn sich der Amazon S3-Bucket in derselben AWS-Konto wie die Automatisierungsinitiierung befindet.

- S3BucketPrefix (optional):

  Jedes Präfix für den Pfad in Amazon S3 zum Speichern der Ergebnisse.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - CheckShieldAdvancedState:

     Prüft, ob der in „S3BucketName“ angegebene Amazon S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen zulässt, ob für den Bucket die Verschlüsselung im Ruhezustand aktiviert ist und ob die in „S3BucketOwner“ angegebene AWS-Konto ID der Eigentümer des Amazon S3-Buckets ist.

   - S3BucketSecurityChecks:

     Prüft, ob der in „S3BucketName“ angegebene Amazon S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen zulässt, ob für den Bucket die Verschlüsselung im Ruhezustand aktiviert ist und ob die in „S3BucketOwner“ angegebene AWS-Konto ID der Eigentümer des Amazon S3-Buckets ist.

   - BranchOnShieldAdvancedStatus:

     Verzweigt Dokumentschritte basierend auf dem AWS Shield Advanced Abonnementstatus und/oder dem Status der Amazon S3-Bucket-Eigentümerschaft.

- ShieldAdvancedConfigurationReview:

  Überprüft Shield Advanced-Konfigurationen, um sicherzustellen, dass die mindestens erforderlichen Details vorhanden sind. Zum Beispiel: Team von IAM Access for AWS Shield Response Team (SRT), Kontaktdaten und Status des proaktiven SRT-Engagements.

- ListShieldAdvancedProtections:

  Listet die Shield Protected Resources auf und erstellt eine Gruppe geschützter Ressourcen für jeden Service.

- BranchOnResourceTypeAndCount:

  Verzweigt Dokumentschritte basierend auf dem Wert des Ressourcentypparameters und der Anzahl der durch Shield geschützten globalen Ressourcen.

- ReviewGlobalResources:

  Überprüft die durch Shield Advanced geschützten globalen Ressourcen wie Route 53 Hosted Zones, CloudFront Distributionen und Global Accelerators.

- BranchOnResourceType:

  Verzweigt Dokumentschritte basierend auf der Ressourcentypauswahl, wenn Global, Regional oder beides.

- ReviewRegionalResources:

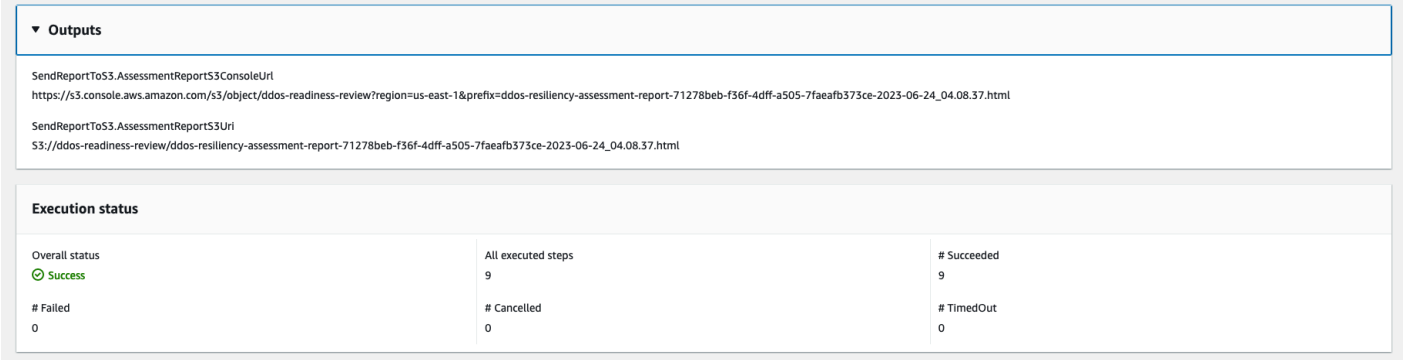
  Überprüft die geschützten regionalen Ressourcen von Shield Advanced wie Application Load Balancer, Network Load Balancer, Classic Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2)-Instances (Elastic IPs).

- SendReportToS3:

  Lädt die Details des DDoS-Bewertungsberichts in den Amazon S3-Bucket hoch.

7. Nach Abschluss wird der URI für die HTML-Datei des Bewertungsberichts im Amazon S3-Bucket bereitgestellt:

   S3-Konsolenlink und Amazon S3-URI für den Bericht über die erfolgreiche Ausführung des Runbooks




Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

AWS -Servicedokumentation

- AWS Shield Advanced

# Amazon SNS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Notification Service bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

## `AWS-EnableSNSTopicDeliveryStatusLogging`

Beschreibung

Das `AWS-EnableSNSTopicDeliveryStatusLogging` Runbook konfiguriert die Protokollierung des Lieferstatus für einen Amazon Data Firehose-HTTP, Lambda- oder Amazon Simple Queue Service (Amazon SQS) -Endpunkt. `Platform application` Auf diese Weise kann Amazon SNS fehlgeschlagene Benachrichtigungen und einen Beispielprozentsatz erfolgreicher Warnmeldungen an Amazon CloudWatch protokollieren. Wenn die Protokollierung des Lieferstatus für das Thema bereits konfiguriert ist, ersetzt das Runbook die bestehende Konfiguration durch die neuen Werte, die Sie für die Eingabeparameter angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EndpointType

  Typ: Zeichenfolge

  Zulässige Werte:
  - HTTP
  - Firehose
  - Lambda
  - Anwendung

- SQS

  Beschreibung: (Erforderlich) Der Typ des Amazon SNS SNS-Themenendpunkts, für den Sie Benachrichtigungen zum Lieferstatus protokollieren möchten.

- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas, für das Sie die Versandstatusprotokollierung konfigurieren möchten.

- SuccessFeedbackRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, an die Amazon SNS Protokolle für erfolgreiche Benachrichtigungen sendet. CloudWatch

- SuccessFeedbackSampleRate

  Typ: Zeichenfolge

  Gültige Werte: 0-100

  Beschreibung: (Erforderlich) Der Prozentsatz der erfolgreichen Nachrichten, die für das angegebene Amazon SNS-Thema geprüft werden sollen.

- FailureFeedbackRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, an die Amazon SNS Protokolle für Fehlerbenachrichtigungen sendet. CloudWatch

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`

- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Wendet den Wert für den `SuccessFeedbackRoleArn` Parameter auf das Amazon SNS SNS-Thema an.
- `aws:executeAwsApi`— Wendet den Wert für den `SuccessFeedbackSampleRate` Parameter auf das Amazon SNS SNS-Thema an.
- `aws:executeAwsApi`— Wendet den Wert für den `FailureFeedbackRoleArn` Parameter auf das Amazon SNS SNS-Thema an.
- `aws:executeScript`— Bestätigt, dass die Protokollierung des Lieferstatus für das Amazon SNS SNS-Thema aktiviert ist.

Ausgaben

VerifyDeliveryStatusLoggingAktiviert. GetTopicAttributesResponse - Antwort von den `GetTopicAttributes` API-Vorgängen.

VerifyDeliveryStatusLoggingAktiviert. VerifyDeliveryStatusLoggingEnabled - Meldung über die erfolgreiche Überprüfung der Protokollierung des Lieferstatus.

## `AWSConfigRemediation-EncryptSNSTopic`

Beschreibung

Das `AWSConfigRemediation-EncryptSNSTopic` Runbook ermöglicht die Verschlüsselung des von Ihnen angegebenen Amazon Simple Notification Service (Amazon SNS) -Themas mithilfe eines AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre Amazon SNS SNS-Themen gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Themen mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KmsKeyArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung des Amazon SNS-Themas verwenden möchten.
- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas, das Sie verschlüsseln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Verschlüsselt das Amazon SNS SNS-Thema, das Sie im `TopicArn` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die Verschlüsselung für das Amazon SNS SNS-Thema aktiviert ist.

## AWS-PublishSNSNotification

Beschreibung

Veröffentlichen Sie eine Benachrichtigung auf Amazon SNS.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Fehlermeldung

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Nachricht für die SNS-Benachrichtigung.

- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des SNS-Themas, an das die Benachrichtigung veröffentlicht wird.

# Amazon SQS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Queue Service (Amazon SQS) bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableSQSEncryption

## `AWS-EnableSQSEncryption`

Beschreibung

Das `AWS-EnableSQSEncryption` Runbook ermöglicht die Verschlüsselung im Ruhezustand für eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange. Eine Amazon SQS-Warteschlange kann mit von Amazon SQS verwalteten Schlüsseln (SSE-SQS) oder mit von AWS Key Management Service (AWS KMS) verwalteten Schlüsseln (SSE-KMS) verschlüsselt werden. Der Schlüssel, den Sie Ihrer Warteschlange zuweisen, muss über eine Schlüsselrichtlinie verfügen, die Berechtigungen für alle Prinzipale enthält, die zur Verwendung der Warteschlange autorisiert sind. Wenn die Verschlüsselung aktiviert ist, werden anonyme - `SendMessage` und -`ReceiveMessage`Anfragen an die verschlüsselte Warteschlange abgelehnt.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- QueueUrl

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der Amazon SQS-Warteschlange, für die Sie die Verschlüsselung aktivieren möchten.
- KmsKeyId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der AWS KMS Schlüssel, der für die Verschlüsselung verwendet werden soll. Dieser Wert kann eine global eindeutige Kennung, ein ARN für einen Alias oder einen Schlüssel oder ein Aliasname mit dem Präfix „alias/“ sein. Sie können den AWS verwalteten Schlüssel auch verwenden, indem Sie den Alias aws/sqs angeben.
- KmsDataKeyReusePeriodSeconds

  Typ: Zeichenfolge

  Gültige Werte: 60–86 400

  Standard: 300

  Beschreibung: (Optional) Die Zeitdauer in Sekunden, die eine Amazon SQS-Warteschlange einen Datenschlüssel zum Verschlüsseln oder Entschlüsseln von Nachrichten vor dem AWS KMS erneuten Aufrufen von verwenden kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Dokumentschritte

- SelectKeyType (aws:branch): Verzweigungen basierend auf dem angegebenen Schlüssel.
- PutAttributeSseKms (aws:executeAwsApi) – Aktualisiert die Amazon SQS-Warteschlange so, dass sie den für die Verschlüsselung angegebenen AWS KMS Schlüssel verwendet.
- PutAttributeSseSqs (aws:executeAwsApi) – Aktualisiert die Amazon SQS-Warteschlange so, dass der Standardschlüssel für die Verschlüsselung verwendet wird.
- VerifySqsEncryptionKms (aws:assertAwsResourceProperty) – Prüft, ob die Verschlüsselung in der Amazon SQSWarteschlange aktiviert ist.
- VerifySqsEncryptionDefault (aws:assertAwsResourceProperty) – Prüft, ob die Verschlüsselung in der Amazon SQS-Warteschlange aktiviert ist.

# Step Functions

AWS Systems Manager Automation bietet vordefinierte Runbooks für AWS Step Functions (Step Functions). Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableStepFunctionsStateMachineLogging

## `AWS-EnableStepFunctionsStateMachineLogging`

Beschreibung

Das `AWS-EnableStepFunctionsStateMachineLogging` Runbook aktiviert oder aktualisiert die Protokollierung auf dem von Ihnen angegebenen AWS Step Functions Zustandsautomaten. Die Mindestprotokollierungsebene muss auf `ALL`, `ERROR`oder festgelegt werden`FATAL`.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Level

  Typ: Zeichenfolge

  Gültige Werte: ALL | ERROR | FATAL

  Beschreibung: (Erforderlich) Die URL der Amazon SQS-Warteschlange, für die Sie die Verschlüsselung aktivieren möchten.
- LogGroupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Amazon- CloudWatch Logs-Protokollgruppe, an die Sie Zustandsautomaten-Protokolle senden möchten.

- StateMachineArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Zustandsautomaten, für den Sie die Protokollierung aktivieren möchten.
- IncludeExecutionData

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Bestimmt, ob Ausführungsdaten in den Protokollen enthalten sind.
- TracingConfiguration

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Bestimmt, ob die AWS X-Ray Nachverfolgung aktiviert ist.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

### Dokumentschritte

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)` – Aktualisiert den angegebenen Zustandsautomaten mit der angegebenen Protokollierungskonfiguration.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)` – Prüft, ob die Protokollierung für den angegebenen Zustandsautomaten aktiviert wurde.

Ausgaben

- EnableStepFunctionsStateMachineLogging.Response – Antwort auf den UpdateStateMachine API-Aufruf.

# Systems Manager

AWS Systems Manager Automation stellt vordefinierte Runbooks für Systems Manager bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## `AWS-BulkDeleteAssociation`

Beschreibung

Mit dem `AWS-BulkDeleteAssociation` Runbook können Sie bis zu 50 Systems Manager State Manager-Verknüpfungen gleichzeitig löschen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AssociationIds

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs der Assoziationen, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:DeleteAssociation`

Dokumentschritte

- `aws:executeScript`- Löscht die Verknüpfungen, die Sie im `AssociationIds` Parameter angeben.

# AWS-BulkEditOpsItems

Beschreibung

Mit dem `AWS-BulkEditOpsItems` Runbook können Sie den Status, den Schweregrad, die Kategorie oder die Priorität von AWS Systems Manager OpsItems bearbeiten. Mit dieser Automatisierung können maximal 50 Dateien OpsItems gleichzeitig bearbeitet werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Kategorie

  Typ: Zeichenfolge

  Zulässige Werte:
  - Verfügbarkeit
  - Kosten
  - Keine Änderung
  - Leistung

- Wiederherstellung
- Sicherheit

Standard: Keine Änderung

Beschreibung: (Optional) Die neue Kategorie, die Sie für die bearbeitete Datei angeben möchten OpsItems.

- OpsItemIDs

Typ: StringList

Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste von OpsItems IDs, die Sie bearbeiten möchten (z. B. OI-xxxxxxxxxxxx, OI-xxxxxxxxxxxx).

- Priorität

Typ: Zeichenfolge

Zulässige Werte:

- Keine Änderung
- 1
- 2
- 3
- 4
- 5

Standard: Keine Änderung

Beschreibung: (Optional) Die Wichtigkeit der bearbeiteten OpsItems Elemente im Vergleich zu anderen OpsItems im System.

- Schweregrad

Typ: Zeichenfolge

Zulässige Werte:

- Keine Änderung
- 1
- 2

- 3
- 4

Standard: Keine Änderung

Beschreibung: (Optional) Der Schweregrad der Bearbeitung OpsItems.

- WaitTimeBetweenEditsInSecs

Typ: Zeichenfolge

Gültige Werte: 0.0-2.0

Standardwert: 0.8

Beschreibung: (Optional) Die Zeit, die die Automatisierung zwischen dem Aufrufen des Vorgangs wartet. `UpdateOpsItems`

- Status

Typ: Zeichenfolge

Zulässige Werte:

- InProgress
- Keine Änderung
- Öffnen
- Gelöst

Standard: Keine Änderung

Beschreibung: (Optional) Der neue Status der Datei „Bearbeitet OpsItems“.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Dokumentschritte

- `aws:executeScript`- Bearbeitet den, den OpsItems Sie im `OpsItemIds` Parameter angegeben haben, auf der Grundlage der Werte, die Sie für die Parameter`Category`, `PrioritySeverity`, und `Status` angeben.

