Manual do usuário

AWS Systems Manager Referência do runbook de automação

AWS Systems Manager Referência do runbook de automação: Manual do usuário

Table of Contents

Referência do runbook do Systems Manager Automation

Para ajudar você a começar rapidamente, AWS Systems Manager fornece runbooks predefinidos. Esses runbooks são mantidos pela Amazon Web Services AWS Support, e. AWS Config A referência do runbook descreve cada um dos runbooks predefinidos fornecidos pelo Systems Manager, e. AWS Support AWS Config

> **Important**
>
> Se você executar um fluxo de trabalho de automação que invoca outros serviços usando um perfil AWS Identity and Access Management de serviço (IAM), esteja ciente de que esta função deve ser configurada com permissão para invocar esses serviços. Esse requisito aplica-se a todos os runbooks do Automation da AWS (runbooks da `AWS-*`), como os runbooks `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup` e `AWS-RestartEC2Instance`, entre outros. Esse requisito também se aplica a todos os runbooks de automação personalizados que você criar e que invocam outros AWS serviços usando ações que chamam outros serviços. Por exemplo, se você usar as ações `aws:executeAwsApi`, `aws:createStack` ou `aws:copyImage`, então você deve configurar um perfil de serviço com permissão para invocar esses serviços. Você pode habilitar permissões para outros AWS serviços adicionando uma política embutida do IAM à função. Para obter mais informações, consulte Adicionar uma política embutida de automação para invocar outros AWS serviços.

Essa referência inclui tópicos que descrevem cada um dos runbooks do Systems Manager que são de propriedade de AWS AWS Support, e. AWS Config Os runbooks são organizados por pessoas relevantes AWS service (Serviço da AWS). Cada página fornece uma explicação dos parâmetros obrigatórios e opcionais que você pode especificar ao usar o runbook. Cada página também lista as etapas no runbook e a saída da execução, se houver.

Essa referência não inclui uma página separada para runbooks que exigem aprovação, como o runbook `AWS-CreateManagedLinuxInstanceWithApproval` ou `AWS-StopEC2InstanceWithApproval`. Qualquer nome do runbook que inclua `WithApproval`, significa que o runbook inclui a ação `aws:approve`. Essa ação pausa temporariamente uma automação até que as entidades principais designadas aprovem ou rejeitem a ação. Depois que o número necessário de aprovações for atingido, a execução da automação será retomada.

Para obter informações sobre como executar automações, consulte Como executar uma automação simples. Para obter informações sobre a execução de automações em vários destinos, consulte Execução de automações que usam destinos e controles de taxa.

Tópicos

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

Exibir conteúdo do runbook

Você pode visualizar o conteúdo dos runbooks no console do Systems Manager.

Para ver o conteúdo do runbook

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

2. No painel de navegação, escolha Documents.

   - ou -

   Se a página AWS Systems Manager inicial abrir primeiro, escolha o ícone do menu (☰) para abrir o painel de navegação e, em seguida, escolha Documentos no painel de navegação.
3. Na seção Categorias, escolha Documentos de Automação.
4. Selecione um runbook e, em seguida, selecione Visualizar detalhes.
5. Escolha a guia Conteúdo.

API Gateway

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon API Gateway. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

AWSConfigRemediation-DeleteAPIGatewayStage

Descrição

O runbook `AWSConfigRemediation-DeleteAPIGatewayStage` exclui um estágio do Amazon API Gateway (API Gateway). O AWS Config deve estar habilitado na Região da AWS em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- StageArn

  Tipo: sequência

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do estágio do API Gateway que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: exclui o estágio do API Gateway especificado no parâmetro `StageArn`.

AWSConfigRemediation-EnableAPIGatewayTracing

Descrição

O runbook `AWSConfigRemediation-EnableAPIGatewayTracing` permite o rastreamento em um estágio do Amazon API Gateway (API Gateway). O AWS Config deve estar habilitado na Região da AWS em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- StageArn

  Tipo: sequência

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do estágio do API Gateway no qual você deseja ativar o rastreamento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `config:GetResourceConfigHistory`

- `apigateway:GET`
- `apigateway:PATCH`

Etapas do documento

- `aws:executeScript`: permite o rastreamento no estágio do API Gateway especificado no parâmetro `StageArn`.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descrição

O runbook `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` atualiza a configuração do método de cache para um recurso de estágio do Amazon API Gateway.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CachingAuthorizedMethods

Tipo: StringList

Descrição: (obrigatório) os métodos autorizados a ter o armazenamento em cache ativado. A lista deve ser uma combinação de `DELETE` , `GET` , `HEAD` , `OPTIONS` , `PATCH` , `POST` e `PUT` . O armazenamento em cache está ativado para métodos selecionados e desativado para métodos não selecionados. O armazenamento em cache está habilitado para todos os métodos se `ANY` estiver selecionado e desabilitado para todos os métodos se `NONE` estiver selecionado.

- StageArn

  Tipo: sequência

  Descrição: (obrigatório) o ARN de estágio do API Gateway para a API `REST`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: aceita o ID do recurso do estágio como entrada, atualiza a configuração do método de cache para um estágio do API Gateway usando a ação da API `UpdateStage` e verifica a atualização.

AWS Batch

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Batch Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

Descrição

O AWSSupport-TroubleshootAWSBatchJob runbook ajuda você a solucionar problemas que impedem que um AWS Batch trabalho passe do status para o status. RUNNABLE STARTING

Como funciona?

Esse runbook executa as seguintes verificações:

- Se o ambiente computacional estiver em um DISABLED estado INVALID ou.
- Se o Max vCPU parâmetro do ambiente computacional for grande o suficiente para acomodar o volume de trabalhos na fila de trabalhos.
- Se os trabalhos exigirem mais vCPUs ou recursos de memória do que os tipos de instância do ambiente computacional podem fornecer.
- Se os trabalhos precisarem ser executados em instâncias baseadas em GPU, mas o ambiente computacional não estiver configurado para usar instâncias baseadas em GPU.
- Se o grupo de Auto Scaling do ambiente computacional falhar ao iniciar as instâncias.
- Se as instâncias lançadas puderem se juntar ao cluster subjacente do Amazon Elastic Container Service (Amazon ECS); caso contrário, ele AWSSupport executará o runbook -TroubleshooTecs. ContainerInstance
- Se algum problema de permissão estiver bloqueando ações específicas necessárias para executar o trabalho.

Important

- Esse runbook deve ser iniciado na mesma AWS região do seu trabalho que está preso no RUNNABLE status.
- Esse runbook pode ser iniciado para AWS Batch trabalhos agendados em instâncias do Amazon ECS ou do AWS Fargate Amazon Elastic Compute Cloud (Amazon EC2). Se a automação for iniciada para um AWS Batch trabalho no Amazon Elastic Kubernetes Service (Amazon EKS), a iniciação será interrompida.
- Se as instâncias estiverem disponíveis para executar o trabalho, mas não conseguirem registrar o cluster do Amazon ECS, esse runbook iniciará o runbook de AWSSupport-TroubleshootECSContainerInstance automação para tentar determinar o motivo.

Para obter mais informações, consulte o runbook AWSSupport-TroubleshooTecs ContainerInstance.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- JobId

  Tipo: string

  Descrição: (Obrigatório) O ID do AWS Batch Job que está preso no `RUNNABLE` status.

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

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

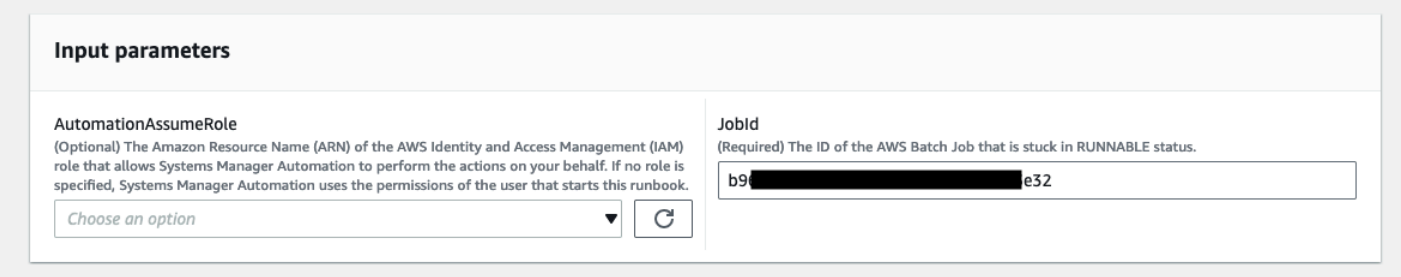
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

Instruções

1. Navegue até a opção AWSSupport-Solução de problemas AWSBatchJob no AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - JobId (Obrigatório):

     O ID do AWS Batch Job que está preso no `RUNNABLE` status.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - PreflightPermissionChecks:

     Executa verificações prévias de permissão do IAM em relação ao usuário/função inicial. Se houver alguma permissão ausente, essa etapa fornece as ações de API ausentes na seção de saída global.
   - ProceedOnlyIfUserHasPermission:

Ramifica com base em se você tem permissões para todas as ações necessárias para o runbook.

- AWSBatchJobEvaluation:

  Executa verificações em relação ao AWS Batch Job, verificando se ele existe e está no `RUNNABLE` status.

- ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

  Ramifica com base na existência e no `RUNNABLE` status dos trabalhos.

- BatchComputeEnvironmentEvaluation:

  Executa verificações em relação ao ambiente AWS Batch de computação.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

  Ramificações com base no sucesso das verificações do ambiente computacional.

- UnderlyingInfraEvaluation:

  Executa verificações em relação ao Grupo de Auto Scaling ou à Solicitação de Frota Spot subjacente.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Ramificações com base na existência de instâncias que não estão ingressando no cluster do Amazon ECS.

- EcsAutomationRunner:

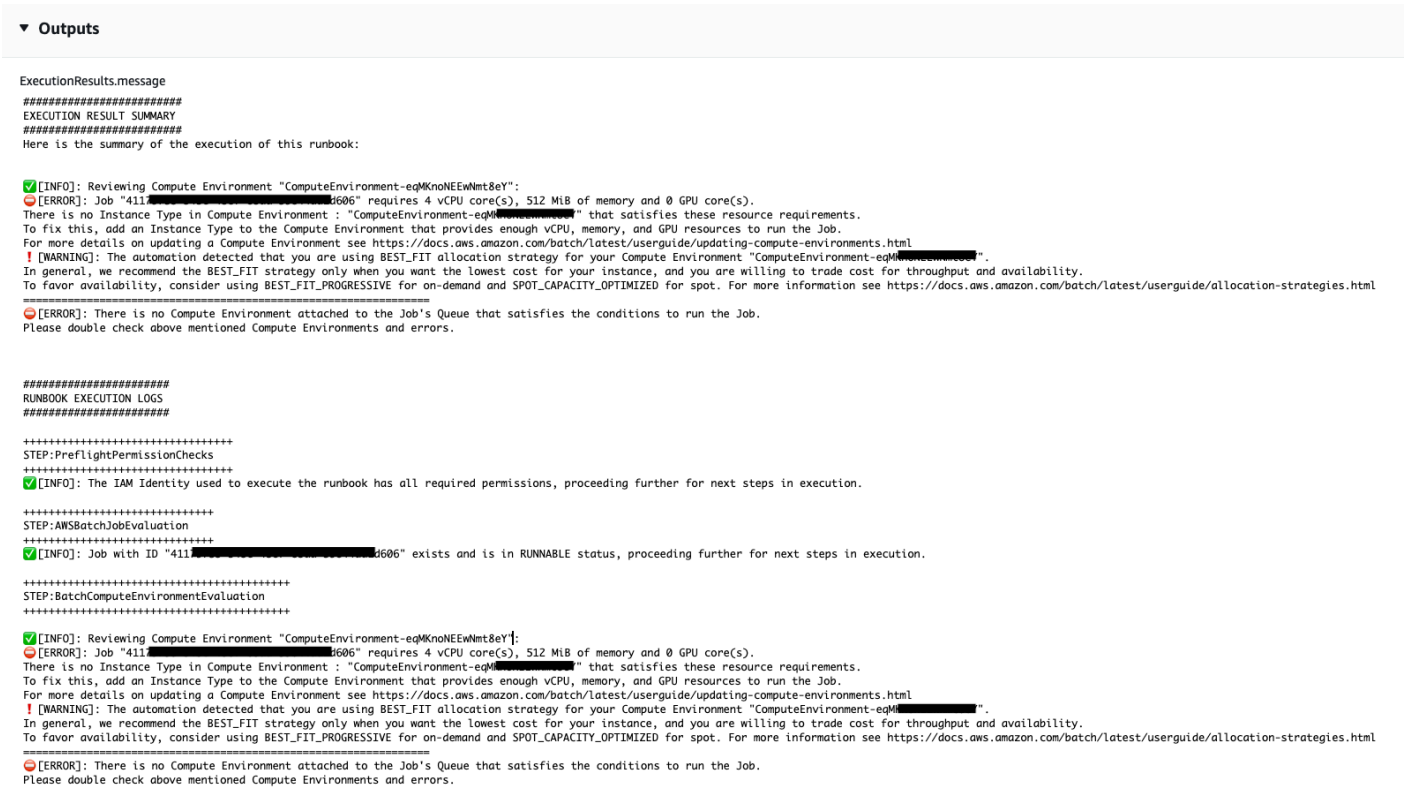
  Executa a automação do Amazon ECS para as instâncias que não se juntam ao cluster.

- ExecutionResults:

  Gera a saída com base nas etapas anteriores.

7. Depois de concluído, o URI para o arquivo HTML do relatório de avaliação é fornecido:

   Link do console S3 e URI do Amazon S3 para o relatório sobre a execução bem-sucedida do runbook



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS CloudFormation

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CloudFormation Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification

- AWS-RunCfnLint
- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

AWS-DeleteCloudFormationStack

Descrição

Excluir uma pilha do AWS CloudFormation.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- StackNameOrId

  Tipo: sequência

  Descrição: (obrigatório) O nome ou ID exclusivo da pilha do CloudFormation a ser excluída

AWS-EnableCloudFormationSNSNotification

Descrição

O AWS-EnableCloudFormationSNSNotification runbook habilita notificações do Amazon Simple Notification Service (Amazon SNS) para a pilha AWS CloudFormation (AWS CloudFormation) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- StackArn

  Tipo: sequência

  Descrição: (Obrigatório) O ARN ou o nome da AWS CloudFormation pilha para a qual você deseja habilitar as notificações do Amazon SNS.
- NotificationArn

  Tipo: sequência

Descrição: (Obrigatório) O ARN do tópico do Amazon SNS que você deseja associar à pilha. AWS CloudFormation

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- sms: GetAutomationExecution
- sms: StartAutomationExecution
- formação de nuvens: DescribeStacks
- formação de nuvens: UpdateStack
- kms:Decrypt
- kms: GenerateDataKey
- sns:Publish
- metros quadrados: GetQueueAttributes

Etapas do documento

- CheckCfnSnsLimits (aws:ExecuteScript) — Verifica se o número máximo de tópicos do Amazon SNS ainda não foi associado à pilha especificada. AWS CloudFormation
- EnableCfnSnsNotification (aws:executeAwsApi) - Ativa notificações do Amazon SNS para a AWS CloudFormation pilha.
- VerificationCfnSnsNotification (aws:ExecuteScript) — Verifica se as notificações do Amazon SNS foram habilitadas para a pilha. AWS CloudFormation

Saídas

CheckCfnSnsLimits. NotificationArnList - Uma lista de ARNs que recebem notificações do Amazon SNS para AWS CloudFormation a pilha.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Resposta da operação da API confirmando que as notificações do Amazon SNS foram habilitadas para AWS CloudFormation a pilha.

AWS-RunCfnLint

Descrição

Este runbook usa um Linter do AWS CloudFormation (`cfn-python-lint`) para validar modelos YAML e JSON em relação à especificação de recurso do AWS CloudFormation. O runbook do `AWS-RunCfnLint` realiza verificações adicionais, como garantir que valores válidos foram inseridos para as propriedades do recurso. Se a validação não for bem-sucedida, a etapa `RunCfnLintAgainstTemplate` falhará e a saída da ferramenta de linter será fornecida em uma mensagem de erro. Este runbook está usando cfn-lint v0.24.4.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ConfigureRuleFlag

  Tipo: sequência

  Descrição: (Opcional) opções de configuração para uma regra a ser passado para o parâmetro `--configure-rule`.

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

- FormatFlag

  Tipo: sequência

  Descrição: (Opcional) valor a ser passado ao parâmetro `--format` para especificar o formato de saída.

  Valores válidos: Default | quiet | parseable | json

  Padrão: Default

- IgnoreChecksFlag

  Tipo: sequência

  Descrição: (Opcional) IDs de regras a serem passadas ao parâmetro --ignore-checks. Essas regras não são verificadas.

  Exemplo: E1001,E1003,W7001

- IncludeChecksFlag

  Tipo: sequência

  Descrição: (Opcional) IDs de regras a serem passadas ao parâmetro `--include-checks`. Essas regras são verificadas.

  Exemplo: E1001,E1003,W7001

- InfoFlag

  Tipo: sequência

  Descrição: (Opcional) opção para o parâmetro `--info`. Inclua a opção para habilitar informações adicionais de registro em log sobre o processamento do modelo.

  Padrão: falso

- TemplateFileName

  Tipo: sequência

  Descrição: o nome ou a chave do arquivo de modelo no bucket do S3.

- TemplateS3BucketName

  Tipo: sequência

  Descrição: o nome do bucket do S3 que contém o modelo do empacotador.
- RegionsFlag

  Tipo: sequência

  Descrição: (opcional) valores a serem passados ao parâmetro `--regions` para testar o modelo em relação ao Regiões da AWS especificado.

  Exemplo: us-east-1,us-west-1

Etapas do documento

RunCfnLintAgainstTemplate: executa a ferramenta `cfn-python-lint` em relação ao modelo do AWS CloudFormation especificado.

Saídas

RunCfnLintAgainstTemplate.output: o stdout da ferramenta `cfn-python-lint`.

AWSSupport-TroubleshootCFNCustomResource

Descrição

O runbook `AWSSupport-TroubleshootCFNCustomResource` ajuda a diagnosticar por que uma pilha do AWS CloudFormation falhou ao criar, atualizar ou excluir um recurso personalizado. O runbook verifica o token de serviço usado para o recurso personalizado e a mensagem de erro que foi retornada. Depois de analisar os detalhes do recurso personalizado, a saída do runbook fornece uma explicação sobre o comportamento da pilha e as etapas de solução de problemas do recurso personalizado.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- StackName

  Tipo: sequência

  Descrição: (obrigatório) o nome da pilha do AWS CloudFormation em que o recurso personalizado falhou.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `validateCloudFormationStack`: verifica se a pilha do AWS CloudFormation existe na mesma Conta da AWS e Região da AWS.
- `checkCustomResource`: analisa a pilha do AWS CloudFormation, verifica o recurso personalizado com falha e gera informações sobre como solucionar o problema do recurso personalizado com falha.

AWS-UpdateCloudFormationStack

Descrição

Atualize uma pilha do AWS CloudFormation usando um modelo do AWS CloudFormation armazenado no bucket do Amazon S3.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

Tipo: sequência

Descrição: (obrigatório) O ARN da função assumida pelo Lambda

- StackNameOrId

  Tipo: sequência

  Descrição: (obrigatório) O nome ou ID exclusivo da pilha do AWS CloudFormation a ser atualizada

- TemplateUrl

  Tipo: sequência

  Descrição: (obrigatório) local do bucket do S3 que contém o modelo atualizado do CloudFormation (por exemplo, `https://s3.amazonaws.com/doc-example-bucket/updated.template`)

CloudFront

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. CloudFront Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject`

Descrição

O runbook do `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` configura o objeto raiz padrão para a distribuição do Amazon CloudFront (CloudFront) que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CloudFrontDistributionId

  Tipo: sequência

  Descrição: (obrigatório) o ID da distribuição do CloudFront para a qual você deseja configurar o objeto raiz padrão.
- DefaultRootObject

  Tipo: sequência

  Descrição: (obrigatório) o objeto que você deseja que o CloudFront retorne quando uma solicitação do visualizador aponta para sua URL raiz.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `cloudfront:UpdateDistribution`

Etapas do documento

- `aws:executeScript`: configura o objeto raiz padrão para a distribuição do CloudFront que você especificar no parâmetro `CloudFrontDistributionId`.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descrição

O `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook permite o registro de acesso para a distribuição Amazon CloudFront (CloudFront) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BucketName

  Tipo: string

Descrição: (Obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) em que você deseja armazenar logs de acesso. Não há suporte para buckets da Região da AWS af-south-1, ap-east-1, eu-south-1 e me-south-1.

- CloudFrontId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição na qual você deseja ativar o login de acesso.

- IncludeCookies

  Tipo: booliano

  Valores válidos: True | False

  Descrição: (Obrigatório) Defina esse parâmetro como`true`, se quiser que os cookies sejam incluídos nos registros de acesso.

- Prefixo

  Tipo: string

  Descrição: (Opcional) Uma string opcional que você CloudFront deseja prefixar no log `filenames` de acesso da sua distribuição, por exemplo,my`prefix/`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

> **Note**
>
> A `s3:GetBucketLocation` API só pode ser usada para buckets do S3 na mesma conta. Você não pode usá-lo para buckets S3 entre contas.

Etapas do documento

- `aws:executeScript`- Ativa o registro de acesso para a CloudFront distribuição especificada no `CloudFrontDistributionId` parâmetro.

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Descrição

O runbook `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` ativa a identidade de acesso de origem para a distribuição do Amazon CloudFront (CloudFront) que você especificar. Esta automação atribui a mesma identidade de acesso de origem do CloudFront para todas as origens do tipo de origem do Amazon Simple Storage Service (Amazon S3) sem identidade de acesso de origem para a distribuição do CloudFront que você especificar. Esta automação não concede permissão de leitura para a identidade de acesso de origem para que o CloudFront acesse objetos em seu bucket do Amazon S3. Você deve atualizar suas permissões de bucket do Amazon S3 para permitir o acesso.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CloudFrontDistributionId

  Tipo: sequência

  Descrição: (obrigatório) o ID da distribuição do CloudFront em que você deseja ativar o failover de origem.

- OriginAccessIdentityId

  Tipo: sequência

  Descrição (obrigatório): a identidade de acesso de origem do CloudFront a ser associada à origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: ativa a identidade de acesso de origem para a distribuição do CloudFront que você especifica no parâmetro `CloudFrontDistributionId` e verifica se a identidade de acesso de origem foi atribuída.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descrição

O runbook `AWSConfigRemediation-EnableCloudFrontOriginFailover` ativa o failover de origem para a distribuição do Amazon CloudFront (CloudFront) que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CloudFrontDistributionId

  Tipo: sequência

  Descrição: (obrigatório) o ID da distribuição do CloudFront em que você deseja ativar o failover de origem.
- OriginGroupId

  Tipo: sequência

  Descrição: (obrigatório) o ID do grupo de origem.
- PrimaryOriginId

  Tipo: sequência

  Descrição: (obrigatório) o ID da origem primária no grupo de origem.

- SecondaryOriginId

  Tipo: sequência

  Descrição: (obrigatório) o ID da origem secundária no grupo de origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: ativa o failover de origem para a distribuição do CloudFront que você especifica no parâmetro `CloudFrontDistributionId` e verifica se o failover foi ativado.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descrição

O runbook `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` ativa a política de protocolo do visualizador para a distribuição do Amazon CloudFront (CloudFront) que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CloudFrontDistributionId

  Tipo: sequência

  Descrição: (obrigatório) o ID da distribuição do CloudFront na qual você deseja ativar a política de protocolo do visualizador.

- ViewerProtocolPolicy

  Tipo: sequência

  Valores válidos: https-only, redirect-to-https

  Descrição: (obrigatório) o protocolo que os visualizadores podem usar para acessar os arquivos na origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: ativa a política de protocolo do visualizador para a distribuição do CloudFront que você especifica no parâmetro `CloudFrontDistributionId` e verifica se a política foi atribuída.

CloudTrail

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CloudTrail Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`

Descrição

O runbook `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` cria uma trilha do AWS CloudTrail (CloudTrail) que fornece arquivos de log de vários Regiões da AWS para o bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BucketName

  Tipo: sequência

  Descrição: (obrigatório) o nome do bucket do Amazon S3 no qual você deseja fazer o upload de logs.
- KeyPrefix

  Tipo: sequência

  Descrição: (opcional) o prefixo da chave do Amazon S3 que é fornecida após o nome do bucket que você designou para a entrega de arquivos de log.
- TrailName

  Tipo: sequência

  Descrição: (obrigatório) o nome da trilha do CloudTrail a ser criada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`

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

Etapas do documento

- `aws:executeAwsApi`: aceita o nome da trilha e o nome do bucket do Amazon S3 como entrada e cria uma trilha do CloudTrail.
- `aws:executeAwsApi`: ativa o registro na trilha criada e inicia a entrega do log para o bucket do Amazon S3 que você especificou.
- `aws:assertAwsResourceProperty`: verifica se a trilha do CloudTrail foi criada.

AWS-EnableCloudTrail

Descrição

Crie uma trilha do AWS CloudTrail e configure o registro em log para um bucket do S3.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- S3BucketName

  Tipo: String

  Descrição: (obrigatória) o nome do bucket do S3 designado para a publicação de arquivos de log.

  > **Note**
  >
  > O bucket do S3 deve existir, e a política do bucket precisa conceder permissão para gravar nele. Para obter informações, consulte Política de bucket do Amazon S3 para o CloudTrail.

- TrailName

  Tipo: String

  Descrição: (obrigatório) o nome da nova trilha.

`AWS-EnableCloudTrailCloudWatchLogs`

Descrição

Esse runbook atualiza a configuração de uma ou mais AWS CloudTrail trilhas para enviar eventos para um grupo de CloudWatch logs do Amazon Logs.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CloudWatchLogsLogGroupArn

  Tipo: String

  Descrição: (Obrigatório) O ARN do grupo de registros de CloudWatch registros em que os CloudTrail registros serão entregues.
- CloudWatchLogsRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função do IAM CloudWatch Logs Logs presume para gravar no grupo de registros especificado.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos nomes das CloudTrail trilhas cujos eventos você deseja enviar para o CloudWatch Logs.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Atualiza as CloudTrail trilhas especificadas para entregar eventos ao grupo de CloudWatch registros de registros especificado.

`AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS`

Descrição

O runbook `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` criptografa uma trilha do AWS CloudTrail (CloudTrail) usando a chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) que você especifica. Esse runbook só deve ser usado como uma linha de base para garantir que suas trilhas do CloudTrail sejam criptografadas de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar várias trilhas com chaves KMS diferentes. Os arquivos de resumo do CloudTrail não são criptografados. Se você já definiu o parâmetro `EnableLogFileValidation` para `true` para a trilha, consulte a seção "Usar criptografia do lado do servidor com chaves AWS KMS gerenciadas" do tópico Melhores práticas de segurança preventiva do CloudTrail no AWS CloudTrail Guia do usuário para obter mais informações.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KMSKeyId

  Tipo: sequência

  Descrição: (obrigatório) O ARN, o ID da chave ou o alias da chave gerenciada pelo cliente que você deseja usar para criptografar a trilha especificada no parâmetro `TrailName`.

- TrailName

  Tipo: sequência

  Descrição: (obrigatório) o ARN ou o nome da trilha que você deseja atualizar para ser criptografada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: ativa a criptografia na trilha que você especifica no parâmetro `TrailName`.
- `aws:executeAwsApi`: reúne o ARN da chave gerenciada pelo cliente que você especifica no parâmetro `KMSKeyId`.
- `aws:assertAwsResourceProperty`: verifica se a criptografia foi ativada na trilha do CloudTrail.

AWS-EnableCloudTrailKmsEncryption

Descrição

Este runbook atualiza a configuração de uma ou mais AWS CloudTrail trilhas para usar a criptografia AWS Key Management Service (AWS KMS).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- KMS KeyId

  Tipo: String

  Descrição: (Obrigatório) O ID da chave gerenciada pelo cliente que você deseja usar para criptografar a trilha especificada no `TrailName` parâmetro. O valor pode ser um nome de alias prefixado por “alias/”, um ARN totalmente especificado para um alias ou um ARN totalmente especificado para uma chave.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas das trilhas que você deseja atualizar para serem criptografadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Ativa a AWS KMS criptografia nas trilhas que você especifica no `TrailName` parâmetro.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Descrição

O runbook do `AWSConfigRemediation-EnableCloudTrailLogFileValidation` ativa a validação do arquivo de log para sua trilha do AWS CloudTrail.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- TrailName

  Tipo: string

  Descrição: (obrigatório) o nome ou o nome do recurso da Amazon (ARN) da trilha para a qual você deseja ativar a validação do log.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: ativa a validação do log para a trilha do AWS CloudTrail que você especifica no parâmetro `TrailName`.
- `aws:assertAwsResourceProperty`: verifica se a validação do log está ativada para sua trilha.

AWS-EnableCloudTrailLogFileValidation

Descrição

O `AWS-EnableCloudTrailLogFileValidation` runbook permite a validação do arquivo de log para as AWS CloudTrail trilhas que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos nomes das CloudTrail trilhas para as quais você deseja habilitar a validação de registros.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Permite a validação do registro para as AWS CloudTrail trilhas que você especifica no `TrailNames` parâmetro.

AWS-QueryCloudTrailLogs

Descrição

O runbook do `AWS-QueryCloudTrailLogs` cria uma tabela do Amazon Athena a partir do bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha que contém logs do AWS

CloudTrail (CloudTrail). Depois de criar a tabela, a automação executa as consultas SQL que você especifica e, em seguida, exclui a tabela.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Consulta

  Tipo: String

  Descrição: (obrigatório) a consulta SQL que você deseja executar.
- SourceBucketPath

  Tipo: String

  Descrição: (obrigatório) o nome do bucket do Amazon S3 que contém os arquivos de log do CloudTrail que você deseja consultar.
- TableName

  Tipo: String

Descrição: (opcional) o nome da tabela do Athena criada pela automação.

Padrão: cloudtrail_logs

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeAwsApi`: cria uma tabela do Athena.
- `aws:executeAwsApi` : executa a sequência de caracteres de consulta que você especifica no parâmetro`Query`.
- `aws:executeScript`: pesquisa e aguarda a conclusão da consulta.
- `aws:executeAwsApi`: obtém os resultados da consulta.

- `aws:executeAwsApi`: exclui a tabela criada pela automação.

CloudWatch

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. CloudWatch Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

`AWS-ConfigureCloudWatchOnEC2Instance`

Descrição

Habilitar ou desabilitar o monitoramento detalhado do Amazon CloudWatch em instâncias gerenciadas.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: String

  Descrição: (obrigatório) o ID da instância do Amazon EC2 na qual você deseja habilitar o monitoramento do CloudWatch.

- propriedades

  Tipo: String

  Descrição: (opcional) esse parâmetro não é compatível. Ele está listado aqui pela compatibilidade com versões anteriores.

- status

  Valores válidos: Enabled | Disabled

  Descrição: (opcional) especifica se você deseja habilitar ou desabilitar o CloudWatch.

  Padrão: Habilitado

Etapas do documento

configureCloudWatch – configura o CloudWatch na instância do Amazon EC2 com o status indicado.

Saídas

Esta automação não tem saída.

AWS-EnableCWAlarm

Descrição

O `AWS-EnableCWAlarm` runbook cria alarmes da Amazon CloudWatch (CloudWatch) para AWS recursos em seu computador Conta da AWS que ainda não têm um. CloudWatch os alarmes são criados para os seguintes AWS recursos:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2)
- Volumes do Amazon Elastic Block Store (Amazon EBS)
- Buckets do Amazon Simple Storage Service (Amazon S3)
- Clusters do Amazon Relational Database Service (Amazon RDS)

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ComparisonOperator

  Tipo: String

  Valores válidos: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpper Threshol | | LessThanLowerThreshold | LessThanOrEqualToThreshold LessThanThreshold

  Descrição: (Obrigatório) A operação aritmética a ser usada ao comparar a estatística e o limite especificados.
- MetricName

Tipo: String

Descrição: (Obrigatório) O nome da métrica associada ao alarme.

- Período

  Tipo: inteiro

  Valores válidos: 10 | 30 | 60 | Um múltiplo de 60

  Descrição: (Obrigatório) O período, em segundos, durante o qual a estatística é aplicada.

- O recurso ganha

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgula dos ARNs dos recursos para os quais criar um alarme CloudWatch

- Estatística

  Tipo: String

  Valores válidos: Média | Máximo | Mínimo | SampleCount | Soma

  Descrição: (Obrigatório) A estatística da métrica associada ao alarme.

- Limite

  Tipo: inteiro

  Descrição: (Obrigatório) O valor a ser comparado com a estatística especificada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `cloudwatch:PutMetricAlarm`

Etapas do documento

- `aws:executeScript`- Cria um CloudWatch alarme de acordo com os valores especificados nos parâmetros do runbook para os recursos que você especifica no `ResourceARNs` parâmetro.

Saídas

Ativar o alarme de alarme. FailedResources: uma lista de ARNs de recursos para os quais um CloudWatch alarme não foi criado e o motivo da falha.

Ativar o alarme de alarme. SuccessfulResources: uma lista de ARNs de recursos para os quais um CloudWatch alarme foi criado com sucesso.

Amazon DocumentDB

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon DocumentDB (com compatibilidade com o MongoDB). Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableDocDbClusterBackupRetentionPeriod

`AWS-EnableDocDbClusterBackupRetentionPeriod`

Descrição

O `AWS-EnableDocDbClusterBackupRetentionPeriod` runbook permite um período de retenção de backup para o cluster Amazon DocumentDB que você especificar. Esse recurso define o número total de dias durante os quais um backup automatizado é retido. Para modificar um cluster, o cluster deve estar no estado disponível com um tipo de mecanismo de`docdb`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DB ClusterResourceId

  Tipo: string

  Descrição: (Obrigatório) O ID do recurso para o cluster Amazon DocumentDB para o qual você deseja habilitar o período de retenção de backup.
- BackupRetentionPeriod

  Tipo: inteiro

  Descrição: (Obrigatório) O número de dias durante os quais os backups automatizados são retidos. Deve ser um valor de 7 a 35 dias.
- PreferredBackupWindow

  Tipo: string

  Descrição: (Opcional) Um intervalo de tempo diário em Tempo Universal Coordenado (UTC) no formato hh24:mm-hh24:mm, por exemplo, 07:14-07:44. O valor deve ser de pelo menos 30 minutos e não pode entrar em conflito com a janela de manutenção preferida.

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

Etapas do documento

- GetDocDbClusterIdentifier (aws:executeAwsApi) - Retorna o identificador do cluster Amazon DocumentDB usando o ID do recurso fornecido.
- VerifyDocDbEngine (aws: assertAwsResource Propriedade) - Verifica se o tipo de mecanismo Amazon DocumentDB `docdb` é para evitar alterações inadvertidas em outros tipos de mecanismo do Amazon RDS.
- VerifyDocDbStatus (aws: waitAwsResource Property) - Verifica se o status do cluster Amazon DocumentDB é. `available`
- ModifyDocDbRetentionPeriod (aws:executeAwsApi) - Define o período de retenção usando os valores fornecidos para o cluster Amazon DocumentDB especificado.
- VerifyDocDbBackupsEnabled (aws:ExecuteScript) — Verifica se o período de retenção do cluster Amazon DocumentDB e a janela de backup preferencial, se especificada, foram configurados com sucesso.

Saídas

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - Resposta da operação `ModifyDBCluster` da API.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse - Saída da `VerifyDocDbBackupsEnabled` etapa que confirma a modificação bem-sucedida do cluster Amazon DocumentDB.

CodeBuild

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CodeBuild Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Descrição

O AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK runbook criptografa os artefatos de construção de um projeto AWS CodeBuild (CodeBuild) usando a chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) que você especifica. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- KMS KeyId

  Tipo: sequência

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) da chave gerenciada pelo AWS KMS cliente que você deseja usar para criptografar o CodeBuild projeto especificado no parâmetro. ProjectId
- ProjectId

  Tipo: sequência

Descrição: (Obrigatório) O ID do CodeBuild projeto cujos artefatos de construção você deseja criptografar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`- Reúne o nome do CodeBuild projeto a partir do ID do projeto.
- `aws:executeAwsApi`- Ativa a criptografia no CodeBuild projeto que você especifica no `ProjectId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica se a criptografia foi ativada no CodeBuild projeto.

Saídas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Resposta da chamada `UpdateFunctionConfiguration` da API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descrição

O runbook `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` exclui as variáveis de ambiente `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY` do projeto do AWS CodeBuild (CodeBuild) que você especificar. O AWS Config deve estar habilitado na Região da AWS em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ResourceId

  Tipo: sequência

  Descrição: (obrigatório) o ID do projeto CodeBuild cujas variáveis de ambiente da chave de acesso você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: exclui as variáveis de ambiente da chave de acesso para o projeto do CodeBuild especificado no parâmetro `ResourceId`.

AWS CodeDeploy

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CodeDeploy Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootCodeDeploy

`AWSSupport-TroubleshootCodeDeploy`

Descrição

O runbook `AWSSupport-TroubleshootCodeDeploy` ajuda a diagnosticar por que uma implantação do AWS CodeDeploy falhou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). O runbook fornece etapas para ajudar você a resolver o problema ou resolver problemas adicionais. As melhores práticas para o CodeDeploy também são fornecidas para ajudar você a evitar problemas semelhantes no futuro.

Este runbook pode ajudá-lo a resolver os seguintes problemas:

- O agente do CodeDeploy não está instalado ou não está em execução na instância do Amazon EC2
- A instância do Amazon EC2 não tem um perfil de instância do AWS Identity and Access Management (IAM) anexado
- O perfil de instância do IAM anexado à instância do Amazon EC2 não tem as permissões necessárias do Amazon Simple Storage Service (Amazon S3)
- Uma revisão armazenada no Amazon S3 está ausente ou o bucket do Amazon S3 usado está em uma Região da AWS que é diferente da instância do Amazon EC2
- Problemas com o arquivo de especificação do aplicativo (AppSpec)
- Erros “O arquivo já existe no local”
- Falha nos hooks de eventos do ciclo de vida gerenciado do CodeDeploy
- Falha nos hooks de eventos do ciclo de vida gerenciado do cliente

- Eventos de escalonamento durante a implantação

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DeploymentId

  Tipo: sequência

  Descrição: (obrigatório) o ID da implantação que falhou.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: verifica os valores fornecidos para os parâmetros `DeploymentId` e `InstanceId`.
- `aws:executeScript`: coleta informações da instância do Amazon EC2, como o estado da instância e detalhes do perfil de instância do IAM.
- `aws:executeScript`: analisa a implantação especificada e retorna uma análise sobre por que a implantação falhou.

AWS Config

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Config Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-SetupConfig

`AWSSupport-SetupConfig`

Descrição

O runbook `AWSSupport-SetupConfig` cria uma função vinculada ao serviço AWS Identity and Access Management (IAM), um gravador de configuração alimentado pelo AWS Config e um canal de entrega com um bucket do Amazon Simple Storage Service (Amazon S3) em que AWS Config envia instantâneos de configuração e arquivos de histórico de configuração. Se você especificar valores para os parâmetros `AggregatorAccountId` e `AggregatorAccountRegion`, o runbook também cria autorizações para agregação de dados para coletar dados de configuração e conformidade do AWS Config de várias Contas da AWS e várias Regiões da AWS. Para saber mais sobre como agregar dados de várias contas e regiões, consulte Agregação de dados de várias regiões e várias contas no Guia do desenvolvedor do AWS Config.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AggregatorAccountId

  Tipo: sequência

  Descrição: (opcional) o ID da Conta da AWS em que um agregador será adicionado aos dados agregados de configuração e conformidade do AWS Config de várias contas e Regiões da AWS. Essa conta também é usada pelo agregador para autorizar as contas de origem.
- AggregatorAccountRegion

  Tipo: sequência

  Descrição: (opcional) a região em que um agregador será adicionado aos dados agregados de configuração e conformidade do AWS Config de várias contas e regiões.
- IncludeGlobalResourcesRegion

  Tipo: sequência

  Padrão: us-east-1

Descrição: (obrigatório) para evitar o registro de dados de recursos globais em cada região, especifique uma região da qual registrar dados de recursos globais.

- Partition

  Tipo: sequência

  Padrão: `aws`

  Descrição: (obrigatório) a partição da qual você deseja coletar dados de configuração e conformidade do AWS Config.

- S3BucketName

  Tipo: sequência

  Padrão: `aws-config-delivery-channel`

  Descrição: (opcional) o nome que você deseja aplicar ao bucket do Amazon S3 criado para o canal de entrega. O ID da conta é anexado ao final do nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript`: cria um perfil do IAM vinculado ao serviço para o AWS Config, caso ainda não exista.
- `aws:executeScript`: cria um gravador de configuração, caso ainda não exista.
- `aws:executeScript`: cria um bucket do Amazon S3 para ser usado pelo canal de entrega, caso ainda não exista.
- `aws:executeScript`: cria um canal de entrega usando os recursos criados pelo runbook.
- `aws:executeAwsApi`: parar ou iniciar o gravador de configuração.
- `aws:executeScript`: se você especificou valores para os parâmetros `AggregatorAccountId` e `AggregatorAccountRegion`, as autorizações para agregação de dados de várias contas e várias regiões serão configuradas.

Amazon Connect

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Connect. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`

Descrição

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`Isso ajuda você a associar números de telefone aos fluxos de contato na sua instância do Amazon Connect. Ao fornecer os mapeamentos de números de telefone e fluxos de contato em um arquivo de entrada de valores separados por vírgula (CSV), o runbook associa o maior número possível de números de telefone aos fluxos de contato em 14,5 minutos. O runbook produz um arquivo CSV de todos os pares de números de telefone e fluxo de contatos que ele não pôde associar dentro do limite de tempo para que você possa inseri-los na próxima execução.

Como funciona?

O runbook `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` ajuda você a associar números de telefone aos fluxos de contato em sua instância do Amazon Connect usando um arquivo CSV de dados de mapeamento que é armazenado em um bucket do Amazon Simple Storage Service (Amazon S3). O arquivo CSV de entrada deve estar alinhado ao formato a seguir, com `PhoneNumber` valores no formato E.164.

Exemplo do arquivo CSV de entrada

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

O runbook de automação também cria os seguintes arquivos no local de destino especificado no `DestinationFileBucket` e. `DestinationFilePath`

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: um arquivo temporário que contém os `ContactFlowId` pares `PhoneNumberId` e que são necessários para a `AssociatePhoneNumberContactFlow` API.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: um arquivo que contém o número de telefone e os pares de fluxo de contatos que não puderam ser processados devido a um erro, como `ResourceNotFoundException` no formato de`PhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: um arquivo que contém o número de telefone e os pares de fluxo de contatos que não foram processados. O runbook tenta processar o maior número possível de números de telefone e fluxos de contato em 14,5 minutos (15 minutos de tempo limite da AWS Lambda função - 30 segundos de buffer). Se houver alguns números de telefone/fluxos de contato que não puderam ser processados devido à restrição de tempo, o runbook os incluirá em um arquivo CSV para usar como entrada para a próxima execução do runbook.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-AssociatePhoneNumbersToConnectContactFlowsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional)

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - ConnectInstanceId (Obrigatório)

     O ID da sua instância do Amazon Connect.
   - SourceFileBucket (Obrigatório)

     O bucket do Amazon S3 que armazena o arquivo CSV que contém o número de telefone e os pares de fluxo de contato.
   - SourceFilePath (Obrigatório)

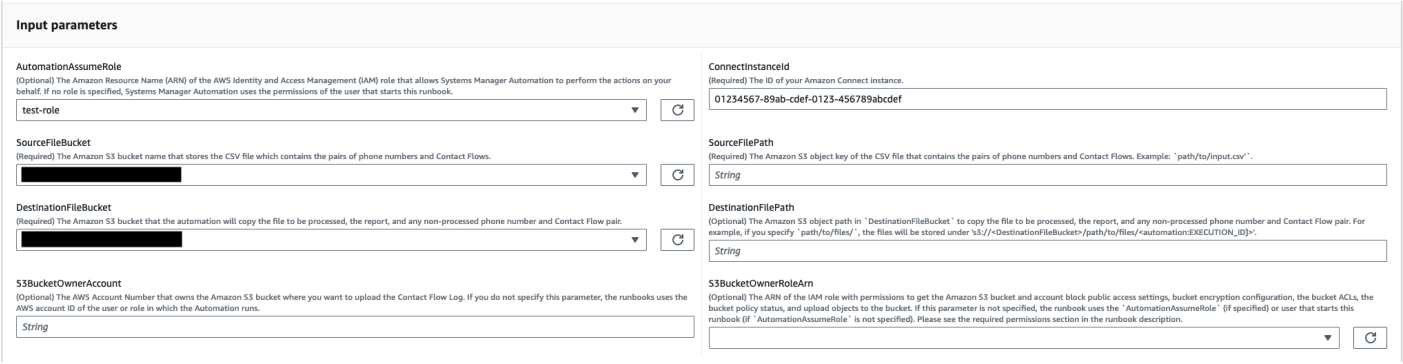
     A chave de objeto do Amazon S3 do arquivo CSV que contém o número de telefone e os pares de fluxo de contato. Por exemplo, `path/to/input.csv`.
   - DestinationFileBucket (Obrigatório)

     O bucket do Amazon S3 no qual a automação colocará um arquivo intermediário e um relatório de resultados.
   - DestinationFilePath (Opcional)

     O caminho do objeto Amazon S3 no `DestinationFileBucket` qual um arquivo intermediário e um relatório de resultados devem ser armazenados. Por exemplo, se você especificar`path/to/files/`, os arquivos serão armazenados em`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.
   - S3 BucketOwnerAccount (opcional)

     O número da AWS conta que possui o bucket do Amazon S3 em que você deseja fazer o upload do registro de fluxo de contatos. Se você não especificar esse parâmetro, os runbooks usarão o ID da AWS conta do usuário ou da função na qual a automação é executada.
   - S3 BucketOwnerRoleArn (opcional)

O ARN da função do IAM com permissões para obter o bucket e a conta do Amazon S3 bloqueia as configurações de acesso público, a configuração da criptografia do bucket, as ACLs do bucket, o status da política do bucket e carrega objetos no bucket. Se esse parâmetro não for especificado, o runbook usa o `AutomationAssumeRole` (se especificado) ou o usuário que inicia esse runbook (se não `AutomationAssumeRole` for especificado). Consulte a seção de permissões necessárias na descrição do runbook.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - CheckConnectInstanceExistance

     Verifica se a instância do Amazon Connect fornecida em `ConnectInstanceId` existe.
   - Verificações 3 BucketPublicStatus

     Verifica se os buckets do Amazon S3 especificados no `SourceFileBucket` e `DestinationFileBucket` permitem permissões de acesso anônimas ou públicas de leitura ou gravação.
   - CheckSourceFileExistenceAndSize

     Verifica se o arquivo CSV de origem especificado no `SourceFilePath` existe e se o tamanho do arquivo excede o limite de 25 MiB.
   - GenerateResourceIdMap

     Faz o download do arquivo CSV de origem especificado na identificação `SourceFilePath` `PhoneNumberId` e `ContactFlowId` para cada recurso. Depois de concluído, ele carrega um arquivo CSV que contémPhoneNumber,, PhoneNumberIdContactFlowName, e `ContactFlowId` para o bucket de destino do Amazon S3 especificado em.

`DestinationFileBucket` Se `PhoneNumberId` não puder ser identificado por um determinado número, o campo ficará vazio no arquivo CSV.

- AssociatePhoneNumbersToContactFlows

  Cria uma AWS Lambda função na sua conta usando uma AWS CloudFormation pilha. A AWS Lambda função associa cada número a um fluxo de contato listado no arquivo CSV de origem especificado em `SourceFileBucket` e `SourceFilePath` e a AWS CloudFormation pilha invoca a função. A AWS Lambda função mapeia o maior número possível de números de telefone para fluxos de contato antes que o tempo limite atinja o tempo limite (15 minutos). A lista de números de telefone e fluxos de contato que não puderam ser processados devido a um erro é carregada em`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Aqueles que não puderam ser processados devido ao excesso do número máximo de números de telefone que podem ser processados em uma única execução são enviados`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Se essa etapa falhar, ela vai para a `DescribeCloudFormationErrorFromStackEvents` etapa para mostrar por que ela falhou nos eventos da AWS CloudFormation pilha.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Espera até que a AWS Lambda função que mapeia números de telefone para fluxos de contato seja criada e a AWS CloudFormation pilha conclua sua invocação.

- GenerateReport

  Gera o relatório que contém o número de números de telefone mapeados para fluxos de contato, aqueles que não puderam ser processados devido a um erro e aqueles que não puderam ser processados devido ao excesso do número máximo de números de telefone que podem ser processados em uma única execução. O relatório também mostra a localização (URI do Amazon S3 e URL do console do Amazon S3) `[automation:EXECUTION_ID]/ErrorResourceList.csv` para `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` ou, se aplicável.

- **`DeleteCloudFormationStack`**

  Exclui a AWS CloudFormation pilha, incluindo a função Lambda para mapeamento.

- **`DescribeCloudFormationErrorFromStackEvent`**

  Descreve os erros da AWS CloudFormation pilha da `AssociatePhoneNumbersToContactFlows` etapa.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

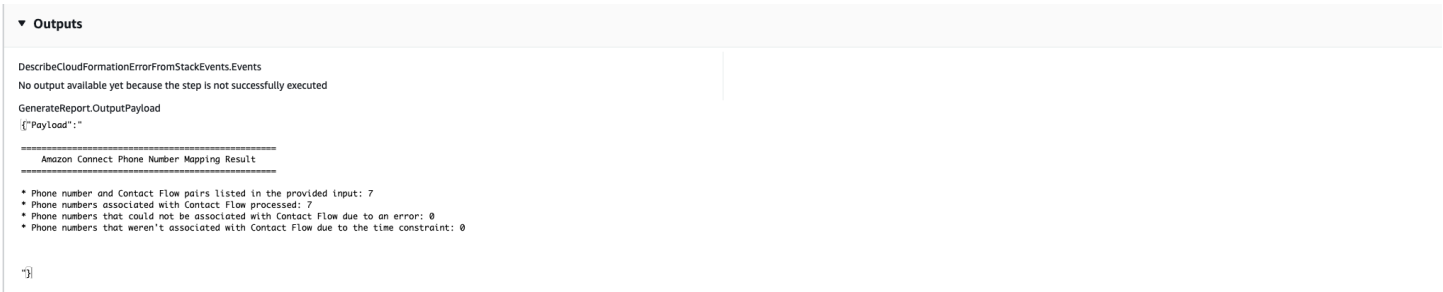
- GenerateReport.OutputPayload

  Saída de associações de número de telefone e fluxo de contatos. Esse relatório contém as seguintes informações:

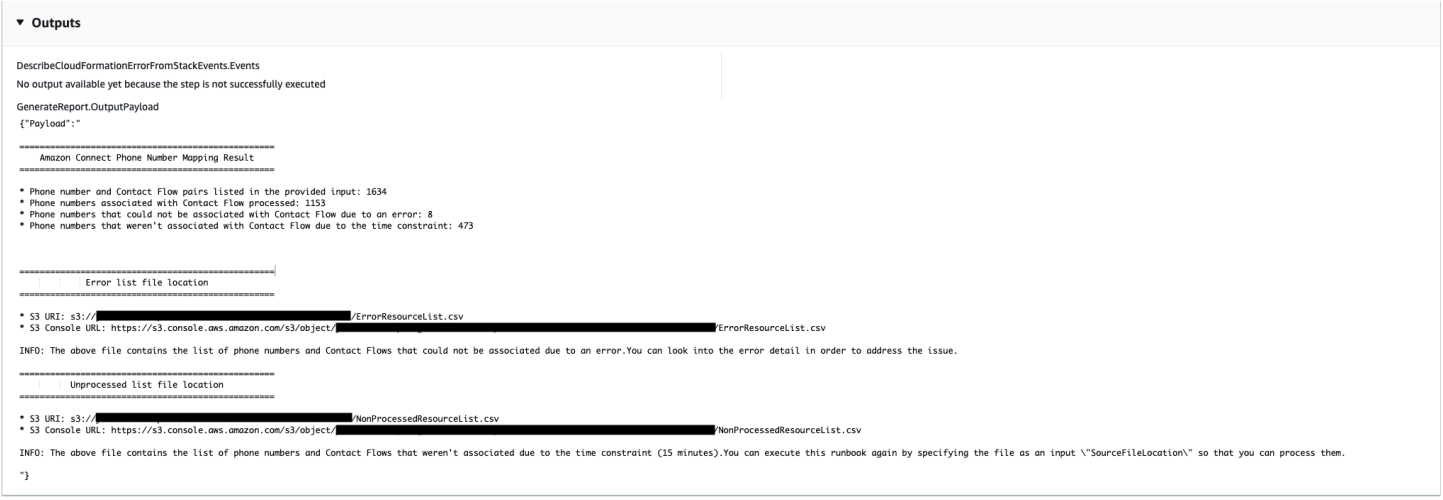
  - O número de pares de números de telefone e fluxo de contatos listados no arquivo CSV de entrada
  - O número de números de telefone associados aos fluxos de contato, conforme especificado no arquivo CSV de entrada
  - O número de números de telefone que não puderam ser associados aos fluxos de contato devido a um erro
  - O número de números de telefone que não estavam associados aos fluxos de contato devido à restrição de tempo
  - A localização (URI do Amazon S3 e URL do console do Amazon S3) do arquivo CSV que contém o número de telefone e os pares de fluxo de contato que não puderam ser associados devido a um erro
  - A localização (URI do Amazon S3 e URL do console do Amazon S3) do arquivo CSV que contém o número de telefone e os pares de fluxo de contato que não foram associados devido à restrição de tempo
- DescribeCloudFormationErrorFromStackEvents.Eventos

  Saída que mostra os eventos da AWS CloudFormation pilha se a `AssociatePhoneNumbersToContactFlows` etapa falhar.

Saída de execução com um pequeno número de números de telefone e fluxos de contato



Saída de execução com um grande número de números de telefone e fluxos de contato e números de telefone que não foram associados devido a erro ou restrição de tempo



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS Directory Service

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Directory Service Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

`AWS-CreateDSManagementInstance`

Descrição

O runbook `AWS-CreateDSManagementInstance` cria uma instância do Windows do Amazon Elastic Compute Cloud (Amazon EC2) que pode ser usada para gerenciar seu diretório do AWS

Directory Service. A instância de gerenciamento não pode ser usada para gerenciar diretórios do AD Connector.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AmiID

  Tipo: sequência

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

  Descrição: (obrigatório) o ID da Amazon Machine Image (AMI) que você deseja usar para iniciar a instância de gerenciamento.
- DirectoryId

  Tipo: sequência

  Descrição: (obrigatório) o ID do diretório do AWS Directory Service que você deseja gerenciar. A instância é ligada ao diretório especificado.

- IamInstanceProfileName

  Tipo: sequência

  Descrição: (obrigatório) o nome que você especifica é aplicado ao perfil de instância do IAM que é criado pela automação e anexado à instância de gerenciamento.

- InstanceType

  Tipo: sequência

  Padrão: t3.medium

  Valores permitidos:

  - 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

  Descrição: (obrigatório) tipo de instância a ser executada.

- KeyPairName

  Tipo: sequência

  Descrição: (opcional) o par de chaves a ser usado ao criar a instância. Se você não especificar um valor, nenhum par de chaves será associado à instância.

- RemoteAccessCidr

Tipo: sequência

Descrição: (obrigatório) o bloco CIDR do qual você deseja permitir o tráfego RDP (porta 3389). O bloco CIDR que você especifica é aplicado a uma regra de entrada que é adicionada ao grupo de segurança criado pela automação.

- SecurityGroupName

  Tipo: sequência

  Descrição: (obrigatório) o nome que você especifica é aplicado ao grupo de segurança criado pela automação e associado à instância de gerenciamento.

- Tags

  Tipo: MapList

  Descrição: (opcional) um par de chave-valor que você deseja aplicar aos recursos criados pela automação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi: reúne detalhes sobre o diretório que você especifica no parâmetro DirectoryId.

- `aws:executeAwsApi`: obtém o bloco CIDR da nuvem privada virtual (VPC) em que o diretório foi iniciado.
- `aws:executeAwsApi`: cria um grupo de segurança usando o valor especificado no parâmetro `SecurityGroupName`.
- `aws:executeAwsApi`: cria uma regra de entrada para o grupo de segurança recém-criado que permite o tráfego RDP do CIDR que você especifica no parâmetro `RemoteAccessCidr`.
- `aws:executeAwsApi`: cria um perfil do IAM e um perfil de instância usando o valor especificado no parâmetro `IamInstanceProfileName`.
- `aws:executeAwsApi`: inicia uma instância do Amazon EC2 com base nos valores que você especifica nos parâmetros do runbook.
- `aws:executeAwsApi`: cria um documento do AWS Systems Manager para ligar a instância recém-iniciada ao seu diretório.
- `aws:runCommand`: liga a nova instância ao seu diretório.
- `aws:runCommand`: instala ferramentas de administração de servidor remoto na nova instância.

`AWSSupport-TroubleshootADConnectorConnectivity`

Descrição

O runbook `AWSSupport-TroubleshootADConnectorConnectivity` verifica os seguintes pré-requisitos para um AD Connector:

- Verifica se o tráfego necessário é permitido pelo grupo de segurança e pelas regras da lista de controle de acesso (ACL) à rede associadas ao seu AD Connector.
- Verifica se os endpoints de VPC da interface do AWS Systems Manager, AWS Security Token Service e Amazon CloudWatch existem na mesma nuvem privada virtual (VPC) do AD Connector.

Quando as verificações de pré-requisitos são concluídas com sucesso, o runbook inicia duas instâncias Linux t2.micro do Amazon Elastic Compute Cloud (Amazon EC2) nas mesmas sub-redes do seu AD Connector. Os testes de conectividade de rede são então realizados usando os utilitários `netcat` e `nslookup`.

Execute esta automação (console)

> **Important**
>
> O uso deste runbook pode gerar cobranças adicionais a sua Conta da AWS para as instâncias do Amazon EC2, volumes do Amazon Elastic Block Store e Amazon Machine Image (AMI) criados durante a automação. Para obter mais informações, consulte Amazon Elastic Compute Cloud Pricing e Amazon Elastic Block Store Pricing.
>
> Se a etapa `aws:deletestack` falhar, acesse o console do AWS CloudFormation para excluir manualmente a pilha. O nome da pilha criada por esse runbook começa com `AWSSupport-TroubleshootADConnectorConnectivity`. Para obter informações sobre como excluir pilhas do AWS CloudFormation, consulte Excluir uma pilha no AWS CloudFormationGuia do usuário.

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DirectoryId

  Tipo: sequência

  Descrição: (obrigatório) o ID do diretório do AD Connector no qual você deseja solucionar problemas de conectividade.

- Ec2InstanceProfile

  Tipo: sequência

  Máximo de caracteres: 128

  Descrição: (obrigatório) o nome do perfil de instância que você deseja atribuir às instâncias que são iniciadas para realizar testes de conectividade. O perfil de instância que você especificar deve ter a política `AmazonSSMManagedInstanceCore` ou as permissões equivalentes anexadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:assertAwsResourceProperty`: confirma que o diretório especificado no parâmetro `DirectoryId` é um AD Connector.
- `aws:executeAwsApi`: reúne informações sobre o AD Connector.
- `aws:executeAwsApi`: reúne informações sobre os grupos de segurança associados ao AD Connector.
- `aws:executeAwsApi`: reúne informações sobre as regras de ACL de rede associadas às sub-redes do AD Connector.
- `aws:executeScript`: avalia as regras do grupo de segurança do AD Connector para verificar se o tráfego de saída necessário é permitido.
- `aws:executeScript`: avalia as regras de ACL de rede do AD Connector para verificar se o tráfego de rede de saída e entrada necessário é permitido.
- `aws:executeScript`: verifica se os endpoints da interface do AWS Systems Manager, AWS Security Token Service e Amazon CloudWatch existem na mesma VPC que o AD Connector.
- `aws:executeScript`: compila as saídas das verificações realizadas nas etapas anteriores.
- `aws:branch`: ramifica a automação dependendo da saída das etapas anteriores. A automação é interrompida aqui se as regras de saída e entrada necessárias estiverem ausentes para os grupos de segurança e as ACLs de rede.
- `aws:createStack`: cria uma pilha do AWS CloudFormation para iniciar instâncias do Amazon EC2 para realizar testes de conectividade.
- `aws:executeAwsApi`: reúne as IDs das instâncias recém-lançadas do Amazon EC2.
- `aws:waitForAwsResourceProperty`: espera que a primeira instância recém-lançada do Amazon EC2 seja reportada como gerenciada por AWS Systems Manager.
- `aws:waitForAwsResourceProperty`: espera que a segunda instância recém-lançada do Amazon EC2 seja reportada como gerenciada por AWS Systems Manager.
- `aws:runCommand`: executa testes de conectividade de rede com os endereços IP do servidor DNS on-premises da primeira instância do Amazon EC2.
- `aws:runCommand`: executa testes de conectividade de rede com os endereços IP do servidor DNS on-premises da segunda instância do Amazon EC2.

- `aws:changeInstanceState`: interrompe as instâncias do Amazon EC2 usadas para os testes de conectividade.
- `aws:deleteStack`: exclui a pilha AWS CloudFormation.
- `aws:executeScript`: produz instruções sobre como excluir manualmente a pilha do AWS CloudFormation se a automação falhar em excluir a pilha.

`AWSSupport-TroubleshootDirectoryTrust`

Descrição

O runbook `AWSSupport-TroubleshootDirectoryTrust` diagnostica problemas de criação de confiança entre um AWS Managed Microsoft AD e um Microsoft Active Directory. A automação garante que o tipo de diretório ofereça suporte a confianças e verifica as regras de grupo de segurança associadas, listas de controle de acesso à rede (ACLs de rede) e tabelas de rotas para verificar possíveis problemas de conectividade.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DirectoryId

  Tipo: sequência

  Padrão permitido: ^d-[a-z0-9]\{10\}$

  Descrição: (obrigatória) o ID do AWS Managed Microsoft AD para solução de problemas.

- RemoteDomainCidrs

  Tipo: StringList

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

  Descrição: (obrigatória) os CIDRs do domínio remoto com o qual você está tentando estabelecer uma relação de confiança. Você pode adicionar vários CIDRs usando valores separados por vírgula. Por exemplo, 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

  Tipo: sequência

  Descrição: (obrigatória) o nome totalmente qualificado do domínio remoto com o qual você está estabelecendo uma relação de confiança.