## AWS-BulkResolveOpsItems

Beschreibung

Das `AWS-BulkResolveOpsItems` Runbook löst Lösungen auf AWS Systems Manager OpsItems , die dem von Ihnen angegebenen Filter entsprechen. OpsItems Mithilfe des Parameters können Sie auch eine OpsItemId angeben, die zur Auflösung hinzugefügt werden soll. `OpsInsightsId` Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, wird eine Ergebniszusammenfassung an den Amazon Simple Storage Service (Amazon S3) -Bucket gesendet. Um eine Benachrichtigung zu erhalten, sobald die Ergebniszusammenfassung an den Amazon S3 S3-Bucket gesendet wurde, geben Sie einen Wert für den `SnsTopicArn` Parameter an. Durch diese Automatisierung können maximal 1.000 Probleme OpsItems gleichzeitig behoben werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Filter

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Schlüssel-Wert-Paare von Filtern, um das zurückzugeben, das OpsItems Sie auflösen möchten. Beispiel, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Weitere Informationen zu den verfügbaren Optionen zum Filtern von OpsItems Antworten finden Sie unter OpsItemFilter in der AWS Systems Manager API-Referenz.

- OpsInsightId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die zugehörige Ressourcen-ID, der Sie hinzufügen möchten, wurde aufgelöst OpsItems.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Amazon S3 S3-Buckets, an den Sie die Ergebniszusammenfassung senden möchten.

- SnsMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Benachrichtigung, die Amazon Simple Notification Service (Amazon SNS) senden soll, wenn die Automatisierung abgeschlossen ist.

- SnsTopicArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN des Amazon SNS SNS-Themas, das Sie benachrichtigen möchten, wenn die Ergebnisübersicht an Amazon S3 gesendet wurde.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

Dokumentschritte

- aws:executeScript- Sammelt und löst sie auf der OpsItems Grundlage der von Ihnen angegebenen Filter auf. Wenn Sie einen Wert für den OpsInsightId Parameter angegeben haben, wird der Wert als zugehörige Ressource hinzugefügt.
- aws:executeScript— Wenn Sie einen Wert für den S3BucketName Parameter angegeben haben, wird eine Ergebniszusammenfassung an den Amazon S3 S3-Bucket gesendet.
- aws:executeScript— Wenn Sie einen Wert für den SnsTopicArn Parameter angegeben haben, wird eine Benachrichtigung an das Amazon SNS SNS-Thema gesendet, nachdem die Ergebniszusammenfassung an Amazon S3 gesendet wurde, einschließlich des SnsMessage Parameterwerts, falls angegeben.

## AWS-ConfigureMaintenanceWindows

Beschreibung

Das AWS-ConfigureMaintenanceWindows Runbook hilft Ihnen, mehrere Systems Manager Manager-Wartungsfenster zu aktivieren oder zu deaktivieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- MaintenanceWindows

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs der Wartungsfenster, die Sie aktivieren oder deaktivieren möchten.
- MaintenanceWindowsStatus

  Typ: Zeichenfolge

  Gültige Werte: „True“ | „False“

  Standard: „Falsch“

  Beschreibung: (Erforderlich) Legt fest, ob Wartungsfenster aktiviert oder deaktiviert sind. Geben Sie „True“ an, um Wartungsfenster zu aktivieren, und „False“, um sie zu deaktivieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Dokumentschritte

- `aws:executeScript`- Erfasst den Status der Wartungsfenster, die Sie im `MaintenanceWindows` Parameter angeben, und aktiviert oder deaktiviert die Wartungsfenster.

## AWS-CreateManagedLinuxInstance

Beschreibung

Erstellen Sie eine EC2-Instanz für Linux, die für Systems Manager konfiguriert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AmiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) AMI ID, die zum Starten der Instanz verwendet werden soll.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupName

  Typ: Zeichenfolge

Standard: SSM-Instanzen SecurityGroup ForLinux

Beschreibung: (Erforderlich) Name der Sicherheitsgruppe, die erstellt werden soll.

- HttpTokens

  Typ: Zeichenfolge

  Gültige Werte: optional | erforderlich

  Standard: optional

  Beschreibung: (Optional) IMDSv2 verwendet tokengestützte Sitzungen. Stellen Sie die Verwendung von HTTP-Token auf `optional` oder ein, um `required` zu bestimmen, ob IMDSv2 optional oder erforderlich ist.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung: (Erforderlich) Typ der zu startenden Instance. Standard ist t2.medium.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Schlüsselpaar für die Erstellung der Instance.

- RemoteAccessApfelwein

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Erforderlich) Erstellt Sicherheitsgruppen mit offenem Port für SSH (Portbereich 22) für von CIDR angegebene IPs (Standard ist 0.0.0.0/0). Wenn die Sicherheitsgruppe bereits vorhanden ist, wird sie nicht modifiziert, und auch die Regeln werden nicht geändert.

- RoleName

  Typ: Zeichenfolge

  Standard: SSM ManagedInstance ProfileRole

Beschreibung: (Erforderlich) Zu erstellender Rollenname.

- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{automation:execution_ID}}

  Beschreibung: (Optional) Geben Sie den Stack-Namen an, der von diesem Runbook verwendet wird

- SubnetId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in diesem Subnetz oder, falls nicht angegeben, im Standard-Subnetz bereitgestellt.

- VpcId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in dieser Amazon Virtual Private Cloud (Amazon VPC) oder, falls nicht angegeben, in der Standard-Amazon-VPC bereitgestellt.

## AWS-CreateManagedWindowsInstance

Beschreibung

Erstellen Sie eine EC2-Instanz für eineWindows Server, die für Systems Manager konfiguriert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Parameter

- AmiId

  Typ: Zeichenfolge

  Standard: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

  Beschreibung: (Erforderlich) AMI ID, die zum Starten der Instanz verwendet werden soll.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupName

  Typ: Zeichenfolge

  Standard: SSM-Instanzen SecurityGroup ForLinux

  Beschreibung: (Erforderlich) Name der Sicherheitsgruppe, die erstellt werden soll.
- HttpTokens

  Typ: Zeichenfolge

  Gültige Werte: optional | erforderlich

  Standard: optional

  Beschreibung: (Optional) IMDSv2 verwendet tokengestützte Sitzungen. Stellen Sie die Verwendung von HTTP-Token auf `optional` oder ein, um `required` zu bestimmen, ob IMDSv2 optional oder erforderlich ist.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung: (Erforderlich) Typ der zu startenden Instance. Standard ist t2.medium.
- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Schlüsselpaar für die Erstellung der Instance.
- RemoteAccessApfelwein

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Erforderlich) Erstellt eine Sicherheitsgruppe mit offenem Port für RDP (Portbereich 3389) für von CIDR angegebene IPs (Standard ist 0.0.0.0/0). Wenn die Sicherheitsgruppe bereits vorhanden ist, wird sie nicht modifiziert, und auch die Regeln werden nicht geändert.
- RoleName

  Typ: Zeichenfolge

  Standard: SSM ManagedInstance ProfileRole

  Beschreibung: (Erforderlich) Zu erstellender Rollenname.
- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{automation:execution_ID}}

  Beschreibung: (Optional) Geben Sie den Stack-Namen an, der von diesem Runbook verwendet wird
- SubnetId

  Typ: Zeichenfolge

  Standard: Standard

Beschreibung: (Erforderlich) Die neue Instance wird in diesem Subnetz oder, falls nicht angegeben, im Standard-Subnetz bereitgestellt.

- VpcId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in dieser Amazon Virtual Private Cloud (Amazon VPC) oder, falls nicht angegeben, in der Standard-Amazon-VPC bereitgestellt.

## AWSConfigRemediation-EnableCWLoggingForSessionManager

Beschreibung

Das `AWSConfigRemediation-EnableCWLoggingForSessionManager` Runbook ermöglicht es AWS Systems Manager Session-Manager-Sitzungen (Session Manager), Ausgabeprotokolle in einer Amazon CloudWatch (CloudWatch) -Protokollgruppe zu speichern.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- DestinationLogGruppe

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der CloudWatch Protokollgruppe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Dokumentschritte

- `aws:executeScript`- Akzeptiert die CloudWatch Protokollgruppe, um das Dokument zu aktualisieren, in dem die Einstellungen für die Sitzungsausgabeprotokolle von Session Manager gespeichert sind, oder erstellt ein Dokument, falls es noch nicht vorhanden ist.

## AWS-ExportOpsDataToS3

Beschreibung

Dieses Runbook ruft eine Liste von OpsData Zusammenfassungen im AWS Systems Manager Explorer ab und exportiert sie in ein Objekt in einem angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- columnFields

  Typ: StringList

  Beschreibung (erforderlich): Spaltenfelder zum Schreiben in die Ausgabedatei.
- -Filter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Filter für die getOpsSummary Anfrage.
- resultAttribute

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Ergebnisattribut für die getOpsSummary Anfrage.
- s3 BucketName

  Typ: Zeichenfolge

  Beschreibung (erforderlich): S3-Bucket, in den Sie die Ausgabedatei herunterladen.
- sns SuccessMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Nachricht, die gesendet werden soll, wenn Runbook fertig ist.

- sns TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Amazon Simple Notification Service (Amazon SNS) -Thema ARN, um zu benachrichtigen, wenn der Download abgeschlossen ist.
- syncName

  Typ: Zeichenfolge

  Beschreibung (optional): der Name der Ressourcendatensynchronisierung.

Dokumentschritte

get OpsSummaryStep — Ruft jetzt bis zu 5.000 Operationszusammenfassungen ab, um sie in eine CSV-Datei zu exportieren.

Ausgaben

OpsData object — Wenn das Runbook erfolgreich ausgeführt wird, finden Sie das exportierte OpsData Objekt in Ihrem Ziel-S3-Bucket.

## AWS-ExportPatchReportToS3

Beschreibung

Dieses Runbook ruft Listen mit Patch-Übersichtsdaten und Patch-Details in AWS Systems Manager Patch Manager ab und exportiert sie in CSV-Dateien in einem angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- assumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Dokument ausführt.

- s3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der S3-Bucket, in den Sie die Ausgabedatei herunterladen möchten.

- sns TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon Simple Notification Service (Amazon SNS) -Thema Amazon Resource Name (ARN), das benachrichtigt werden soll, wenn der Download abgeschlossen ist.

- sns SuccessMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Text der Nachricht, die gesendet werden soll, wenn das Runbook fertig ist.

- targets

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Instanz-ID oder ein Platzhalterzeichen (*), um anzugeben, ob Patch-Daten für eine bestimmte Instance oder für alle Instances gemeldet werden sollen.

Dokumentschritte

ExportReportStep — Die Aktion für diesen Schritt hängt vom Wert des `targets` Parameters ab. Wenn `targets` es das Format von ha`instanceids=*`, ruft der Schritt bis zu 10.000 Patch-Zusammenfassungen für Instanzen in Ihrem Konto ab und exportiert die Daten in eine CSV-Datei.

Wenn `targets` das Format vorliegt`instanceids=<instance-id>`, ruft der Schritt sowohl die Patch-Zusammenfassung als auch alle Patches für die angegebene Instanz in Ihrem Konto ab und exportiert sie in eine CSV-Datei.

Ausgaben

PatchSummary/Patches-Objekt — Wenn das Runbook erfolgreich ausgeführt wird, wird das exportierte Patch-Berichtsobjekt in Ihren S3-Ziel-Bucket heruntergeladen.

## `AWS-SetupInventory`

Beschreibung

Erstellen Sie eine Systems Manager Manager-Inventarzuordnung für eine oder mehrere verwaltete Instanzen. Das System erfasst Metadaten aus Ihren-Instances gemäß dem Zeitplan in der Zuordnung. Weitere Informationen finden Sie unter AWS Systems Manager Bestand.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- Anwendungen

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Metadaten über installierte Anwendungen.
- AssociatedDocName

  Typ: Zeichenfolge

Standard: `AWS-GatherSoftwareInventory`

Beschreibung: (Optional) Der Name des Runbooks, das zum Sammeln von Inventar aus der verwalteten Instanz verwendet wird.

- AssociationName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein Name für die Inventory-Zuordnung, die der Instance zugewiesen wird.

- AssocWaitZeit

  Typ: Zeichenfolge

  Standard: PT5M

  Beschreibung: (Optional) Zeit, für die die Inventory-Erfassung unterbrochen werden soll, wenn die Startzeit für die Inventory-Zuordnung erreicht ist. Die Uhrzeit wird im ISO 8601-Format verwendet.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- `AwsComponents`

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Sammeln Sie Metadaten für AWS Komponenten wie amazon-ssm-agent.

- CustomInventory

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von benutzerdefinierten Bestandsmetadaten.

- Dateien

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erfassen von Metadaten über Dateien auf Ihren Instances. Weitere Informationen zum Sammeln dieser Art von Inventardaten finden Sie unter Arbeiten mit Datei- und Windows-Registrierungsinventar. Erfordert SSMAgent Version 2.2.64.0 oder höher. Linux-Beispiel: `[{"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}]`

- InstanceDetailedInformationen

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen zusätzlicher Informationen zu der Instance, einschließlich CPU-Modell, Geschwindigkeit und der Anzahl der Kerne, um nur einige zu nennen.

- InstanceIds

  Typ: Zeichenfolge

  Standard: *

  Beschreibung: (Erforderlich) EC2-Instances, die Sie inventarisieren möchten.

- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- NetworkConfig

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Metadaten über Netzwerkkonfigurationen.

- Ausgänge 3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name eines Amazon S3 S3-Buckets, in den Sie Inventarprotokolldaten schreiben möchten.

- gibt 3 aus KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie Inventarprotokolldaten schreiben möchten.

- OutputS3Region

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Ortes AWS-Region , an dem Amazon S3 existiert.

- Plan

  Typ: Zeichenfolge

  Standard: cron(0 */30 * * * ? *)

  Beschreibung: (Optional) Ein cron-Ausdruck für den Inventory-Zuordnungplan. Der Standardwert ist alle 30 Minuten.

- Services

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional, nur Windows-BS, erfordert SSMAgent-Version 2.2.64.0 und höher) Erfassen von Daten für Servicekonfigurationen.

- WindowsRegistry

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erfassen von Metadaten über Microsoft Windows Registry-Schlüssel. Weitere Informationen zur Erfassung dieser Art von Inventardaten finden Sie unter Arbeiten mit Datei- und Windows-Registrierungsinventar. Erfordert SSM Agent-Version 2.2.64.0

oder höher. Beispiel: [{"Path“ :"HKEY_CURRENT_CONFIG\ System“, "Recursive“ :true}, {"Path“ :"HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ „," „: [" aName "]}] MachineImage ValueNames

- WindowsRoles

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Informationen über Windows-Rollen auf der Instance. Gilt nur für Windows-Betriebssysteme. Erfordert SSMAgent Version 2.2.64.0 oder höher.

- WindowsUpdates

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Daten über alle Windows-Updates auf der Instance.

## AWS-SetupManagedInstance

Beschreibung

Konfigurieren Sie eine Instanz mit einer AWS Identity and Access Management (IAM-) Rolle für den Systems Manager Manager-Zugriff.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der zu konfigurierenden EC2-Instance.
- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.
- RoleName

  Typ: Zeichenfolge

  Standard: SSM RoleFor ManagedInstance

  Beschreibung: (Optional) Der Name der IAM-Rolle für die EC2-Instance. Wenn diese Rolle nicht vorhanden ist, wird sie erstellt. Stellen Sie bei der Angabe dieses Werts sicher, dass die Rolle die von AmazonSSM verwaltete ManagedInstance Kernrichtlinie enthält.