- RequiredTrafficACL

  Tipo: sequência

  Descrição: (obrigatória) os requisitos para a porta padrão do AWS Managed Microsoft AD. Na maioria dos casos, não modifique o valor padrão.

  Padrão: {"entrada":{"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]]},"saída":{"-1":[[0,65535]]}}

- RequiredTrafficSG

  Tipo: sequência

  Descrição: (obrigatória) os requisitos para a porta padrão do AWS Managed Microsoft AD. Na maioria dos casos, não modifique o valor padrão.

Padrão: {"entrada":{"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]]},"saída":{"-1":[[0,65535]]}}

- TrustId

  Tipo: sequência

  Descrição: (opcional) o ID do relacionamento de confiança a ser solucionado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:assertAwsResourceProperty`: confirma que o tipo de diretório é AWS Managed Microsoft AD.
- `aws:executeAwsApi`: obtém informações sobre AWS Managed Microsoft AD.
- `aws:branch`: ramifica a automação se um valor for fornecido para o parâmetro de entrada `TrustId`.
- `aws:executeAwsApi`: obtém informações sobre o relacionamento de confiança.
- `aws:executeAwsApi`: obtém os endereços IP DNS de encaminhador condicional para o `RemoteDomainName`.
- `aws:executeAwsApi`: obtém informações sobre rotas IP adicionadas ao AWS Managed Microsoft AD.
- `aws:executeAwsApi`: obtém os CIDRs das sub-redes AWS Managed Microsoft AD.

- `aws:executeAwsApi`: obtém informações sobre os grupos de segurança associados a AWS Managed Microsoft AD.
- `aws:executeAwsApi`: obtém informações sobre as ACLs de rede associadas ao AWS Managed Microsoft AD.
- `aws:executeScript`: confirma que os `RemoteDomainCidrs` são valores válidos. Confirma que o AWS Managed Microsoft AD tem encaminhadores condicionais para os `RemoteDomainCidrs`, e que as rotas IP necessárias foram adicionadas ao AWS Managed Microsoft AD se os `RemoteDomainCidrs` não forem endereços IP RFC 1918.
- `aws:executeScript`: avalia as regras do grupo de segurança.
- `aws:executeScript`: avalia ACLs de rede.

Saídas

evalDirectorySecurityGroup.output – resultará da avaliação se as regras do grupo de segurança associadas ao AWS Managed Microsoft AD permitirem o tráfego necessário para a criação de confiança.

evalAclEntries.output – resulta da avaliação para verificar se as ACLs de rede associadas ao AWS Managed Microsoft AD permitem o tráfego necessário para a criação de confiança

evaluateRemoteDomainCidr.output – resulta da avaliação para verificar se os valores de `RemoteDomainCidrs` são válidos. Confirma que o AWS Managed Microsoft AD tem encaminhadores condicionais para os `RemoteDomainCidrs`, e que as rotas IP necessárias foram adicionadas ao AWS Managed Microsoft AD se os `RemoteDomainCidrs` não forem endereços IP RFC 1918.

AWS AppSync

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS AppSync Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

Descrição

O `AWS-EnableAppSyncGraphQLApiLogging` runbook permite o registro em nível de campo e registro em nível de solicitação para a API AWS AppSync GraphQL que você especificar. O runbook aplicará as alterações na API GraphQL especificada, mesmo que o registro já tenha sido habilitado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ApiId

  Tipo: string

  Descrição: (Obrigatório) O ID da API para a qual você deseja ativar o registro.
- FieldLogLevel

  Tipo: string

  Valores válidos: ERROR | ALL

Descrição: (Obrigatório) O nível de registro do campo.

- CloudWatchLogsRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função de serviço que AWS AppSync pressupõe publicar no Amazon Logs. CloudWatch

- ExcludeVerboseContent

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Defina como `True` para excluir informações como cabeçalhos, contexto e modelos de mapeamento avaliados, independentemente do nível de registro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- aws: executeAwsApi - Reúne o tipo de autenticação e as informações de configuração relevantes para o tipo de autenticação principal.
- aws:branch - Ramificações com base no tipo de autenticação.
- aws: executeAwsApi - Atualiza a configuração de registro da API AWS AppSync GraphQL com base nos valores especificados para os parâmetros de entrada do runbook.

Saídas

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.

Amazon Athena

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Athena. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWS-EnableAthenaWorkGroupEncryptionAtRest`

Descrição

O `AWS-EnableAthenaWorkGroupEncryptionAtRest` runbook permite a criptografia em repouso para o grupo de trabalho do Amazon Athena que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- WorkGroup

  Tipo: string

  Descrição: (Obrigatório) O grupo de trabalho para o qual você deseja habilitar a criptografia em repouso.

- EncryptionOption

  Tipo: string

  Valores válidos: SSE_S3 | SSE_KMS | CSE_KMS

  Descrição: (Obrigatório) Especifica qual opção de criptografia é usada. Você pode escolher criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE_S3), criptografia do lado do servidor com chaves gerenciadas (SSE_KMS) ou criptografia do lado do cliente com chaves AWS KMS gerenciadas (CSE_KMS). AWS KMS

- KmsKeyId

  Tipo: string

  Descrição: (Opcional) Se você estiver usando uma opção de AWS KMS criptografia, especifique o ARN da chave, o ID da chave ou o alias da chave que você deseja usar.

- EnableMinimumEncryptionConfiguration

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Impõe um nível mínimo de criptografia para o grupo de trabalho para resultados de consulta e cálculo que são gravados no Amazon S3. Quando ativada, os usuários do

grupo de trabalho podem definir a criptografia somente no nível mínimo definido pelo administrador ou superior ao enviarem consultas. Essa configuração não se aplica aos grupos de trabalho habilitados para Spark.

- EnforceWorkGroupConfiguration

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`True`, as configurações do grupo de trabalho substituem as configurações do lado do cliente. Se definido como`False`, as configurações do lado do cliente serão usadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- aws:branch - Ramificações com base na opção de criptografia especificada no `EncryptionOption` parâmetro.
- aws: executeAwsApi - Esta etapa atualiza o Athena Work Group com a configuração de criptografia especificada.
- aws: executeAwsApi - Atualiza o Athena Work Group com a configuração de criptografia especificada.
- aws: assertAwsResource Propriedade - Verifica se a criptografia para o grupo de trabalho foi ativada.

DynamoDB

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon DynamoDB. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWS-ChangeDDBRWCapacityMode

Descrição

O `AWS-ChangeDDBRWCapacityMode` runbook altera o modo de capacidade de leitura/gravação de uma ou mais tabelas do Amazon DynamoDB (DynamoDB) para o modo sob demanda ou para o modo provisionado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CapacityMode

  Tipo: String

  Valores válidos: PROVISIONED | PAY_PER_REQUEST

  Descrição: (Obrigatório) O modo de capacidade de leitura/gravação desejado. Ao mudar da capacidade sob demanda (pay-per-request) para a capacidade provisionada, os valores iniciais da capacidade provisionada devem ser definidos. Os valores iniciais da capacidade provisionada são estimados com base na capacidade de leitura e gravação consumida da sua tabela e dos índices secundários globais nos últimos 30 minutos.
- ReadCapacityUnits

  Tipo: inteiro

  Padrão: 0

  Descrição: (Opcional) O número máximo de leituras altamente consistentes consumidas por segundo antes que o DynamoDB retorne uma exceção de limitação.
- TableNames

  Tipo: String

  Descrição: (Obrigatório) Lista separada por vírgula de nomes de tabelas do DynamoDB para alterar o modo de capacidade de leitura/gravação para..
- WriteCapacityUnits

  Tipo: inteiro

Padrão: 0

Descrição: (Opcional) O número máximo de gravações consumidas por segundo antes que o DynamoDB retorne uma exceção de limitação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Altera o modo de capacidade de leitura/gravação das tabelas do DynamoDB especificadas no parâmetro. `TableNames`

Saídas

DBRW alteradoCapacityMode. SuccessesTables - Lista de nomes de tabelas do DynamoDB em que o modo de capacidade foi alterado com sucesso

DBRW alteradoCapacityMode. FailedTables - Lista mapeada dos nomes das tabelas do DynamoDB em que a alteração do modo de capacidade falhou e o motivo da falha.

AWS-CreateDynamoDBBackup

Descrição

Criar um backup da tabela do Amazon DynamoDB.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BackupName

  Tipo: sequência

  Descrição: (obrigatório) Nome do backup a ser criado.
- LambdaAssumeRole

  Tipo: sequência

  Descrição: (Opcional) O ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- TableName

  Tipo: sequência

  Descrição: (obrigatório) Nome da tabela do DynamoDB.

AWS-DeleteDynamoDbBackup

Descrição

Excluir o backup de uma tabela do Amazon DynamoDB.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BackupArn

  Tipo: sequência

  Descrição: (obrigatório) ARN do backup da tabela do DynamoDB a ser excluído.

AWSConfigRemediation-DeleteDynamoDbTable

Descrição

O runbook `AWSConfigRemediation-DeleteDynamoDbTable` exclui a tabela do Amazon DynamoDB (DynamoDB) que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- TableName

  Tipo: sequência

  Descrição: (obrigatório) nome da tabela do DynamoDB que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: exclui a tabela do DynamoDB especificada no parâmetro `TableName`.
- `aws:executeScript`: verifica se a tabela do DynamoDB foi excluída.

AWS-DeleteDynamoDbTableBackups

Descrição

Excluir backups de tabelas do DynamoDB com base em dias ou contagem de retenção.

Execute esta Automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- RetentionCount

  Tipo: String

  Padrão: 10

  Descrição: (opcional) o número de backups a serem retidos para a tabela. Se existir mais backups do que o número especificado, os backups mais antigos além desse número são excluídos. Pode-se usar o RetentionCount ou RetentionDays, mas não ambos.

- RetentionDays

  Tipo: String

  Descrição: (opcional) o número de dias a reter backups para a tabela. Os backups mais antigos que o número especificado de dias são excluídos. Pode-se usar o RetentionCount ou RetentionDays, mas não ambos.

- TableName

  Tipo: String

  Descrição: (obrigatório) nome da tabela do DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descrição

O `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` runbook criptografa uma tabela do Amazon DynamoDB (DynamoDB) usando a chave gerenciada pelo cliente AWS KMS() que você especifica para AWS Key Management Service o parâmetro. `KMSKeyId`

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KMS KeyId

  Tipo: sequência

  Descrição: (obrigatório) o ARN da chave gerenciada pelo cliente que você deseja usar para criptografar a tabela do DynamoDB especificada no parâmetro `TableName`.

- TableName

  Tipo: sequência

  Descrição: (obrigatório) nome da tabela do DynamoDB que você deseja criptografar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: criptografa a tabela do DynamoDB que você especifica no parâmetro `TableName`.
- `aws:waitForAwsResourceProperty`: verifica se a propriedade `Enabled` do `SSESpecification` da tabela do DynamoDB está definida como `true`.
- `aws:assertAwsResourceProperty`: verifica se a tabela do DynamoDB está criptografada com a chave gerenciada pelo cliente especificada no parâmetro `KMSKeyId`.

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descrição

O runbook `AWSConfigRemediation-EnablePITRForDynamoDbTable` habilita a recuperação para um ponto no tempo (PITR) na tabela do Amazon DynamoDB que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- TableName

  Tipo: sequência

  Descrição: (obrigatório) o nome da tabela do DynamoDB para habilitar a recuperação para um ponto no tempo.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `dynamodb:UpdateContinuousBackups`

Etapas do documento

- `aws:executeAwsApi`: permite a recuperação pontual na tabela do DynamoDB que você especifica no parâmetro `TableName`.
- `aws:assertAwsResourceProperty`: confirma que a recuperação em um ponto anterior no tempo está habilitada na tabela do DynamoDB.

AWS-EnableDynamoDbAutoscaling

Descrição

O `AWS-EnableDynamoDbAutoscaling` runbook habilita o Application Auto Scaling para a tabela de capacidade provisionada do Amazon DynamoDB que você especificar. O Application Auto Scaling ajusta dinamicamente a capacidade de transferência provisionada em resposta aos padrões de tráfego. Para obter mais informações, consulte Gerenciamento automático da capacidade de transferência com o auto scaling do DynamoDB no Amazon DynamoDB Developer Guide.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- TableName

  Tipo: sequência

  Descrição: (Obrigatório) O nome da tabela do DynamoDB na qual você deseja ativar o Application Auto Scaling.
- MinReadCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número mínimo de unidades de capacidade de leitura de throughput provisionadas para a tabela do DynamoDB.
- MaxReadCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número máximo de unidades de capacidade de leitura de throughput provisionadas para a tabela do DynamoDB.
- TargetReadCapacityUtilization

  Tipo: inteiro

  Descrição: (Obrigatório) A meta de utilização da capacidade de leitura desejada. A meta de utilização é a porcentagem da taxa de transferência provisionada consumida em um determinado momento. Você pode definir os valores de utilização alvo do auto scaling entre 20 e 90 por cento.
- ReadScaleOutCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo, em segundos, de espera até que uma atividade anterior de expansão da capacidade de leitura entre em vigor.
- ReadScaleInCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo em segundos após a conclusão de uma atividade de expansão da capacidade de leitura antes que outra atividade de expansão possa ser iniciada.
- MinWriteCapacity

  Tipo: inteiro

Descrição: (Obrigatório) O número mínimo de unidades de gravação de taxa de transferência provisionadas para a tabela do DynamoDB.

- MaxWriteCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número máximo de unidades de gravação de taxa de transferência provisionadas para a tabela do DynamoDB.

- TargetWriteCapacityUtilization

  Tipo: inteiro

  Descrição: (Obrigatório) A utilização desejada da capacidade de gravação. A meta de utilização é a porcentagem da taxa de transferência provisionada consumida em um determinado momento. Você pode definir os valores de utilização alvo do auto scaling entre 20 e 90 por cento.

- WriteScaleOutCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo, em segundos, de espera até que uma atividade anterior de expansão da capacidade de gravação entre em vigor.

- WriteScaleInCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo em segundos após a conclusão de uma atividade de expansão da capacidade de gravação antes que outra atividade de expansão possa ser iniciada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `application-autoscaling:PutScalingPolicy`
- `application-autoscaling:RegisterScalableTarget`

- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi) - Configura o Application Auto Scaling na tabela do DynamoDB que você especificar.
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep) - Dorme para evitar a limitação da API.
- PutScalingPolicyWrite (aws:executeAwsApi) - Configura a utilização da capacidade de gravação de destino para a tabela do DynamoDB.
- PutScalingPolicyWriteDelay (aws:sleep) - Dorme para evitar a limitação da API.
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi) - Configura as unidades de capacidade mínima e máxima de leitura para a tabela do DynamoDB.
- RegisterAppAutoscalingTargetReadDelay (aws:sleep) - Dorme para evitar a limitação da API.
- PutScalingPolicyRead (aws:executeAwsApi) - Configura a meta de utilização da capacidade de leitura para a tabela do DynamoDB.
- VerifyDynamoDbAutoscalingEnabled (aws:ExecuteScript) — Verifica se o Application Auto Scaling está habilitado para a tabela do DynamoDB de acordo com os valores que você especificar.

Saídas

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

AWS-RestoreDynamoDBTable

Descrição

O runbook `AWS-RestoreDynamoDBTable` restaura a tabela do Amazon DynamoDB que você especifica usando a recuperação para um ponto no tempo (PITR).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EnablePointInTimeRecoverAsNeeded

  Tipo: booliano

  Padrão: true

  Descrição: (opcional) determina se a automação ativa a recuperação pontual conforme necessário para restaurar a tabela.
- GlobalSecondaryIndexOverride

  Tipo: sequência

  Descrição: (opcional) os novos índices secundários globais para substituir os índices secundários existentes na nova tabela.
- LocalSecondaryIndexOverride

  Tipo: sequência

  Descrição: (opcional) os novos índices secundários locais para substituir os índices secundários existentes na nova tabela.
- RestoreDateTime

Tipo: sequência

Descrição: (obrigatório) a recuperação pontual para a qual você deseja restaurar a tabela durante os últimos 35 dias. Especifique a data e a hora no seguinte formato: `DD/MM/YYYY HH:MM:SS`

- SourceTableArn

  Tipo: sequência

  Descrição: (obrigatório) o ARN da tabela que deseja restaurar.

- SseSpecificationOverride

  Tipo: sequência

  Descrição: (opcional) as configurações de criptografia do lado do servidor a serem usadas na nova tabela.

- TargetTableName

  Tipo: sequência

  Descrição: (obrigatório) o nome da tabela a ser restaurada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: restaura a tabela do DynamoDB que você especifica no parâmetro `TargetTableName` usando a recuperação pontual.

Amazon EBS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Block Store. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSSupport-AnalyzeEBSResourceUsage`

Descrição

O runbook de `AWSSupport-AnalyzeEBSResourceUsage` automação é usado para analisar o uso de recursos no Amazon Elastic Block Store (Amazon EBS). Ele analisa o uso do volume e identifica volumes, imagens e instantâneos abandonados em uma determinada região. AWS

Como funciona?

O runbook executa as quatro tarefas a seguir:

1. Verifica se existe um bucket do Amazon Simple Storage Service (Amazon S3) ou cria um novo bucket do Amazon S3.
2. Reúne todos os volumes do Amazon EBS no estado disponível.
3. Reúne todos os snapshots do Amazon EBS cujo volume de origem foi excluído.
4. Reúne todas as Amazon Machine Images (AMIs) que não estão em uso por nenhuma instância não encerrada do Amazon Elastic Compute Cloud (Amazon EC2).

O runbook gera relatórios CSV e os armazena em um bucket Amazon S3 fornecido pelo usuário. O bucket fornecido deve ser protegido seguindo as melhores práticas de AWS segurança, conforme descrito no final. Se o bucket do Amazon S3 fornecido pelo usuário não existir na conta, o runbook cria um novo bucket do Amazon S3 com o formato do nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma chave personalizada AWS Key Management Service (AWS KMS), com o controle de versão do objeto ativado, acesso público bloqueado e exige solicitações para usar SSL/TLS.

Se você quiser especificar seu próprio bucket do Amazon S3, certifique-se de que ele esteja configurado de acordo com estas melhores práticas:

- Bloqueie o acesso público `IsPublic` ao bucket (definido como`False`).
- Ative o registro de acesso ao Amazon S3.
- Permita somente solicitações SSL em seu bucket.
- Ative o controle de versão de objetos.
- Use uma chave AWS Key Management Service (AWS KMS) para criptografar seu bucket.

> **Important**
>
> O uso desse runbook pode gerar cobranças adicionais em sua conta pela criação de buckets e objetos do Amazon S3. Consulte os preços do Amazon S3 para obter mais detalhes sobre as cobranças que podem ocorrer.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- S3 BucketName

  Tipo: `AWS::S3::Bucket::Name`

  Descrição: (Obrigatório) O bucket do Amazon S3 em sua conta para fazer o upload do relatório. Certifique-se de que a política de bucket não conceda permissões desnecessárias de leitura/gravação a partes que não precisam acessar os registros coletados. Se o intervalo especificado não existir na conta, a automação cria um novo intervalo na região em que a automação é iniciada com o formato do nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma AWS KMS chave personalizada.

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

  Tipo: string

  Descrição: (Opcional) A AWS KMS chave personalizada Amazon Resource Name (ARN) para criptografar o novo bucket do Amazon S3 que será criado se o bucket especificado não existir na conta. A automação falhará se a criação do bucket for tentada sem especificar um ARN de AWS KMS chave personalizada.

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

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Exemplo de política com permissões mínimas exigidas do IAM para executar este runbook:

```
{
    "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:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/"
                ]
            }, {
                "Sid": "S3_Create_Permissions",
                "Effect": "Allow",
                "Action": [
                    "s3:CreateBucket",
                    "s3:PutObject",
                    "s3:PutBucketLogging",
                    "s3:PutBucketPolicy",
                    "s3:PutBucketPublicAccessBlock",
                    "s3:PutBucketTagging",
                    "s3:PutBucketVersioning",
                    "s3:PutEncryptionConfiguration"
                ],
                "Resource": "*"
            }]
```

```
        }
```

Instruções

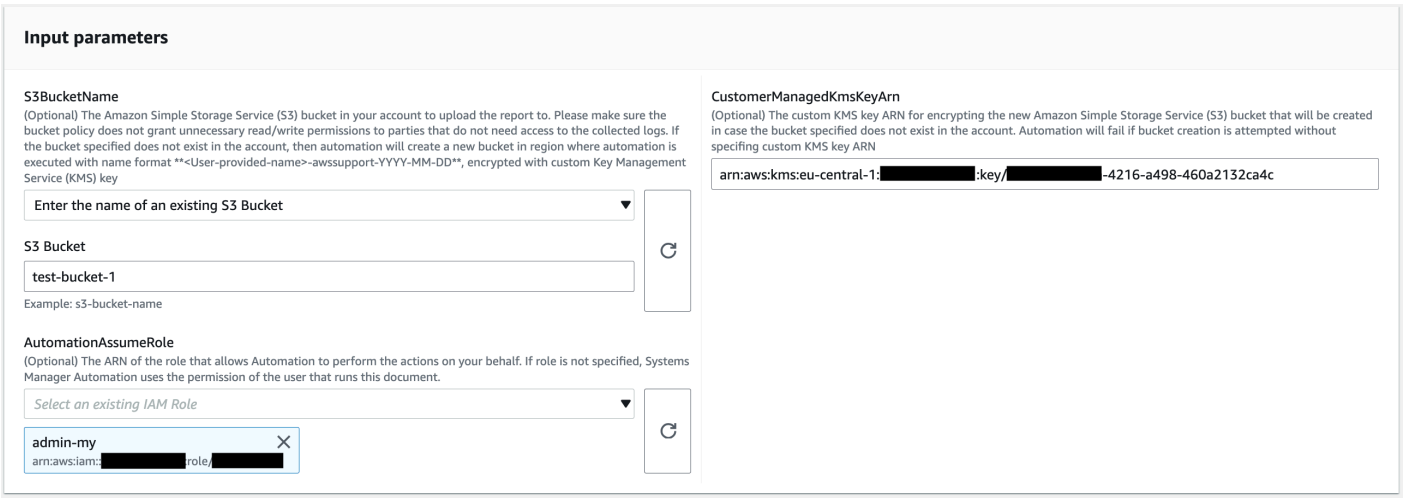
Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-AnalyzeEBS no console. ResourceUsage AWS Systems Manager
2. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - S3 BucketName (obrigatório):

     O bucket do Amazon S3 em sua conta para fazer o upload do relatório.
   - CustomerManagedKmsKeyArn (Opcional):

     A AWS KMS chave personalizada Amazon Resource Name (ARN) para criptografar o novo bucket do Amazon S3 que será criado se o bucket especificado não existir na conta.



3. Selecione Executar.
4. A automação é iniciada.
5. O runbook de automação realiza as seguintes etapas:
   - Verifique a simultaneidade:

Garante que haja apenas uma iniciação desse runbook na região. Se o runbook encontrar outra execução em andamento, ele retornará um erro e terminará.

- verifyOrCreateCaçamba S3:

  Verifica se o bucket do Amazon S3 existe. Caso contrário, ele cria um novo bucket do Amazon S3 na região onde a automação é iniciada com o formato de nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma chave personalizadaAWS KMS.

- gatherAmiDetails:

  A pesquisa por AMIs, que não estão em uso por nenhuma instância do Amazon EC2, gera o relatório com o `<region>-images.csv` formato do nome e o carrega no bucket do Amazon S3.

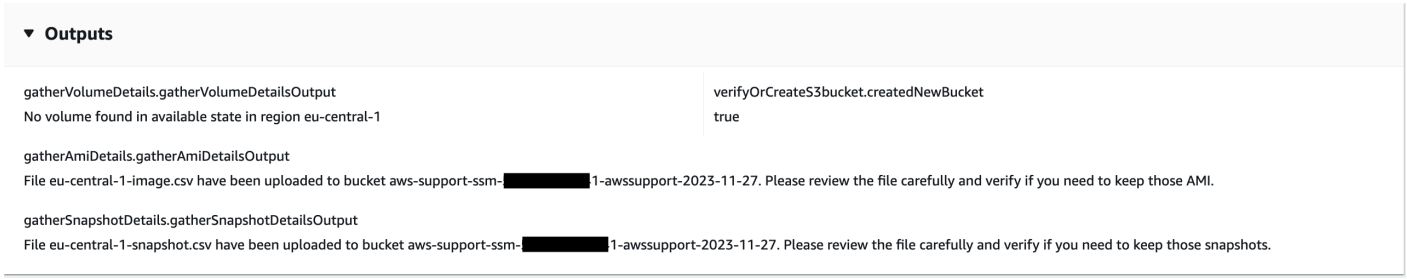
- gatherVolumeDetails:

  Verifica os volumes do Amazon EBS no estado disponível, gera o relatório com o formato `<region>-volume.csv` do nome e o carrega em um bucket do Amazon S3.

- gatherSnapshotDetails:

  Procura os snapshots do Amazon EBS dos volumes do Amazon EBS que já foram excluídos, gera o relatório com o formato `<region>-snapshot.csv` do nome e o carrega no bucket do Amazon S3.

6. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação

- Página inicial dos fluxos de trabalho de automação

AWS-ArchiveEBSSnapshots

Descrição

O runbook da `AWS-ArchiveEBSSnapshots` ajuda a arquivar snapshots para volumes do Amazon Elastic Block Store (Amazon EBS), especificando a tag que foi aplicada aos snapshots. Como alternativa, você pode fornecer o ID de um volume se os seus snapshots estiverem sem tags.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Descrição

  Tipo: string

  Descrição: (opcional) uma descrição para o snapshot da Amazon EBS.
- DryRun

  Tipo: string

Valores válidos: sim | não

Descrição: (obrigatório) verifica se você tem as permissões necessárias para a ação, sem realmente fazer a solicitação, e fornece uma resposta de erro.

- RetentionCount

  Tipo: string

  Descrição: (opcional) o número de snapshots que você deseja arquivar. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetentionDays`.

- RetentionDays

  Tipo: string

  Descrição: (opcional) o número de dias anteriores de snapshots que você deseja arquivar. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetentionCount`.

- SnapshotWithTag

  Tipo: string

  Valores válidos: sim | não

  Descrição: (obrigatório) especifica se os snapshots que deseja arquivar estão marcados.

- TagKey

  Tipo: string

  Descrição: (opcional) a chave da tag atribuída aos snapshots que deseja arquivar.

- TagValue

  Tipo: string

  Descrição: (opcional) o valor da tag atribuída aos snapshots que deseja arquivar.

- VolumeId

  Tipo: string

  Descrição: (opcional) o ID do volume cujos snapshots deseja arquivar. Use esse parâmetro se os snapshots não estiverem marcados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

`aws:executeScript`: arquiva os snapshots usando a tag especificada usando os parâmetros `TagKey` e `TagValue` ou o parâmetro do `VolumeId`.

AWS-AttachEBSVolume

Descrição

Anexar um volume do Amazon Elastic Block Store (Amazon EBS) a uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Dispositivo

  Tipo: string

  Descrição: (obrigatório) o nome do dispositivo (por exemplo, /dev/sdh ou xvdh).
- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância à qual você deseja associar o volume.
- VolumeId

  Tipo: string

  Descrição: (obrigatório) o ID do volume do Amazon EBS. O volume e a instância devem estar na mesma zona de disponibilidade.

AWSSupport-CalculateEBSPerformanceMetrics

Descrição

O `AWSSupport-CalculateEBSPerformanceMetrics` runbook ajuda a diagnosticar problemas de desempenho do Amazon EBS calculando e publicando métricas de desempenho em um painel. CloudWatch O painel exibe a média estimada de IOPS e a taxa de transferência de um volume alvo do Amazon EBS ou de todos os volumes anexados à instância de destino do Amazon Elastic Compute Cloud (Amazon EC2). Para instâncias do Amazon EC2, ele também mostra a média de IOPS e a taxa de transferência da instância. O runbook gera o link para o CloudWatch painel recém-criado que exibe as métricas calculadas CloudWatch relevantes. O CloudWatch painel é criado em sua conta com o nome:`AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

Como funciona?

O runbook executa as seguintes etapas:

- Garante que os carimbos de data/hora especificados sejam válidos.
- Valida se o ID do recurso (volume do Amazon EBS ou instância do Amazon EC2) é válido.
- Quando você fornece um Amazon EC2 como ResourceID, ele cria um CloudWatch painel com o total real de IOPs/taxa de transferência para essa instância do Amazon EC2 e um gráfico de média

estimada de IOPs/taxa de transferência para todos os volumes do Amazon EBS anexados a uma instância do Amazon EC2.

- Quando você fornece um volume do Amazon EBS como um ResourceID, ele cria CloudWatch um painel com gráfico de IOPS/taxa de transferência média estimada para esse volume.
- Depois que o CloudWatch painel for gerado, se a média estimada de IOPS ou a taxa de transferência média estimada for maior que a IOPS máxima ou a taxa de transferência máxima, respectivamente, o microbursting será possível para o volume ou volumes anexados a uma instância do Amazon EC2.

> **Note**
>
> Para volumes com capacidade de intermitência (gp2, sc2 e st1), o máximo de IOPs/throughput deve ser considerado até que você tenha um equilíbrio de intermitência. Depois que o equilíbrio de ruptura for completamente utilizado, ou seja, se tornar zero, considere as métricas básicas de IOPS/taxa de transferência.

> **Important**
>
> A criação CloudWatch do painel pode resultar em cobranças extras em sua conta. Para obter mais informações, consulte o guia de CloudWatch preços da Amazon.

Execute esta automação (console)

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Política de amostra

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-CalculateEBSPerformanceMetricsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - ResourceID (obrigatório):

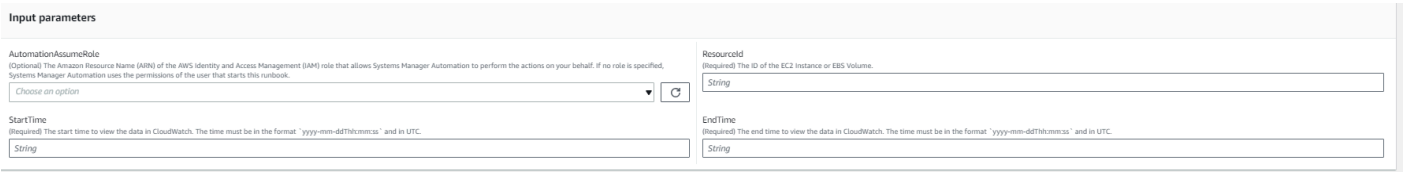
     O ID da instância do Amazon EC2 ou do volume do Amazon EBS.

- Hora de início (obrigatório):

  A hora de início para visualizar os dados CloudWatch. A hora deve estar no formato `yyyy-mm-ddThh:mm:ss` e em UTC.

- Hora de término (obrigatório):

  A hora de término para visualizar os dados CloudWatch. A hora deve estar no formato `yyyy-mm-ddThh:mm:ss` e em UTC.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckResourceIdAndTimeStamps:

     Verifica se a hora de término é maior que a hora de início em pelo menos um minuto e se o recurso fornecido existe.

   - CreateCloudWatchDashboard:

     Calcula o desempenho do Amazon EBS e exibe um gráfico com base no seu ID de recurso. Se você fornecer um ID de volume do Amazon EBS para o parâmetro Resource ID, esse runbook cria um painel com IOPS médio estimado e taxa de transferência média estimada para o volume do Amazon EBS. Se você fornecer um ID de instância do Amazon EC2 para o parâmetro Resource ID, esse runbook cria um CloudWatch painel com média total de IOPS e taxa de transferência total média para a instância do Amazon EC2 e com média estimada de IOPS e taxa de transferência média estimada para todos os volumes do Amazon EBS vinculados à instância do Amazon EC2.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

Exemplo de CloudWatch painel para ID de recurso como instância do Amazon EC2

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

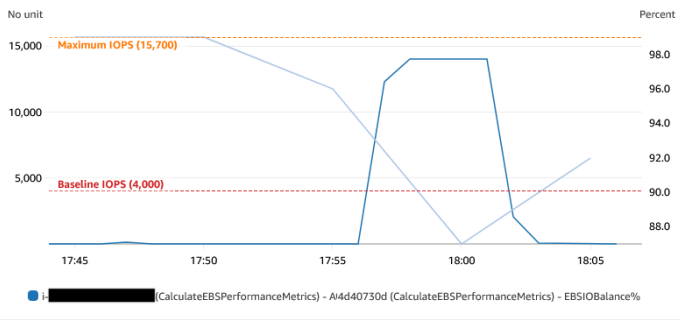
More details on EBS Optimized instances | More details on EBS Volume Types

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

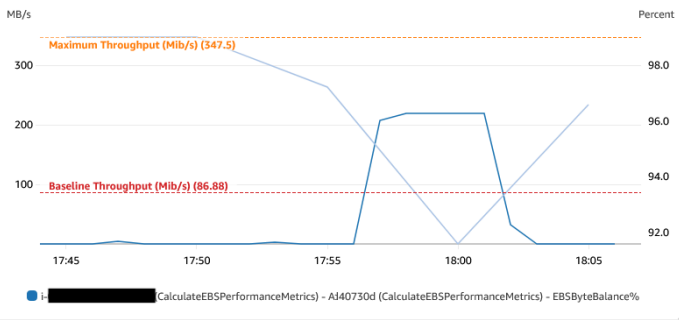
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

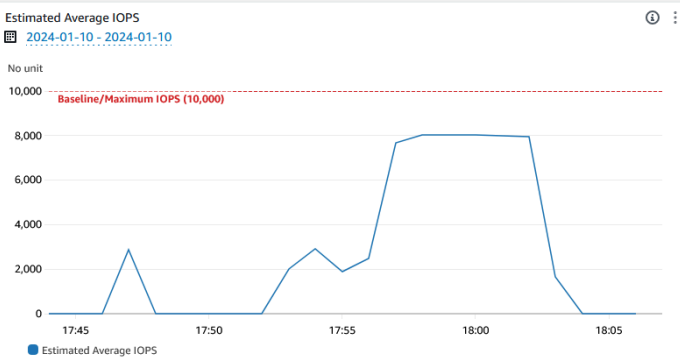
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

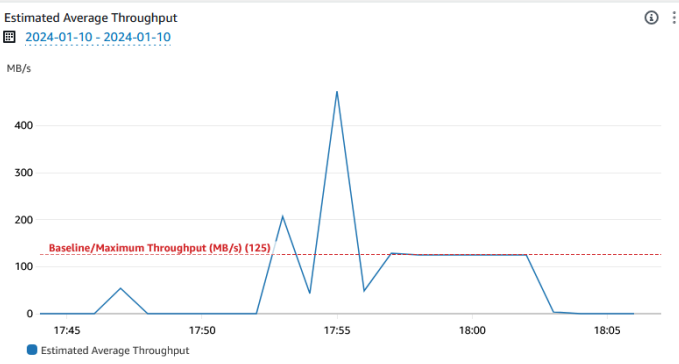
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

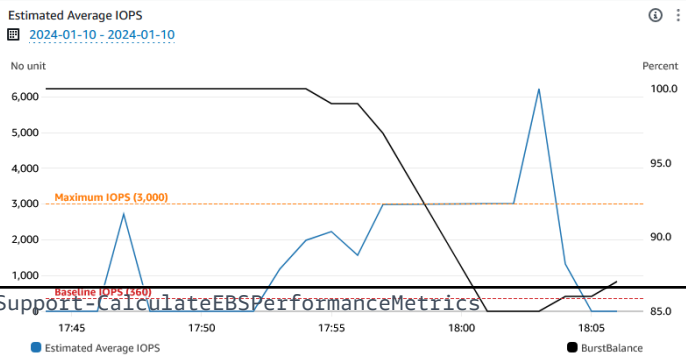


Estimated Average Throughput
2024-01-10 - 2024-01-10

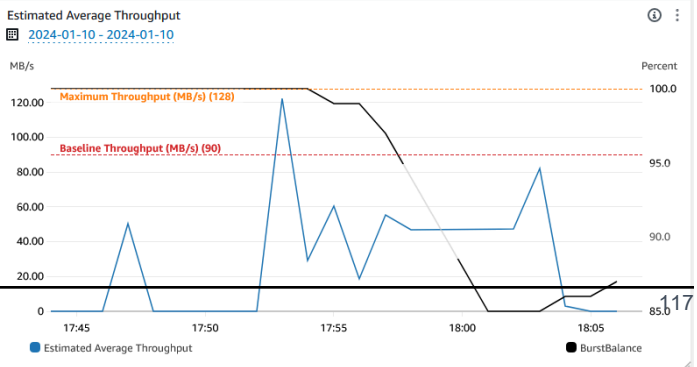


Volume: vol[redacted] | Type: gp2

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



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

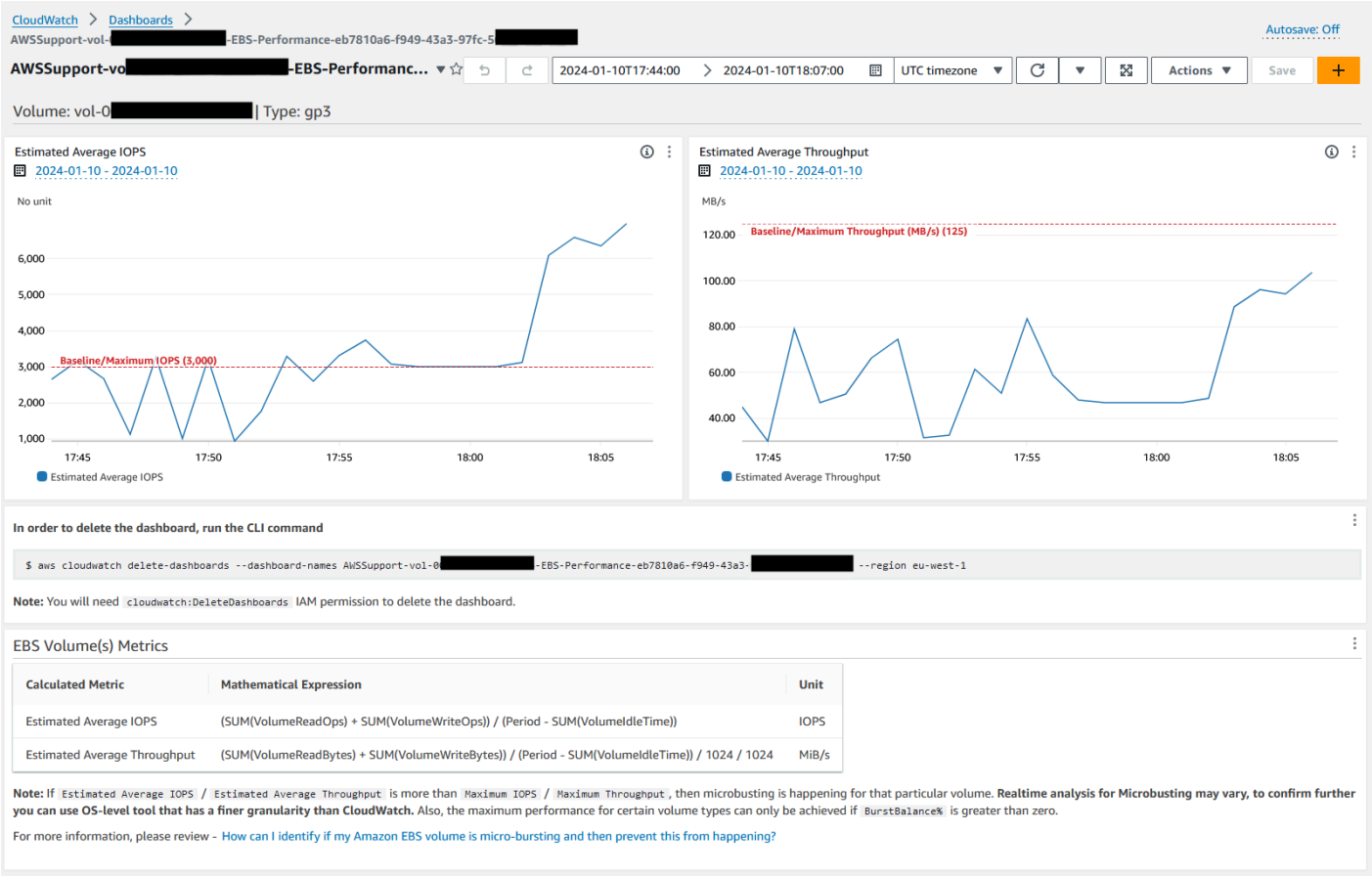


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

Exemplo de CloudWatch painel para ID de recurso como ID de volume do Amazon EBS



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSDocumentação do serviço

- Como posso identificar se meu volume do Amazon EBS está microestourando e, em seguida, evitar que isso aconteça?
- Como faço CloudWatch para visualizar as métricas agregadas de desempenho do Amazon EBS para uma instância do EC2?

AWS-CopySnapshot

Descrição

Copia um point-in-time snapshot de um volume do Amazon Elastic Block Store (Amazon EBS). Você pode copiar o instantâneo dentro da mesma região Região da AWS ou de uma região para outra. Cópias de snapshots criptografados do Amazon EBS permanecem criptografadas. Cópias de snapshots não criptografados permanecem não criptografadas. Para copiar um snapshot criptografado que foi compartilhado de outra conta, é necessário ter permissões para a chave KMS usada para criptografar o snapshot. Os snapshots criados ao copiar outro snapshot têm um ID arbitrário de volume que não deve ser usado para nenhuma outra finalidade.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Descrição

  Tipo: string

  Descrição: (opcional) uma descrição para o snapshot da Amazon EBS.
- SnapshotId

Tipo: string

Descrição: (obrigatório) o ID do snapshot do Amazon EBS a ser copiado.

- SourceRegion

  Tipo: string

  Descrição: (obrigatório) a região em que o snapshot de origem existe atualmente.

Etapas do documento

copySnapshot: Copia um snapshot de um volume do Amazon EBS.

Saídas

Copiar Snapshot. SnapshotId - O ID do novo instantâneo.

AWS-CreateSnapshot

Descrição

Criar um snapshot de um volume do Amazon EBS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Descrição

  Tipo: string

  Description: (opcional) uma descrição para o snapshot

- VolumeId

  Tipo: string

  Descrição: (obrigatório) o ID do volume.

AWS-DeleteSnapshot

Descrição

Excluir um snapshot de um volume do Amazon EBS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- SnapshotId

  Tipo: string

  Descrição: (obrigatório) o ID do snapshot do EBS.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedEBSVolume` exclui um volume não utilizado do Amazon Elastic Block Store (Amazon EBS).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CreateSnapshot

  Tipo: booliano

  Descrição: (opcional) se configurada como `true`, a automação cria um snapshot do volume do Amazon EBS antes de ser excluído.

- VolumeId

  Tipo: string

  Descrição: (obrigatório) o ID do volume do Amazon EBS que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: verifica se o volume do Amazon EBS especificado no parâmetro `VolumeId` não está em uso e cria um snapshot dependendo do valor escolhido para o parâmetro `CreateSnapshot`.
- `aws:branch`: ramifica com base no valor escolhido para o parâmetro `CreateSnapshot`.
- `aws:waitForAwsResourceProperty`: aguarda a conclusão do snapshot.
- `aws:executeAwsApi`: exclui o snapshot se a criação do snapshot falhar.
- `aws:executeAwsApi`: exclui o volume do Amazon EBS que foi especificado no parâmetro `VolumeId`.
- `aws:executeScript`: verifica se o volume do Amazon EBS foi excluído.

AWS-DeregisterAMIs

Descrição

O runbook `AWS-DeregisterAMIs` ajuda a cancelar o registro de Amazon Machine Images (AMIs) especificando a tag que foi aplicada ao AMIs.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DryRun

  Tipo: string

  Valores válidos: sim | não

  Descrição: (obrigatório) verifica se você tem as permissões necessárias para a ação, sem realmente fazer a solicitação, e fornece uma resposta de erro.
- RetainNumber

  Tipo: string

Descrição: (opcional) o número de AMIs que você deseja reter. Não especifique um valor para esse parâmetro se foi especificado um valor para `Age`.

- Idade

  Tipo: string

  Descrição: (opcional) o número de dias anteriores de AMIs que você deseja reter. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetainNumber`.

- TagKey

  Tipo: string

  Descrição: (obrigatório) a chave da tag atribuída à AMIs que você deseja cancelar o log.

- TagValue

  Tipo: string

  Descrição: (obrigatório) o valor da tag atribuída à AMIs que você deseja cancelar o log.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: valida os valores que foram especificados para os parâmetros de entrada do runbook.
- `aws:executeAwsApi` :cancela o log de AMIs usando a tag que foi especificada usando os parâmetros `TagKey` e `TagValue`.

AWS-DetachEBSVolume

Descrição

Separar um volume do Amazon EBS de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função assumida pelo lambda
- VolumeId

  Tipo: string

  Descrição: (obrigatório) o ID do volume do EBS. O volume e a instância devem estar na mesma zona de disponibilidade

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descrição

O `AWSConfigRemediation-EnableEbsEncryptionByDefault` runbook permite a criptografia em todos os novos volumes do Amazon Elastic Block Store (Amazon EBS) no Amazon Elastic Block Store (Amazon EBS) Conta da AWS e Região da AWS onde você executa a automação. Os volumes criados antes de executar a automação não são criptografados.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi` :Habilita a definição padrão de criptografia do Amazon EBS na conta atual e na região.
- `aws:assertAwsResourceProperty` :Verifica se a definição padrão de criptografia do Amazon EBS foi habilitada.

AWS-ExtendEbsVolume

Descrição

O runbook `AWS-ExtendEbsVolume` aumenta o tamanho de um volume do Amazon EBS e estende o sistema de arquivos. Essa automação oferece suporte aos sistemas de arquivos `xfs` e `ext4`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DriveLetter

  Tipo: string

Descrição: (opcional) A letra da unidade cujo sistema de arquivos você deseja estender. Esse parâmetro é obrigatório para instâncias do Windows.

- InstanceId

  Tipo: string

  Descrição: (opcional) O ID da instância do Amazon EC2 à qual o volume do Amazon EBS a ser estendido está anexado.

- KeepSnapshot

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Determina se o snapshot criado deve ser mantido antes de aumentar o tamanho do volume do Amazon EBS.

- MountPoint

  Tipo: string

  Descrição: (opcional) O ponto de montagem da unidade cujo sistema de arquivos você deseja estender. Esse parâmetro é necessário para instâncias do Linux.

- SizeGib

  Tipo: string

  Descrição: (obrigatório) O tamanho em GiB para o qual deseja modificar seu volume do Amazon EBS.

- VolumeId

  Tipo: string

  Descrição: (obrigatório) O ID do volume do EBS que você deseja estender.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:CreateSnapshot`

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

Etapas do documento

- `aws:executeScript` :Aumenta o tamanho do volume até o valor especificado no parâmetro do `VolumeId` e estende o sistema de arquivos.

AWSSupport-ModifyEBSSnapshotPermission

Descrição

O runbook `AWSSupport-ModifyEBSSnapshotPermission` ajuda a modificar permissões para vários snapshots do Amazon Elastic Block Store (Amazon EBS). Usando este runbook, você pode criar snapshots `Public` ou `Private` e compartilhá-los com outras Contas da AWS. Os snapshots criptografados com uma chave KMS padrão não podem ser compartilhados com outras contas usando este runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AccountIds

  Tipo: StringList

  Padrão: nenhum

  Descrição: (opcional) Os IDs das contas com as quais deseja compartilhar os snapshots. Esse parâmetro será necessário se um valor `No` for especificado para o parâmetro `Private`.

- AccountPermissionOperation

  Tipo: string

  Valores válidos: add | remove

  Padrão: nenhum

  Descrição: (opcional) O tipo de operação a ser executada.

- Privado

  Tipo: string

  Valores válidos: sim | não

  Descrição: (obrigatório) Insira o valor `No` se quiser compartilhar snapshots com contas específicas.

- SnapshotIds

  Tipo: StringList

  Descrição: (obrigatório) Os IDs dos snapshots do Amazon EBS cuja permissão você deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

1. `aws:executeScript` :Verifica os IDs dos snapshots fornecidos no parâmetro `SnapshotIds`. Depois de verificar os IDs, o script verifica se há snapshots criptografados e gera uma lista, se algum for encontrado.
2. `aws:branch` :Ramifica a automação com base no valor inserido para o parâmetro `Private`.
3. `aws:executeScript` :Modifica as permissões dos snapshots especificados para compartilhá-los com as contas especificadas.
4. `aws:executeScript` :Modifica as permissões dos snapshots para alterá-los de `Public` para `Private`.

Saídas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSConfigRemediation-ModifyEBSVolumeType

Descrição

O runbook `AWSConfigRemediation-ModifyEBSVolumeType` modifica o tipo de volume do Amazon Elastic Block Store (Amazon EBS). Depois que o tipo de volume é modificado, o volume entra no estado `optimizing`. Para obter mais informações sobre monitoração do progresso das modificações de volumes, consulte Monitorar o progresso das modificações de volumes no Guia do usuário do Amazon EC2 para instâncias do Linux.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EbsVolumeId

  Tipo: string

  Descrição: (obrigatório) O ID do volume do Amazon EBS que deseja modificar.
- EbsVolumeType

  Tipo: string

  Valores válidos: standart | io1 | io2 | gp2 | gp3 | sc1 | st1

  Descrição: O tipo de volume para o qual deseja alterar o volume do Amazon EBS. Para obter mais informações sobre cada tipo de volume do Amazon EBS, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:waitForAwsResourceProperty` :Verifica se o estado do volume é `available` ou `in-use`.
- `aws:executeAwsApi` :Modifica o volume do Amazon EBS especificado no parâmetro de `EbsVolumeId`.
- `aws:waitForAwsResourceProperty` :Verifica se o tipo do volume foi alterado para o valor especificado no parâmetro de `EbsVolumeType`.

Amazon EC2

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Compute Cloud. Os runbooks do Amazon Elastic Block Store estão localizados na seção Amazon EBS de referência do runbook. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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

Descrição

Altere o estado de espera de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em um grupo do Auto Scaling.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatória) o ID de uma instância do Amazon EC2 para a qual você deseja alterar o estado de espera em um grupo do Auto Scaling.

- LambdaRoleArn

  Tipo: sequência

  Descrição: (Opcional) O ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

AWS-ASGExitStandby

Descrição

Altere o estado de espera de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em um grupo do Auto Scaling.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatória) o ID de uma instância do EC2 para a qual você deseja alterar o estado de espera em um grupo do Auto Scaling.

- LambdaRoleArn

  Tipo: sequência

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

AWS-CreateImage

Descrição

Inicia uma nova Amazon Machine Image (AMI) de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatória) o ID da instância do EC2.
- NoReboot

  Tipo: booliano

  Descrição: (opcional) Não reinicialize a instância antes de criar a imagem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

```
}
```

AWS-DeleteImage

Descrição

Exclua uma Amazon Machine Image (AMI) e todos os instantâneos associados.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ImageId