## AWS-SetupManagedRoleOnEC2Instance

Beschreibung

Konfigurieren Sie eine Instanz mit der RoleForManagedInstance SSM-verwalteten IAM-Rolle für den Systems Manager Manager-Zugriff.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der zu konfigurierenden EC2-Instance.
- LambdaAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.
- RoleName

  Typ: Zeichenfolge

  Standard: SSM RoleFor ManagedInstance

  Beschreibung: (Optional) Der Name der IAM-Rolle für die EC2-Instance. Wenn diese Rolle nicht vorhanden ist, wird sie erstellt. Stellen Sie bei der Angabe dieses Werts sicher, dass die Rolle die von AmazonSSM verwaltete ManagedInstance Kernrichtlinie enthält.

# AWSSupport-TroubleshootManagedInstance

Beschreibung

Das `AWSSupport-TroubleshootManagedInstance` Runbook hilft Ihnen zu ermitteln, warum eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance nicht als von verwaltet meldetAWS Systems Manager. Dieses Runbook überprüft die VPC-Konfiguration für die Instance, einschließlich Sicherheitsgruppenregeln, VPC-Endpunkte, Netzwerkzugriffskontrolllisten (ACL)-Regeln und Routing-Tabellen. Es bestätigt auch, dass der Instance ein AWS Identity and Access Management (IAM)-Instance-Profil angefügt ist, das die erforderlichen Berechtigungen enthält.

> **Important**
>
> Dieses Automatisierungs-Runbook wertet keine IPv6-Regeln aus.

Ausführen dieser Automatisierung (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance, die nicht wie von Systems Manager verwaltet meldet.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

### Dokumentschritte

- `aws:executeScript` – Sammelt die `PingStatus` der Instance.
- `aws:branch` – Verzweigungen, die darauf basieren, ob die Instance bereits als von Systems Manager verwaltet gemeldet wird.

- `aws:executeAwsApi` – Sammelt Details zur Instance, einschließlich der VPC-Konfiguration.
- `aws:executeScript` – Falls zutreffend, sammelt zusätzliche Details zu VPC-Endpunkten, die für die Verwendung mit Systems Manager bereitgestellt wurden, und bestätigt, dass die an den VPC-Endpunkt angehängten Sicherheitsgruppen eingehenden Datenverkehr auf TCP-Port 443 von der Instance zulassen.
- `aws:executeScript` – Prüft, ob die Routing-Tabelle Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager-Endpunkten zulässt.
- `aws:executeScript` – Prüft, ob die Netzwerk-ACL-Regeln Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager-Endpunkten zulassen.
- `aws:executeScript` – Prüft, ob ausgehender Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager-Endpunkten von der Sicherheitsgruppe zugelassen wird, die der Instance zugeordnet ist.
- `aws:executeScript` – Prüft, ob das an die Instance angefügte Instance-Profil eine verwaltete Richtlinie enthält, die die erforderlichen Berechtigungen bereitstellt.
- `aws:branch` – Verzweigungen, die auf dem Betriebssystem der Instance basieren.
- `aws:executeScript` – Bietet Verweis auf das `ssmagent-toolkit-linux` Shell-Skript.
- `aws:executeScript` – Bietet Verweis auf das `ssmagent-toolkit-windows` PowerShell Skript.
- `aws:executeScript` – Generiert die endgültige Ausgabe für die Automatisierung.
- `aws:executeScript` – Wenn der `PingStatus` der `Online` Instance ist, gibt zurück, dass die Instance bereits von Systems Manager verwaltet wird.

## AWSSupport-TroubleshootPatchManagerLinux

Beschreibung

Das `AWSSupport-TroubleshootPatchManagerLinux` Runbook behebt häufige Probleme, die einen Patch-Fehler auf Linux-basierten verwalteten Knoten verursachen können, indem die AWS Systems Manager Funktion „Patch Manager“ verwendet wird. Das Hauptziel dieses Runbooks besteht darin, die Ursache für das Fehlschlagen des Patch-Befehls zu identifizieren und einen Korrekturplan vorzuschlagen.

Wie funktioniert es?

Das `AWSSupport-TroubleshootPatchManagerLinux` Runbook berücksichtigt die von Ihnen bereitgestellte Instance-ID/Befehls-ID zur Fehlerbehebung. Wenn keine Befehls-ID angegeben

wird, wählt sie den letzten fehlgeschlagenen Patch-Befehl innerhalb der letzten 30 Tage auf der bereitgestellten Instance aus. Nachdem Sie den Befehlsstatus, die Voraussetzungen erfüllt und die Betriebssystemverteilung überprüft haben, lädt das Runbook ein Protokollanalysatorpaket herunter und führt es aus. Die Ausgabe enthält die Ursache des Problems sowie die erforderliche Aktion zur Behebung des Problems.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

- Amazon Linux 2 und 2023
- Red Hat Enterprise Linux 8.X und 9.X
- Centos 8.X und 9.X
- SUSE 15.X

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

## Anweisungen

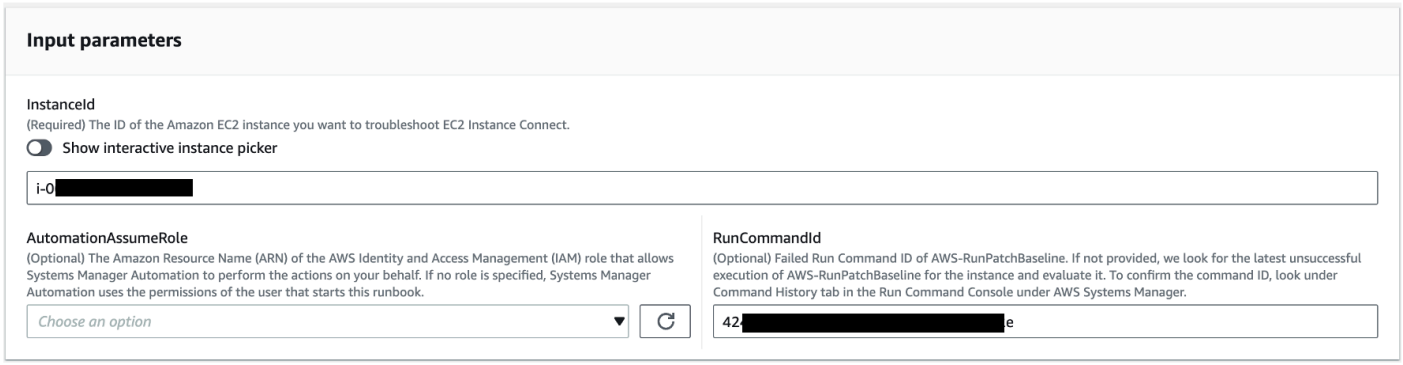
Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie zur AWSSupport-TroubleshootPatchManagerLinux in der -AWS Systems ManagerKonsole.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId (Erforderlich):

     Verwenden Sie die interaktive Instance-Auswahl, um die ID des Linux-basierten SSM-verwalteten Knotens (Amazon Elastic Compute Cloud (Amazon EC2) oder des Hybrid-aktivierten Servers) auszuwählen, für den der Patch-Befehl fehlgeschlagen ist, oder geben Sie die ID der SSM-verwalteten Instance manuell ein.
   - AutomationAssumeRole (Optional):

     Geben Sie den ARN der IAM-Rolle ein, mit der Automation Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - RunCommandId (Optional):

     Geben Sie die ID des fehlgeschlagenen Run Command des `AWS-RunPatchBaseline` Dokuments ein. Wenn Sie keine Befehls-ID angeben, sucht das Runbook innerhalb der letzten 30 Tage auf der ausgewählten Instance nach dem letzten fehlgeschlagenen Patch-Befehl.




4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckConcurrency:

Stellt sicher, dass es nur eine Ausführung dieses Runbooks gibt, die auf dieselbe Instance ausgerichtet ist. Wenn das Runbook eine weitere Ausführung findet, die auf dieselbe Instance abzielt, gibt es einen Fehler zurück und endet.

- ValidateCommandID:

  Überprüft, ob die angegebene Befehls-ID als Eingabeparameter für das `AWS-RunPatchBaseline` SSM-Dokument ausgeführt wurde. Wenn keine Befehls-ID angegeben wird, berücksichtigt das Runbook die letzte fehlgeschlagene Ausführung von `AWS-RunPatchBaseline` innerhalb der letzten 30 Tage auf der ausgewählten Instance.

- BranchOnCommandStatus:

  Bestätigt, dass der Status des bereitgestellten Befehls fehlgeschlagen ist. Andernfalls beendet das Runbook die Ausführung und generiert einen Bericht, der besagt, dass der bereitgestellte Befehl erfolgreich ausgeführt wurde.

- VerifyPrerequistes:

  Bestätigt, dass die oben genannten Voraussetzungen erfüllt sind.

- GetPlatformDetails:

  Ruft die Verteilung und Version des Betriebssystems (OS) ab.

- GetDownloadURL:

  Ruft die Download-URL für das PatchManager Log-Analyzer-Paket ab.

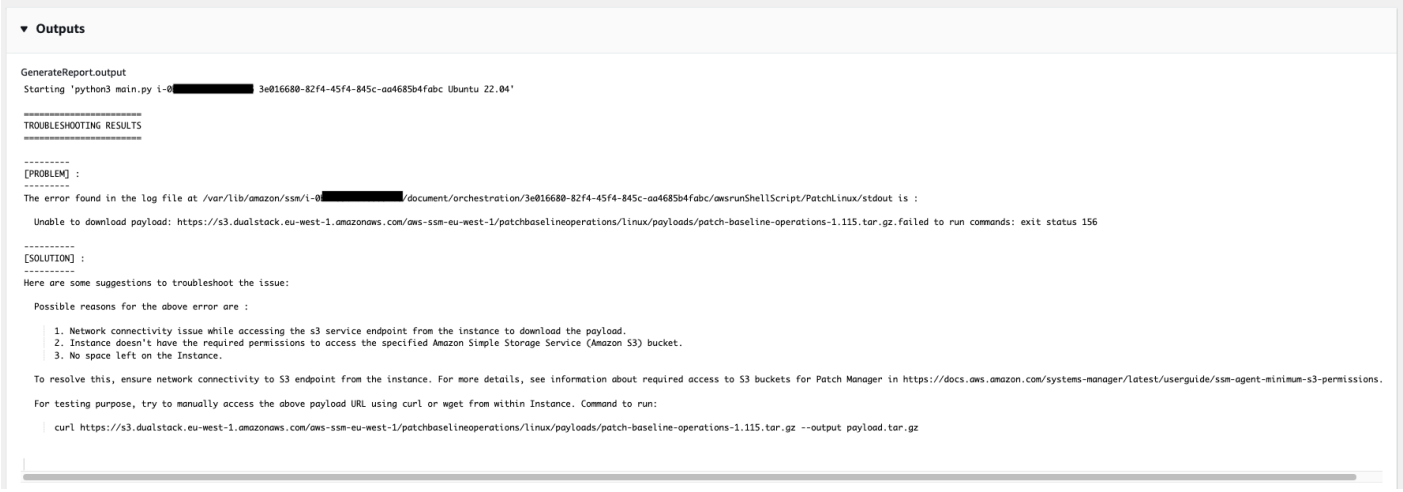
- EvaluatePatchManagerLogs:

  Lädt das PatchManager Log-Analyzer-Python-Paket auf der Instance herunter und führt es aus, um die Protokolldatei auszuwerten.

- GenerateReport:

  Generiert einen endgültigen Bericht über die Ausführung des Runbooks, der das identifizierte Problem und die vorgeschlagene Lösung enthält.

7. Nachdem Sie abgeschlossen sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten:




Referenzen

Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

## AWSSupport-TroubleshootSessionManager

Beschreibung

Das `AWSSupport-TroubleshootSessionManager` Runbook hilft Ihnen bei der Behebung häufiger Probleme, die Sie daran hindern, mithilfe von Session Manager eine Verbindung zu verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Instances herzustellen. Session Manager ist eine Funktion von. AWS Systems Manager Dieses Runbook überprüft Folgendes:

- Prüft, ob die Instanz läuft und meldet, wie sie von Systems Manager verwaltet wird.
- Führt das `AWSSupport-TroubleshootManagedInstance` Runbook aus, wenn die Instanz nicht als von Systems Manager verwaltet gemeldet wird.
- Überprüft die Version des SSM-Agenten, der auf der Instanz installiert ist.
- Prüft, ob ein Instance-Profil, das eine empfohlene AWS Identity and Access Management (IAM-) Richtlinie für Session Manager enthält, an die Amazon EC2 EC2-Instance angehängt ist.
- Sammelt SSM-Agent-Protokolle von der Instance.

- Analysiert Ihre Session Manager-Einstellungen.
- Führt das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook aus, um die Konnektivität der Instance mit den Endpunkten für Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs (CloudWatch Logs) zu analysieren.

Überlegungen

- Verwaltete Hybrid-Knoten werden nicht unterstützt.
- Dieses Runbook prüft nur, ob eine empfohlene verwaltete IAM-Richtlinie an das Instanzprofil angehängt ist. Es analysiert weder IAM noch die in Ihrem AWS KMS Instanzprofil enthaltenen Berechtigungen.

> **Important**
>
> Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook verwendet VPC Reachability Analyzer, um die Netzwerkkonnektivität zwischen einer Quelle und einem Dienstendpunkt zu analysieren. Ihnen wird pro Analyselauf zwischen einer Quelle und einem Ziel in Rechnung gestellt. Weitere Informationen finden Sie unter Amazon VPC-Preise.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, zu der Sie mit Session Manager keine Verbindung herstellen können.

- SessionPreferenceDokument

  Typ: Zeichenfolge

  Standard: SSM- SessionManager RunShell

  Beschreibung: (Optional) Der Name Ihres Dokuments mit den Sitzungseinstellungen. Wenn Sie beim Starten von Sitzungen kein benutzerdefiniertes Dokument mit den Sitzungseinstellungen angeben, verwenden Sie den Standardwert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:waitForAwsResourceProperty: Wartet bis zu 6 Minuten, bis Ihre Ziel-Instance die Statusprüfungen bestanden hat.
2. aws:executeScript: Analysiert das Dokument mit den Sitzungseinstellungen.
3. aws:executeAwsApi: Ruft den ARN des Instanzprofils ab, das an Ihre Instance angehängt ist.
4. aws:executeAwsApi: Prüft, ob Ihre Instance als vom Systems Manager verwaltet gemeldet wird.
5. aws:branch: Verzweigungen basieren darauf, ob Ihre Instance als von Systems Manager verwaltet gemeldet wird.
6. aws:executeScript: Prüft, ob der auf Ihrer Instance installierte SSM-Agent Session Manager unterstützt.

7. `aws:branch`: Branches, die auf der Plattform Ihrer Instance basieren, um `ssm-cli` Logs zu sammeln.
8. `aws:runCommand`: Sammelt Logs, die `ssm-cli` von einer Linux macOS Oder-Instanz ausgegeben wurden.
9. `aws:runCommand`: Sammelt Logdateien, die `ssm-cli` von einer Windows Instanz ausgegeben wurden.
10. `aws:executeScript`: Analysiert die `ssm-cli` Protokolle.
11. `aws:executeScript`: Prüft, ob eine empfohlene IAM-Richtlinie an das Instanzprofil angehängt ist.
12. `aws:branch`: Legt fest, ob die `ssmmessages` Endpunktkonnektivität anhand von `ssm-cli` Protokollen bewertet werden soll.
13. `aws:executeAutomation`: Prüft, ob die Instanz eine Verbindung zu einem `ssmmessages` Endpunkt herstellen kann.
14. `aws:branch`: Legt anhand von `ssm-cli` Protokollen und Ihren Sitzungseinstellungen fest, ob die Amazon S3 S3-Endpunktkonnektivität bewertet werden soll.
15. `aws:executeAutomation`: Prüft, ob die Instance eine Verbindung zu einem Amazon S3 S3-Endpunkt herstellen kann.
16. `aws:branch`: Legt anhand von `ssm-cli` Protokollen und Ihren Sitzungspräferenzen fest, ob die AWS KMS Endpunktkonnektivität bewertet werden soll.
17. `aws:executeAutomation`: Prüft, ob die Instanz eine Verbindung zu einem AWS KMS Endpunkt herstellen kann.
18. `aws:branch`: Legt anhand von CloudWatch Protokollen und Ihren Sitzungseinstellungen fest, ob die Konnektivität des `ssm-cli` Logs-Endpunkts bewertet werden soll.
19. `aws:executeAutomation`: Prüft, ob die Instance eine Verbindung zu einem CloudWatch Logs-Endpunkt herstellen kann.
20. `aws:executeAutomation`: Führt das `AWSSupport-TroubleshootManagedInstance` Runbook aus.
21. `aws:executeScript`: Kompiliert die Ausgabe der vorherigen Schritte und gibt einen Bericht aus.

Gibt aus

- `generateReport.EvalReport`- Die Ergebnisse der vom Runbook durchgeführten Prüfungen im Klartext.

# Drittanbieter

AWS Systems Manager Automation stellt vordefinierte Runbooks für Produkte und Dienste von Drittanbietern bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWS-CreateJiraIssue

Beschreibung

Erstellen Sie ein Problem in Jira.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AssigneeName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Benutzername der Person, der das Problem zugewiesen werden soll.
- DueDate

Typ: Zeichenfolge

Beschreibung: (Optional) Das Fälligkeitsdatum für das Problem im yyyy-mm-dd Format.

- IssueDescription

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine detaillierte Beschreibung des Problems.

- IssueSummary

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine kurze Zusammenfassung des Problems.

- IssueTypeName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Problemtyps, den Sie erstellen möchten (z. B. Aufgabe, Unteraufgabe, Fehler usw.).

- JiraURL

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der Jira-Instance.

- JiraUsername

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Benutzers, der das Problem erstellt.

- PriorityName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Priorität des Problems.

- ProjectKey

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Schlüssel des Projekts, in dem das Problem erstellt wird.

- SSM ParameterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name eines verschlüsselten SSM-Parameter mit dem API-Schlüssel oder Passwort des Jira-Benutzers.

Dokumentschritte

`aws:createStack`- Erstellen Sie einen CloudFormation Stack, um eine Lambda-IAM-Rolle und -Funktion zu erstellen.

`aws:invokeLambdaFunction`- Rufen Sie die Lambda-Funktion auf, um das Jira-Problem zu erstellen

`aws:deleteStack`- Löscht den erstellten Stack CloudFormation .

Ausgaben

IssueId: ID des neu erstellten Jira-Problems

## `AWS-CreateServiceNowIncident`

Beschreibung

Erstellen Sie einen Vorfall in der ServiceNow Incident-Tabelle.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Kategorie

  Typ: Zeichenfolge

  Beschreibung (optional): Die Kategorie des Vorfalls.

  Gültige Werte: Keine | Anfrage/Hilfe | Software | Hardware | Netzwerk | Datenbank

  Standardwert: Keine
- Beschreibung

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Eine detaillierte Erklärung zum Vorfall.
- Auswirkung

  Typ: Zeichenfolge

  Beschreibung (optional): Die Auswirkungen, die ein Vorfall auf das Geschäft hat.

  Gültige Werte: Hoch | Mittel | Niedrig

  Standardwert: Niedrig
- ServiceNowInstanceUsername

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Der Name des Benutzers, der den Vorfall erstellt.
- ServiceNowInstancePassword

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name eines verschlüsselten SSM-Parameters, der das Passwort für den ServiceNow Benutzer enthält.

- ServiceNowinstanceUrl

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der Instanz ServiceNow

- ShortDescription

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Eine kurze Beschreibung des Vorfalls.

- Unterkategorie

  Typ: Zeichenfolge

  Beschreibung (optional): Die Unterkategorie des Vorfalls.

  Gültige Werte: Keine | Antivirus | E-Mail | Interne Anwendung | Betriebssystem | CPU | Festplatte | Tastatur | Hardware | Speicher | Monitor | Maus | DHCP | DNS | IP-Adresse | VPN | Wireless | DB2 | MS SQL Server | Oracle

  Standardwert: Keine

Dokumentschritte

Push_Incident — Leitet die Informationen zum Vorfall an weiter. ServiceNow

Ausgaben

push_incident.IncidentId — Die erstellte Incident-ID.

## AWS-RunPacker

Beschreibung

Dieses Runbook verwendet das HashiCorp Packer-Tool, um Packer-Vorlagen zu validieren, zu korrigieren oder zu erstellen, die zur Erstellung von Maschinenimages verwendet werden. Dieses Runbook verwendet Packer v1.7.2.

> **Note**
>
> Wenn Sie einen `vpc_id`-Wert angeben, müssen Sie auch den `subnet_id`-Wert eines öffentlichen Subnetzes angeben. Wenn Sie das öffentliche Adressierungsattribut IPv4 Ihres Subnetzes nicht ändern, müssen Sie auch `associate_public_ip_address` auf true setzen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Force

  Typ: Boolesch

  Beschreibung: Eine Packer-Option, mit der ein Builder ausgeführt wird, wenn Artefakte aus einem vorherigen Build ansonsten verhindern, dass ein Build ausgeführt wird.
- Mode

  Typ: Zeichenfolge

Beschreibung: Der Modus oder der Befehl, in dem Packer bei der Validierung anhand der Vorlage verwendet werden soll. Zu den Optionen gehören `BuildValidate`, und`Fix`.

- TemplateFileName

  Typ: Zeichenfolge

  Beschreibung: der Name oder der Schlüssel der Vorlagendatei im S3-Bucket.

- Vorlagen 3 BucketName

  Typ: Zeichenfolge

  Beschreibung: der Name des S3-Buckets, der die Packer-Vorlage enthält.

Dokumentschritte

RunPackerProcessTemplate — Führt den ausgewählten Modus mit dem Packer-Tool anhand der Vorlage aus.

Ausgaben

RunPackerProcessTemplate.output — Die Standardausgabe aus dem Packer-Tool.

RunPackerProcessTemplate.fixed_template_key — Der Name der Vorlage, die in einem S3-Bucket gespeichert ist und nur verwendet werden soll, wenn sie im „Fix“ -Modus ausgeführt wird.

RunPackerProcessTemplate.s3_bucket — Der Name des S3-Buckets, der die feste Vorlage enthält, die nur verwendet werden soll, wenn sie im „Fix“ -Modus ausgeführt wird.

# Amazon VPC

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon Virtual Private Cloud. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Dieses Runbook entfernt alle Eingangs- und Ausgangsregeln aus der von Ihnen angegebenen Sicherheitsgruppe.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- SecurityGroupID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, die Sie schließen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangs- und Ausgangsregeln aus der Sicherheitsgruppe, die Sie im Parameter angeben. `SecurityGroupId`

# AWSSupport-ConfigureDNSQueryLogging

Beschreibung

Das `AWSSupport-ConfigureDNSQueryLogging` Runbook konfiguriert die Protokollierung für DNS-Abfragen, die ihren Ursprung in Ihrer Virtual Private Cloud (VPC) haben, oder für gehostete Zonen von Amazon Route 53. Sie können wählen, ob Sie Abfrageprotokolle in Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) oder Amazon Data Firehose veröffentlichen möchten. Weitere Informationen zur Abfrageprotokollierung und Resolver-Abfrageprotokollen finden Sie unter Öffentliche DNS-Abfrageprotokollierung und Resolver-Abfrageprotokollierung.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LogDestinationArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der CloudWatch Logs-Gruppe, des Amazon S3 S3-Buckets oder des Firehose-Streams, an den Sie Abfrageprotokolle senden möchten. Beachten Sie,

dass die öffentliche DNS-Abfrageprotokollierung von Route 53 nur CloudWatch Logs-Gruppen unterstützt. Wenn Sie keinen Wert für diesen Parameter angeben, erstellt die Automatisierung eine CloudWatch Logs-Gruppe mit dem Format `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` und einer IAM-Ressourcenrichtlinie zur Veröffentlichung der Abfrageprotokolle. Die durch die Automatisierung erstellte CloudWatch Protokollgruppe hat eine Aufbewahrungsfrist von 14 Tagen.

- QueryLogGeben Sie ein

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Arten von Abfragen, die Sie protokollieren möchten.

  Gültige Werte: Public | Resolver/Private

  Standard: Öffentlich

- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Ressource, deren Abfragen Sie protokollieren möchten. Wenn Sie `Public` für den `QueryLogType` Parameter angeben, muss es sich bei der Ressource um die ID einer privaten gehosteten Route 53-Zone handeln. Wenn Sie `Resolver/Private` für den `QueryLogType` Parameter angeben, muss die Ressource die ID einer VPC sein.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- `aws:executeScript`- Überprüft, ob die Ressource, die Sie für den `ResourceId` Parameter angeben, vorhanden ist, und prüft, ob der Ressourcentyp der erforderlichen `QueryLogType` Option entspricht.
- `aws:executeScript`- Überprüft, ob der Wert, den Sie für den `LogDestinationArn` Parameter angeben, dem erforderlichen Wert entspricht. `QueryLogType`
- `aws:executeScript`- Überprüft die erforderlichen Berechtigungen für Route 53, um Protokolle in der Protokollgruppe CloudWatch Logs zu veröffentlichen, und erstellt die erforderliche IAM-Ressourcenrichtlinie, falls diese nicht vorhanden ist.
- `aws:executeScript`- Aktiviert die DNS-Abfrageprotokollierung am ausgewählten Ziel.

## `AWSSupport-ConfigureTrafficMirroring`

Beschreibung

Das `AWSSupport-ConfigureTrafficMirroring` Runbook konfiguriert die Verkehrsspiegelung, um Ihnen bei der Behebung von Verbindungsproblemen zwischen einem Load Balancer und Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu helfen. Die Verkehrsspiegelung kopiert eingehenden und ausgehenden Datenverkehr von den Netzwerkschnittstellen, die mit Ihren Instances verbunden sind. Um die Verkehrsspiegelung zu konfigurieren, erstellt dieses Runbook die erforderlichen Ziele, Filter und Sitzungen. Standardmäßig konfiguriert das Runbook die Spiegelung für den gesamten eingehenden und ausgehenden Datenverkehr für alle Protokolle außer Amazon DNS. Wenn Sie den Datenverkehr von bestimmten Quellen und Zielen spiegeln möchten, können Sie die Regeln für eingehenden und ausgehenden Datenverkehr nach Abschluss der Automatisierung ändern.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Quelle: ENI

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die elastic network interface, für die Sie die Verkehrsspiegelung konfigurieren möchten.
- Ziel

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das Ziel für den gespiegelten Datenverkehr. Sie müssen die ID einer Netzwerkschnittstelle, eines Network Load Balancer oder eines Gateway Load Balancer-Endpunkts angeben. Wenn Sie einen Network Load Balancer angeben, müssen UDP-Listener auf Port 4789 vorhanden sein.
- SessionNumber

  Typ: Zeichenfolge

  Gültige Werte: 1-32766

  Beschreibung: (Erforderlich) Die Nummer der Spiegelsitzung, die Sie verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`

- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilter
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

Dokumentschritte

- aws:executeScript- Führt ein Skript aus, um ein Ziel zu erstellen.
- aws:executeAwsApi- Erstellt eine Filterregel.
- aws:executeAwsApi- Erstellt eine Spiegelfilterregel für den gesamten eingehenden Datenverkehr.
- aws:executeAwsApi- Erstellt eine Spiegelfilterregel für den gesamten ausgehenden Datenverkehr.
- aws:executeAwsApi- Erstellt eine Traffic Mirror-Sitzung.
- aws:executeAwsApi- Löscht den Filter, wenn die Erstellung des Filters oder der Sitzung fehlschlägt.
- aws:executeAwsApi- Löscht das Ziel, wenn die Filter- oder Sitzungserstellung fehlschlägt.

Ausgaben

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.targetIDOutput

## AWSSupport-ConnectivityTroubleshooter

Beschreibung

Das `AWSSupport-ConnectivityTroubleshooter` Runbook diagnostiziert Verbindungsprobleme zwischen den folgenden Komponenten:

- AWS Ressourcen innerhalb einer Amazon Virtual Private Cloud (Amazon VPC)
- AWS Ressourcen in verschiedenen Amazon-VPCs innerhalb derselben AWS-Region , die über VPC-Peering verbunden sind
- AWS Ressourcen in einer Amazon VPC und eine Internetressource, die ein Internet-Gateway verwendet
- AWS Ressourcen in einer Amazon VPC und eine Internetressource, die ein NAT-Gateway (Network Address Translation) verwendet

## Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Ziel-IP

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die IPv4-Adresse der Ressource, zu der Sie eine Verbindung herstellen möchten.

- DestinationPort

  Typ: Zeichenfolge

  Standard: true

  Beschreibung: (Erforderlich) Die Portnummer, zu der Sie eine Verbindung auf der Zielressource herstellen möchten.
- DestinationVpc

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die ID der Amazon VPC, mit der Sie die Konnektivität testen möchten.
- SourceIP

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die private IPv4-Adresse der AWS Ressource in Ihrer Amazon VPC, von der aus Sie die Konnektivität testen möchten.
- SourcePortBereich

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Portbereich, der von der AWS Ressource in Ihrer Amazon VPC verwendet wird, von der aus Sie die Konnektivität testen möchten.
- SourceVpc

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die ID der Amazon VPC, von der aus Sie die Konnektivität testen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- aws:executeScript- Sammelt Details zu der AWS Ressource, die Sie im SourceIP Parameter angeben.
- aws:executeScript- Ermittelt das Ziel des Netzwerkverkehrs von der AWS Ressource anhand der im vorherigen Schritt gesammelten Routen.
- aws:branch- Verzweigungen auf der Grundlage des Ziels des Netzwerkverkehrs.
- aws:executeAwsApi- Sammelt Details zur Zielressource.
- aws:executeScript— Bestätigt, dass die für die Amazon-Ziel-VPC zurückgegebene ID mit dem im DestinationVpc Parameter angegebenen Wert übereinstimmt, falls vorhanden.
- aws:executeAwsApi- Sammelt die Sicherheitsgruppenregeln für die Quell- und Zielressourcen.
- aws:executeScript- Bestätigt, ob die Sicherheitsgruppenregeln den erforderlichen Verkehr zwischen den Quell- und Zielressourcen zulassen.
- aws:executeAwsApi- Sammelt die Netzwerkzugriffskontrolllisten (NACLs), die den Subnetzen für die Quell- und Zielressourcen zugeordnet sind.
- aws:executeScript- Bestätigt, ob die NACLs den erforderlichen Verkehr zwischen den Quell- und Zielressourcen zulassen.
- aws:executeScript- Bestätigt, ob der Quelle eine öffentliche IP-Adresse zugeordnet ist, wenn das Routenziel ein Internet-Gateway ist.
- aws:executeAwsApi- Sammelt die Sicherheitsgruppenregeln für die Quellressource.
- aws:executeScript- Bestätigt, ob die Sicherheitsgruppenregeln den erforderlichen Verkehr von der Quell- zur Zielressource zulassen.
- aws:executeAwsApi- Sammelt die NACLs, die dem Subnetz für die Quellressource zugeordnet sind.
- aws:executeScript- Bestätigt, ob die NACLs den benötigten Verkehr von der Quellressource zulassen.