  Tipo: sequência

  Descrição: (obrigatório) O ID do AMI.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

```
{
```

```
    "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

Descrição

Aplique patch em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um grupo do Auto Scaling.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: sequência

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância onde o patch será aplicado. Não especifique um ID de instância que está configurado para ser executado durante uma janela de manutenção.

- LambdaRoleArn

  Tipo: sequência

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função do Lambda.

- WaitForInstance

  Tipo: sequência

  Padrão: PT2M

  Descrição: (opcional) duração que a Automação deve dormir para permitir que a instância volte ao serviço.

- WaitForReboot

  Tipo: sequência

  Padrão: PT5M

  Descrição: (opcional) duração que a Automação deve dormir para permitir que uma instância com patch reinicialize.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Descrição

Coloca uma instância do EC2 em conformidade com a lista de referência de patches aplicável. Reverte o volume raiz em caso de falha.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) InstanceId do EC2 ao qual aplicamos a linha de base do patch.
- LambdaAssumeRole

  Tipo: sequência

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- ReportS3Bucket

  Tipo: sequência

  Descrição: (opcional) destino de bucket do Amazon S3 para o relatório de conformidade gerado durante o processo.

Etapas do documento

Número da etapa	Nome da etapa	Ação de Automação
1	createDocumentStack	`aws:createStack`
2	IdentifyRootVolume	`aws:invokeLambdaFunction`
3	PrePatchSnapshot	`aws:executeAutomation`
4	installMissingUpdates	`aws:runCommand`
5	SleepThruInstallation	`aws:invokeLambdaFunction`
6	CheckCompliance	`aws:invokeLambdaFunction`
7	SaveComplianceReportToS3	`aws:invokeLambdaFunction`
8	ReportSuccessOrFailure	`aws:invokeLambdaFunction`
9	RestoreFromSnapshot	`aws:invokeLambdaFunction`
10	DeleteSnapshot	`aws:invokeLambdaFunction`
11	deleteCloudFormationTemplate	`aws:deleteStack`

Saídas

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

AWS-QuarantineEC2Instance

Descrição

Com o runbook `AWS-QuarantineEC2Instance`, é possível atribuir um grupo de segurança a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que não permite nenhum tráfego de entrada ou saída.

> **Important**
>
> As alterações nas configurações do RDP devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID da instância gerenciada para gerenciar as configurações de RDP.

- IsolationSecurityGroup

  Tipo: sequência

  Descrição: (obrigatório) o nome do grupo de segurança que você deseja atribuir à instância para evitar tráfego de entrada ou saída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: reúne detalhes sobre a instância.
- `aws:executeScript`: verifica se a instância não faz parte de um grupo do Auto Scaling.
- `aws:executeAwsApi`: cria um snapshot do novo volume raiz anexado à instância.
- `aws:waitForAwsResourceProperty`: espera que o estado do instantâneo seja `completed`.

- `aws:executeAwsApi`: atribui o grupo de segurança especificado no parâmetro `IsolationSecurityGroup` à sua instância.

Saídas

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Descrição

Altere o tipo de instância de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) O ID da instância.
- InstanceType

  Tipo: sequência

  Descrição: (obrigatório) O tipo de instância.
- LambdaAssumeRole

  Tipo: sequência

  Descrição: (opcional) o ARN da função assumida pelo lambda.

AWS-RestartEC2Instance

Descrição

Reiniciar uma ou mais Instâncias do Amazon Elastic Compute Cloud (Amazon EC2)

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: StringList

  Descrição: (obrigatório) os IDs da instância do Amazon EC2 para reiniciar.

AWS-SetupJupyter

Descrição

O runbook `AWS-SetupJupyter` ajuda a configurar o caderno Jupyter em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você pode especificar uma instância existente ou fornecer um ID Amazon Machine Image (AMI) para que a automação inicie e configure uma nova instância. Antes de começar, é necessário criar um parâmetro `SecureString` no repositório de parâmetros para usar como senha do caderno Jupyter. O repositório de parâmetros é uma capacidade do AWS Systems Manager. Para obter mais informações sobre criação de parâmetro, consulte Criação de parâmetros no Guia do usuário do AWS Systems Manager.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AmiId

  Tipo: String

  Descrição: (opcional) o ID do AMI que você deseja usar para iniciar uma nova instância e configurar o caderno Jupyter.

- InstanceId

  Tipo: String

  Descrição: (obrigatório) o ID da instância do caderno Jupyter que você deseja reinicializar.

- InstanceType

  Tipo: String

  Padrão: t3.medium

  Descrição: (opcional) se você estiver iniciando uma nova instância para configurar o caderno Jupyter, especifique o tipo de instância que deseja usar.

- JupyterPasswordSSMKey

  Tipo: String

  Descrição: (obrigatório) o nome do parâmetro `SecureString` no repositório de parâmetros que você deseja usar como senha para o caderno Jupyter.

- KeyPairName

  Tipo: String

  Descrição: (opcional) o par de chaves que você deseja associar à instância recém-iniciada.

- RemoteAccessCidr

  Tipo: String

Padrão: 0.0.0.0/0

Descrição: (opcional) o intervalo CIDR do qual você deseja permitir o tráfego SSH.

- RoleName

  Tipo: String

  Padrão: SSMManagedInstanceProfileRole

  Descrição: (opcional) o nome do perfil da instância recém-iniciada.

- StackName

  Tipo: String

  Padrão: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  Descrição: (opcional) o nome da pilha do AWS CloudFormation que você deseja que a automação use.

- SubnetId

  Tipo: String

  Padrão: Default

  Descrição: (opcional) a sub-rede na qual você deseja iniciar a nova instância para usar.

- VpcId

  Tipo: String

  Padrão: Default

  Descrição: (opcional) o ID da nuvem privada virtual (VPC) na qual você deseja iniciar a nova instância.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeScript: configura o caderno Jupyter na instância especificada ou em uma instância recém-lançada, usando os valores que você especifica para os parâmetros de entrada do runbook.

AWS-StartEC2Instance

Descrição

Iniciar uma ou mais Instâncias do Amazon Elastic Compute Cloud (Amazon EC2)

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: StringList

  Descrição: (obrigatória) instâncias do EC2 a serem iniciadas.

AWS-StopEC2Instance

Descrição

Interromper uma ou mais instâncias do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: StringList

  Descrição: (obrigatório) instâncias do EC2 a serem interrompidas.

AWS-TerminateEC2Instance

Descrição

Encerrar uma ou mais instâncias do Amazon Elastic Compute Cloud (Amazon EC2).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: StringList

  Descrição: (obrigatório) IDs de uma ou mais instâncias do EC2 a serem encerradas.

AWS-UpdateLinuxAmi

Descrição

Atualizar uma Amazon Machine Image (AMI) com pacotes de distribuição Linux e softwares da Amazon.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ExcludePackages

  Tipo: string

  Padrão: nenhum

  Descrição: (Opcional) Nomes de pacotes para evitar atualizações, em todas as condições. Por padrão ("none"), nenhum pacote é excluído.

- IamInstanceProfileName

  Tipo: string

  Padrão: ManagedInstanceProfile

  Descrição: (obrigatório) o nome do perfil de instância que permite que o Systems Manager gerencie a instância.

- IncludePackages

  Tipo: string

  Padrão: all

  Descrição: (Opcional) Somente atualiza esses pacotes nomeados. Por padrão ("all"), todas as atualizações disponíveis são aplicadas.

- InstanceType

  Tipo: string

  Padrão: t2.micro

  Descrição: (Opcional) O tipo de instância a ser executada como o host do espaço de trabalho. Os tipos de instância variam de acordo com a região.

- MetadataOptions

  Tipo: StringMap

Padrão: {” HttpEndpoint “: “ativado”, "HttpTokens“: “opcional"}

Descrição: (opcional) as opções de meta-dados para a instância. Para obter mais informações, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

  Tipo: string

  Padrão: nenhum

  Descrição: (Opcional) URL de um script a ser executado depois de as atualizações de pacote serem aplicadas. O padrão ("none") é não executar um script.

- PreUpdateScript

  Tipo: string

  Padrão: nenhum

  Descrição: (Opcional) A URL de um script a ser executado antes de as atualizações serem aplicadas. O padrão ("none") é não executar um script.

- SourceAmiId

  Tipo: string

  Descrição: (Obrigatório) O ID de Imagem de máquina da Amazon de origem.

- SubnetId

  Tipo: string

  Descrição: (opcional) o ID da sub-rede na qual você deseja iniciar a instância. Se você excluiu sua VPC padrão, esse parâmetro é obrigatório.

- TargetAmiName

  Tipo: string

  Padrão: UpdateLinuxAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

  Descrição: (Opcional) O nome da nova AMI que será criada. O padrão é uma string gerada pelo sistema que inclui o ID da AMI de origem, bem como a data e a hora de criação.

AWS-UpdateWindowsAmi

Descrição

Atualize uma Amazon Machine Image (AMI) do Microsoft Windows. Por padrão, esse runbook instala todas as atualizações do Windows, softwares da Amazon e drivers da Amazon. Depois, ele executa o Sysprep para criar uma nova AMI. Compatível com Windows Server 2008 R2 ou posterior.

> **Important**
>
> Se suas instâncias se conectarem ao AWS Systems Manager usando endpoints da VPC, este runbook falhará, a menos que seja usado na região us-east-1. As instâncias devem ter o TLS 1.2 ativado para usar esse runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Categorias

  Tipo: string

Descrição: (opcional) especifique uma ou mais categorias de atualização. Você pode filtrar categorias usando valores separados por vírgulas. Opções: Aplicativo, Conectores, CriticalUpdates, DefinitionUpdates DeveloperKits, Drivers, OrientaçãoFeaturePacks, Microsoft,, SecurityUpdates ServicePacks, FerramentasUpdateRollups, Atualizações. Os formatos válidos incluem uma única entrada, por exemplo:CriticalUpdates. Ou você pode especificar uma lista separada por vírgulas:CriticalUpdates,SecurityUpdates. NOTA: Não pode haver nenhum espaço em torno do vírgulas.

- ExcludeKbs

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais IDs de artigo da Base de Dados de Conhecimento Microsoft (KB) para excluir. Você pode excluir vários IDs usando valores separados por vírgulas. Formatos válidos: KB9876543 ou 9876543.

- IamInstanceProfileName

  Tipo: string

  Padrão: ManagedInstanceProfile

  Descrição: (obrigatório) o nome da função que permite que o Systems Manager gerencie a instância.

- IncludeKbs

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais IDs de artigo da Base de Dados de Conhecimento Microsoft (KB) para incluir. Você pode instalar vários IDs usando valores separados por vírgulas. Formatos válidos: KB9876543 ou 9876543.

- InstanceType

  Tipo: string

  Padrão: t2.medium

  Descrição: (Opcional) O tipo de instância a ser executada como o host do espaço de trabalho. Os tipos de instância variam de acordo com a região. O padrão é t2.medium.

- MetadataOptions

Tipo: StringMap

Padrão: {” HttpEndpoint “: “ativado”, "HttpTokens“: “opcional"}

Descrição: (opcional) as opções de meta-dados para a instância. Para obter mais informações, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

  Tipo: string

  Descrição: (Opcional) Um script fornecido como string. Ele será executado após a instalação das atualizações do sistema operacional.

- PreUpdateScript

  Tipo: string

  Descrição: (Opcional) Um script fornecido como string. Ele será executado antes da instalação de atualizações do sistema operacional.

- PublishedDateAfter

  Tipo: string

  Descrição: (Opcional) Especifique a data depois da qual as atualizações devem ser publicadas. Por exemplo, se 01/01/2017 for especificado, todas as atualizações que foram encontrados durante a pesquisa do Windows Update que foram publicadas em ou depois de 01/01/2017 será retornado.

- PublishedDateBefore

  Tipo: string

  Descrição: (Opcional) Especifique a data antes da qual as atualizações devem ser publicadas. Por exemplo, se 01/01/2017 for especificado, todas as atualizações que foram encontradas durante a pesquisa do Windows Update que foram publicadas em ou antes de 01/01/2017 serão retornadas.

- PublishedDaysOld

  Tipo: string

  Descrição: (Opcional) Especifique a quantidade de dias que as atualizações devem ter a partir da data publicada. Por exemplo, se 10 for especificado, todas as atualizações que foram encontradas

durante a pesquisa do Windows Update que foram publicadas 10 ou mais dias atrás serão retornadas.

- SeverityLevels

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais níveis de gravidade MSRC associados a uma atualização. Você pode filtrar os níveis de gravidade usando valores separados por vírgulas. Por padrão, patches para todos os níveis de segurança são selecionados. Se o valor for fornecido, a lista de atualização será filtrada por esses valores. Opções: Crítica, Importante, Baixa, Moderada ou Não especificada. Os formatos válidos incluem uma única entrada, por exemplo: Crítica. Como alternativa, você pode especificar uma lista separada por vírgulas: Crítica, Importante, Baixa.

- SourceAmiId

  Tipo: string

  Descrição: (Obrigatório) O ID de Imagem de máquina da Amazon de origem.

- SubnetId

  Tipo: string

  Descrição: (opcional) o ID da sub-rede na qual você deseja iniciar a instância. Se você excluiu sua VPC padrão, esse parâmetro é obrigatório.

- TargetAmiName

  Tipo: string

  Padrão: UpdateWindowsAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

  Descrição: (Opcional) O nome da nova AMI que será criada. O padrão é uma string gerada pelo sistema que inclui o ID da AMI de origem, bem como a data e a hora de criação.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Descrição

O runbook `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` ativa as verificações de integridade para o grupo do Amazon EC2 Auto Scaling (ajuste de escala automático) que você especificar.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AutoScalingGroupARN

  Tipo: String

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do grupo do Auto Scaling no qual você deseja ativar as verificações de integridade.
- HealthCheckGracePeriod

  Tipo: inteiro

  Padrão: 300

  Descrição: (opcional) o tempo em segundos que o ajuste de escala automático aguardará antes de verificar o status de integridade de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que entrou em serviço.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: ativa verificações de integridade no grupo do Auto Scaling que você especifica no parâmetro `AutoScalingGroupARN`.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descrição

O runbook `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` exige que a instância do Amazon Elastic Compute Cloud (Amazon EC2) especificada use o Instance Metadata Service Version 2 (IMDSv2).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- InstanceId

Tipo: sequência

Descrição: (obrigatório) o ID da instância do Amazon EC2 que você deseja que use o IMDSv2.

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- HttpPutResponseHopLimit

  Tipo: inteiro

  Descrição: (Opcional) O limite de resposta do Hop do serviço IMDS de volta ao solicitante. Defina como 2 ou mais para instâncias EC2 que hospedam contêineres. Defina como 0 para não mudar (Padrão).

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

  Padrão: 0

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: define a opção `HttpTokens` como `required` na instância do Amazon EC2 que você especifica no parâmetro `InstanceId`.
- `aws:assertAwsResourceProperty`: verifica se o IMDSv2 é necessário na instância do Amazon EC2.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descrição

Crie uma AMI de uma instância do EC2 para o Windows Server que executa o SQL Server 2008 (ou posterior) e atualize a AMI para uma versão mais recente do SQL Server.

Os caminhos de atualização com suporte são os seguintes:

- SQL Server 2008 para SQL Server 2017, 2016 ou 2014
- SQL Server 2008 R2 para SQL Server 2017, 2016 ou 2014
- SQL Server 2012 para SQL Server 2019, 2017, 2016 ou 2014
- SQL Server 2014 para SQL Server 2019, 2017 ou 2016
- SQL Server 2016 para SQL Server 2019 ou 2017
- SQL Server 2017para SQL Server 2019

Se você estiver usando uma versão anterior do Windows Server que é incompatível com o SQL Server 2019, o documento de automação deve atualizar sua versão do Windows Server para 2016.

A atualização é um processo de várias etapas que pode levar 2 horas para ser concluído. A automação cria uma AMI na instância e depois inicia uma instância temporária na do novo AMI no `SubnetID` especificado. Os grupos de segurança associados à instância original são aplicados à instância temporária. O automação executa uma atualização in-loco para a `TargetSQLVersion` na instância temporária. Após o upgrade, a automação cria uma nova AMI na instância temporária e encerra a instância temporária.

Você pode testar a funcionalidade do aplicativo iniciando a nova AMI na sua VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade do aplicativo antes de mudar completamente para a instância atualizada.

> **Note**
>
> Se quiser modificar o nome do computador da instância do EC2 executada na nova AMI, consulte Renomear um computador que hospeda uma instância independente do SQL Server.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Pré-requisitos

- TLS versão 1.2.
- A instância do EC2 deve usar uma versão do Windows Server que seja Windows Server 2008 R2 (ou posterior) e SQL Server 2008 (ou posterior).
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em instâncias do EC2 no Windows Server.
- Configure a instância para usar uma função do perfil de instância do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização da instância.
- Para instâncias que usam uma versão Traga sua própria licença (BYOL) do SQL Server, os seguintes pré-requisitos adicionais se aplicam:
  - Forneça um ID de snapshot do EBS que inclua a mídia de instalação do SQL Server. Para fazer isso:

    1. Verifique se a instância do EC2 está executando o Windows Server 2008 R2 ou posterior.
    2. Crie um volume do EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
    3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
    4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\

5. Crie um snapshot do EBS do volume de 6 GB criado na etapa 2.

Limitações

- A atualização só pode ser realizada em um SQL Server usando a autenticação do Windows.
- Verifique se há atualizações de patch de segurança pendentes nas instâncias. Abra Control Panel (Painel de controle) e, em seguida, escolha Check for updates (Verificar atualizações).
- Implantações do SQL Server no modo HA e espelhamento não são compatíveis.

Parâmetros

- IamInstanceProfile

  Tipo: String

  Descrição: (obrigatório) o perfil de instância do IAM.
- InstanceId

  Tipo: String

  Descrição: (obrigatória) a instância que executa o Windows Server 2008 R2 (ou posterior) e o SQL Server 2008 (ou posterior).
- KeepPreUpgradeImageBackUp

  Tipo: String

  Descrição: (opcional) se definido como `true`, a automação não excluirá a AMI criada da instância antes da atualização. Se definida como `true`, você deverá excluir a AMI. Por padrão, a AMI é excluída.
- SubnetId

  Tipo: String

  Descrição: (obrigatório) Forneça uma sub-rede para o processo de atualização. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, Amazon S3 e Microsoft (para fazer download de patches).
- SQLServerSnapshotId

Tipo: String

Descrição: (condicional) ID do snapshot da mídia de instalação do SQL Server. Esse parâmetro é necessário para instâncias que usam uma versão BYOL do SQL Server. Esse parâmetro é opcional para instâncias com licença inclusa do SQL Server (instâncias executadas usando uma imagem de máquina da Amazon fornecida pela AWS para o Windows Server com Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

  Tipo: String

  Descrição: (opcional) se definido como `true`, a automação reinicializará a instância antes de criar uma AMI de pré-atualização. Por padrão, a automação não reinicializa antes da atualização.

- TargetSQLVersion

  Tipo: String

  Descrição: (opcional) selecione a versão do servidor SQL de destino.

  Destinos possíveis:

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

  Destino padrão: SQL Server 2016

Saídas

AMIId: o ID da AMI criada a partir da instância que foi atualizada para uma versão mais recente do SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descrição

Crie um Amazon Machine Image (AMI) a partir de uma instância Windows Server 2008 R2, 2012 R2, 2016 ou 2019 e, em seguida, atualize-a AMI para Windows Server 2016, 2019 ou 2022. Os caminhos de atualização com suporte são os seguintes.

- Windows Server2008 R2 a Windows Server 2016.
- Windows Server 2012 R2 para Windows Server 2016.
- Windows Server 2012 R2 para Windows Server 2019.
- Windows Server 2012 R2 para Windows Server 2022.
- Windows Server 2016 a Windows Server 2019.
- Windows Server 2016 a Windows Server 2022.
- Windows Server 2019 a Windows Server 2022.

A operação de atualização é um processo de várias etapas que pode levar 2 horas para ser concluído. Recomendamos a execução de uma atualização do sistema operacional em instâncias com pelo menos 2 vCPUs e 4 GB de RAM. A automação cria uma AMI a partir da instância e depois executa uma instância temporária na AMI recém-criada no `SubnetId` especificado. Os grupos de segurança associados à instância original são aplicados à instância temporária. O automação executa uma atualização in-loco para a `TargetWindowsVersion` na instância temporária. Para atualizar a instância do Windows Server 2008 R2 para o Windows Server 2016, 2019 ou 2022, uma atualização in-loco é realizada duas vezes porque a atualização direta do Windows Server 2008 R2 para o Windows Server 2016, 2019 ou 2022 não é compatível. A automação também atualiza ou instala os drivers da AWS exigidos pela instância temporária. Após a atualização, a automação cria uma nova AMI na instância temporária e encerra a instância temporária.

Você pode testar a funcionalidade do aplicativo iniciando uma instância de teste na AMI atualizada em sua Amazon Virtual Private Cloud (Amazon VPC). Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade do aplicativo antes de mudar completamente para a AMI atualizada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Edições Standard e Datacenter do Windows Server 2008 R2, 2012 R2, 2016, ou 2019

Pré-requisitos

- TLS versão 1.2.
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em instâncias do EC2 no Windows Server.
- O Windows PowerShell 3.0 ou posterior deve estar instalado na sua instância.
- Para instâncias ingressadas em um domínio do Microsoft Active Directory, é recomendável especificar um `SubnetId` que não tenha conectividade com seus controladores de domínio para ajudar a evitar conflitos de nome de host.
- A sub-rede da instância deve ter conectividade de saída com a Internet, que fornece acesso ao Serviços da AWS Amazon S3 e acesso ao download de patches da Microsoft. Esse requisito será atendido se a sub-rede for pública e a instância tiver um endereço IP público ou se a sub-rede for uma sub-rede privada com uma rota que envie o tráfego da Internet para um dispositivo NAT público.
- Essa automação só funciona com instâncias do Windows Server 2008 R2, 2012 R2, 2016 e 2019.
- Configure a Windows Server instância com um perfil de instância AWS Identity and Access Management (IAM) que forneça as permissões necessárias para o Systems Manager. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização.
- Se a instância não usar uma licença do Windows AWS fornecida, especifique um ID de snapshot do Amazon EBS que inclua a mídia de instalação Windows Server 2012 R2. Para fazer isso:
  - Verifique se a instância do EC2 está executando o Windows Server 2012 ou posterior.
  - Crie um volume do EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
  - Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
  - Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
  - Crie um snapshot do EBS do volume de 6 GB criado na etapa 2 acima.

Limitações

Essa automação não é compatível com a atualização de controladores de domínio do Windows, clusters ou sistemas operacionais de desktop do Windows. Essa automação também não é compatível com instâncias do EC2 para o Windows Server com as seguintes funções instaladas.

- Host de sessão de área de trabalho remota (RDSH)
- Agente de conexão de área de trabalho remota (RDCB)
- Host de virtualização de área de trabalho remota (RDVH)
- Acesso via Web à Área de Trabalho Remota (RDWA)

Parâmetros

- AlternativeKeyPairName

  Tipo: String

  Descrição: (opcional) o nome de um par de chaves alternativo a ser usado durante o processo de atualização. Isso é útil em situações em que o par de chaves atribuído à instância original não está disponível. Se a instância original não tiver sido atribuída a um par de chaves, você deverá especificar um valor para esse parâmetro.
- BYOL WindowsMediaSnapshotId

  Tipo: String

  Descrição: (opcional) o ID do snapshot do Amazon EBS a ser copiado que inclui a mídia de instalação do Windows Server 2012R2. Obrigatória somente se você estiver atualizando uma instância BYOL.
- IamInstanceProfile

  Tipo: String

  Descrição: (obrigatório) o nome do perfil da instância do IAM que permite que o Systems Manager gerencie a instância.
- InstanceId

  Tipo: String

  Descrição: (obrigatória) a instância EC2 que executa o Windows Server 2008 R2, 2012 R2, 2016 ou 2019.

- KeepPreUpgradeImageBackUp

  Tipo: String

  Descrição: (opcional) se definida como Verdadeiro, a Automação não exclui a AMI criada a partir da instância EC2 antes da atualização. Se definida como Verdadeiro, você deverá excluir a AMI. Por padrão, a AMI é excluída.

- SubnetId

  Tipo: String

  Descrição: (obrigatório) esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída com AWS serviços, Amazon S3 e Microsoft (para baixar patches).

- TargetWindowsVersion

  Tipo: String

  Descrição: (obrigatória) selecione a versão de destino do Windows.

  Padrão: 2022

- RebootInstanceBeforeTakingImage

  Tipo: String

  Descrição: (opcional) Se definida como Verdadeiro, a Automação reinicializa a instância antes de criar uma AMI pré-atualização. Por padrão, a Automação não reinicializa antes da atualização.

AWSEC2-ConfigureSTIG

Guias de implementação técnica de segurança (STIGs) são os padrões de fortalecimento de configuração criados pela Agência de Sistemas de Informação de Defesa (DISA) para proteger os sistemas e softwares de informação. Para que seus sistemas estejam em conformidade com os padrões STIG, você deve instalar, definir e testar uma variedade de configurações de segurança.

O Amazon EC2 fornece um runbook do Systems Manager, AWSEC2-ConfigureSTIG, que você pode usar para aplicar as configurações do STIG a uma instância. Este documento ajuda você a criar rapidamente imagens compatíveis com os padrões do STIG. O documento do STIG Systems Manager verifica se há configurações incorretas e executa um script de correção. Ele também

é instalado InstallRoot do Departamento de Defesa (DoD) em AMIs do Windows para instalar e atualizar os certificados do DoD e remover certificados desnecessários para manter a conformidade com o STIG. Não há cobranças adicionais pelo uso do documento do STIG Systems Manager.

> **Important**
>
> Com poucas exceções, os componentes de fortalecimento do STIG que o documento do Systems Manager baixa não instalam pacotes de terceiros. Se pacotes de terceiros já estiverem instalados na instância e se houver STIGs relacionados que o Amazon EC2 suporta para aquele pacote, esses STIGs são aplicados.

Esta página lista todos os STIGs que o Amazon EC2 suporta e que os componentes de fortalecimento do STIG se aplicam à sua instância do EC2.

Você pode escolher qual categoria de conformidade do STIG deseja aplicar.

Níveis de conformidade

- Alto (categoria I)

  O risco mais grave. Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade.
- Médio (categoria II)

  Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade, mas os riscos podem ser mitigados.
- Baixo (categoria III)

  Inclui qualquer vulnerabilidade que degrade medidas de proteção contra perda de confidencialidade, disponibilidade ou integridade.

Tópicos

Downloads de componentes de fortelecimento do STIG

A Amazon agrupa os componentes de fortalecimento do STIG em pacotes relacionados ao sistema operacional para cada versão. Os pacotes são arquivos de arquivamento apropriados para o sistema operacional de destino em que são baixados e executados. Os pacotes de componentes Linux são armazenados como arquivos TAR (extensão de arquivo .tgz). Os pacotes de componentes do Windows são armazenados como arquivos ZIP (extensão de arquivo .zip).

A Amazon armazena os pacotes de componentes no bucket `STIG` do S3 do Image Builder em cada Região da AWS. Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.

Os padrões e exemplos de caminhos de armazenamento de componentes e nomes de arquivos de pacotes são os seguintes:

Caminho de armazenamento de componentes

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

Variáveis do caminho do componente

region

Região da AWS (Cada região tem seu próprio bucket de componentes.)

bundle file name

O formato é <nome de sistema do pacote>_ <AAAA>_Q <trimestre>[_<versão>]. <extensão de arquivo>. Observe que o nome tem sublinhados entre os nós, não pontos.

os bundle name

O prefixo do nome padrão para o pacote do sistema operacional é `LinuxAWSConfigureSTIG` ou `AWSConfigureSTIG`. Para manter a compatibilidade com versões anteriores, o download para Windows não inclui um prefixo de plataforma.

YYYY

O ano de quatro dígitos do lançamento.

quarter

Identifica o trimestre do ano: 1, 2, 3 ou 4.

release

Número incremental que começa em um e aumenta em um para cada nova versão. A versão não está incluída na primeira versão em um trimestre e só é adicionada nas versões subsequentes.

file extension

Formato de arquivo compactado `tgz` (Linux) ou `zip` (Windows).

Exemplos de nomes de arquivos de pacotes

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

Configurações do STIG no Windows

As AMIs e os componentes de fortalecimento do STIG do Amazon EC2 no Windows foram projetados para servidores autônomos e aplicam a Política de Grupo Local. Componentes compatíveis com STIG são instalados InstallRoot do Departamento de Defesa (DoD) em AMIs do Windows para baixar, instalar e atualizar os certificados do DoD. Eles também removem certificados desnecessários para manter a conformidade com o STIG. Atualmente, o Amazon EC2 suporta as linhas de base do STIG para as seguintes versões do Windows Server: 2012 R2, 2016, 2019 e 2022.

Esta seção lista as configurações atuais do STIG que o Amazon EC2 suporta para sua infraestrutura Windows, seguidas por um log do histórico de versões.

Você pode aplicar configurações de STIG baixas, médias ou altas.

STIG do Windows baixa (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

- Windows Server 2022 STIG versão 1 release 1

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- Windows Server 2019 STIG Versão 2 Release 5

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- Windows Server 2016 STIG Versão 2 Release 5

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060
- Windows Server 2012 R2 MS STIG Versão 3 Release 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 e V-225250
- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Nenhuma configuração STIG é aplicada ao Microsoft .NET Framework para vulnerabilidades de Categoria III.
- Windows Firewall STIG Versão 2 Release 1

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008
- Internet Explorer 11 STIG Versão 2 Release 3

  V-46477, V-46629 e V-97527
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)

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

Windows STIG Medium (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem

afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG Medium inclui todas as configurações de fortalecimento do STIG listadas que se aplicam à STIG do Windows low (categoria III), além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

- Windows Server 2022 STIG versão 1 release 1

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  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 e V-254512
- Windows Server 2019 STIG Versão 2 Release 5

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

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 e V-236001

- Windows Server 2016 STIG Versão 2 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  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 e V-236000

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  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 e V-225239

- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-225238

- Windows Firewall STIG Versão 2 Release 1

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

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

- Internet Explorer 11 STIG Versão 2 Release 3

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  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 e V-75171

- Microsoft Edge STIG Versão 1 Release 6 (somente 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 e V-246736

- Defender STIG Versão 2 Release 4 (somente 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 e V-213466

STIG do Windows High (categoria I)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG High inclui todas as configurações de fortalecimento do STIG listadas que se aplicam às categorias Windows STIG Medium and Low, além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

- Windows Server 2022 STIG versão 1 release 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 e V-254500

- Windows Server 2019 STIG Versão 2 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  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 e V-205919

- Windows Server 2016 STIG Versão 2 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

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 e V-225079

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  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 e V-225274

- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa) do Microsoft.NET Framework. Nenhuma configuração adicional do STIG se aplica a vulnerabilidades da Categoria I.

- Windows Firewall STIG Versão 2 Release 1

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-241992, V-241997 e V-242002

- Internet Explorer 11 STIG Versão 2 Release 3

  Inclui todas as configurações de proteção do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa) do Internet Explorer 11. Nenhuma configuração adicional do STIG se aplica a vulnerabilidades da Categoria I.

- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-235758 e V-235759

- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-213426, V-213452 e V-213453

Histórico de versões do Windows STIG

Esta seção registra o histórico de versões do componente do Windows para as atualizações trimestrais do STIG. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações.

Alterações no primeiro trimestre de 2024 - 23/02/2024 (sem alterações):

Não houve alterações no componente STIGS do Windows para a versão do primeiro trimestre de 2024.

Alterações no quarto trimestre de 2023 - 12/07/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para a versão do quarto trimestre de 2023.

Alterações no terceiro trimestre de 2023 - 04/10/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2023.

Alterações no segundo trimestre de 2023 - 03/05/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do segundo trimestre de 2023.

Alterações no primeiro trimestre de 2023 - 27/03/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2023.

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