- `aws:executeAwsApi`- Sammelt Details über das NAT-Gateway.
- `aws:executeAwsApi`— Sammelt die NACLs, die dem Subnetz für das NAT-Gateway zugeordnet sind.
- `aws:executeScript`- Bestätigt, ob die NACLs den erforderlichen Verkehr aus dem Subnetz für das NAT-Gateway zulassen.
- `aws:executeScript`- Sammelt die Routen, die dem Subnetz für das NAT-Gateway zugeordnet sind.
- `aws:executeScript`- Bestätigt, ob das NAT-Gateway eine Route zu einem Internet-Gateway hat.
- `aws:executeAwsApi`- Sammelt Details über die VPC-Peering-Verbindung.
- `aws:executeScript`— Bestätigt, dass sich beide VPCs in derselben Region befinden und dass die für die Ziel-VPC zurückgegebene ID mit dem `DestinationVpc` im Parameter angegebenen Wert übereinstimmt, falls vorhanden.
- `aws:executeAwsApi`- Gibt das Subnetz der Zielressource zurück.
- `aws:executeScript`- Sammelt die Routen, die dem Subnetz für die Peering-VPC zugeordnet sind.
- `aws:executeScript`— Bestätigt, ob die Peering-VPC über eine Route zur Peering-Verbindung verfügt.
- `aws:executeScript`- Bestätigt, ob Datenverkehr von der Quellressource zulässig ist, wenn das Ziel von der Automatisierung nicht unterstützt wird.

## AWSSupport-TroubleshootVPN

Beschreibung

Das `AWSSupport-TroubleshootVPN` Runbook hilft Ihnen, Fehler in einer -AWS Site-to-Site VPNVerbindung zu verfolgen und zu beheben. Die Automatisierung umfasst mehrere automatisierte Prüfungen, die darauf ausgelegt sind, - `IKEv1` oder -`IKEv2`Fehler im Zusammenhang mit AWS Site-to-Site VPN Verbindungstunneln zu verfolgen. Die Automatisierung versucht, bestimmte Fehler abzugleichen, und die entsprechende Lösung bildet eine Liste häufiger Probleme.

Hinweis: Diese Automatisierung behebt die Fehler nicht. Es wird für den genannten Zeitraum ausgeführt und scannt die Protokollgruppe auf Fehler in der VPN- CloudWatch Protokollgruppe .

Wie funktioniert es?

Das Runbook führt eine Parametervalidierung durch, um zu bestätigen, ob die im Eingabeparameter enthaltene Amazon- CloudWatch Protokollgruppe vorhanden ist, ob Protokollstreams in der Protokollgruppe vorhanden sind, die der VPN-Tunnelprotokollierung entsprechen, ob die VPN-Verbindungs-ID vorhanden ist und ob die Tunnel-IP-Adresse vorhanden ist. Es führt Logs-Insights-API-Aufrufe für Ihre CloudWatch Protokollgruppe durch, die für die VPN-Protokollierung konfiguriert sind.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der für die AWS Site-to-Site VPN Verbindungsprotokollierung konfigurierte Amazon- CloudWatch Protokollgruppenname

  Zulässiges Muster: `^[\.\-_/#A-Za-z0-9]{1,512}`
- VpnConnectionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die zu behebende AWS Site-to-Site VPN Verbindungs-ID.

Zulässiges Muster: `^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die IPv4-Adresse für Tunnelnummer 1, die Ihrem zugeordnet istAWS Site-to-Site VPN.

  Zulässiges Muster: `^((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

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die IPv4-Adresse des Tunnels Nummer 2, die Ihrem zugeordnet istAWS Site-to-Site VPN.

  Zulässiges Muster: `^((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

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Wählen Sie aus, welche IKE-Version Sie verwenden. Zulässige Werte: IKEv1, IKEv2

  Zulässige Werte: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  Typ: Zeichenfolge

  Beschreibung: (Optional) Startzeit für die Protokollanalyse. Sie können entweder StartTimeinEpoch/ EndTimeinEpoch oder LookBackPeriod für die Protokollanalyse verwenden

  Zulässiges Muster: `^\d{10}|^$`

- EndTimeinEpoch

  Typ: Zeichenfolge

Beschreibung: (Optional) Endzeit für die Protokollanalyse. Sie können entweder StartTimeinEpoch/ EndTimeinEpoch oder LookBackPeriod für die Protokollanalyse verwenden. Wenn sowohl StartTimeinEpoch/ als auch LookBackPeriod angegeben istEndTimeinEpoch LookBackPeriod , hat sie Vorrang

Zulässiges Muster: `^\d{10}|^$`

- LookBackPeriod

  Typ: Zeichenfolge

  Beschreibung: (Optional) Zweistellige Zeit in Stunden, um nach der Protokollanalyse zu suchen. Gültiger Bereich: 01–99. Dieser Wert hat Vorrang, wenn Sie auch StartTimeinEpoch und angeben EndTime

  Zulässiges Muster: `^(\d?[1-9]|[1-9]0)|^$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Anweisungen

Hinweis: Diese Automatisierung funktioniert für die CloudWatch Protokollgruppen, die für Ihre VPN-Tunnelprotokollierung konfiguriert sind, wenn das Protokollierungsausgabeformat JSON ist.

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie in der -AWS Systems ManagerKonsole zur AWSSupport-TroubleshootVPN.
2. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Optional):

Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM)-Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LogGroupName (Erforderlich):

  Der zu validierende Amazon- CloudWatch Protokollgruppenname. Dies muss die CloudWatch Protokollgruppe sein, an die VPN Protokolle senden kann.

- VpnConnectionId (Erforderlich):

  Die AWS Site-to-Site VPN Verbindungs-ID, deren Protokollgruppe auf VPN-Fehler nachverfolgt wird.

- TunnelAIPAddress (erforderlich):

  Die IP-Adresse des Tunnels A, die Ihrer AWS Site-to-Site VPN Verbindung zugeordnet ist.

- TunnelBIPAddress (optional):

  Die IP-Adresse des Tunnels B, die Ihrer AWS Site-to-Site VPN Verbindung zugeordnet ist.

- IKEVersion (erforderlich):

  Wählen Sie die IKEversion aus, die Sie verwenden. Zulässige Werte: IKEv1, IKEv2.

- StartTimeinEpoch (Optional):

  Der Beginn des Zeitraums, der nach Fehlern abgefragt werden soll. Der Bereich ist inklusive, sodass die angegebene Startzeit in der Abfrage enthalten ist. Als Epochenzeit angegeben, die Anzahl der Sekunden seit dem 1. Januar 1970, 00:00:00 UTC.

- EndTimeinEpoch (Optional):

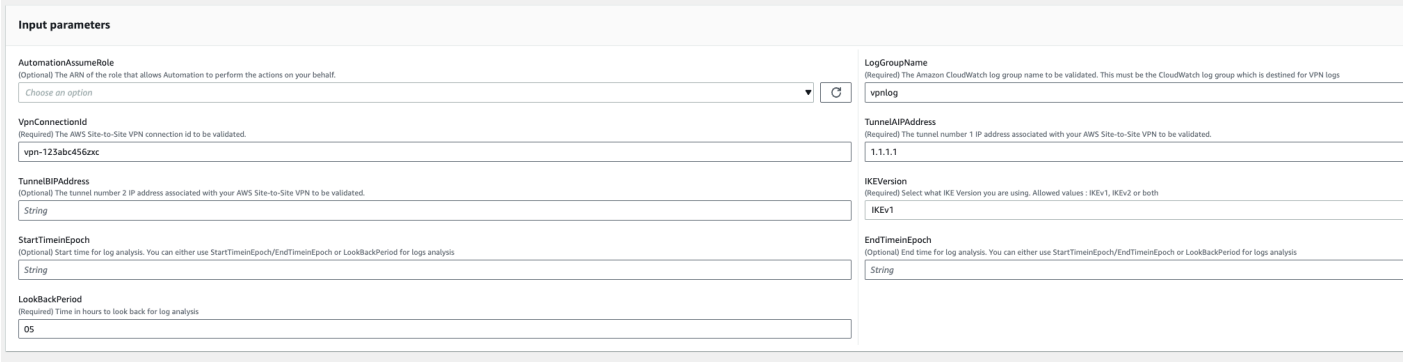
  Das Ende des Zeitraums, in dem nach Fehlern abgefragt werden soll. Der Bereich ist inklusive, sodass die angegebene Endzeit in der Abfrage enthalten ist. Als Epochenzeit angegeben, die Anzahl der Sekunden seit dem 1. Januar 1970, 00:00:00 UTC.

- LookBackPeriod (Erforderlich):

  Zeit in Stunden, um nach Fehlern zu suchen.

Hinweis: Konfigurieren Sie eine oder StartTimeinEpoch EndTimeinEpoch, LookBackPeriod um den Zeitraum für die Protokollanalyse zu korrigieren. Geben Sie eine zweistellige Zahl in Stunden

an, um nach Fehlern in der Vergangenheit ab der Startzeit der Automatisierung zu suchen. Oder, wenn der Fehler in der Vergangenheit innerhalb eines bestimmten Zeitraums liegt, schließen Sie StartTimeinEpoch und EndTimeinEpochanstelle von ein LookBackPeriod.




3. Wählen Sie Ausführen aus.
4. Die Automatisierung wird initiiert.
5. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - parameterValidation:

     Führt eine Reihe von Validierungen für Eingabeparameter aus, die in der Automatisierung enthalten sind.
   - branchOnValidationOfLogGroup:

     Prüft, ob die im Parameter erwähnte Protokollgruppe gültig ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.
   - branchOnValidationOfLogStream:

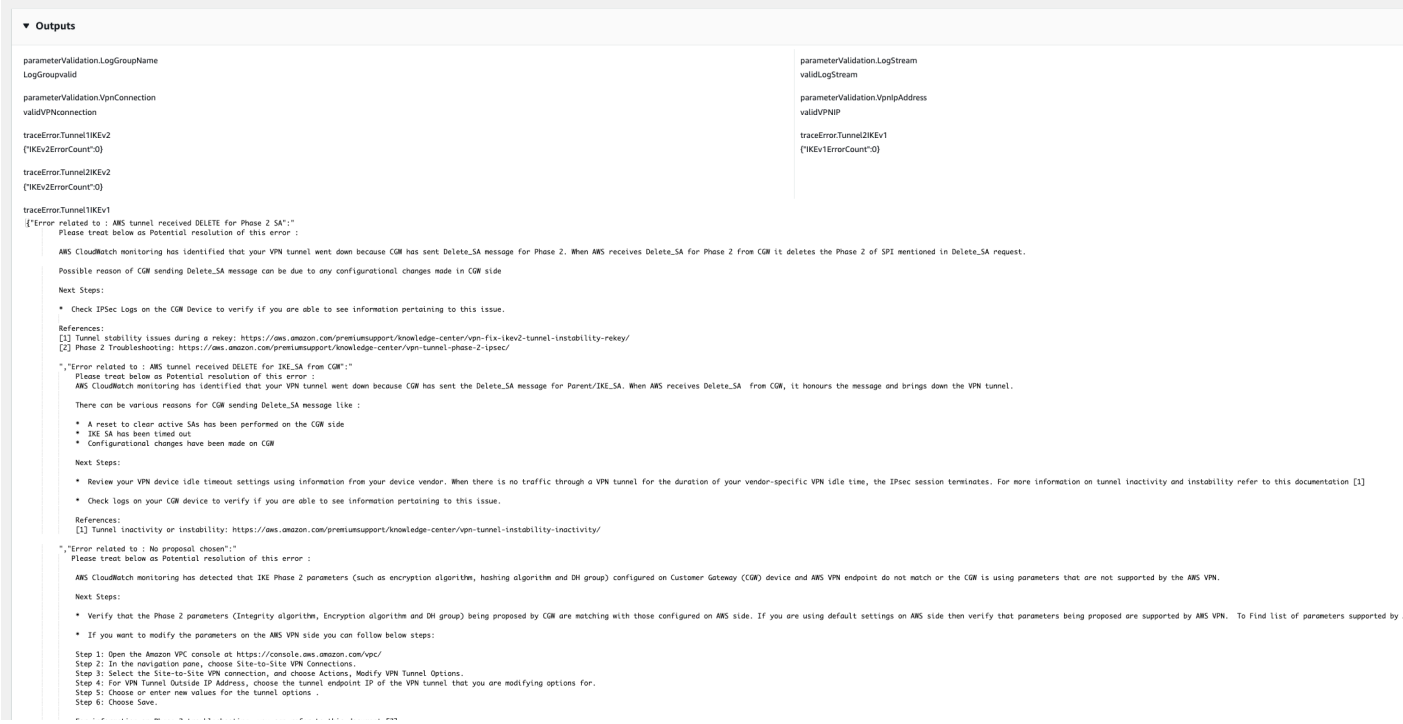
     Prüft, ob der Protokollstream in der enthaltenen CloudWatch Protokollgruppe vorhanden ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.
   - branchOnValidationOfVpnConnectionId:

     Prüft, ob die im Parameter enthaltene VPN-Verbindungs-ID gültig ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.
   - branchOnValidationOfVpnIp:

     Prüft, ob die im Parameter erwähnte Tunnel-IP-Adresse gültig ist oder nicht. Wenn dies ungültig ist, wird die weitere Ausführung von Automatisierungsschritten gestoppt.
   - traceError:

Führt einen Logs-Insights-API-Aufruf in Ihrer eingeschlossenen CloudWatch Protokollgruppe durch und sucht nach dem Fehler im Zusammenhang mit IKEv1/IKEv2 zusammen mit einer zugehörigen vorgeschlagenen Lösung.

6. Nachdem Sie fertig sind, überprüfen Sie den Abschnitt Outputs, um die detaillierten Ergebnisse der Ausführung zu erhalten.




## Referenzen

### Systems Manager Automation

- Ausführen dieser Automatisierung (Konsole)
- Ausführen einer Automatisierung
- Einrichten einer Automatisierung
- Landingpage zur Unterstützung von Automation Workflows

### AWS -Servicedokumentation

- Inhalt von Site-to-Site-VPN-Protokollen

# AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Beschreibung

Das `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` Runbook löscht das von Ihnen angegebene Internet-Gateway nur für ausgehenden Datenverkehr.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EgressOnlyInternetGatewayID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Internet-Gateways für ausgehenden Datenverkehr, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Dokumentschritte

- `aws:executeScript`- Löscht das im Parameter angegebene Internet-Gateway, das nur für ausgehenden Datenverkehr bestimmt ist. `EgressOnlyInternetGatewayId`
- `aws:executeScript`- Überprüft, ob das Internet-Gateway für ausgehenden Datenverkehr gelöscht wurde.

## `AWSConfigRemediation-DeleteUnusedENI`

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedENI` Runbook löscht ein elastic network interface (ENI) mit dem Anhangsstatus. `detached`

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- NetworkInterfaceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der ENI, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die ENI, die Sie im `NetworkInterfaceId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob die ENI gelöscht wurde.

## AWSConfigRemediation-DeleteUnusedSecurityGroup

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedSecurityGroup` Runbook löscht die Sicherheitsgruppe, die Sie im `GroupId` Parameter angeben. Wenn Sie versuchen, eine Sicherheitsgruppe zu löschen, die mit einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance verknüpft ist oder auf die von einer anderen Sicherheitsgruppe verwiesen wird, schlägt die Automatisierung fehl. Diese Automatisierung löscht keine Standardsicherheitsgruppe.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Dokumentschritte

- `aws:executeAwsApi`- Gibt den Namen der Sicherheitsgruppe unter Verwendung des Werts zurück, den Sie im `GroupId` Parameter angeben.
- `aws:branch`- Bestätigt, dass der Gruppenname nicht „Standard“ ist.