STIG-Build-Windows-Low versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5

- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)

STIG-Build-Windows-Medium versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

STIG-Build-Windows-High versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022.

STIG-Build-Windows-Low versão 1.5.0

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

STIG-Build-Windows-Medium versão 1.5.0

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

STIG-Build-Windows-High versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1

- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no primeiro trimestre de 2022 - 02/08/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2022.

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021.

STIG-Build-Windows-Low versão 1.5.0

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

STIG-Build-Windows-Medium versão 1.5.0

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

STIG-Build-Windows-High versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3

- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021.

STIG Build-Windows-Low versão 1.4.0

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

STIG-Build-Windows-Medium versão 1.4.0

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

STIG-Build-Windows-High versão 1.4.0

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7

- Internet Explorer 11 STIG Versão 1 Release 19

Configurações de STIG no Linux

Esta seção contém informações sobre as configurações de fortalecimento do STIG do Linux suportadas pelo Amazon EC2, seguidas por um log do histórico de versões. Se a distribuição do Linux não tiver configurações próprias de proteção STIG, o Amazon EC2 usa as configurações da RHEL. As configurações de fortalecimento do STIG suportadas se aplicam às AMIs e componentes Linux do Amazon EC2 com base na distribuição do Linux, da seguinte forma:

- Configurações do Red Hat Enterprise Linux (RHEL) 7 STIG
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Configurações do RHEL 8 STIG
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)

Linux STIG Low (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

RHEL 7 STIG Versão 3 Versão 14

- RHEL 7/CentOS 7

  V-204452, V-204576 e V-204605
- AL2

V-204452, V-204576 e V-204605

RHEL 8 STIG Versão 1 Versão 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-230497, V-230498, V-230498, V-230496, V-230497, V-230498, V-230498, V-230496 230499 e V-230281

Ubuntu 18.04 STIG versão 2 versão 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 e V-219333

Ubuntu 20.04 STIG Versão 1 Versão 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 e V-238308

Linux STIG Medium (categoria II)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Linux STIG Medium inclui todas as configurações de fortalecimento do STIG listadas que se aplicam à Linux STIG Low (categoria III), além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

RHEL 7 STIG Versão 3 Versão 14

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

- 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-204593, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204597, V-204597, V-204597, V-204597 4598, 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-204514, 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-204519, V-20451, V-204619, V-204519, V-20451 79, V-204631, V-204633 e 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-204593, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204597, V-204597, V-204597, V-204597 4598, 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-204514, 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-204519, V-20451, V-204619, V-204519, V-20451 79, V-204631, V-204633 e V-256970

RHEL 8 STIG Versão 1 Versão 13

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

- 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-230231, V-23033 24, 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-244533, V-244533, 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-230343, V-230345, V-230343, V-230345, V-230343, V-230345 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-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-230489, V-230489 230559, V-230560, V-230561, V-237640 e V-256974

Ubuntu 18.04 STIG versão 2 versão 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-222303, V-222V-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-219216, V-219216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216, V-2216 V-219217, V-219218, 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-219234, V-219234, V-219234 235, 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-219275 219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, 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-219331, V-219331 37 e V-219335

Ubuntu 20.04 STIG Versão 1 Versão 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-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-238255, V-238255, V-238255 8256, 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-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 e V-238334

Linux STIG High (categoria I)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem

afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria de STIG do Linux média inclui todas as configurações de fortalecimento do STIG listadas que se aplicam às categorias Linux STIG Medium and Low, além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

RHEL 7 STIG Versão 3 Versão 14

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 7/CentOS 7

  V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620 e V-204621
- AL2:

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

RHEL 8 STIG Versão 1 Versão 13

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 8/CentOS 8/AL 2023

  V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533 e V-230558

Ubuntu 18.04 STIG versão 2 versão 13

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316 e V-251507

Ubuntu 20.04 STIG Versão 1 Versão 11

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

Histórico de versões do STIG do Linux

Esta seção registra o histórico de versões do componente do Linux para as atualizações trimestrais do STIG. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações.

Alterações no primeiro trimestre de 2024 - 02/06/2024:

Versões atualizadas do STIG e aplicou o STIGS para a versão do primeiro trimestre de 2024 da seguinte forma:

STIG-Build-Linux-low versão 2024.1.x

- RHEL 7 STIG Versão 3 Versão 14
- RHEL 8 STIG Versão 1 Versão 13
- Ubuntu 18.04 STIG versão 2 versão 13
- Ubuntu 20.04 STIG Versão 1 Versão 11

STIG-Build-Linux versão média 2024.1.x

- RHEL 7 STIG Versão 3 Versão 14
- RHEL 8 STIG Versão 1 Versão 13
- Ubuntu 18.04 STIG versão 2 versão 13
- Ubuntu 20.04 STIG Versão 1 Versão 11

STIG-Build-Linux-High versão 2024.1.x

- RHEL 7 STIG Versão 3 Versão 14
- RHEL 8 STIG Versão 1 Versão 13
- Ubuntu 18.04 STIG versão 2 versão 13
- Ubuntu 20.04 STIG Versão 1 Versão 11

Alterações no quarto trimestre de 2023 - 12/07/2023:

Versões atualizadas do STIG e aplicou STIGS para a versão do quarto trimestre de 2023 da seguinte forma:

STIG-Build-Linux-low versão 2023.4.x

- RHEL 7 STIG Versão 3 Versão 13
- RHEL 8 STIG Versão 1 Versão 12
- Ubuntu 18.04 STIG versão 2 versão 12
- Ubuntu 20.04 STIG Versão 1 Versão 10

STIG-Build-Linux versão média 2023.4.x

- RHEL 7 STIG Versão 3 Versão 13
- RHEL 8 STIG Versão 1 Versão 12
- Ubuntu 18.04 STIG versão 2 versão 12
- Ubuntu 20.04 STIG Versão 1 Versão 10

STIG-Build-Linux-High versão 2023.4.x

- RHEL 7 STIG Versão 3 Versão 13
- RHEL 8 STIG Versão 1 Versão 12
- Ubuntu 18.04 STIG versão 2 versão 12
- Ubuntu 20.04 STIG Versão 1 Versão 10

Alterações no terceiro trimestre de 2023 - 04/10/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11

- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Alterações no segundo trimestre de 2023 - 03/05/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11

- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Alterações no primeiro trimestre de 2023 - 27/03/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Linux para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Suporte do Ubuntu introduzido, versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 7

- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Alterações no primeiro trimestre de 2022 - 26/04/2022:

Refatorado para incluir melhor suporte para contêineres. Script AL2 anterior combinado com o RHEL 7. Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 4

- RHEL 8 STIG Versão 1 Release 3

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

AWSEC2-PatchLoadBalancerInstance

Descrição

Atualize e faça o patch versões secundárias de uma instância do Amazon EC2 (Windows ou Linux) anexada a qualquer balanceador de carga (clássico, ALB ou NLB). O tempo padrão de drenagem da conexão é aplicado antes que a instância seja corrigida. Você pode substituir o tempo de espera inserindo seu tempo de drenagem personalizado em minutos (1-59) para o parâmetro ConnectionDrainTime.

O workflow da automação é o seguinte:

1. O balanceador de carga ou o grupo de destino ao qual a instância está vinculada é determinado e a instância é verificada como íntegra.
2. A instância é removida do balanceador de carga ou do grupo de destino.
3. A automação aguarda o período de tempo especificado para o tempo de drenagem da conexão.
4. A automação AWS-RunPatchBaseline é chamada para corrigir a instância.
5. A instância é reanexada ao balanceador de carga ou ao grupo de destino.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Pré-requisitos

- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Trabalho com o SSM Agent em instâncias do EC2 para o Windows Server.

Parâmetros

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) ID da instância a ser corrigida associada a um balanceador de carga (clássico, ALB ou NLB).

- ConnectionDrainTime

  Tipo: sequência

  Descrição: (opcional) o tempo de drenagem da conexão do balanceador de carga, em minutos (1-59).

AWSEC2-SQLServerDBRestore

Descrição

O runbook do `AWSEC2-SQLServerDBRestore` restaura os backups de banco de dados do Microsoft SQL Server armazenados no Amazon S3 para o SQL Server 2017 em execução em uma instância Linux do Amazon Elastic Compute Cloud (EC2). Você pode fornecer sua própria instância do EC2 executando o SQL Server 2017 para Linux. Se uma instância do EC2 não for fornecida, a automação será iniciado e configurado uma nova instância do EC2 Ubuntu 16.04 com o SQL Server 2017. A automação oferece suporte à restauração de backups de logs completos, diferenciais e transacionais. Essa automação aceita vários arquivos de backup de banco de dados e restaura automaticamente o backup válido mais recente de cada banco de dados nos arquivos fornecidos.

Para automatizar o backup e a restauração de um banco de dados SQL Server on-premises em uma instância do EC2 executando o SQL Server 2017 Linux, você pode usar o script PowerShell assinado pela AWS `MigrateSQLServerToEC2Linux`.

> **Important**
>
> Esse runbook redefine a senha do usuário SA do SQL Server sempre que o fluxo de trabalho é executado. Depois que a automação estiver concluída, você deverá definir sua própria senha de usuário SA novamente antes de se conectar à instância do SQL Server.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Pré-requisitos

Para executar esta automação, você deve cumprir os seguintes pré-requisitos:

- O usuário ou a função do IAM que executa esta automação deve ter uma política embutida anexada às permissões descritas em Permissões obrigatórias do IAM.
- Se você fornecer sua própria instância do EC2:
  - A instância do EC2 que você fornece deve ser uma instância Linux executando o Microsoft SQL Server 2017.
  - A instância do EC2 que você fornece deve ser configuradad com um perfil de instância do AWS Identity and Access Management (IAM) que tenha a política gerenciada `AmazonSSMManagedInstanceCore` anexada. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
  - O SSM Agent deve estar instalado na sua instância do EC2. Para obter mais informações, consulte Instalar e configurar SSM Agent em instâncias EC2 do Linux.
  - A instância do EC2 deve ter espaço em disco suficiente para fazer o download e a restauração dos backups do SQL Server.

Limitações

Essa automação não é compatível com a restauração para o SQL Server em execução em instâncias do EC2 para Windows Server. Essa automação restaura apenas os backups de banco de dados compatíveis com o SQL Server para Linux 2017. Para obter mais informações, consulte Edições e recursos compatíveis do SQL Server 2017 no Linux.

Parâmetros

Essa automação tem os seguintes parâmetros:

- DatabaseNames

  Tipo: sequência

  Descrição: (opcional) Uma lista separada por vírgulas dos nomes de bancos de dados a serem restaurados.

- DataDirectorySize

  Tipo: sequência

  Descrição: (opcional) Tamanho do volume desejado (GiB) do diretório Data do SQL Server para a nova instância do EC2.

  Valor padrão: 100

- KeyPair

  Tipo: sequência

  Descrição: (opcional) O par de chaves a ser usado ao criar a nova instância do EC2.

- IamInstanceProfileName

  Tipo: sequência

  Descrição: (opcional) O perfil de instância do IAM a ser anexado à nova instância do EC2. O perfil de instância do IAM deve ter a política gerenciada pelo `AmazonSSMManagedInstanceCore` anexada.

- InstanceId

  Tipo: sequência

Descrição: (opcional) A instância executando o SQL Server 2017 no Linux. Se nenhum InstanceId for fornecido, a automação iniciará uma nova instância do EC2 usando o InstanceType e o SQLServerEdition fornecidos.

- InstanceType

  Tipo: sequência

  Descrição: (opcional) O tipo da instância do EC2 a ser executada.

- IsS3PresignedUrl

  Tipo: sequência

  Descrição: (opcional) Se S3Input for um URL do S3 pré-assinado, indique `yes`.

  Valor padrão: Não

  Valores válidos: sim | não

- LogDirectorySize

  Tipo: sequência

  Descrição: (opcional) Tamanho do volume desejado (GiB) do diretório Log do SQL Server para a nova instância do EC2.

  Valor padrão: 100

- S3Input

  Tipo: sequência

  Descrição: (obrigatório) Nome do bucket do S3, lista separada por vírgulas de chaves de objeto do S3 ou uma lista separada por vírgulas de URLs do S3 pré-assinadas que contém os arquivos de backup SQL a serem restaurados.

- SQLServerEdition

  Tipo: sequência

  Descrição: (opcional) A edição do SQL Server 2017 a ser instalada na instância do EC2 recém-criada.

Valores permitidos: Standard | Enterprise | Web | Express

- SubnetId

  Tipo: sequência

  Descrição: (opcional) A sub-rede na qual executar a nova instância do EC2. A sub-rede deve ter conectividade de saída com serviços da AWS. Se um valor para SubnetId não for fornecido, a automação usará a sub-rede padrão.

- TempDbDirectorySize

  Tipo: sequência

  Descrição: (opcional) Tamanho do volume desejado (GiB) do diretório TempDB do SQL Server para a nova instância do EC2.

  Valor padrão: 100

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

Para usar esta automação, siga as etapas que se aplicam ao seu tipo de instância:

Para novas instâncias do EC2:

1. `aws:executeAwsApi`: recupera o ID da AMI para o SQL Server 2017 no Ubuntu 16.04.
2. `aws:runInstances`: executa uma nova instância do EC2 para Linux.
3. `aws:waitForAwsResourceProperty`: aguarda até que a instância EC2 recém-criada esteja pronta.
4. `aws:executeAwsApi`: reinicializa a instância se ela não estiver pronta.
5. `aws:assertAwsResourceProperty`: verifica se o SSM Agent está instalado.
6. `aws:runCommand`: executa o script de restauração do SQL Server no PowerShell.

Para instâncias do EC2 existentes:

1. `aws:waitForAwsResourceProperty`: verifica se a instância do EC2 está pronta
2. `aws:executeAwsApi`: reinicializa a instância se ela não estiver pronta.
3. `aws:assertAwsResourceProperty`: verifica se o SSM Agent está instalado.
4. `aws:runCommand`: executa o script de restauração do SQL Server no PowerShell.

Saídas

getInstance.InstanceId

restoreToNewInstance.Output

restoreToExistingInstance.Output

AWSSupport-ActivateWindowsWithAmazonLicense

Descrição

O runbook `AWSSupport-ActivateWindowsWithAmazonLicense` ativa uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para Windows Server com uma licença fornecida pela Amazon. A automação verifica e define as configurações necessárias do sistema operacional do serviço de gerenciamento de chaves e tenta a ativação. Isso inclui rotas do sistema operacional para os servidores de gerenciamento de chaves do Amazon e configurações do sistema operacional do serviço de gerenciamento de chaves. A definição do parâmetro `AllowOffline` como `true` permite que a automação atinja com êxito as instâncias que não são gerenciadas pelo AWS Systems Manager, mas que requerem uma interrupção e início da instância.

> **Note**
>
> Esse runbook não pode ser usado em instâncias do tipo Bring Your Own License (BYOL) do Windows Server. Para obter informações sobre como usar sua própria licença, consulte Licenciamento da Microsoft na AWS.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AllowOffline

  Tipo: String

  Valores válidos: verdadeiro | falso

Padrão: falso

Descrição: (opcional) defina como `true` se você permitir a correção da ativação do Windows offline caso houver falha na correção de problemas online ou caso a instância fornecida não seja uma instância gerenciada.

> **Important**
>
> O método offline requer que a instância do EC2 fornecida seja interrompida e depois iniciada. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ForceActivation

  Tipo: String

  Valores válidos: verdadeiro | falso

  Padrão: falso

  Descrição: (opcional) defina como `true` se você deseja continuar, mesmo se o Windows já estiver ativado.

- InstanceId

  Tipo: String

  Descrição: (obrigatória) o ID de sua instância do EC2 gerenciada para o Windows Server.

- SubnetId

  Tipo: String

Padrão: CreateNewVPC

Descrição: (Opcional) Apenas offline - O ID de sub-rede para a instância EC2Rescue usado para executar a solução de problemas offline. Use `SelectedInstanceSubnet` para usar a mesma sub-rede como sua instância, ou `CreateNewVPC` para criar uma nova VPC. IMPORTANTE: a sub-rede deve estar na mesma zona de disponibilidade que o InstanceId, e deve permitir acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a instância do EC2 que recebe o comando tenha um perfil do IAM com a política gerenciada pela Amazon AmazonSSMManagedInstanceCore anexada. Você deve ter pelo menos ssm:StartAutomationExecution e ssm:SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída de automação. Para a correção offline, consulte as permissões exigidas pelo `AWSSupport-StartEC2RescueWorkflow`.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifique se a plataforma da instância fornecida é Windows.
2. `aws:assertAwsResourceProperty`: confirme se a instância fornecida é uma instância gerenciada:
   a. (Correção de ativação online) Se a instância de entrada for uma instância gerenciada, execute `aws:runCommand` para executar o script do PowerShell e tentar corrigir a ativação do Windows.
   b. (Correção de ativação offline) Se a instância de entrada não for uma instância gerenciada:
      i. `aws:assertAwsResourceProperty`: verifica se o sinalizador `AllowOffline` está definido como `true`. Se esse for o caso, a correção offline é iniciada; caso contrário, o fluxo de trabalho termina.
      ii. `aws:executeAutomation`: invocar `AWSSupport-StartEC2RescueWorkflow` com o script de correção offline de ativação do Windows. O script utiliza o EC2Config ou o EC2Launch, de acordo com a versão do SO.
      iii. `aws:executeAwsApi`: lê o resultado de `AWSSupport-StartEC2RescueWorkflow`.

Saídas

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descrição

O runbook `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` analisa a conectividade de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou interface de rede elástica com um endpoint do AWS service (Serviço da AWS) . O IPv6 não é compatível. O runbook usa o valor que você especifica para o parâmetro `ServiceEndpoint` para analisar a conectividade com um endpoint. Se não for possível encontrar um endpoint do AWS PrivateLink em sua VPC, o runbook usa um endereço IP público para o serviço na Região da AWS atual. Esta automação usa o Reachability Analyzer da Amazon Virtual Private Cloud. Para obter mais informações, consulte O que é o Reachability Analyzer?, no Reachability Analyzer.

Esta automação verifica o seguinte:

- Verifica se sua nuvem privada virtual (VPC) está configurada para usar o servidor DNS fornecido pela Amazon.
- Verifica se existe um AWS PrivateLink endpoint na VPC para AWS service (Serviço da AWS) o que você especifica. Se um endpoint for encontrado, a automação verifica se o atributo `privateDns` está ativado.
- Verifica se o AWS PrivateLink endpoint está usando a política de endpoint padrão.

Considerações

- Você é cobrado por análise executada entre a origem e o destino. Para obter mais informações, consulte Definição de preço da Amazon VPC.
- Durante a automação, um caminho de insights de rede e uma análise de insights de rede são criados. Se a automação for concluída com êxito, o runbook excluirá esses recursos. Se a etapa de limpeza falhar, o caminho de insights de rede não será excluído pelo runbook e você precisará excluí-lo manualmente. Se você não excluir o caminho de insights de rede manualmente, ele continuará contando para a cota da sua Conta da AWS. Para obter mais informações sobre cotas para o Reachability Analyzer, consulte Cotas para o Reachability Analyzer no Reachability Analyzer.

- Configurações em nível de sistema operacional, como o uso de um proxy, resolvedor de DNS local ou arquivo de hosts, podem afetar a conectividade mesmo se o Reachability Analyzer retornar `PASS`.
- Revise a avaliação de todas as verificações realizadas pelo Reachability Analyzer. Se alguma das verificações retornar com um status de `FAIL`, isso poderá afetar a conectividade, mesmo que a verificação geral de acessibilidade retorne um status de `PASS`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Origem

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2 ou da interface de rede a partir da qual você deseja analisar a acessibilidade.
- ServiceEndpoint

  Tipo: sequência

Descrição: (obrigatório) o nome do host do endpoint do serviço ao qual você deseja analisar a acessibilidade.

- RetainVpcReachabilityAnalysis

  Tipo: sequência

  Padrão: False

  Descrição: (opcional) determina se o caminho de insight de rede e a análise relacionada criada são retidos. Por padrão, os recursos usados para analisar a acessibilidade são excluídos após uma análise bem-sucedida. Se você optar por reter a análise, o runbook não excluirá a análise e você poderá visualizá-la no console do Amazon VPC. Um link do console está disponível na saída de automação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

1. `aws:executeScript`: valida o endpoint do serviço ao tentar resolver o nome do host.
2. `aws:executeScript`: reúne detalhes sobre a VPC e a sub-rede.
3. `aws:executeScript`: avalia a configuração de DNS da VPC.
4. `aws:executeScript`: avalia as verificações do endpoint da VPC.
5. `aws:executeScript`: localiza um gateway da Internet para se conectar ao endpoint de serviço público.
6. `aws:executeScript`: determina o destino a ser usado para análise de acessibilidade.
7. `aws:executeScript`: analisa a acessibilidade da origem ao endpoint usando o Reachability Analyzer e limpa os recursos se a análise for bem-sucedida.
8. `aws:executeScript`: gera um relatório de avaliação de acessibilidade.
9. `aws:executeScript`: gera a saída em JSON.

Saídas

- `generateReport.EvalReport`: os resultados das verificações realizadas pela automação em formato de texto.
- `generateJsonOutput.Output`: uma versão mínima dos resultados no formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descrição

O runbook `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` automatiza as migrações das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com tecnologia Intel para os tipos equivalentes de instâncias com tecnologia AMD. Este runbook oferece suporte a instâncias de uso geral (M), de uso geral intermitente (T), otimizadas para computação (C) e otimizadas para memória (R) criadas no sistema Nitro. Este runbook pode ser usado em instâncias que não são gerenciadas pelo Systems Manager.

Para reduzir o risco potencial de perda de dados e tempo de inatividade, o runbook verifica o comportamento de parada da instância, se a instância está em um grupo do Amazon EC2

Auto Scaling, a integridade da instância e se o tipo de instância equivalente com tecnologia AMD está disponível na mesma zona de disponibilidade. Por padrão, este runbook não alterará o tipo de instância se os volumes de armazenamento de instâncias estiverem anexados ou se a instância fizer parte de uma pilha do AWS CloudFormation. Se você quiser alterar esse comportamento, especifique `yes` para um dos parâmetros `AllowInstanceStoreInstances` e `AllowCloudFormationInstances`.

> **Important**
>
> O acesso aos runbooks da `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar os planos do AWS Support.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook.
- A alteração do tipo de instância exige que o runbook interrompa sua instância. Quando uma instância é interrompida, todos os dados armazenados na RAM ou nos volumes de armazenamento da instância são perdidos e o endereço IPv4 público automático é liberado. Para obter mais informações, consulte Interromper e iniciar sua instância.
- Se você não especificar um valor para o parâmetro `TargetInstanceType`, o runbook tentará identificar a instância AMD equivalente em termos de CPUs virtuais e memória dentro da mesma família de instâncias. O runbook termina se não for capaz de identificar um tipo de instância AMD equivalente.
- Ao usar a opção `DryRun`, você pode capturar o tipo de instância AMD equivalente e validar os requisitos sem realmente alterar o tipo de instância.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Reconhecer

  Tipo: sequência

  Descrição: (obrigatório) digite `yes` para confirmar que sua instância de destino será interrompida se estiver em execução.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2 cujo tipo você deseja alterar.
- TargetInstanceType

  Tipo: sequência

  Padrão: automático

  Descrição: (opcional) o tipo de instância AMD para a qual você deseja alterar sua instância. O valor `automatic` padrão usa o tipo de instância equivalente em termos de CPUs virtuais e memória. Por exemplo, um m5.large seria alterado para m5a.large.
- AllowInstanceStoreInstances

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

Descrição: (opcional) se você especificar `yes`, o runbook é executado em instâncias que têm volumes de armazenamento de instâncias anexados.

- AllowCloudFormationInstances

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se definido como `yes`, o runbook é executado em instâncias que fazem parte de uma pilha do AWS CloudFormation.

- AllowCrossGeneration

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se definido como `yes`, o runbook tenta encontrar o tipo de instância AMD equivalente mais recente dentro da mesma família de instâncias.

- DryRun

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se definido como `yes`, o runbook retorna o tipo de instância AMD equivalente e valida os requisitos de migração sem fazer alterações no tipo de instância.

- SleepWait

  Tipo: sequência

  Padrão: PT3S

  Descrição: (opcional) o tempo que o runbook deve esperar antes de iniciar uma nova automação. O valor fornecido para esse parâmetro deve corresponder ao padrão ISO 8601. Para obter mais

informações sobre a criação de sequências de caracteres ISO 8601, consulte Formatar strings de data e hora para o Systems Manager.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

1. `aws:assertAwsResourceProperty`: confirma que o status da instância de destino do Amazon EC2 é `running`, `pending`, `stopped` ou `stopping`. Caso contrário, a automação termina.
2. `aws:executeAwsApi`: reúne propriedades da instância de destino do Amazon EC2.
3. `aws:branch`: ramifica a automação com base no estado da instância do Amazon EC2.
   a. Se `stopped` ou `stopping`, a automação executa `aws:waitForAwsResourceProperty` até que a instância do Amazon EC2 seja totalmente interrompida.
   b. Se `running` ou `pending`, a automação executa `aws:waitForAwsResourceProperty` até que a instância do Amazon EC2 passe as verificações de status.
4. `aws:assertAwsResourceProperty`: confirma que a instância do Amazon EC2 não faz parte de um grupo do Auto Scaling verificando se a tag `aws:autoscaling:groupName` está aplicada.

5. `aws:executeAwsApi`: reúne as propriedades do tipo de instância atual para encontrar o tipo de instância AMD equivalente.
6. `aws:assertAwsResourceProperty`: confirma que um código de produto do AWS Marketplace não está associado à instância do Amazon EC2. Alguns produtos não estão disponíveis em todos os tipos de instâncias.
7. `aws:branch`: ramifica a automação dependendo se você deseja que a automação verifique se a instância do Amazon EC2 faz parte de uma pilha do AWS CloudFormation
   a. Se a tag `aws:cloudformation:stack-name` for aplicada à instância, a automação executa `aws:assertAwsResourceProperty` para confirmar que a instância não faz parte de uma pilha do AWS CloudFormation.
8. `aws:branch`: ramifica a automação com base no fato de o tipo de volume raiz da instância ser Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: confirma se o comportamento de desligamento da instância é `stop`, e não `terminate`.
10. `aws:executeScript`: confirma que há apenas uma automação desse runbook direcionada à instância atual. Se outra automação já estiver em andamento visando a mesma instância, ela retornará um erro e terminará.
11. `aws:executeAwsApi`: retorna uma lista dos tipos de instância AMD com a mesma quantidade de memória e vCPUs.
12. `aws:executeScript`: verifica se o tipo de instância atual é compatível e retorna o tipo de instância AMD equivalente. Se não houver equivalente, a automação termina.
13. `aws:executeScript`: confirma que o tipo de instância AMD está disponível na mesma zona de disponibilidade e verifica as permissões do IAM fornecidas.
14. `aws:branch`: ramifica a automação com base no valor do parâmetro `DryRun` ser `yes`.
15. `aws:branch`: verifica se o tipo de instância original e de destino são iguais. Se forem iguais, a automação termina.
16. `aws:executeAwsApi`: obtém o estado atual da instância.
17. `aws:changeInstanceState`: interrompe a instância do Amazon EC2.
18. `aws:changeInstanceState`: força a instância a parar se ela estiver presa no estado de parada.
19. `aws:executeAwsApi`: altera o tipo de instância para o tipo de instância AMD de destino.
20. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.

21. `aws:branch`: ramifica a automação com base no estado anterior da instância. Se foi `running`, a instância é iniciada.
    a. `aws:changeInstanceState`: inicia a instância do Amazon EC2 se ela estava em execução antes de alterar o tipo de instância.
    b. `aws:waitForAwsResourceProperty`: espera que a instância do Amazon EC2 passe nas verificações de status. Se a instância não passar nas verificações de status, altere-a de volta para seu tipo original.
        i. `aws:changeInstanceState`: interrompe a instância do Amazon EC2 antes de alterá-la para seu tipo original.
        ii. `aws:changeInstanceState`: força a instância do Amazon EC2 a parar antes de alterá-la para o tipo de instância original, caso ela fique presa em um estado de parada.
        iii. `aws:executeAwsApi`: altera a instância do Amazon EC2 para seu tipo original.
        iv. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
        v. `aws:changeInstanceState`: inicia a instância do Amazon EC2 se ela estava em execução antes de alterar o tipo de instância.
        vi. `aws:waitForAwsResourceProperty`: espera que a instância do Amazon EC2 passe nas verificações de status.
22. `aws:sleep`: espera antes de terminar o runbook.

AWSSupport-CheckXenToNitroMigrationRequirements

Descrição

O runbook `AWSSupport-CheckXenToNitroMigrationRequirements` verifica se uma instância do Amazon Elastic Compute Cloud (Amazon EC2) atende aos pré-requisitos para alterar com êxito o tipo de instância de uma instância do tipo Xen para um tipo de instância baseada em Nitro. Esta automação verifica o seguinte:

- O dispositivo raiz é um volume do Amazon Elastic Block Store (Amazon EBS).
- O atributo `enaSupport` está ativado.
- O módulo ENA está instalado na instância.
- O módulo NVMe está instalado na instância. Se sim, o módulo é instalado e um script verifica se o módulo está carregado na imagem `initramfs`.

- Analisa `/etc/fstab` e procura dispositivos de blocos que estão sendo montados usando nomes de dispositivos.
- Determina se o sistema operacional (SO) usa nomes previsíveis de interface de rede por padrão.

Este runbook é compatível com os seguintes sistemas operacionais:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: String

  Padrão: falso

  Descrição: (obrigatório) o ID da instância do Amazon EC2 para a qual você deseja verificar os pré-requisitos antes de migrar para um tipo de instância baseado em Nitro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeAwsApi`: reúne detalhes sobre a instância.
- `aws:executeAwsApi`: coleta informações sobre o hipervisor da instância.

- `aws:branch`: ramifica com base no fato de a instância de destino já estar executando um tipo de instância baseado em Nitro.
- `aws:branch`: verifica se o SO da instância é compatível com instâncias baseadas em Nitro.
- `aws:assertAwsResourceProperty`: verifica se a instância especificada é gerenciada pelo Systems Manager e se o status é `Online`.
- `aws:branch`: ramifica com base no fato de o dispositivo raiz da instância ser um volume do Amazon EBS.
- `aws:branch`: ramifica considerando se o atributo ENA está ativado para a instância.
- `aws:runCommand`: verifica se há drivers do ENA na instância.
- `aws:runCommand`: verifica se há drivers do NVMe na instância.
- `aws:runCommand`: verifica o arquivo `fstab` em busca de formatos não reconhecidos.
- `aws:runCommand`: verifica a configuração previsível do nome da interface na instância.
- `aws:executeScript`: gera saída com base nas etapas anteriores.

Saídas

finalOutput.output - os resultados das verificações realizadas pela automação.

AWSSupport-ConfigureEC2Metadata

Descrição

Este runbook ajuda a configurar opções do serviço de metadados de instância (IMDS) para instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Usando este runbook é possível configurar o seguinte:

- Impor o uso do IMDSv2 para metadados da instância.
- Configurar o valor de `HttpPutResponseHopLimit`.
- Permitir ou negar o acesso a metadados da instância.

Para obter mais informações sobre metadados da instância, consulte Configurar o serviço de metadados de instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EnforceIMDSv2

  Tipo: String

  Valores válidos: obrigatório | opcional

  Padrão: Optional

  Descrição: (opcional) Enforce IMDSv2. Se você escolher `required`, a instância do Amazon EC2 usará somente o IMDSv2. Se você escolher `optional`, poderá escolher entre IMDSv1 e IMDSv2 para acesso aos metadados.

  > **Important**
  >
  > Se você impor o IMDSv2, os aplicativos que usam o IMDSv1 podem não funcionar corretamente. Antes de impor o IMDSv2, certifique-se de que seus aplicativos que usam o IMDS estejam atualizados para uma versão compatível com o IMDSv2. Para obter mais informações sobre serviço de metadados de instância versão 2 (IMDSv2), consulte Configurar o serviço de metadados de instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

- HttpPutResponseHopLimit

  Tipo: Integer

  Valores válidos: de 0 a 64

  Padrão: 0

  Descrição: (opcional) o limite (1 a 64) de salto de resposta HTTP PUT desejado para solicitações de metadados de instância. Esse valor controla o número de saltos que a resposta PUT pode percorrer. Para evitar que a resposta saia da instância, especifique o 1 para o valor do parâmetro.
- InstanceId

  Tipo: String

  Descrição: (obrigatório) o ID da instância do Amazon EC2 cujas configurações de metadados você deseja definir.
- MetadataAccess

  Tipo: String

  Valores válidos: Enabled | Disabled

  Padrão: habilitado

  Descrição: (opcional) permita ou negue o acesso aos metadados da instância na instância do Amazon EC2. Se você especificar `disabled`, todos os outros parâmetros serão ignorados e o acesso aos metadados será negado para a instância.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

1. branchOnMetadataAccess: ramifica a automação com base no valor do parâmetro `MetadataAccess`.
2. disableMetadataAccess: chama a ação da API ModifyInstanceMetadataOptions para desativar o acesso ao endpoint de metadados.
3. branchOnHttpPutResponseHopLimit: ramifica a automação com base no valor do parâmetro `HttpPutResponseHopLimit`.
4. maintainHopLimitAndConfigureImdsVersion: se `HttpPutResponseHopLimit` for 0, mantém o limite de salto atual e altera outras opções de metadados.
5. waitBeforeAssertingIMDSv2State: espera 30 segundos antes de declarar o status do IMDSv2.
6. setHopLimitAndConfigureIMDSVersion: se `HttpPutResponseHopLimit` for maior que 0, configura as opções de metadados usando os parâmetros de entrada fornecidos.
7. waitBeforeAssertingHopLimit: espera 30 segundos antes de declarar as opções de metadados.
8. assertHopLimit: declara que a propriedade `HttpPutResponseHopLimit` está definida com o valor que você especificou.
9. branchVerificationOnIMDSv2Option: ramifica a verificação com base no valor do parâmetro `EnforceIMDSv2`.
10. assertIMDSv2IsOptional: declara o valor `HttpTokens` definido como `optional`.
11. assertIMDSv2IsEnforced: declara o valor `HttpTokens` definido como `required`.
12. waitBeforeAssertingMetadataState: aguarda 30 segundos antes de afirmar que o estado dos metadados está desativado.
13. assertMetadataIsDisabled: declara que os metadados estão `disabled`.
14. describeMetadataOptions: obtém as opções de metadados após a aplicação das alterações que você especificou.

Saídas

describeMetadataOptions.State

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

AWSSupport-CopyEC2Instance

Descrição

O runbook `AWSSupport-CopyEC2Instance` fornece uma solução automatizada para o procedimento descrito no artigo do Centro de Conhecimentos Como faço para mover minha instância do EC2 para outra sub-rede, zona de disponibilidade ou VPC? A automação se ramifica dependendo dos valores que você especifica para os parâmetros `Region` e `SubnetId`.

Se você especificar um valor para o parâmetro `SubnetId`, mas não um valor para o parâmetro `Region`, a automação cria uma Amazon Machine Image (AMI) da instância de destino e inicia uma nova instância na AMI da sub-rede especificada.

Se você especificar um valor para o parâmetro `SubnetId` e o parâmetro `Region`, a automação cria uma AMI da instância de destino, copia a AMI para a Região da AWS que você especificou e executa uma nova instância na AMI da sub-rede especificada.

Se você especificar um valor para o parâmetro `Region`, mas não um valor para o parâmetro `SubnetId`, a automação cria uma AMI da instância de destino, copia a AMI para a região especificada e inicia uma nova instância na AMI da sub-rede padrão da sua nuvem privada virtual (VPC) na região de destino.

Se nenhum valor for especificado para os parâmetros `Region` ou `SubnetId`, a automação cria uma AMI da instância de destino e executa uma nova instância na AMI da sub-rede padrão da sua VPC.

Para copiar uma AMI para uma região diferente, você deve fornecer um valor para o parâmetro `AutomationAssumeRole`. Se a automação expirar durante a etapa `waitForAvailableDestinationAmi`, a AMI talvez ainda esteja copiando. Se for esse o caso, você pode aguardar a conclusão da cópia e iniciar a instância manualmente.

Antes de executar esta automação, observe o seguinte:

- As AMIs são baseadas em snapshots do Amazon Elastic Block Store (Amazon EBS). Para sistemas de arquivos grandes sem um snapshot anterior, a criação de AMI pode levar várias horas. Para diminuir o tempo de criação de AMI, crie um snapshots do Amazon EBS antes de criar a AMI.
- Criar uma AMI não cria um snapshot para volumes de armazenamento de instâncias na instância. Para obter informações sobre como fazer backup de volumes de armazenamento de instâncias no Amazon EBS, consulte Como faço backup de um volume de armazenamento de instâncias na minha instância do Amazon EC2 para o Amazon EBS?

- A nova instância do Amazon EC2 tem um endereço IP IPv4 privado ou IPv6 público diferente. Você deve atualizar todas as referências aos endereços IP antigos (por exemplo, nas entradas de DNS) com os novos endereços IP atribuídos à nova instância. Se estiver usando um endereço IP elástico na instância de origem, certifique-se de anexá-lo à nova instância.
- Problemas de conflito do identificador de segurança de domínio (SID) podem ocorrer quando a cópia é iniciada e tenta entrar em contato com o domínio. Antes de capturar a AMI, use o Sysprep ou remova a instância associada ao domínio do domínio para evitar problemas de conflito. Para obter mais informações, consulte Como posso usar o Sysprep para criar e instalar AMIs reutilizáveis personalizadas do Windows?

Execute esta automação (console)

> **Important**
>
> Não recomendamos usar este runbook para copiar instâncias do controlador de domínio do Microsoft Active Directory.

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância que você deseja reinicializar.

- KeyPair

  Tipo: sequência

  Descrição: (opcional) o par de chaves que você deseja associar à instância recém-copiada. Se você estiver copiando a instância para uma região diferente, verifique se o par de chaves existe na região especificada.

- região

  Tipo: sequência

  Descrição: (opcional) a região para a qual você deseja copiar a instância. Se você especificar um valor para esse parâmetro, mas não especificar valores para os parâmetros `SubnetId` e `SecurityGroupIds`, a automação tentará iniciar a instância na VPC padrão com o grupo de segurança padrão. Se o EC2-Classic estiver ativado na região de destino, a inicialização falhará.

- SubnetId

  Tipo: sequência

  Descrição: (opcional) o ID da sub-rede na qual você deseja copiar a instância. Se o EC2-Classic estiver ativado na região de destino, você deverá fornecer um valor para esse parâmetro.

- InstanceType

  Tipo: sequência

  Descrição: (opcional) o tipo da instância que a instância copiada deve ser lançada. Se você não especificar um valor para esse parâmetro, será usado o tipo de instância de origem. Se o tipo de instância de origem não for suportado na região para a qual a instância está sendo copiada, a automação falhará.

- SecurityGroupIds

  Tipo: sequência

Descrição: (opcional) Uma lista separada por vírgulas de IDs de grupos de segurança que você deseja associar à instância copiada. Se você não especificar um valor para esse parâmetro e a instância não estiver sendo copiada para uma região diferente, os grupos de segurança associados à instância de origem serão usados. Se você estiver copiando a instância para uma região diferente, o grupo de segurança padrão da VPC padrão na região de destino será usado.

- KeepImageSourceRegion

  Tipo: booliano

  Valores válidos: verdadeiro | falso

  Padrão: true

  Descrição: (opcional) se você especificar `true` para esse parâmetro, a automação não excluirá a AMI da instância de origem. Se você especificar `false` para esse parâmetro, a automação cancelará o registro da AMI e excluirá os instantâneos associados.

- KeepImageDestinationRegion

  Tipo: booliano

  Valores válidos: verdadeiro | falso

  Padrão: true

  Descrição: (opcional) se você especificar `true` para esse parâmetro, a automação não excluirá a AMI que é copiada para a região especificada. Se você especificar `false` para esse parâmetro, a automação cancelará o registro da AMI e excluirá os instantâneos associados.

- NoRebootInstanceBeforeTakingImage

  Tipo: booliano

  Valores válidos: verdadeiro | falso

  Padrão: falso

  Descrição: (opcional) se você especificar `true` para esse parâmetro, a instância de origem não será reiniciada antes de criar a AMI. Quando esta opção é usada, não é possível garantir a integridade do sistema de arquivos na imagem criada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Se estiver copiando a instância em outra região, você também precisará das seguintes permissões:

- `ec2:CopyImage`

Etapas do documento

- describeOriginalInstanceDetails: reúne detalhes da instância a ser copiada.
- assertRootVolumeIsEBS: verifica se o tipo de dispositivo de volume raiz é `ebs`, se não, encerra a automação.
- evalInputParameters: avalia os valores fornecidos para os parâmetro de entrada.
- createLocalAmi: cria uma AMI da instância de origem.
- tagLocalAmi: marca a AMI criada na etapa anterior.
- branchAssertRegionIsSame: ramifica com base no fato de a instância estar sendo copiada na mesma região ou para outra região.
- branchAssertSameRegionWithKeyPair: ramifica com base no fato de um valor ter sido fornecido para o parâmetro `KeyPair` de uma instância que está sendo copiada na mesma região.
- sameRegionLaunchInstanceWithKeyPair: lança uma instância do Amazon EC2 na AMI da instância de origem na mesma sub-rede ou na sub-rede especificada usando o par de chaves que você especificou.
- sameRegionLaunchInstanceWithoutKeyPair: lança uma instância do Amazon EC2 na AMI da instância de origem na mesma sub-rede ou na sub-rede especificada sem um par de chaves.
- copyAmiToRegion: copia a AMI para a região de destino.
- waitForAvailableDestinationAmi: espera que o estado copiado da AMI se torne `available`.

- destinationRegionLaunchInstance: lança uma instância do Amazon EC2 usando a AMI copiada.
- branchAssertDestinationAmiToDelete: ramifica com base no valor fornecido para o parâmetro `KeepImageDestinationRegion`.
- deregisterDestinationAmiAndDeleteSnapshots: cancela o registro das AMIs copiadas e exclui os instantâneos associados.
- branchAssertSourceAmiTodelete: ramifica com base no valor fornecido para o parâmetro `KeepImageSourceRegion`.
- deregisterSourceAmiAndDeleteSnapshots: cancela o registro das AMIs criadas a partir da instância de origem e exclui os instantâneos associados.
- sleep: coloca a automação em repouso por 2 segundos. Estea é uma etapa terminal.

Saídas

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstance.DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

Descrição

O runbook `AWSSupport-EnableWindowsEC2SerialConsole` ajuda você a habilitar o Amazon EC2 Serial Console, o Special Admin Console (SAC) e o menu de inicialização em sua instância Windows do Amazon EC2. Com o recurso Amazon Elastic Compute Cloud (Amazon EC2) Serial Console, você tem acesso à porta serial da sua instância do Amazon EC2 para solucionar problemas de inicialização, configuração de rede e outros problemas. O runbook automatiza as etapas necessárias para habilitar o recurso em instâncias em estado de execução e gerenciadas por AWS Systems Manager, bem como naquelas em estado parado ou não gerenciadas por. AWS Systems Manager

Como funciona?

O runbook de `AWSSupport-EnableWindowsEC2SerialConsole` automação ajuda a habilitar o SAC e o menu de inicialização nas instâncias do Amazon EC2 que executam o Microsoft Windows Server. Para instâncias em estado de execução e gerenciadas por AWS Systems Manager, o

runbook executa um PowerShell script AWS Systems Manager Executar comando para ativar o SAC e o menu de inicialização. Para instâncias em estado parado ou não gerenciadas por AWS Systems Manager, o runbook usa o AWSSupport-startEC2 RescueWorkflow para criar uma instância temporária do Amazon EC2 para realizar as alterações necessárias off-line.

Para obter mais informações, consulte Amazon EC2 Serial Console para instâncias do Windows.

Important

- Se você habilitar o SAC em uma instância, os serviços do Amazon EC2 que dependem da recuperação de senha não funcionarão no console do Amazon EC2. Para mais informações, consulte Use SAC to troubleshoot your Windows instance (Usar o SAC para solucionar problemas de instâncias do Windows).
- Para configurar o acesso ao console serial, você deve conceder acesso ao console serial no nível da conta e, em seguida, configurar políticas AWS Identity and Access Management (IAM) para conceder acesso aos seus usuários. Você também deve configurar um usuário com senha em cada instância para que seus usuários possam usar o console serial para solução de problemas. Para obter mais informações, consulte Configurar o acesso ao console serial do Amazon EC2.
- Para ver se o console serial está ativado em sua conta, consulte Exibir o status de acesso da conta ao console serial.
- O acesso ao console serial só é suportado em instâncias virtualizadas criadas no Sistema Nitro.

Para obter mais informações, consulte os pré-requisitos do console serial do Amazon EC2.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-EnableWindowsEC2SerialConsole` no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId: (Obrigatório)

     O ID da instância do Amazon EC2 que você deseja habilitar para o console serial do Amazon EC2 (SAC) e o menu de inicialização.
   - AutomationAssumeRole: (Opcional)

     O Amazon Resource Name (ARN) da função do IAM que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - HelperInstanceType: (Condicional)

     O tipo de instância do Amazon EC2 que o runbook provisiona para configurar o console serial do Amazon EC2 para uma instância offline.
   - HelperInstanceProfileName: (Condicional)

     O nome de um perfil de instância do IAM existente para a instância auxiliar. Se você estiver habilitando o SAC e o menu de inicialização em uma instância que está parada ou não é gerenciada por AWS Systems Manager, isso é necessário. Se um perfil de instância do IAM não for especificado, a automação cria um em seu nome.
   - SubnetId: (Condicional)

     O ID da sub-rede de uma instância auxiliar. Por padrão, ele usa a mesma sub-rede em que a instância fornecida reside.

     > **Important**
     >
     > Se você fornecer uma sub-rede personalizada, ela deverá estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do Systems Manager. Isso só

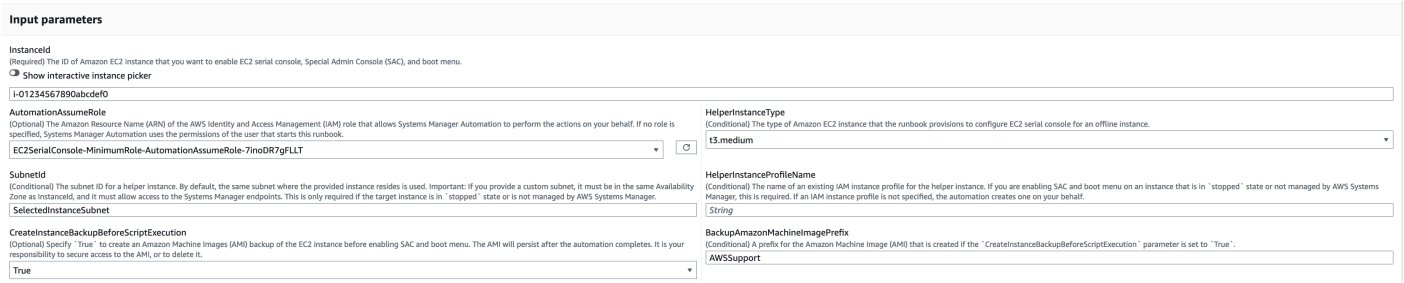
é necessário se a instância de destino estiver parada ou não for gerenciada pelo AWS Systems Manager.

- CreateInstanceBackupBeforeScriptExecution: (Opcional)

  Especifique True para criar um backup da Amazon Machine Images (AMI) da instância do Amazon EC2 antes de ativar o SAC e o menu de inicialização. A AMI persistirá depois da conclusão da automação. É sua responsabilidade proteger o acesso à AMI ou excluí-la.

- BackupAmazonMachineImagePrefix: (Condicional)

  Um prefixo para a Amazon Machine Image (AMI) que é criado se o `CreateInstanceBackupBeforeScriptExecution` parâmetro estiver definido como. `True`



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckIfEc2SerialConsoleAccessEnabled:

     Verifica se o acesso ao console serial do Amazon EC2 está habilitado no nível da conta. Nota: O acesso ao console serial não está disponível por padrão. Para obter mais informações, consulte Configurar o acesso ao console serial do Amazon EC2.

   - CheckIfEc2InstanceIsWindows:

     Afirma se a plataforma da instância de destino é o Windows.

   - GetInstanceType:

     Recupera o tipo de instância da instância de destino.

   - CheckIfInstanceTypeIsNitro:

     Verifica se o hipervisor do tipo de instância é baseado em Nitro. O acesso ao console serial só é suportado em instâncias virtualizadas criadas no sistema Nitro.

- CheckIfInstanceIsInAutoScalingGrupo:

  Verifica se a instância do Amazon EC2 faz parte de um grupo do Amazon EC2 Auto Scaling chamando a API. `DescribeAutoScalingInstances` Se a instância fizer parte de um grupo do Amazon EC2 Auto Scaling, ela garante que a instância do Porting Assistant para o.NET esteja no estado de ciclo de vida em espera.

- WaitForEc2InstanceStateStablized:

  Espera que a instância esteja em execução ou parada.

- GetEc2InstanceState:

  Obtém o estado atual da instância.

- BranchOnEc2InstanceState:

  Ramificações com base no estado da instância recuperado na etapa anterior. Se esse estado de instância estiver em execução, ele vai para a `CheckIfEc2InstanceIsManagedBySSM` etapa e, se não, vai para a `CheckIfHelperInstanceProfileIsProvided` etapa.

- CheckIfEc2 InstanceIsManagedBy SMS:

  Verifica se a instância é gerenciada pelo AWS Systems Manager. Se gerenciado, o runbook ativa o SAC e o menu de inicialização usando um PowerShell comando Executar.

- BranchOnPreEC2: RescueBackup

  Ramificações com base no parâmetro `CreateInstanceBackupBeforeScriptExecution` de entrada.

- CreateAmazonMachineImageBackup:

  Cria um backup da AMI da instância.

- Habilite o SAC: AndBootMenu

  Ativa o SAC e o menu de inicialização executando um script PowerShell Executar comando.

- RebootInstance:

  Reinicializa a instância do Amazon EC2 para aplicar a configuração. Essa é a etapa final se a instância estiver on-line e for gerenciada pelo AWS Systems Manager.

- CheckIfHelperInstanceProfileIsProvided:

Verifica se o `HelperInstanceProfileName` especificado existe antes de ativar o SAC e o menu de inicialização off-line usando uma instância temporária do Amazon EC2.

- RunAutomationToInjectOfflineScriptForHabilitando o SAC: AndBootMenu

  Executa o `AWSSupport-StartEC2RescueWorkflow` para ativar o SAC e o menu de inicialização quando a instância está parada ou não é gerenciada pelo AWS Systems Manager.

- GetExecutionDetails:

  Recupera o ID da imagem do backup e da saída do script offline.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   - Habilite o SAC. Saída: AndBootMenu

     Saída da execução do comando na `EnableSACAndBootMenu` etapa.

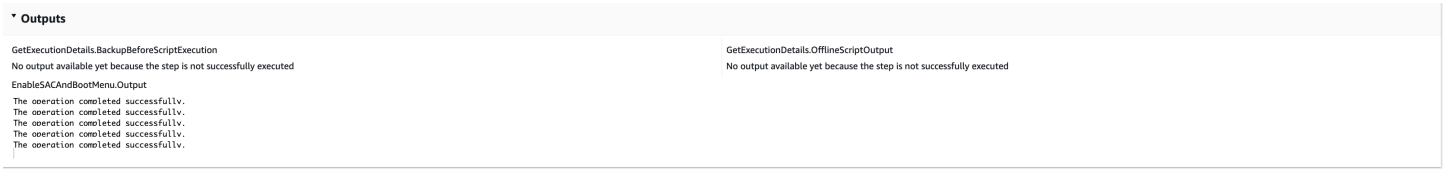
   - GetExecutionDetails.OfflineScriptOutput:

     Saída do script off-line executado na `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` etapa.

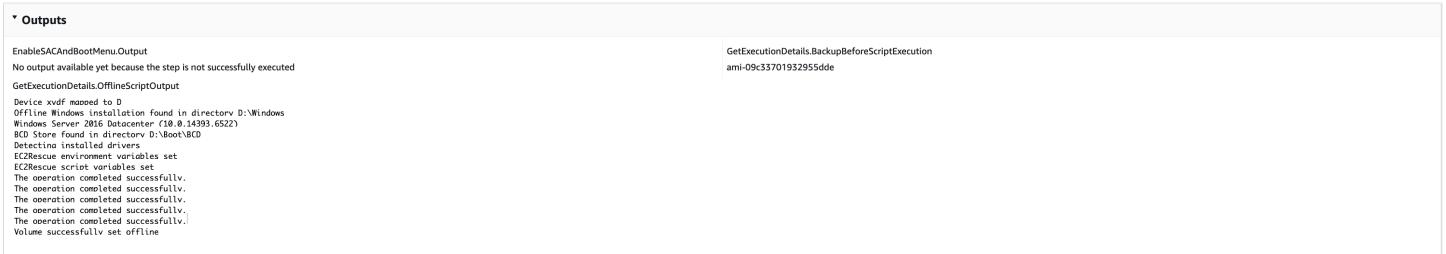
   - GetExecutionDetails.BackupBeforeScriptExecution:

     ID da imagem do backup da AMI obtido se o parâmetro `CreateInstanceBackupBeforeScriptExecution` de entrada for True.

Saída de execução em uma instância que está sendo executada e gerenciada pelo AWS Systems Manager



Saída da execução em uma instância interrompida ou não gerenciada pelo AWS Systems Manager



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-ExecuteEC2Rescue

Descrição

Este runbook usa a ferramenta EC2Rescue para solucionar problemas e, quando possível, reparar problemas comuns de conectividade com a instância do Amazon Elastic Compute Cloud (Amazon EC2) para Linux ou Windows Server. Não há suporte para instâncias com volumes raiz criptografados.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EC2RescueInstanceType

  Tipo: sequência

  Valores permitidos: t2.small | t2.medium | t2.large

  Padrão: t2.small

  Descrição: (obrigatório) o tipo de instância do EC2 para a instância do EC2Rescue. Tamanho recomendado: `t2.small`

- LogDestination

  Tipo: sequência

  Descrição: (opcional) nome do bucket do Amazon S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- SubnetId

  Tipo: sequência

  Padrão: CreateNewVPC

  Descrição: (opcional) o ID de sub-rede para a instância do EC2Rescue. Por padrão, a Automação do AWS Systems Manager cria uma nova VPC. Como alternativa, Use `SelectedInstanceSubnet` para usar a mesma sub-rede que sua instância ou especifique um ID de sub-rede personalizado.

  > **Important**
  >
  > A sub-rede deve estar na mesma zona de disponibilidade que o `UnreachableInstanceId`, e deve permitir acesso aos endpoints SSM.

- UnreachableInstanceId

  Tipo: sequência

  Descrição: (Obrigatório) ID de sua instância do EC2 inacessível.

> **Important**
>
> O Systems Manager Automation interrompe essa instância e cria uma AMI antes de tentar qualquer operação. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um endereço IP elástico.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Você deve ter pelo menos `ssm:StartAutomationExecution` e `ssm:GetAutomationExecution` para poder ler a saída de automação. Para mais informações sobre as permissões necessárias, consulte `AWSSupport-StartEC2RescueWorkflow`.

Etapas do documento

1. `aws:assertAwsResourceProperty`: afirma se a instância fornecida é Windows Server:
   a. (EC2Rescue para Windows Server) se a instância fornecida for uma instância do Windows Server:
      i. `aws:executeAutomation`: invoca `AWSSupport-StartEC2RescueWorkflow` com o EC2Rescue para script offline do Windows Server.
      ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.
      iii. `aws:executeAwsApi`: recupera o resumo do EC2Rescue da automação aninhada.
   b. (EC2Rescue para Linux) se a instância fornecida for uma instância do Linux:
      i. `aws:executeAutomation`: invoca `AWSSupport-StartEC2RescueWorkflow` com o EC2Rescue para scripts offline do Linux
      ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.
      iii. `aws:executeAwsApi`: recupera o resumo do EC2Rescue da automação aninhada.

Saídas

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descrição

O runbook `AWSSupport-ListEC2Resources` retorna informações sobre instâncias do Amazon EC2 e recursos relacionados, como volumes do Amazon Elastic Block Store (Amazon EBS), endereços IP elásticos e grupos do Amazon EC2 Auto Scaling das Regiões da AWS que você especificar. Por padrão, as informações são coletadas de todas as regiões e exibidas na saída da automação. Opcionalmente, você pode especificar um bucket do Amazon Simple Storage Service (Amazon S3) para o qual as informações serão carregadas, como um arquivo de valores separados por vírgula (.csv).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Bucket

Tipo: sequência

Descrição: (opcional) o nome do bucket do S3 onde as informações coletadas são carregadas.

- DisplayResourceDeletionDocumentation

  Tipo: sequência

  Padrão: true

  Descrição: (opcional) se definida como `true`, a automação cria links na saída para a documentação relacionada à exclusão de seus recursos.

- RegionsToQuery

  Tipo: sequência

  Padrão: all

  Descrição: (opcional) as regiões das quais você deseja coletar informações relacionadas ao Amazon EC2.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Além disso, para carregar com sucesso as informações coletadas no bucket do S3 que você especificar, a `AutomationAssumeRole` requer as seguintes ações:

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

Etapas do documento

- aws:executeAwsApi: reúne as regiões ativadas para a conta.
- aws:executeScript: confirma que as regiões ativadas para a conta suportam as regiões especificadas no parâmetro RegionsToQuery.
- aws:branch: se nenhuma região estiver ativada para a conta, a automação será encerrada.
- aws:executeScript: lista todas as instâncias do EC2 para a conta e as regiões que você especificar.
- aws:executeScript: lista todas as imagens de máquina da Amazon (AMI) para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os volumes do EBS para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os endereços IP elásticos da conta e das regiões que você especificar.
- aws:executeScript: lista todas as interfaces de rede elástica para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os grupos do Auto Scaling da conta e das regiões que você especificar.
- aws:executeScript: lista todos os balanceadores de carga da conta e das regiões que você especificar.
- aws:executeScript: carrega as informações coletadas no bucket do S3 especificado se você fornecer um valor para o parâmetro Bucket.

AWSSupport-ManageRDPSettings

Descrição

O AWSSupport-ManageRDPSettings runbook permite que o usuário gerencie configurações comuns do Remote Desktop Protocol (RDP), como a porta do RDP e o Network Layer Authentication (NLA). Por padrão, o runbook lê e exibe os valores das configurações.

> **Important**
>
> As alterações nas configurações do RDP devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: String

  Descrição: (Obrigatório) O ID da instância gerenciada para gerenciar as configurações de RDP.
- NLASettingAction

  Tipo: String

  Valores válidos: Check | Enable | Disable

  Padrão: Check

Descrição: (obrigatório) uma ação para executar na configuração NLA: Check, Enable, Disable.

- RDPPort

  Tipo: String

  Padrão: 3389

  Descrição: (Opcional) Especifique a nova porta do RDP. Usado apenas quando a ação é definida como Modify. O número da porta deve estar entre 1025 e 65535. Observação: Após a porta ser alterada, o serviço do RDP será reiniciado.

- RDPPortAction

  Tipo: String

  Valores válidos: Check | Modify

  Padrão: Check

  Descrição: (obrigatório) uma ação a ser aplicada à porta do RDP.

- RemoteConnections

  Tipo: String

  Valores válidos: Check | Enable | Disable

  Padrão: Check

  Descrição: (obrigatório) uma ação para executar na configuração fDenyTSConnections.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

A instância do EC2 que recebe o comando deve ter uma função do IAM com a política gerenciada da Amazon AmazonSSMManagedInstanceCore anexada. O usuário deve ter pelo menos ssm:SendCommand para enviar o comando para a instância, além de ssm:GetCommandInvocation para poder ler a saída do comando.

Etapas do documento

`aws:runCommand`: execute o script do PowerShell para alterar ou verificar as configurações do RDP na instância de destino.

Saídas

manageRDPSettings.Output

AWSSupport-ManageWindowsService

Descrição

O runbook `AWSSupport-ManageWindowsService` permite que você pare, inicie, reinicie, pause ou desative qualquer serviço do Windows na instância de destino.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância gerenciada para gerenciar os serviços de

- ServiceAction

  Tipo: sequência

  Valores permitidos: Check,Restart,Force-Restart,Start,Stop,Force-Stop,Pause

  Padrão: Check

  Descrição: (obrigatório) uma ação a ser aplicada ao serviço do Windows. Observe que `Force-Restart` e `Force-Stop` podem ser usados para reiniciar e interromper um serviço que tem serviços dependentes.
- StartupType

  Tipo: sequência

  Valores permitidos: Check | Auto | Demand | Disabled | DelayedAutoStart

  Padrão: Check

  Descrição: (Obrigatório) Um tipo de startup a ser aplicado ao serviço Windows.
- WindowsServiceName

  Tipo: sequência

  Descrição: (Obrigatório) Um nome de serviço válido do Windows.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a instância do EC2 que recebe o comando tenha uma função do IAM com a política gerenciada pela Amazon AmazonSSMManagedInstanceCore anexada. O usuário deve ter pelo menos ssm:StartAutomationExecution and ssm:SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída de automação.

Etapas do documento

`aws:runCommand`: executar o script do PowerShell para aplicar a configuração desejada ao serviço do Windows na instância de destino.

Saídas

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

Descrição

O runbook `AWSSupport-MigrateEC2ClassicToVPC` migra uma instância do Amazon Elastic Compute Cloud (Amazon EC2) do EC2-Classic para uma nuvem privada virtual (VPC). Esse runbook oferece suporte à migração de instâncias do Amazon EC2 do tipo de virtualização de máquina virtual de hardware (HVM) com volumes raiz do Amazon Elastic Block Store (Amazon EBS).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ApproverIAM

  Tipo: StringList

  Descrição: (Opcional) Os nomes de recursos da Amazon (ARNs) dos usuários do IAM que podem aprovar ou negar a ação. Esse parâmetro só é aplicável se você especificar o valor `CutOver` para o parâmetro `MigrationType`.

- DestinationSecurityGroupId

  Tipo: StringList

  Descrição: (Opcional) O ID do grupo de segurança que você deseja associar à instância do Amazon EC2 que é iniciada em sua VPC. Se você não especificar um valor para esse parâmetro, a automação cria um grupo de segurança em sua VPC e copia as regras do grupo de segurança no EC2-Classic. Se as regras não forem copiadas para o novo grupo de segurança, o padrão da VPC estará associado à instância do Amazon EC2.

- DestinationSubnetId

  Tipo: sequência

  Descrição: (opcional) o ID da sub-rede para a qual você deseja migrar a instância do Amazon EC2. Se você não especificar um valor para esse parâmetro, a automação escolherá aleatoriamente uma sub-rede da VPC.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2 para a qual você deseja migrar.

- MigrationType

  Tipo: sequência

  Valores válidos: CutOver | Test

  Descrição: (obrigatório) o tipo de migração que você deseja executar.

  A opção `CutOver` exige aprovação para interromper sua instância do Amazon EC2 que está sendo executada no EC2-Classic. Depois que essa ação é aprovada, a instância do Amazon EC2 é interrompida e a automação cria uma Amazon Machine Image (AMI). Quando o status da AMI é `available`, uma nova instância do Amazon EC2 é iniciada a partir dessa AMI no `DestinationSubnetId` que você especifica em sua VPC. Se sua instância do Amazon EC2 que está sendo executada no EC2-Classic tiver um endereço IP elástico anexado, a instância será movida para a instância recém-criada do Amazon EC2 em sua VPC. Se a instância do Amazon EC2 iniciada em sua VPC falhar na criação por qualquer motivo, ela será encerrada e a aprovação será solicitada para iniciar sua instância do Amazon EC2 no EC2-Classic.

A opção `Test` cria uma AMI da sua instância do Amazon EC2 que está sendo executada no EC2-Classic sem reinicialização. Como a instância do Amazon EC2 não é reinicializada, não podemos garantir a integridade do sistema de arquivos da imagem criada. Quando o status da AMI é `available`, uma nova instância do Amazon EC2 é iniciada a partir dessa AMI no `DestinationSubnetId` que você especifica em sua VPC. Se sua instância do Amazon EC2 que está sendo executada no EC2-Classic tiver um endereço IP elástico anexado, a automação verificará se o `DestinationSubnetId` que você especificou é público. Se a instância do Amazon EC2 iniciada em sua VPC falhar na criação por qualquer motivo, ela será encerrada e a automação terminará.

- SNSNotificationARNforApproval

  Tipo: sequência

  Descrição: (opcional) o ARN do tópico do Amazon Simple Notification Service (Amazon SNS) para o qual você deseja enviar solicitações de aprovação. Esse parâmetro só é aplicável se você especificar o valor `CutOver` para o parâmetro `MigrationType`.

- TargetInstanceType

  Tipo: sequência

  Padrão: t2.2xlarge

  Descrição: (opcional) o ID da instância do Amazon EC2 que você deseja iniciar em seu VPC. Somente tipos de instância baseados em Xen, como T2, M4 ou C4, são suportados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi: reúne detalhes sobre a instância do Amazon EC2 especificada no parâmetro InstanceId.
- aws:assertAwsResourceProperty: confirma que o tipo de instância que você especifica no parâmetro TargetInstanceType é baseado em Xen.
- aws:assertAwsResourceProperty: confirma que a instância do Amazon EC2 que você especifica no parâmetro InstanceId é do tipo virtualização de HVM.

- `aws:assertAwsResourceProperty`: confirma que a instância do Amazon EC2 que você especifica no parâmetro `InstanceId` tem um volume raiz do Amazon EBS.
- `aws:executeScript`: cria um grupo de segurança conforme necessário, dependendo do valor que você especificar para o parâmetro `DestinationSecurityGroupId`.
- `aws:branch`: ramifica com base no valor que você especifica no parâmetro `DestinationSubnetId`.
- `aws:executeAwsApi`: identifica a VPC padrão na Região da AWS em que você executa essa automação.
- `aws:executeAwsApi`: escolhe aleatoriamente o ID de uma sub-rede localizada na VPC padrão.
- `aws:createImage`: cria uma AMI sem reinicializar a instância do Amazon EC2.
- `aws:branch`: ramifica com base no valor que você especifica para o parâmetro `MigrationType`.
- `aws:branch`: ramifica com base no valor que você especifica para o parâmetro `DestinationSubnetId`.
- `aws:runInstances`: inicia uma nova instância a partir da AMI criada sem reinicializar a instância do Amazon EC2 no EC2-Classic.
- `aws:changeInstanceState`: encerra a instância recém-iniciada do Amazon EC2 se a etapa anterior falhar por qualquer motivo.
- `aws:runInstances`: lança uma nova instância a partir da AMI criada sem reinicializar a instância do Amazon EC2 no EC2-Classic no `DestinationSubnetId`, se fornecido.
- `aws:changeInstanceState`: encerra a instância recém-iniciada do Amazon EC2 se a etapa anterior falhar por qualquer motivo.
- `aws:assertAwsResourceProperty`: confirma o comportamento de parada da instância do Amazon EC2 em execução no EC2-Classic.
- `aws:approve`: aguarda a aprovação para interromper a instância do Amazon EC2.
- `aws:changeInstanceState`: interrompe a execução da instância do Amazon EC2 no EC2-Classic.
- `aws:changeInstanceState`: força a interrupção da execução da instância do Amazon EC2 no EC2-Classic, se necessário.
- `aws:createImage`: cria uma AMI da instância do Amazon EC2 depois que ela é interrompida.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `DestinationSubnetId`.
- `aws:runInstances`: inicia uma nova instância a partir da AMI criada da instância interrompida do Amazon EC2 no EC2-Classic.

- `aws:approve`: aguarda a aprovação para encerrar a instância recém-iniciada e inicia a instância do Amazon EC2 no EC2-Classic se a etapa anterior falhar por qualquer motivo.
- `aws:changeInstanceState`: encerra a instância do Amazon EC2 recém-iniciada.
- `aws:runInstances`: inicia uma nova instância a partir da AMI criada da instância interrompida do Amazon EC2 no EC2-Classic a partir do parâmetro `DestinationSubnetId`.
- `aws:approve`: aguarda a aprovação para encerrar a instância recém-iniciada e inicia a instância do Amazon EC2 no EC2-Classic se a etapa anterior falhar por qualquer motivo.
- `aws:changeInstanceState`: encerra a instância do Amazon EC2 recém-iniciada.
- `aws:changeInstanceState`: inicia a instância do Amazon EC2 que foi interrompida no EC2-Classic.
- `aws:branch`: ramifica com base em se a instância do Amazon EC2 tem um endereço IP público.
- `aws:executeAwsApi`: verifica se o endereço IP público é um endereço IP elástico.
- `aws:branch`: ramifica com base no valor que você especifica no parâmetro `MigrationType`.
- `aws:executeAwsApi`: move o endereço IP elástico para sua VPC.
- `aws:executeAwsApi`: coleta o ID de alocação do endereço IP elástico que foi movido para a VPC.
- `aws:branch`: ramifica com base em qual sub-rede a instância do Amazon EC2 em execução na sua VPC foi iniciada.
- `aws:executeAwsApi`: anexa o endereço IP elástico à instância recém-iniciada em sua VPC.
- `aws:executeScript`: confirma à sub-rede que a instância recém-iniciada do Amazon EC2 em execução na sua VPC é pública.

Saídas

`getInstanceProperties.virtualizationType`: o tipo de virtualização da instância do Amazon EC2 em execução no EC2-Classic.

`getInstanceProperties.rootDeviceType`: o tipo de dispositivo raiz da instância do Amazon EC2 em execução no EC2-Classic.

`createAMIWithoutReboot.ImageId`: o ID da AMI criada sem reinicializar a instância do Amazon EC2 em execução no EC2-Classic.

`getDefaultVPC.VpcId`: o ID da VPC padrão em que a nova instância do Amazon EC2 é iniciada se um valor para o parâmetro `DestinationSubnetId` não for fornecido.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`: o ID da sub-rede na VPC padrão em que a nova instância do Amazon EC2 é iniciada se um valor para o parâmetro `DestinationSubnetId` não for fornecido.

`launchTestInstanceDefaultVPC.InstanceIds`: o ID da instância recém-iniciada do Amazon EC2 em sua VPC padrão durante o tipo de migração `Test`.

`launchTestInstanceProvidedSubnet.InstanceIds`: o ID da instância recém-iniciada do Amazon EC2 na `DestinationSubnetId` que você especificou durante o tipo de migração `Test`.

`createAMIAfterStoppingInstance.ImageId`: o ID da AMI criada após interromper a execução da instância do Amazon EC2 no EC2-Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`: o ID da instância recém-iniciada do Amazon EC2 na `DestinationSubnetId` que você especificou durante o tipo de migração `CutOver`.