- `aws:executeAwsApi`- Löscht die im `GroupId` Parameter angegebene Sicherheitsgruppe.
- `aws:executeScript`- Bestätigt, dass die Sicherheitsgruppe gelöscht wurde.

## `AWSConfigRemediation-DeleteUnusedVPCNetworkACL`

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` Runbook löscht eine Network Access Control List (ACL), die keinem Subnetz zugeordnet ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- NetworkAclID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Netzwerk-ACL, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die im Parameter angegebene Netzwerk-ACL. `NetworkAclId`
- `aws:executeScript`- Bestätigt, dass die im `NetworkAclId` Parameter angegebene Netzwerk-ACL gelöscht wurde.

## AWSConfigRemediation-DeleteVPCFlowLog

Beschreibung

Das `AWSConfigRemediation-DeleteVPCFlowLog` Runbook löscht das von Ihnen angegebene VPC-Flow-Protokoll (Virtual Private Cloud).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- FlowLogID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Löscht das Flow-Protokoll, das Sie im `FlowLogId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob das Flow-Protokoll gelöscht wurde.

## AWSConfigRemediation-DetachAndDeleteInternetGateway

Beschreibung

Das `AWSConfigRemediation-DetachAndDeleteInternetGateway` Runbook trennt und löscht das von Ihnen angegebene Internet-Gateway. Wenn Amazon EC2 EC2-Instances in Ihrer Virtual Private Cloud (VPC) elastische IP-Adressen oder öffentliche IPv4-Adressen zugeordnet sind, schlägt das Runbook fehl.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- InternetGatewayID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Internet-Gateways, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Statuseigenschaft des virtuellen privaten Gateways ändert `available` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`— Ruft eine angegebene Virtual Private Gateway-Konfiguration ab.
- `aws:branch`- Verzweigt auf der Grundlage des VpcAttachments Parameterwerts .state.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert `attached` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`- Akzeptiert die ID des Virtual Private Gateways und die ID der Amazon VPC als Eingabe und trennt das Virtual Private Gateway von der Amazon VPC.
- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert oder das Zeitlimit überschritten wird. `detached`

- `aws:executeAwsApi`- Akzeptiert die ID des virtuellen privaten Gateways als Eingabe und löscht sie.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des Virtual Private Gateways als Eingabe und verifiziert deren Löschung.

`aws:executeAwsApi`- Erfasst die VPC-ID aus der Internet-Gateway-ID.

- `aws:executeAwsApi`- Trennt die Internet-Gateway-ID von der VPC.
- `aws:executeAwsApi`- Löscht das Internet-Gateway.

## AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Beschreibung

Das `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` Runbook trennt und löscht ein bestimmtes virtuelles privates Gateway von Amazon Elastic Compute Cloud (Amazon EC2), das an eine mit Amazon Virtual Private Cloud (Amazon VPC) erstellte Virtual Private Cloud (VPC) angehängt ist.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- VpnGatewayID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Virtual Private Gateways, das gelöscht werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Statuseigenschaft des virtuellen privaten Gateways ändert `available` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`— Ruft eine angegebene Virtual Private Gateway-Konfiguration ab.
- `aws:branch`- Verzweigt auf der Grundlage des VpcAttachments Parameterwerts .state.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert `attached` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`- Akzeptiert die ID des Virtual Private Gateways und die ID der Amazon VPC als Eingabe und trennt das Virtual Private Gateway von der Amazon VPC.
- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert oder das Zeitlimit überschritten wird. `detached`

- `aws:executeAwsApi`- Akzeptiert die ID des virtuellen privaten Gateways als Eingabe und löscht sie.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des Virtual Private Gateways als Eingabe und verifiziert deren Löschung.

## `AWS-DisableIncomingSSHOnPort22`

Beschreibung

Das `AWS-DisableIncomingSSHOnPort22` Runbook entfernt Regeln, die uneingeschränkten eingehenden SSH-Verkehr auf TCP-Port 22 für Sicherheitsgruppen zulassen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- SecurityGroupIDs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs der Sicherheitsgruppen, für die Sie den SSH-Verkehr einschränken möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeAwsApi`- Entfernt alle Regeln, die eingehenden SSH-Verkehr auf TCP-Port 22 aus den Sicherheitsgruppen zulassen, die `SecurityGroupIds` Sie im Parameter angeben.

Ausgaben

DisableIncomingSSH-Vorlage. RestrictedSecurityGroupIds - Eine Liste der IDs der Sicherheitsgruppen, bei denen die SSH-Regeln für eingehende Anrufe entfernt wurden.

# AWS-DisablePublicAccessForSecurityGroup

Beschreibung

Dieses Runbook deaktiviert standardmäßige SSH- und RDP-Ports, die für alle IP-Adressen geöffnet sind.

**Important**

Dieses Runbook schlägt mit einem "fehl. InvalidPermission NotFound"Fehler für Sicherheitsgruppen, die beide der folgenden Kriterien erfüllen: 1) Die Sicherheitsgruppe befindet sich in einer nicht standardmäßigen VPC; und 2) Die Regeln für eingehende Nachrichten für die Sicherheitsgruppe geben keine offenen Ports an, die alle vier der folgenden Muster verwenden:

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

**Note**

Dieses Runbook ist in China nicht verfügbar. AWS-Regionen

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, für die die Ports deaktiviert werden sollen.
- IpAddressToBlock

  Typ: Zeichenfolge

  Beschreibung: (Optional) Zusätzliche IPv4-Adressen, von denen aus der Zugriff blockiert werden soll, im Format. `1.2.3.4/32`

## AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Beschreibung

Das `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` Runbook deaktiviert das IPv4-Attribut für die öffentliche Adressierung für das von Ihnen angegebene Subnetz.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Subnetzes, für das Sie das automatische Zuweisen öffentlicher IPv4-Adressen deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Dokumentschritte

- `aws:executeAwsApi`— Deaktiviert das automatische Zuweisen öffentlicher IPv4-Adressen für das Subnetz, das Sie im Parameter angegeben haben. `SubnetId`
- `aws:assertAwsResourceProperty`— Überprüft, ob das Attribut deaktiviert wurde.

## AWSSupport-EnableVPCFlowLogs

Beschreibung

Das `AWSSupport-EnableVPCFlowLogs` Runbook erstellt Amazon Virtual Private Cloud (Amazon VPC) Flow Logs für Subnetze, Netzwerkschnittstellen und VPCs in Ihrem. AWS-Konto Wenn Sie ein Flow-Protokoll für ein Subnetz oder eine VPC erstellen, wird jede elastic network interface in diesem Subnetz oder dieser Amazon VPC überwacht. Flow-Protokolldaten werden in der Amazon CloudWatch Logs-Protokollgruppe oder dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket veröffentlicht. Weitere Informationen zu Flow-Protokollen finden Sie unter VPC Flow Logs im Amazon VPC-Benutzerhandbuch.

**Important**

Wenn Sie Flow-Logs in Logs oder Amazon S3 veröffentlichen, fallen Gebühren für Datenaufnahme und Archivierung für verkaufte CloudWatch Logs an. Weitere Informationen finden Sie unter Preise für Flow Logs

Führen Sie diese Automatisierung aus (Konsole)

**Note**

Stellen Sie bei der Auswahl `s3` als Protokollziel sicher, dass die Bucket-Richtlinie dem Log-Lieferdienst Zugriff auf den Bucket gewährt. Weitere Informationen finden Sie unter Amazon S3 S3-Bucket-Berechtigungen für Flow-Logs.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DeliverLogsPermissionArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN für die IAM-Rolle, der es Amazon Elastic Compute Cloud (Amazon EC2) ermöglicht, Flow-Logs in der CloudWatch Logs-Protokollgruppe in Ihrem Konto zu veröffentlichen. Wenn Sie `s3` für den `LogDestinationType` Parameter angeben, geben Sie keinen Wert für diesen Parameter an. Weitere Informationen finden Sie unter Veröffentlichen von CloudWatch Flow-Protokollen in Logs im Amazon VPC-Benutzerhandbuch.

- LogDestinationARN

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Ressource, auf der die Flow-Protokolldaten veröffentlicht werden. Wenn für den `LogDestinationType` Parameter angegeben `cloud-watch-logs` ist, geben Sie den ARN der CloudWatch Logs-Protokollgruppe an, in der Sie Flow-Log-Daten veröffentlichen möchten. Alternativ können Sie stattdessen `LogGroupName` verwenden. Wenn für den `LogDestinationType` Parameter angegeben `s3` ist, müssen Sie für diesen Parameter den ARN des Amazon S3 S3-Buckets angeben, in dem Sie Flow-Protokolldaten veröffentlichen möchten. Sie können auch einen Ordner im Bucket angeben.

  > **Important**
  >
  > Wenn `LogDestinationType` Sie sich für den ausgewählten Bucket entscheiden`s3`, sollten Sie sicherstellen, dass der ausgewählte Bucket den Best Practices für die Sicherheit von Amazon S3 Bucket entspricht und dass Sie die Datenschutzgesetze für Ihr Unternehmen und Ihre geografische Region einhalten.

- LogDestinationType

  Typ: Zeichenfolge

  Gültige Werte: cloud-watch-logs | s3

Beschreibung: (Erforderlich) Legt fest, wo Flow-Protokolldaten veröffentlicht werden. Wenn Sie `LogDestinationType` als angeben`s3`, geben Sie nicht `DeliverLogsPermissionArn` oder an`LogGroupName`.

- LogFormat

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Felder, die in das Flow-Protokoll aufgenommen werden sollen, und die Reihenfolge, in der sie im Datensatz erscheinen sollen. Eine Liste der verfügbaren Felder finden Sie unter Flow-Protokolldatensätze im Amazon VPC-Benutzerhandbuch. Wenn Sie keinen Wert für diesen Parameter angeben, wird das Flow-Protokoll im Standardformat erstellt. Wenn Sie diesen Parameter angeben, müssen Sie mindestens ein Feld angeben.

- LogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der CloudWatch Logs-Protokollgruppe, in der Flow-Log-Daten veröffentlicht werden. Wenn Sie `s3` für den `LogDestinationType` Parameter angeben, geben Sie keinen Wert für diesen Parameter an.

- ResourceIds

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs für die Subnetze, Elastic Network-Schnittstellen oder VPC, für die Sie ein Flow-Protokoll erstellen möchten.

- TrafficType

  Typ: Zeichenfolge

  Gültige Werte: ACCEPT | REJECT | ALL

  Beschreibung: (Erforderlich) Der Typ des zu protokollierenden Datenverkehrs. Sie können den Datenverkehr protokollieren, den die Ressource akzeptiert oder ablehnt, oder den gesamten Datenverkehr.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

### Beispiel für eine Richtlinie

```
        {
            "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}/*"
```

```
                ]
            }
        ]
    }
```

Dokumentschritte

- `aws:branch`- Verzweigt auf der Grundlage des für den `LogDestinationType` Parameter angegebenen Werts.
- `aws:executeScript`- Prüft, ob der Ziel-Amazon Simple Storage Service (Amazon S3) möglicherweise Lese - oder **`public`**Schreibzugriff auf seine Objekte gewährt.
- `aws:executeScript`- Erstellt eine Protokollgruppe, wenn kein Wert für den `LogDestinationARN` Parameter angegeben wurde, und für den `LogDestinationType` Parameter `cloud-watch-logs` wird ein Wert angegeben.
- `aws:executeScript`- Erstellt Flussprotokolle auf der Grundlage der in den Runbook-Parametern angegebenen Werte.

## `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch`

Beschreibung

Das `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` Runbook ersetzt ein vorhandenes Amazon VPC-Flow-Protokoll, das Flow-Protokolldaten in Amazon Simple Storage Service (Amazon S3) veröffentlicht, durch ein Flow-Protokoll, das Flow-Protokolldaten in der von Ihnen angegebenen Amazon CloudWatch Logs (CloudWatch Logs) -Protokollgruppe veröffentlicht.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- DestinationLogGruppe

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der CloudWatch Logs-Protokollgruppe, in der Sie Flow-Log-Daten veröffentlichen möchten.

- DeliverLogsPermissionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der AWS Identity and Access Management (IAM) -Rolle, die Sie verwenden möchten und der Amazon Elastic Compute Cloud (Amazon EC2) die erforderlichen Berechtigungen zum Veröffentlichen von Flow-Protokolldaten in Logs gewährt. CloudWatch

- FlowLogID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das auf Amazon S3 veröffentlicht wird, das Sie ersetzen möchten.

- MaxAggregationIntervall

  Typ: Ganzzahl

  Gültige Werte: 60 | 600

  Beschreibung: (Optional) Das maximale Zeitintervall in Sekunden, in dem ein Paketfluss erfasst und in einem Flow-Protokolldatensatz zusammengefasst wird.

- TrafficType

Typ: Zeichenfolge

Gültige Werte: ACCEPT | REJECT | ALL

Beschreibung: (Erforderlich) Der Typ der Flow-Protokolldaten, die Sie aufzeichnen und veröffentlichen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst Details zu Ihrer VPC aus dem Wert, den Sie im `FlowLogId` Parameter angeben.
- `aws:executeAwsApi`- Erstellt ein Flow-Protokoll auf der Grundlage der Werte, die Sie für die Runbook-Parameter angeben.
- `aws:assertAwsResourceProperty`— Überprüft, ob das neu erstellte Flow-Protokoll in Logs veröffentlicht wird. CloudWatch
- `aws:executeAwsApi`— Löscht das Flow-Protokoll, das auf Amazon S3 veröffentlicht wird.
- `aws:executeScript`— Bestätigt, dass das auf Amazon S3 veröffentlichte Flow-Protokoll gelöscht wurde.

## AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Beschreibung

Das `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` Runbook ersetzt ein vorhandenes Amazon VPC-Flow-Protokoll, das Flow-Protokolldaten in Amazon CloudWatch Logs (CloudWatch Logs) veröffentlicht, durch ein Flow-Protokoll, das Flow-Protokolldaten in dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket veröffentlicht.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Ziele: 3 BucketArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon S3 S3-Buckets, in dem Sie Flow-Protokolldaten veröffentlichen möchten.
- FlowLogID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das in CloudWatch Logs veröffentlicht wird, die Sie ersetzen möchten.
- MaxAggregationIntervall

Typ: Ganzzahl

Gültige Werte: 60 | 600

Beschreibung: (Optional) Das maximale Zeitintervall in Sekunden, in dem ein Paketfluss erfasst und in einem Flow-Protokolldatensatz zusammengefasst wird.

- TrafficType

  Typ: Zeichenfolge

  Gültige Werte: ACCEPT | REJECT | ALL

  Beschreibung: (Erforderlich) Der Typ der Flow-Protokolldaten, die Sie aufzeichnen und veröffentlichen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst Details zu Ihrer VPC aus dem Wert, den Sie im `FlowLogId` Parameter angeben.
- `aws:executeAwsApi`- Erstellt ein Flow-Protokoll auf der Grundlage der Werte, die Sie für die Runbook-Parameter angeben.
- `aws:assertAwsResourceProperty`— Überprüft, ob das neu erstellte Flow-Protokoll auf Amazon S3 veröffentlicht wird.
- `aws:executeAwsApi`— Löscht das Flow-Protokoll, das in Logs veröffentlicht wird. CloudWatch

- `aws:executeScript`- Bestätigt, dass das in CloudWatch Logs veröffentlichte Flow-Protokoll gelöscht wurde.

## AWS-ReleaseElasticIP

Beschreibung

Freigeben der angegebenen Elastic-IP-Adresse mithilfe der Zuordnungs-ID.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AllocationId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Zuweisungs-ID der Elastic IP-Adresse.

## AWS-RemoveNetworkACLUnrestrictedSSHRDP

Beschreibung

Das `AWS-RemoveNetworkACLUnrestrictedSSHRDP` Runbook entfernt alle ACL-Regeln (Network Access Control List) aus der angegebenen Netzwerk-ACL, die eingehenden Datenverkehr von allen Quelladressen zu Standard-SSH- und RDP-Anschlüssen zulassen. Regeln, die Portbereiche enthalten, die sich mit den standardmäßigen SSH- und RDP-Ports überschneiden, werden nicht entfernt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- NetworkAclID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Netzwerk-ACL, für die Sie uneingeschränkte Regeln entfernen möchten, die eingehenden Datenverkehr von allen Quelladressen zu Standard-SSH- und RDP-Anschlüssen zulassen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangsregeln, die Datenverkehr von allen Quelladressen der Sicherheitsgruppe zulassen, die Sie im Parameter angegeben haben. `SecurityGroupId`

Ausgaben

RemoveNaclEntriesAndÜberprüfen Sie. VerificationMessage - Bestätigungsmeldungen der erfolgreich gelöschten Netzwerk-ACL-Regeln.

RemoveNaclEntriesAndÜberprüfen. RulesDeletedAndApiResponses - Die Netzwerk-ACL-Regeln, die gelöscht wurden, und die Antworten der `DeleteNetworkAclEntry` API-Operationen.

## `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules`

Beschreibung

Das `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` Runbook entfernt alle Eingangsregeln aus der von Ihnen angegebenen Sicherheitsgruppe, die Datenverkehr von allen Quelladressen zulassen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- SecurityGroupID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, aus der Sie Eingangsregeln entfernen möchten, die Datenverkehr von allen Quelladressen zulassen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangsregeln, die Datenverkehr von allen Quelladressen der Sicherheitsgruppe zulassen, die Sie im Parameter angegeben haben. `SecurityGroupId`

## AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Beschreibung

Das `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` Runbook entfernt alle Regeln aus der Standardsicherheitsgruppe der von Ihnen angegebenen Virtual Private Cloud (VPC).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, aus der Sie alle Regeln entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass die Sicherheitsgruppe, die Sie im `GroupId` Parameter angegeben haben, den Namen default trägt.
- `aws:executeScript`- Entfernt alle Regeln aus der Sicherheitsgruppe, die Sie im `GroupId` Parameter angegeben haben.

## `AWSSupport-SetupIPMonitoringFromVPC`

Beschreibung

`AWSSupport-SetupIPMonitoringFromVPC`erstellt eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance im angegebenen Subnetz und überwacht ausgewählte Ziel-IPs (IPv4 oder IPv6), indem kontinuierlich Ping-, MTR-, Traceroute- und Tracetcp-Tests ausgeführt werden. Die Ergebnisse werden in Amazon CloudWatch Logs-Protokollen gespeichert, und Metrikfilter werden angewendet, um Latenz- und Paketverlust-Statistiken schnell in einem CloudWatch Dashboard zu visualisieren.

Zusätzliche Informationen

Die CloudWatch Logs-Daten können zur Fehlerbehebung im Netzwerk und zur Analyse von Mustern/Trends verwendet werden. Darüber hinaus können Sie CloudWatch Alarme mit Amazon SNS SNS-Benachrichtigungen konfigurieren, wenn Paketverlust und/oder Latenz einen Schwellenwert erreichen. Die Daten können auch verwendet werden, wenn ein Fall mit eröffnet wird AWS Support, um ein Problem schnell zu isolieren und die Zeit bis zur Lösung bei der Untersuchung eines Netzwerkproblems zu verkürzen.

> **Note**
>
> Um Ressourcen zu bereinigen, die von erstellt wurden`AWSSupport-SetupIPMonitoringFromVPC`, können Sie das Runbook `AWSSupport-TerminateIPMonitoringFromVPC` verwenden. Weitere Informationen finden Sie unter `AWSSupport-TerminateIPMonitoringFromVPC`.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- CloudWatchLogGroupNamePrefix

  Typ: Zeichenfolge

  Standard:/`AWSSupport-SetupIPMonitoringFromVPC`

  Beschreibung: (Optional) Präfix, das für jede CloudWatch Protokollgruppe verwendet wird, die für die Testergebnisse erstellt wurde.
- CloudWatchLogGroupRetentionInTage

  Typ: Zeichenfolge

  Gültige Werte: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  Standard: 7

  Beschreibung: (Optional) Die Anzahl der Tage, für die Sie die Netzwerküberwachungsergebnisse behalten möchten.
- InstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

Standard: t2.micro

Beschreibung: (Optional) Der EC2-Instance-Typ für die EC2Rescue-Instance. Empfohlene Größe: t2.micro.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Subnetz-ID für die Überwachungs-Instance. Beachten Sie, dass Sie, wenn Sie ein privates Subnetz angeben, sicherstellen müssen, dass ein Internetzugang vorhanden ist, damit die Monitor-Instance den Test einrichten kann (d. h. den CloudWatch Logs-Agent installieren, mit Systems Manager interagieren und CloudWatch).

- TargetIPs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommata getrennte Liste der zu überwachenden IPv4s und/oder IPv6s. Leerzeichen sind nicht zulässig. Die maximale Größe beträgt 255 Zeichen. Beachten Sie: Wenn Sie eine ungültige IP angeben, schlägt die Automatisierung fehl, und die Testeinrichtung wird zurückgesetzt.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dem Benutzer, der die Automatisierung ausführt, die von AmazonSSM verwaltete AutomationRole IAM-Richtlinie beizufügen. Außerdem muss der Benutzer die folgende Richtlinie an sein Benutzerkonto, seine Gruppe oder seine Rolle angefügt haben:

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

Dokumentschritte

1. **`aws:executeAwsApi`**- beschreiben Sie das bereitgestellte Subnetz.
2. **`aws:branch`**- wertet die TargeTips-Eingabe aus.

   (IPv6) Wenn TargetIPs IPv6 enthält:

   **`aws:assertAwsResourceProperty`**- überprüft, ob dem angegebenen Subnetz ein IPv6-Pool zugeordnet ist

3. **aws:executeScript**- Ruft die Architektur des Instance-Typs und des öffentlichen Parameterpfads für das neueste Amazon Linux 2 abAMI.
4. **aws:executeAwsApi**- Holen Sie sich das neueste Amazon Linux 2 AMI aus dem Parameter Store.
5. **aws:executeAwsApi**- Erstellen Sie eine Sicherheitsgruppe für den Test in der VPC des Subnetzes.

   (Cleanup) Wenn die Erstellung der Sicherheitsgruppe fehlschlägt:

   **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.
6. **aws:executeAwsApi**- lässt den gesamten ausgehenden Verkehr in der Testsicherheitsgruppe zu.

   (Cleanup) Wenn die Erstellung der Regel für den ausgehenden Datenverkehr fehlschlägt:

   **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.
7. **aws:executeAwsApi**- Erstellen Sie eine IAM-Rolle für die Test-EC2-Instance

   (Cleanup) Wenn die Erstellung der Rolle fehlschlägt:

   a. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte IAM-Rolle, falls sie existiert.
   b. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.
8. **aws:executeAwsApi**— fügen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie bei

   (Cleanup) Wenn das Anfügen der Richtlinie fehlschlägt:

   a. **aws:executeAwsApi**— Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde, sofern sie angehängt wurde.
   b. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.
   c. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

9. **aws:executeAwsApi**- fügen Sie eine Inline-Richtlinie hinzu, um die Einrichtung von Aufbewahrungsfristen für CloudWatch Protokollgruppen und die Erstellung eines Dashboards zu ermöglichen CloudWatch

   (Cleanup) Wenn das Anfügen der Inline-Richtlinie fehlschlägt:

   a. **aws:executeAwsApi**- Löschen Sie die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde, falls sie erstellt wurde.

   b. **aws:executeAwsApi**— Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

   c. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

   d. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

10. **aws:executeAwsApi**- erstellt ein IAM-Instanzprofil.

    (Cleanup) Wenn die Erstellung des Instance-Profils fehlschlägt:

    a. **aws:executeAwsApi**— löscht das durch die Automatisierung erstellte IAM-Instanzprofil, falls es existiert.

    b. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

    c. **aws:executeAwsApi**- Löschen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

    d. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

    e. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

11. **aws:executeAwsApi**- Ordnen Sie das IAM-Instanzprofil der IAM-Rolle zu.

    (Cleanup) Wenn Die Zuordnung des Instance-Profils und der Rolle fehlschlägt:

    a. **aws:executeAwsApi**— entfernt das IAM-Instanzprofil aus der Rolle, falls es zugeordnet ist.

    b. **aws:executeAwsApi**— löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

    c. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

    d. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

    e. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

f. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

12 **aws:sleep**- Warten Sie, bis das Instanzprofil verfügbar ist.

13 **aws:runInstances**- erstellt die Testinstanz im angegebenen Subnetz und mit dem zuvor erstellten Instanzprofil als Anhang.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

14 **aws:branch**- wertet die TargeTips-Eingabe aus.

(IPv6) Wenn TargetIPs IPv6 enthält:

**aws:executeAwsApi**- weist der Testinstanz ein IPv6 zu.

15 **aws:waitForAwsResourceProperty**- Warten Sie, bis die Testinstanz zu einer verwalteten Instanz wird.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

16 **aws:runCommand**- Testvoraussetzungen installieren:

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

17 **aws:runCommand**- überprüft, ob es sich bei den angegebenen IPs um syntaktisch korrekte IPv4- und/oder IPv6-Adressen handelt:

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

18 **aws:runCommand**- Definieren Sie den MTR-Test für jede der bereitgestellten IPs.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

19 **aws:runCommand**- Definieren Sie den ersten Ping-Test für jede der bereitgestellten IPs.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

20 **aws:runCommand**- Definieren Sie den zweiten Ping-Test für jede der bereitgestellten IPs.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

21 **aws:runCommand**- Definieren Sie den Tracepath-Test für jede der bereitgestellten IPs.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

22 **aws:runCommand**- Definieren Sie den Traceroute-Test für jede der bereitgestellten IPs.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

23 **aws:runCommand**- CloudWatch Protokolle konfigurieren.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

24 **aws:runCommand**- planen Sie Cronjobs so, dass jeder Test jede Minute ausgeführt wird.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

25 **aws:sleep**- Warten Sie, bis die Tests einige Daten generiert haben.

26 **aws:runCommand**- legen Sie die gewünschten CloudWatch Aufbewahrungszeiten für Protokollgruppen fest.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

27 **aws:runCommand**- legt die Metrikfilter für die CloudWatch Protokollgruppe fest.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:changeInstanceState**- beendet die Testinstanz.

b. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

c. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

d. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

e. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

g. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

28 **aws:runCommand**- Erstellen Sie das CloudWatch Dashboard.

(Cleanup) Wenn der Schritt fehlschlägt:

a. **aws:executeAwsApi**- lösche das CloudWatch Dashboard, falls es existiert.

b. **aws:changeInstanceState**- beendet die Testinstanz.

c. **aws:executeAwsApi**- entfernt das IAM-Instanzprofil aus der Rolle.

d. **aws:executeAwsApi**- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.

e. **aws:executeAwsApi**— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.

f. **aws:executeAwsApi**- Trennen Sie die von AmazonSSM ManagedInstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.

g. **aws:executeAwsApi**— löscht die durch die Automatisierung erstellte IAM-Rolle.

h. **aws:executeAwsApi**- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

## Ausgaben

create CloudWatch Dashboards.Output — die URL des Dashboards. CloudWatch

ManagedInstanceerstellen. InstanceIds - die Testinstanz-ID.

## AWSSupport-TerminateIPMonitoringFromVPC

Beschreibung

AWSSupport-TerminateIPMonitoringFromVPCbeendet einen IP-Überwachungstest, der zuvor von AWSSupport-SetupIPMonitoringFromVPC gestartet wurde. Daten im Zusammenhang mit der angegebenen Test-ID werden gelöscht.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AutomationExecutionID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ausführungs-ID der Automatisierung, als Sie das AWSSupport-SetupIPMonitoringFromVPC Runbook zuvor ausgeführt haben. Alle Ressourcen, die dieser Ausführungs-ID zugeordnet sind, werden gelöscht.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Instance-ID für die Überwachungs-Instance.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Subnetz-ID für die Überwachungs-Instance.

### Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dem Benutzer, der die Automatisierung ausführt, die von AmazonSSM verwaltete AutomationRole IAM-Richtlinie beizufügen. Darüber hinaus muss dem Benutzer, seiner Gruppe oder Rolle die folgende Richtlinie zugewiesen sein:

```
{
"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"
    ]
}
```

Dokumentschritte

1. `aws:assertAwsResourceProperty` - überprüfen AutomationExecutionId und InstanceId beziehen sich auf denselben Test.
2. `aws:assertAwsResourceProperty` - überprüfen SubnetId und InstanceId beziehen sich auf denselben Test.
3. `aws:executeAwsApi` - ruft die Testsicherheitsgruppe ab.
4. `aws:executeAwsApi` - löscht das CloudWatch Dashboard.
5. `aws:changeInstanceState` - beendet die Testinstanz.
6. `aws:executeAwsApi` - entfernt das IAM-Instanzprofil aus der Rolle.

7. `aws:executeAwsApi`- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.
8. `aws:executeAwsApi`— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.
9. `aws:executeAwsApi`— Trennen Sie die verwaltete AmazonSSM ManagedInstance Core-Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.
10. `aws:executeAwsApi`— löscht die durch die Automatisierung erstellte IAM-Rolle.
11. `aws:executeAwsApi`- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

Ausgaben

None

# AWS WAF

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS WAF Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

## AWS-AddWAFRegionalRuleToRuleGroup

Beschreibung

Das `AWS-AddWAFRegionalRuleToRuleGroup` Runbook fügt einer AWS WAF regionalen Regelgruppe eine bestehende AWS WAF regionale Regel hinzu. Es werden nur AWS WAF klassische regionale Regelgruppen unterstützt. AWS WAF Klassische regionale Regelgruppen können maximal 10 Regeln haben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- RuleGroupID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Regelgruppe, die Sie aktualisieren möchten.
- RulePriority

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Priorität für die neue Regel. Die Regelpriorität bestimmt die Reihenfolge, in der Regeln in einer regionalen Gruppe bewertet werden. Regeln mit einem niedrigeren Wert haben eine höhere Priorität als Regeln mit einem höheren Wert. Der Wert muss eine eindeutige ganze Zahl sein. Wenn Sie einer regionalen Regelgruppe mehrere Regeln hinzufügen, müssen die Werte nicht aufeinander folgen.
- RuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die Regel, die Sie zu Ihrer regionalen Regelgruppe hinzufügen möchten.

- RuleAction

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Gibt die Aktion an, AWS WAF die ausgeführt wird, wenn eine Webanforderung den Bedingungen der Regel entspricht.

  Gültige Werte: ALLOW | BLOCK | COUNT

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Dokumentschritte

- getWAF ChangeToken (aws:executeAwsApi) — Ruft ein AWS WAF Änderungstoken ab, um sicherzustellen, dass das Runbook keine widersprüchlichen Anfragen an den Dienst sendet.
- addWAF RuleTo WAF RegionalRuleGroup (aws:ExecuteScript) — Fügt die angegebene Regel der regionalen Regelgruppe hinzu. AWS WAF
- VerifyChangeTokenPropagating (aws:wait ForAwsResourceProperty) — Überprüft, ob das Änderungstoken den Status oder hat. `PENDING` `INSYNC`
- VerifyRuleAddedToRuleGroup (aws:ExecuteScript) — Überprüft, ob die angegebene AWS WAF Regel der regionalen Zielregelgruppe hinzugefügt wurde.

Ausgaben

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Ergebnis des Schritts zur Überprüfung, ob die neue Regel der regionalen Regelgruppe hinzugefügt wurde.

- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Ausgabe des `ListActivatedRulesInRuleGroup` API-Vorgangs.

## AWS-AddWAFRegionalRuleToWebAcl

Beschreibung

Das `AWS-AddWAFRegionalRuleToWebAcl` Runbook fügt eine bestehende AWS WAF regionale Regel, Regelgruppe oder ratenbasierte Regel zu einer regionalen AWS WAF Classic Web Access Control List (ACL) hinzu. Dieses Runbook aktualisiert keine vorhandenen regionalen AWS WAF Classic-Web-ACLs, die von verwaltet werden. AWS Firewall Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- WebACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Web-ACL, die Sie aktualisieren möchten.

- ActivatedRulePriorität

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Priorität für die neue Regel. Die Regelpriorität bestimmt die Reihenfolge, in der Regeln in einer Web-ACL ausgewertet werden. Regeln mit einem niedrigeren Wert haben eine höhere Priorität als Regeln mit einem höheren Wert. Der Wert muss eine eindeutige ganze Zahl sein. Wenn Sie einer regionalen Web-ACL mehrere Regeln hinzufügen, müssen die Werte nicht aufeinander folgen.
- ActivatedRuleRuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die reguläre Regel, ratenbasierte Regel oder Gruppe, die Sie der Web-ACL hinzufügen möchten.
- ActivatedRuleAktion

  Typ: Zeichenfolge

  Gültige Werte: ALLOW | BLOCK | COUNT

  Beschreibung: (Optional) Gibt die Aktion an, die AWS WAF ausgeführt wird, wenn eine Webanforderung den Bedingungen der Regel entspricht.
- ActivatedRuleTyp

  Typ: Zeichenfolge

  Gültige Werte: REGULAR | RATE_BASED | GROUP

  Standard: REGULAR

  Beschreibung: (Optional) Der Regeltyp, den Sie der Web-ACL hinzufügen. Dieses Feld ist zwar optional, beachten Sie jedoch, dass die Anforderung fehlschlägt, wenn Sie versuchen, einer Web-ACL eine `RATE_BASED` Regel hinzuzufügen, ohne den Typ festzulegen, da die Anforderung standardmäßig eine `REGULAR` Regel verwendet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Dokumentschritte

- DetermineWebACL NotIn FMS AndRulePriority (aws:ExecuteScript) — Überprüft, ob sich die AWS WAF Web-ACL in einer Firewall Manager Manager-Sicherheitsrichtlinie befindet, und überprüft, ob die Prioritäts-ID nicht mit einer vorhandenen ACL in Konflikt steht.
- AddRuleOrRuleGroupToWebACL (aws:ExecuteScript) — Fügt die angegebene Regel zur Web-ACL hinzu. AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:ExecuteScript) — Überprüft, ob die angegebene Regel zur Ziel-Web-ACL hinzugefügt wurde. AWS WAF

Ausgaben

- DetermineWebNotInACL AndRule FMS-Priorität. PrereqResponse: Ausgabe des `DetermineWebACLNotInFMSAndRulePriority` Schritts.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebaclResponse: Ausgabe des `AddRuleOrRuleGroupToWebACL` Schritts.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebaclResponse: Ausgabe des Schritts`VerifyRuleOrRuleGroupAddedToWebAcl`.

## `AWSConfigRemediation-EnableWAFClassicLogging`

Beschreibung

Das `AWSConfigRemediation-EnableWAFClassicLogging` Runbook ermöglicht die Protokollierung bei Amazon Data Firehose (Firehose) für die von Ihnen angegebene AWS WAF Web Access Control List (Web ACL).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DeliveryStreamName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Firehose-Lieferstreams, an den Sie Protokolle senden möchten.
- WebACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der AWS WAF Web-ACL, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`

- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Dokumentschritte

- `aws:executeAwsApi`- Bestätigt, dass der von Ihnen angegebene Lieferdatenstrom `DeliveryStreamName` existiert.
- `aws:executeAwsApi`- Sammelt den ARN der im `WebACLId` Parameter angegebenen AWS WAF Web-ACL.
- `aws:executeAwsApi`- Aktiviert die Protokollierung für die Web-ACL.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Protokollierung auf der AWS WAF Web-ACL aktiviert wurde.

## `AWSConfigRemediation-EnableWAFClassicRegionalLogging`

Beschreibung

Das `AWSConfigRemediation-EnableWAFClassicRegionalLogging` Runbook ermöglicht die Protokollierung bei Amazon Data Firehose (Firehose) für die von Ihnen angegebene AWS WAF Web Access Control List (ACL).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LogDestinationKonfigurationen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Firehose-Lieferstreams, an den Sie Protokolle senden möchten.
- WebACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der AWS WAF Web-ACL, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Dokumentschritte

- `aws:executeAwsApi`- Sammelt den ARN der im `WebACLId` Parameter angegebenen AWS WAF Web-ACL.
- `aws:executeAwsApi`- Aktiviert die Protokollierung für die Web-ACL.

- `aws:assertAwsResourceProperty`- Überprüft, ob die Protokollierung auf der AWS WAF Web-ACL aktiviert wurde.

## `AWSConfigRemediation-EnableWAFV2Logging`

Beschreibung

Das `AWSConfigRemediation-EnableWAFV2Logging` Runbook ermöglicht die Protokollierung für eine AWS WAF (AWS WAF V2) Web Access Control List (Web ACL) mit dem angegebenen Amazon Data Firehose (Firehose) -Lieferstream.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LogDestinationKonfigurationen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Firehose-Lieferstream-ARN, den Sie der Web-ACL zuordnen möchten.

> **Note**
>
> Der Firehose-Lieferstream-ARN muss mit dem Präfix `aws-waf-logs-` beginnen. Beispiel, `aws-waf-logs-us-east-2-analytics`. Weitere Informationen finden Sie unter Amazon Data Firehose.

- WebAclArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ARN der Web-ACL, für die die Protokollierung aktiviert wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Dokumentschritte

- `aws:executeScript`- Aktiviert die Protokollierung für die AWS WAF V2-Web-ACL und überprüft, ob die Protokollierung die angegebene Konfiguration hat.

# Amazon WorkSpaces

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon WorkSpaces bereit. Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## AWS-CreateWorkSpace

Beschreibung

Das `AWS-CreateWorkSpace` Runbook erstellt einen neuen WorkSpaces virtuellen Amazon-Desktop, auch bekannt als a WorkSpace, basierend auf den Werten, die Sie für die Eingabeparameter angeben. Weitere Informationen dazu WorkSpaces finden Sie unter Was ist Amazon WorkSpaces? im  WorkSpaces Amazon-Administratorhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BundleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Bundles, das für das WorkSpace verwendet werden soll.

- ComputeTypeName

  Typ: Zeichenfolge

  Gültige Werte: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  Beschreibung: (Optional) Der Berechnungstyp für Ihren. WorkSpace
- DirectoryId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Verzeichnisses, zu dem Sie hinzugefügt werden WorkSpace sollen.
- RootVolumeEncryptionEnabled

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Ermittelt, ob das Root-Volume von verschlüsselt WorkSpace ist.
- RootVolumeSizeGib

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Größe des Root-Volumes für WorkSpace.
- RunningMode

  Typ: Zeichenfolge

  Gültige Werte: ALWAYS_ON | AUTO_STOP

  Beschreibung: (Erforderlich) Der Laufmodus von. WorkSpace
- RunningModeAutoStopTimeoutInMinuten

  Typ: Ganzzahl

  Beschreibung: (Optional) Die Zeit nach dem Abmelden eines Benutzers, wenn der WorkSpaces beendet wird. Geben Sie einen Wert in 60-Minuten-Intervallen an.

- Tags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, auf die Sie anwenden möchten. WorkSpace
- UserName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Benutzername, dem zugeordnet werden soll WorkSpace.
- UserVolumeEncryptionEnabled

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Legt fest, ob das Benutzervolume von verschlüsselt WorkSpace ist.
- UserVolumeSizeGib

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Größe des Benutzervolumes für WorkSpace.
- VolumeEncryptionSchlüssel

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der symmetrische AWS Key Management Service Schlüssel, den Sie zum Verschlüsseln der auf Ihrem gespeicherten Daten verwenden möchten. WorkSpace

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Dokumentschritte

- `aws:executeScript`- Erstellt eine, die auf den Werten WorkSpace basiert, die Sie für die Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Überprüft den Status von WorkSpace ist`AVAILABLE`.

Ausgaben

`CreateWorkspace.WorkspaceId`

## AWSSupport-RecoverWorkSpace

Beschreibung

Das `AWSSupport-RecoverWorkSpace` Runbook führt Wiederherstellungsschritte auf dem WorkSpaces virtuellen Amazon-Desktop durch WorkSpace, den Sie angeben. Das Runbook startet das neu WorkSpace, und wenn der Status unverändert ist, stellt es auf der WorkSpace Grundlage der Werte`UNHEALTHY`, die Sie für die Eingabeparameter angegeben haben, wieder her oder erstellt es neu. Bevor Sie dieses Runbook verwenden, empfehlen wir Ihnen, die WorkSpaces Problembehebung im WorkSpaces Amazon-Administratorhandbuch zu lesen.

> **Important**
>
> Das Wiederherstellen oder Neuerstellen eines WorkSpace ist eine potenziell zerstörerische Aktion, die zum Verlust von Daten führen kann. Dies liegt daran, dass der aus dem letzten verfügbaren Snapshot wiederhergestellt WorkSpace wird und Daten, die aus Snapshots wiederhergestellt wurden, bis zu 12 Stunden alt sein können.
> Mit der Wiederherstellungsoption werden sowohl das Stammvolume als auch das Benutzervolume auf der Grundlage der neuesten Snapshots neu erstellt. Mit der Neuerstellungsoption wird das Benutzer-Volume aus dem letzten Snapshot und das aus dem Image, das dem Bundle zugeordnet ist, WorkSpace aus dem es erstellt wurde, neu erstellt. WorkSpace Anwendungen, die installiert wurden, oder Systemeinstellungen, die nach der Erstellung geändert wurden, WorkSpace gehen verloren. Weitere Informationen zur Wiederherstellung und WorkSpaces Neuerstellung finden Sie unter Restore a WorkSpace und Rebuild a WorkSpace im Amazon WorkSpaces Administration Guide.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Bestätigen

  Typ: Zeichenfolge

  Gültige Werte: Ja

  Beschreibung: (Erforderlich) Die Eingabe von Ja bedeutet, dass Sie verstehen, dass bei den Wiederherstellungs- und Neuerstellungsaktionen versucht wird, die Daten WorkSpace aus dem letzten Snapshot wiederherzustellen, und dass Daten, die aus diesen Snapshots wiederhergestellt wurden, bis zu 12 Stunden alt sein können.
- Neustart

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Ja

  Beschreibung: (Erforderlich) Legt fest, ob der WorkSpace neu gestartet wurde.
- Neu aufbauen

  Typ: Zeichenfolge

Gültige Werte: Ja | Nein

Standard: Nein

Beschreibung: (Erforderlich) Legt fest, ob der neu erstellt WorkSpace wird.

- Wiederherstellung

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Nein

  Beschreibung: (Erforderlich) Legt fest, ob WorkSpace das wiederhergestellt wurde.

- WorkspaceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Datei, die WorkSpace Sie wiederherstellen möchten.

## Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

## Dokumentschritte

- `aws:executeAwsApi`- Erfasst den Status von, den WorkSpace Sie im `WorkspaceId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft den Status von WorkSpace ist`AVAILABLE`,, `ERROR` `IMPAIREDSTOPPED`, oder. `UNHEALTHY`
- `aws:branch`- Filialen, die auf dem WorkSpace Bundesstaat basieren.
- `aws:executeAwsApi`- Startet das WorkSpace.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `Action` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet nach dem Start auf WorkSpace den Status.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status `UNHEALTHY` nach dem `AVAILABLE` Start zu`ERROR`,`IMPAIRED`, oder wechselt.
- `aws:executeAwsApi`- Erfasst den Status von WorkSpace nach dem Start.
- `aws:branch`- Verzweigungen, die auf dem Status von basieren, WorkSpace nachdem sie gestartet wurden.
- `aws:executeAwsApi`- Sammelt die verfügbaren Schnappschüsse für die Wiederherstellung oder Neuerstellung von. WorkSpace
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den Parameter angeben. `Reboot`
- `aws:executeAwsApi`- Startet den WorkSpace neu.
- `aws:executeAwsApi`- Erfasst den Status von WorkSpace nach dem Start.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status von geändert wird WorkSpace . `REBOOTING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach dem Neustart wechselt.
- `aws:executeAwsApi`- Erfasst den Status von nach dem WorkSpace Neustart.
- `aws:branch`- Verzweigungen, die auf dem Status von nach dem WorkSpace Neustart basieren.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `Restore` Parameter angeben.
- `aws:executeAwsApi`- Stellt die wieder her WorkSpace. Schlägt die Wiederherstellung fehl, versucht das Runbook, den WorkSpace neu zu erstellen.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status von geändert wird WorkSpace . `RESTORING`

- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach der Wiederherstellung wechselt.
- `aws:executeAwsApi`- Sammelt den Zustand von WorkSpace nach der Wiederherstellung.
- `aws:branch`- Verzweigungen basieren auf dem Zustand der Datei WorkSpace nach der Wiederherstellung.
- `aws:branch`- Verzweigungen, die auf dem Wert basieren, den Sie für den `Rebuild` Parameter angeben.
- `aws:executeAwsApi`- Baut die WorkSpace neu auf.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status des WorkSpace wechselt. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach dem Wiederaufbau wechselt.
- `aws:executeAwsApi`- Sammelt den Zustand von WorkSpace nach dem Wiederaufbau.
- `aws:assertAwsResourceProperty`- Bestätigt den Zustand des WorkSpace is`AVAILABLE`.

# X-Ray

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS X-Ray Weitere Informationen zu Runbooks finden Sie unter Arbeiten mit Runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen



## `AWSConfigRemediation-UpdateXRayKMSKey`

Beschreibung

Das `AWSConfigRemediation-UpdateXRayKMSKey` Runbook ermöglicht die Verschlüsselung Ihrer AWS X-Ray Daten mithilfe eines AWS Key Management Service (AWS KMS) -Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre AWS X-Ray Daten gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Datensätze mit unterschiedlichen KMS-Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des KMS-Schlüssels, den Sie AWS X-Ray zum Verschlüsseln von Daten verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Verschlüsselung Ihrer X-Ray-Daten mit dem KMS-Schlüssel, den Sie im `KeyId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Verschlüsselungskonfigurationsstatus Ihres X-Ray erreicht ist`ACTIVE`.
- `aws:executeAwsApi`- Sammelt den ARN des Schlüssels, den Sie im `KeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Verschlüsselung auf Ihrem X-Ray aktiviert wurde.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.