`launchCutOverInstanceDefaultVPC.InstanceIds`: o ID da instância recém-iniciada do Amazon EC2 em sua VPC padrão durante o tipo de migração `CutOver`.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`: se a sub-rede escolhida pela automação em sua VPC padrão é pública.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`: se a sub-rede que você especificou no `DestinationSubnetId` é pública.

AWSSupport-MigrateXenToNitroLinux

Descrição

O runbook `AWSSupport-MigrateXenToNitroLinux` clona, prepara e migra uma instância Linux Xen do Amazon Elastic Compute Cloud (Amazon EC2) para um tipo de instância Nitro. Este runbook fornece duas opções para tipos de operação:

- `Clone&Migrate`: Esse workflow de opção consiste nas fases verificações preliminares, testes e Clone&Migrate. O workflow é executado usando o runbook `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro`.
- `FullMigration`: essa opção executa o runflow `Clone&Migrate` e, em seguida, executa a etapa adicional de Substituir volumes raiz do Amazon EBS.

> **Important**
>
> O uso desse runbook gera custos para sua conta do tempo de execução das instâncias do Amazon EC2, criação de volumes do Amazon Elastic Block Store (Amazon EBS) e AMIs. Para obter mais detalhes, consulte Amazon EC2 Pricing e Amazon EBS Pricing.

Verificações preliminares

A automação realiza as seguintes verificações preliminares antes de continuar com a migração. Se alguma das verificações falha, a automação é encerrada. Essa fase é apenas parte do workflow `Clone&Migrate`.

- Verifica se a instância de destino já é um tipo de instância Nitro.
- Verifica se a opção de compra de instâncias spot foi usada para a instância de destino.
- Verifica se os volumes de armazenamento de instâncias estão anexados à instância de destino.
- Verifica se a instância do sistema operacional de destino é Linux.
- Verifica se a instância de destino faz parte de um grupo do Amazon EC2 Auto Scaling. Se fizer parte de um grupo do Auto Scaling, a automação verifica se a instância está no estado `standby`.
- Verifica se a instância é gerenciada pelo AWS Systems Manager.

no dispositivo

A automação cria um Amazon Machine Image (AMI) a partir da instância de destino e inicia uma instância de teste a partir da AMI recém-criada. Essa fase é apenas parte do workflow `Clone&Migrate`.

Se a instância de teste passar por todas as verificações de status, a automação será interrompida e a aprovação das entidades principais designadas será solicitada por meio de notificação do Amazon Simple Notification Service (Amazon SNS). Se a aprovação for fornecida, a automação encerra a instância de teste, interrompe a instância de destino e continua com a migração, enquanto o registro da AMI recém-criada é cancelado no final do workflow `Clone&Migrate`.

> **Note**
>
> Antes de fornecer a aprovação, recomendamos verificar se todos os aplicativos em execução na instância de destino foram fechados corretamente.

Clonar e migrar

A automação cria outra AMI a partir da instância de destino e inicia uma nova instância para mudar para um tipo de instância Nitro. A automação conclui as seguintes verificações preliminares antes de continuar com a migração. Se alguma das verificações falha, a automação é encerrada. Essa fase também é apenas parte do workflow `Clone&Migrate`.

- Ativa o atributo de redes avançadas (ENA).
- Instala a versão mais recente dos drivers ENA, se ainda não estiverem instalados, ou atualiza a versão dos drivers ENA para a versão mais recente. Para garantir o máximo desempenho da rede, é necessário atualizar para a versão mais recente do driver ENA se o tipo de instância Nitro for da 6ª geração.
- Verifica se o módulo NVMe está instalado. Se o módulo estiver instalado, a automação verificará se o módulo está carregado em `initramfs`.
- Analisa `/etc/fstab` e substitui entradas por nomes de dispositivos de blocos (`/dev/sd*` ou `/dev/xvd*`) por seus respectivos UUIDs. Antes de modificar a configuração, a automação cria um backup do arquivo no caminho `/etc/fstab*`.
- Desativa a nomenclatura previsível da interface adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no arquivo `/etc/default/grub`, se ela existir, ou ao kernel em `/boot/grub/menu.lst`.
- Remove o arquivo `/etc/udev/rules.d/70-persistent-net.rules`, se ele existir. Antes de remover o arquivo, a automação cria um backup do arquivo no caminho `/etc/udev/rules.d/`.

Depois de verificar todos os requisitos, o tipo de instância é alterado para o tipo de instância Nitro que você especificar. A automação espera que a instância recém-criada passe por todas as verificações de status depois de começar como um tipo de instância Nitro. Em seguida, a automação aguarda a aprovação das entidades principais designadas para criar uma AMI das instâncias Nitro iniciadas com sucesso. Se a aprovação for negada, a automação será encerrada, deixando a instância recém-criada em execução e a instância de destino permanecerá parada.

Substituir um volume do Amazon EBS

Se você escolher `FullMigration` como `OperationType`, a automação migrará a instância de destino do Amazon EC2 para o tipo de instância Nitro que você especificar. A automação solicita aprovação das entidades principais designadas para substituir o volume raiz do Amazon EBS da instância de destino do Amazon EC2 pelo volume raiz da instância clonada do Amazon EC2. Depois que a migração for bem-sucedida, a instância clonada do Amazon EC2 será encerrada. Se

a automação falhar, o volume raiz original do Amazon EBS será anexado à instância de destino do Amazon EC2. Se o volume raiz do Amazon EBS anexado à instância do Amazon EC2 de destino tiver tags com o prefixo `aws:` aplicado, a operação `FullMigration` não será suportada.

Antes de começar

A instância de destino deve ter acesso de saída à internet. Isso serve para acessar repositórios de drivers e dependências como kernel-devel, gcc, patch, rpm-build, wget, dracut, make, linux-headers e unzip. O gerenciador de pacotes é usado se necessário.

É necessário um tópico do Amazon SNS para enviar notificações de aprovações e atualizações. Para obter mais informações sobre como criar um tópico Amazon SNS, consulte Criar um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Este runbook é compatível com os seguintes sistemas operacionais:

- RHEL 7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS e 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

Tipo: sequência

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Acknowledgement

  Tipo: sequência

  Descrição: (obrigatório) lê os detalhes completos das ações executadas por esse runbook de automação e insere **`Yes, I understand and acknowledge`** para continuar usando o runbook.

- ApproverIAM

  Tipo: sequência

  Descrição: (obrigatório) os ARNs dos perfis, usuários ou nomes de usuário do IAM que podem fornecer aprovações para a automação. Você pode especificar um máximo de 10 aprovadores.

- DeleteResourcesOnFailure

  Tipo: booliano

  Descrição: (opcional) determina se a instância e a AMI recém-criadas para a migração serão excluídas se a automação falhar.

  Valores válidos: True | False

  Padrão: True

- MinimumRequiredApprovals

  Tipo: sequência

  Descrição: (opcional) o número mínimo de aprovações necessárias para continuar executando a automação quando as aprovações são solicitadas.

  Valores válidos: de 1 a 10

  Padrão: 1

- NitroInstanceType

  Tipo: sequência

  Descrição: (obrigatório) o tipo de instância Nitro para o qual você deseja alterar a instância. Os tipos de instância compatíveis incluem M5, M6, C5, C6, R5, R6 e T3.

  Padrão: m5.xlarge
- OperationType

  Tipo: sequência

  Descrição: (obrigatório) o operação que você deseja executar. A opção `FullMigration` executa as mesmas tarefas que `Clone&Migrate` e, além disso, substitui o volume raiz da sua instância de destino. O volume raiz da instância de destino é substituído pelo volume raiz da instância recém-criada após o processo de migração. A operação `FullMigration` não suporta volumes raiz definidos pelo Logical Volume Manager (LVM).

  Valores válidos: Clone&Migrate | FullMigration
- SNSTopicArn

  Tipo: sequência

  Descrição: (obrigatório) o ARN do tópico do Amazon SNS no qual publicar a notificação. O tópico do Amazon SNS é usado para enviar as notificações de aprovação necessárias durante a automação.
- TargetInstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2.

workflow do Clone&Migrate

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- `startOfPreliminaryChecksBranch`: ramifica o workflow de verificações preliminares.
- `getTargetInstanceProperties`: reúne detalhes da instância de destino.

- `checkIfNitroInstanceTypeIsSupportedInAZ`: determina se o tipo de instância de destino do Amazon EC2 é compatível com a mesma zona de disponibilidade da instância de destino.
- `getXenInstanceTypeDetails`: reúne detalhes sobre o tipo de instância de origem.
- `checkIfInstanceHypervisorIsNitroAlready`: verifica se a instância de destino já está sendo executada como um tipo de instância Nitro.
- `checkIfTargetInstanceLifecycleIsSpot`: verifica se a opção de compra de instância de destino é Spot.
- `checkIfOperatingSystemIsLinux`: verifica se o sistema operacional da instância de destino é Linux.
- `verifySSMConnectivityForTargetInstance`: verifica se a instância de destino é gerenciada pelo Systems Manager.
- `checkIfEphemeralVolumeAreSupported`: verifica se o tipo de instância atual da instância de destino é compatível com volumes de armazenamento de instância.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`: verifica se a instância de destino tem volumes de armazenamento de instância anexados.
- `checkIfRootVolumeIsEBS`: verifica se o tipo de volume raiz da instância de destino é EBS.
- `checkIfTargetInstanceIsInASG`: verifica se a instância de destino faz parte de um grupo do Auto Scaling.
- `endOfPreliminaryChecksBranch`: fim da ramificação de verificações preliminares.
- `startOfTestBranch`: ramifica para o workflow de testes.
- `createTestImage`: cria uma AMI de teste da instância de destino.
- `launchTestInstanceInSameSubnet`: inicia uma instância de teste a partir da AMI de teste usando a mesma configuração da instância de destino.
- `cleanupTestInstance`: encerra a instância de teste.
- `endOfTestBranch`: fim da ramificação de testes.
- `checkIfTestingBranchSucceeded`: verifica o status da ramificação de testes.
- `approvalToStopTargetInstance`: aguarda a aprovação das entidades principais designadas para interromper a instância de destino.
- `stopTargetEC2Instance`: interrompe a instância de destino.
- `forceStopTargetEC2Instance`: força a interrupção da instância de destino somente se a etapa anterior não conseguir interromper a instância.
- `startOfCloneAndMigrateBranch`: ramifica para o workflow Clone&Migrate.

- `createBackupImage`: cria uma AMI da instância de destino para servir como backup.
- `launchInstanceInSameSubnet`: inicia uma nova instância a partir da AMI de backup usando a mesma configuração da instância de origem.
- `waitForClonedInstanceToPassStatusChecks`: espera que a instância recém-criada passe por todas as verificações de status.
- `verifySSMConnectivityForClonedInstance`: verifica se a instância recém-criada é gerenciada pelo Systems Manager.
- `checkAndInstallENADrivers`: verifica se os drivers ENA estão instalados na instância recém-criada e instala os drivers, se necessário.
- `checkAndAddNVMEDrivers`: verifica se os drivers NVMe estão instalados na instância recém-criada e instala os drivers, se necessário.
- `checkAndModifyFSTABEntries`: verifica se os nomes dos dispositivos são usados em `/etc/fstab` e os substitui por UUIDs, se necessário.
- `stopClonedInstance`: interrompe a instância recém-criada.
- `forceStopClonedInstance`: força a interrupção da instância recém-criada somente se a etapa anterior não conseguir interromper a instância.
- `checkENAAttributeForClonedInstance`: verifica se o atributo de rede avançada está ativado para a instância recém-criada.
- `setNitroInstanceTypeForClonedInstance`: altera o tipo de instância da instância recém-criada para o tipo de instância Nitro que você especificar.
- `startClonedInstance`: inicia a instância recém-criada cujo tipo de instância você alterou.
- `approvalForCreatingImageAfterDriversInstallation`: se a instância for iniciada com sucesso como um tipo de instância Nitro, a automação aguardará a aprovação das entidades principais necessárias. Se a aprovação for fornecida, uma AMI será criada para ser usada como Golden AMI.
- `createImageAfterDriversInstallation`: cria uma AMI para ser usada como Golden AMI.
- `endOfCloneAndMigrateBranch`: fim da ramificação Clone&Migrate.
- `cleanupTestImage`: cancela o registro da AMI criada para teste.
- `failureHandling`: verifica se você optou por encerrar recursos em caso de falha.
- `onFailureTerminateClonedInstance`: encerra a instância recém-criada se a automação falhar.
- `onFailurecleanupTestImage`: cancela o registro da AMI criada para teste.

- onFailureApprovalToStartTargetInstance: se a automação falhar, aguarda a aprovação das entidades principais designadas para iniciar a instância de destino.
- onFailureStartTargetInstance: se a automação falhar, inicia a instância de destino.

workflow do FullMigration

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

O workflow FullMigration executa as mesmas etapas do workflow Clone&Migrate e, além disso, executa as seguintes etapas:

- checkConcurrency: verifica se há apenas uma automação desse runbook direcionada à instância do Amazon EC2 que você especificar. Se o runbook encontrar outra automação em andamento visando a mesma instância, a automação terminará.
- getTargetInstanceProperties: reúne detalhes da instância de destino.
- checkRootVolumeTags: determina se o volume raiz da instância de destino do Amazon EC2 contém alguma tag reservada da AWS.
- cloneTargetInstanceAndMigrateToNitro: inicia uma automação secundária usando o runbook AWS-CloneXenInstanceToNitro.
- branchOnTheOperationType: ramifica com base no valor que você especifica para o parâmetro OperationType.
- getClonedInstanceId: recupera o ID da instância recém-iniciada da automação secundária.
- checkIfRootVolumeIsBasedOnLVM: determina se a partição raiz é gerenciada pelo LVM.
- branchOnTheRootVolumeLVMStatus: se as aprovações mínimas exigidas forem recebidas das entidades principais, a automação prosseguirá com a substituição do volume raiz.
- manualInstructionsInCaseOfLVM: se o volume raiz for gerenciado pelo LVM, a automação enviará uma saída contendo instruções sobre como substituir manualmente os volumes raiz.
- startOfReplaceRootEBSVolumeBranch: inicia o workflow da ramificação Substituir volume raiz do EBS.

- `checkIfTargetInstanceIsManagedByCFN`: determina se a instância de destino é gerenciada por uma pilha do AWS CloudFormation.
- `branchOnCFNStackStatus`: ramifica com base no status da pilha do CloudFormation.
- `approvalForRootVolumesReplacement(WithCFN)`: se a instância de destino foi iniciada pelo CloudFormation, a automação aguarda aprovação depois que a instância recém-iniciada tiver sucesso como um tipo de instância Nitro. Quando as aprovações são fornecidas, os volumes do Amazon EBS da instância de destino são substituídos pelos volumes raiz da instância recém-iniciada.
- `approvalForRootVolumesReplacement`: aguarda a aprovação após a instância recém-iniciada ter sucesso como um tipo de instância Nitro. Quando as aprovações são fornecidas, os volumes do Amazon EBS da instância de destino são substituídos pelos volumes raiz da instância recém-iniciada.
- `assertIfTargetEC2InstanceIsStillStopped` verifica se a instância de destino está em um estado `stopped` antes de substituir o volume raiz.
- `stopTargetInstanceForRootVolumeReplacement` se a instância de destino estiver em execução, a automação interromperá a instância antes de substituir o volume raiz.
- `forceStopTargetInstanceForRootVolumeReplacement` força a interrupção da instância de destino se a etapa anterior falhar.
- `stopClonedInstanceForRootVolumeReplacement` interrompe a instância recém-criada antes de substituir os volumes do Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement` força a interrupção da instância recém-criada se a etapa anterior falhar.
- `getBlockDeviceMappings` recupera os mapeamentos de dispositivos de blocos para as instâncias de destino e recém-criadas.
- `replaceRootEbsVolumes` substitui o volume raiz da instância de destino pelo volume raiz da instância recém-criada.
- `EndOfReplaceRootEBSVolumeBranch` fim do workflow da ramificação Substituir volume raiz do EBS.
- `checkENAAttributeForTargetInstance` verifica se o atributo de rede avançada (ENA) está ativado para a instância de destino do Amazon EC2.
- `enableENAAttributeForTargetInstance` ativa o atributo ENA para a instância de destino do Amazon EC2, se necessário.
- `setNitroInstanceTypeForTargetInstance` altera a instância de destino para o tipo de instância Nitro que você especificar.

- `replicateRootVolumeTags` replica as tags no volume raiz do Amazon EBS da instância de destino do Amazon EC2.
- `startTargetInstance` inicia a instância de destino do Amazon EC2 após alterar o tipo de instância.
- `onFailureStopTargetEC2Instance` interrompe a instância de destino do Amazon EC2 se ela falhar ao iniciar como um tipo de instância Nitro.
- `onFailureForceStopTargetEC2Instance` força a interrupção da instância de destino do Amazon EC2 se a etapa anterior falhar.
- `OnFailureRevertOriginalInstanceType` reverte a instância de destino do Amazon EC2 para o tipo de instância original se a instância de destino não iniciar como um tipo de instância Nitro.
- `onFailureRollbackRootVolumeReplacement` reverte todas as alterações feitas pela etapa `replaceRootEbsVolumes`, se necessário.
- `onFailureApprovalToStartTargetInstance` aguarda a aprovação da entidade principal designada para iniciar a instância de destino do Amazon EC2 depois de reverter as alterações anteriores.
- `onFailureStartTargetInstance` inicia a instância do Amazon EC2 de destino.
- `terminateClonedEC2Instance` encerra a instância clonada do Amazon EC2 após substituir o volume raiz do Amazon EBS.

AWSSupport-ResetAccess

Descrição

Este runbook usará a ferramenta EC2Rescue na instância do EC2 especificada para habilitar novamente a descriptografia de senha por meio do console do EC2 (Windows) ou para gerar e adicionar um novo par de chaves SSH (Linux). Se você perder o par de chaves, essa automação criará uma AMI com senha que você pode usar para iniciar uma nova instância do EC2 com um par de chaves que você possui (Windows).

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EC2RescueInstanceType

  Tipo: sequência

  Valores permitidos: t2.small | t2.medium | t2.large

  Padrão: t2.small

  Descrição: (obrigatório) o tipo de instância do EC2 para a instância EC2Rescue. Tamanho recomendado: t2.small.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do EC2 para a qual você deseja redefinir acesso.

> **Important**
>
> O Systems Manager Automation interrompe essa instância e cria uma AMI antes de tentar qualquer operação. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- SubnetId

  Tipo: sequência

  Padrão: CreateNewVPC

  Descrição: (Opcional) O ID de sub-rede para a instância EC2Rescue. Por padrão, a Systems Manager Automation cria uma nova VPC. Como alternativa, Use SelectedInstanceSubnet para usar a mesma sub-rede que sua instância ou especifique um ID de sub-rede personalizado

  > **Important**
  >
  > A sub-rede deve estar na mesma zona de disponibilidade que o InstanceId, e deve permitir acesso aos endpoints SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Você deve ter pelo menos ssm:StartAutomationExecution, ssm:GetParameter (para recuperar o nome do parâmetro da chave SSH) e ssm:GetAutomationExecution para ler a saída de automação. Para mais informações sobre as permissões necessárias, consulte [AWSSupport-StartEC2RescueWorkflow].

Etapas do documento

1. `aws:assertAwsResourceProperty`: declara se a instância fornecida é Windows.
   a. (EC2Rescue para Windows) Se a instância fornecida for Windows:
      i. `aws:executeAutomation`: invoca `AWSSupport-StartEC2RescueWorkflow` com o script de redefinição de senha offline do EC2Rescue para Windows
      ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.
      iii. `aws:executeAwsApi`: recupera o ID AMI com senha habilitada da automação aninhada
      iv. `aws:executeAwsApi`: recupera o resumo do EC2Rescue da automação aninhada
   b. (EC2Rescue para Linux) Se a instância fornecida for Linux:
      i. `aws:executeAutomation`: invoca `AWSSupport-StartEC2RescueWorkflow` com o script de injeção de chave SSH offline do EC2Rescue para Linux
      ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.

iii. `aws:executeAwsApi`: recupera o nome do parâmetro SSM para a chave SSH injetada

iv. `aws:executeAwsApi`: recupera o resumo do EC2Rescue da automação aninhada

Saídas

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getWindowsPasswordEnabledAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

getLinuxSSHKeyParameter.Name

AWSSupport-ResetLinuxUserPassword

Descrição

O runbook `AWSSupport-ResetLinuxUserPassword` ajuda você a redefinir a senha de um usuário do sistema operacional (SO) local. Este runbook é especialmente útil para usuários que precisam acessar as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) usando o console serial. O runbook cria uma instância temporária do Amazon EC2 em sua Conta da AWS e um perfil (IAM) do AWS Identity and Access Management com permissões para recuperar um valor secreto do AWS Secrets Manager contendo a senha.

O runbook interrompe a instância do Amazon EC2 de destino, separa o volume raiz do Amazon Elastic Block Store (Amazon EBS) e o anexa à instância temporária do Amazon EC2. Usando o comando Executar, um script é executado na instância temporária para definir a senha do usuário do sistema operacional que você especificar. Em seguida, o volume raiz do Amazon EBS é reconectado à sua instância de destino. O runbook também oferece uma opção para criar um snapshot do volume raiz no início da automação.

Antes de começar

Crie um segredo do Secrets Manager com o valor da senha que você deseja atribuir ao usuário do sistema operacional. O valor deve estar em texto sem formatação. Para obter mais informações, consulte Criar um segredo do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook. Considere definir o valor do parâmetro `CreateSnapshot` como **`Yes`**.
- A alteração da senha do usuário local exige que o runbook interrompa sua instância. Quando uma instância é interrompida, os dados armazenados na memória ou nos volumes de armazenamento da instância são perdidos. Além disso, todos os endereços IPv4 públicos atribuídos automaticamente são liberados. Para obter mais informações sobre o que acontece quando você interrompe uma instância, consulte Interromper e iniciar sua instância no Manual do usuário do Amazon EC2 para instâncias do Linux.
- Se os volumes do Amazon EBS anexados à sua instância do Amazon EC2 de destino forem criptografados com uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente, certifique-se de que a chave AWS KMS não seja `deleted` ou `disabled` ou sua instância não iniciará.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância Linux do Amazon EC2 que contém a senha de usuário do OS que você deseja redefinir.

- LinuxUserName

  Tipo: sequência

  Padrão: ec2-user

  Descrição: (opcional) a conta de usuário do sistema operacional cuja senha você deseja redefinir.

- SecretArn

  Tipo: sequência

  Descrição: (obrigatório) o ARN do segredo do Secrets Manager contendo a nova senha.

- SecurityGroupId

  Tipo: sequência

  Descrição: (opcional) o ID do grupo de segurança a ser anexado a uma instância temporária do Amazon EC2. Se você não fornecer um valor para esse parâmetro, o grupo de segurança padrão da Amazon Virtual Private Cloud (Amazon VPC) é usado.

- SubnetId

  Tipo: sequência

  Descrição: (opcional) o ID da sub-rede na qual você deseja iniciar a instância temporária do Amazon EC2. Por padrão, a automação escolhe a mesma sub-rede da sua instância de destino. Se você optar por fornecer uma sub-rede diferente, ela deve estar na mesma zona de disponibilidade da instância de destino e ter acesso aos endpoints do Systems Manager.

- CreateSnapshot

  Tipo: sequência

  Valores válidos: sim | não

  Padrão: sim

Descrição: (opcional) determina se um snapshot do volume raiz da sua instância de destino do Amazon EC2 é criado antes da execução da automação.

- StopConsent

  Tipo: sequência

  Valores válidos: sim | não

  Padrão: não

  Descrição: Digite **`Yes`** para confirmar que sua instância de destino do Amazon EC2 será interrompida durante essa automação. Quando a instância do Amazon EC2 é interrompida, todos os dados armazenados na memória ou nos volumes de armazenamento de instância são perdidos e o endereço IPv4 público automático é liberado. Para ter mais informações, consulte Interromper e iniciar a instância, no Guia do usuário do Amazon EC2 para instâncias Linux.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:branch: ramifica com base no seu fornecimento de consentimento para interromper a instância de destino do Amazon EC2.
2. aws:assertAwsResourceProperty garante que o status da instância do Amazon EC2 esteja em um estado running ou stopped. Caso contrário, a automação termina.
3. aws:executeAwsApi obtém as propriedades da instância do Amazon EC2.
4. aws:executeAwsApi obtém as propriedades do volume raiz.
5. aws:branch ramifica a automação dependendo se um ID de sub-rede para a instância temporária do Amazon EC2 foi fornecido.
6. aws:assertAwsResourceProperty garante que a sub-rede que você especifica no parâmetro SubnetId esteja na mesma zona de disponibilidade da instância do Amazon EC2 de destino.

7. `aws:assertAwsResourceProperty` garante que o volume raiz da instância do Amazon EC2 de destino é um volume do Amazon EBS.
8. `aws:assertAwsResourceProperty` garante que a arquitetura da instância do Amazon EC2 seja `arm64` ou `x86_64`.
9. `aws:assertAwsResourceProperty` garante que o comportamento de desligamento da instância do Amazon EC2 seja `stop`, e não `terminate`.
10. `aws:branch` garante que a instância do Amazon EC2 não seja uma instância spot. Caso contrário, a automação termina.
11. `aws:executeScript` garante que a instância do Amazon EC2 não faça parte de um grupo do Auto Scaling. Se a instância fizer parte de um grupo do Auto Scaling, a automação confirma que a instância do Amazon EC2 está em um estado de ciclo de vida `Standby`.
12. `aws:createStack` cria uma instância temporária do Amazon EC2 que é usada para redefinir a senha do usuário do OS que você especificar.
13. `aws:waitForAwsResourceProperty` espera até que a instância temporária recém-iniciada do Amazon EC2 esteja em execução.
14. `aws:executeAwsApi` obtém o ID da instância temporária do Amazon EC2.
15. `aws:waitForAwsResourceProperty` espera que a instância temporária do Amazon EC2 reporte como gerenciada pelo Systems Manager.
16. `aws:changeInstanceState` interrompe a instância de destino do Amazon EC2.
17. `aws:changeInstanceState` força a instância de destino do Amazon EC2 a parar caso ela fique presa em um estado de parada.
18. `aws:branch` ramifica a automação dependendo se um snapshot do volume raiz da instância de destino do Amazon EC2 foi solicitado.
19. `aws:executeAwsApi` cria um snapshot do volume raiz do Amazon EBS de destino da instância do Amazon EC2.
20. `aws:waitForAwsResourceProperty` espera que o instantâneo esteja em um estado `completed`.
21. `aws:executeAwsApi` separa o volume raiz do Amazon EBS da instância do Amazon EC2.
22. `aws:waitForAwsResourceProperty` espera que o volume raiz do Amazon EBS seja separado da instância de destino do Amazon EC2.
23. `aws:executeAwsApi` anexa o volume raiz do Amazon EBS à instância temporária do Amazon EC2.

24 `aws:waitForAwsResourceProperty` espera que o volume raiz do Amazon EBS seja anexado à instância temporária do Amazon EC2.

25 `aws:runCommand` redefine a senha do usuário de destino executando um script de shell usando o comando executar na instância temporária do Amazon EC2.

26 `aws:executeAwsApi` separa o volume raiz do Amazon EBS da instância temporária do Amazon EC2.

27 `aws:waitForAwsResourceProperty` espera que o volume raiz do Amazon EBS seja separado da instância temporária do Amazon EC2.

28 `aws:executeAwsApi` separa o volume raiz do Amazon EBS da instância temporária do Amazon EC2 após um erro.

29 `aws:waitForAwsResourceProperty` espera que o volume raiz do Amazon EBS seja separado da instância temporária do Amazon EC2 após um erro.

30 `aws:branch` ramifica a automação dependendo se um instantâneo do volume raiz foi solicitado para determinar o caminho de recuperação em caso de erro.

31 `aws:executeAwsApi` reconecta o volume raiz do Amazon EBS à instância do Amazon EC2 de destino.

32 `aws:waitForAwsResourceProperty` espera que o volume raiz do Amazon EBS seja anexado à instância do Amazon EC2.

33 `aws:executeAwsApi` cria um novo volume do Amazon EBS a partir do instantâneo do volume raiz da instância do Amazon EC2 de destino.

34 `aws:waitForAwsResourceProperty` espera até que o novo volume do Amazon EBS esteja em um estado `available`.

35 `aws:executeAwsApi` anexa o novo volume do Amazon EBS à instância de destino como volume raiz.

36 `aws:waitForAwsResourceProperty` espera que o volume do Amazon EBS esteja em um estado `attached`.

37 `aws:executeAwsApi` descreve os eventos da pilha do AWS CloudFormation se os runbooks falharem em criar ou atualizar a pilha do AWS CloudFormation.

38 `aws:branch` ramifica a automação de acordo com o estado anterior da instância do Amazon EC2. Se o estado foi `running`, a instância será iniciada. Se estivesse em um estado `stopped`, a automação continua.

39 `aws:changeInstanceState` inicia a instância do Amazon EC2, se necessário.

40. `aws:waitForAwsResourceProperty` espera até que a pilha do AWS CloudFormation esteja em um status de terminal antes de excluí-la.
41. `aws:executeAwsApi` exclui a pilha do AWS CloudFormation, incluindo a instância temporária do Amazon EC2.

AWSPremiumSupport-ResizeNitroInstance

Descrição

O runbook `AWSPremiumSupport-ResizeNitroInstance` fornece uma solução automatizada para redimensionar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) criadas no sistema Nitro.

Para reduzir o risco potencial de perda de dados e tempo de inatividade, o runbook verifica o seguinte:

- Comportamento da interrupção da instância.
- Se a instância fizer parte de um grupo do Amazon EC2 Auto Scaling e estiver no modo `standby`.
- Estado da instância e locação.
- O tipo de instância para o qual você deseja alterar é compatível com o número de interfaces de rede atualmente conectadas à sua instância.
- A arquitetura do processador e o tipo de virtualização do tipo de instância atual e de destino são os mesmos.
- Se a instância estiver em execução, ela está passando todas as verificações de status.
- O tipo de instância que você selecionou não está disponível na mesma zona de disponibilidade.

Se o Amazon EC2 não passar nas verificações de status após alterar o tipo de instância, o runbook reverte automaticamente para o tipo de instância anterior.

Por padrão, esse runbook não alterará o tipo de instância se estiver em execução e os volumes de armazenamento de instância estiverem anexados. O runbook também não alterará o tipo de instância se a instância fizer parte de uma pilha do AWS CloudFormation. Se você quiser alterar qualquer um desses comportamentos, especifique `yes` para os parâmetros `AllowInstanceStoreInstances` e `AllowCloudFormationInstances`.

O runbook fornece duas maneiras diferentes de especificar o tipo de instância para a qual você deseja alterar:

- Para automações simples direcionadas a uma única instância, especifique o tipo de instância para a qual você deseja alterar usando o parâmetro `TargetInstanceTypeFromParameter`.
- Para executar automações em grande escala para alterar o tipo de instância de várias instâncias, especifique o tipo de instância usando o parâmetro `TargetInstanceTypeFromTagValue`. Para obter informações sobre como executar automações em grande escala, consulte Executar automações em grande escala.

Se você não especificar um valor para nenhum dos parâmetros, ocorrerá uma falha na automação.

> **Important**
>
> O acesso aos runbooks da `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar PlanosAWS Support.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook.
- Para obter informações sobre compatibilidade para alterar os tipos de instância, consulte Compatibilidade para alterar o tipo de instância.
- Se a automação falhar e voltar para o tipo de instância original, consulte Solucionar problemas de alteração de tipo de instância.
- A alteração do tipo de instância exige que o runbook interrompa sua instância. Quando uma instância é interrompida ou encerrada, os dados nos volumes de armazenamento da instância são perdidos. Além disso, todos os endereços IPv4 públicos atribuídos automaticamente são liberados. Para obter informações sobre o que acontece quando você interrompe uma instância do Mac, consulte Interromper e encerrar sua instância.
- Ao usar o parâmetro `SkipInstancesWithTagKey`, você pode ignorar instâncias que têm uma chave de tag específica do Amazon EC2 aplicada.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Reconhecer

  Tipo: sequência

  Descrição: (obrigatório) digite **`yes`** para confirmar que sua instância será interrompida se estiver em execução no momento.
- AllowInstanceStoreInstances

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, você permite que o runbook seja executado em instâncias que têm volumes de armazenamento de instâncias anexados.
- AllowCloudFormationInstances

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, o runbook é executado em instâncias que fazem parte de uma pilha do AWS CloudFormation.

- DryRun

  Tipo: sequência

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, o runbook valida os requisitos de redimensionamento sem fazer alterações no tipo de instância.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2 cujo tipo você deseja alterar.

- SkipInstancesWithTagKey

  Tipo: sequência

  Descrição: (opcional) A automação ignora uma instância de destino se a chave de tag especificada for aplicada à instância.

- SleepTime

  Tipo: sequência

  Padrão: 3

  Descrição: (opcional) o número de segundos que esse runbook deve repousar após a conclusão.

- TagInstance

  Tipo: sequência

  Descrição: (opcional) marque as instâncias com a chave e o valor de sua escolha usando o seguinte formato: *`Key=ChangingType,Value=True`*. Essa opção permite rastrear instâncias que foram alvo desse runbook. As chaves e os valores de tags diferenciam maiúsculas de minúsculas.

- TargetInstanceTypeFromParameter

  Tipo: sequência

Descrição: (opcional) o tipo de instância para o qual você deseja alterar sua instância. Deixe esse parâmetro vazio se quiser usar o valor da chave de tag fornecida no parâmetro `TargetInstanceTypeFromTagValue`.

- TargetInstanceTypeFromTagValue

  Tipo: sequência

  Descrição: (opcional) a chave de tag aplicada às suas instâncias de destino cujo valor contém o tipo de instância para a qual você deseja alterar. Se você não especificar um valor para esse parâmetro, ele substitui qualquer valor que você especificar para esse parâmetro `TargetInstanceTypeFromParameter`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

1. `aws:assertAwsResourceProperty`: garante que a instância do Amazon EC2 não seja marcada com a chave de tag de recurso especificada no parâmetro

`SkipInstancesWithTagKey`. Se a chave de tag for encontrada aplicada à instância, a etapa falhará e a automação será encerrada.

2. `aws:assertAwsResourceProperty`: confirma que o status da instância de destino do Amazon EC2 é `running`, `pending`, `stopped` ou `stopping`. Caso contrário, a automação termina.
3. `aws:executeAwsApi`: reúne propriedades da instância do Amazon EC2.
4. `aws:executeAwsApi`: reúne detalhes sobre o tipo de instância atual do Amazon EC2.
5. `aws:branch`: verifica se o tipo de instância atual e o tipo de instância especificado no parâmetro `TargetInstanceTypeFromParameter` são iguais. Se forem iguais, a automação termina.
6. `aws:assertAwsResourceProperty`: garante que a instância esteja em execução no sistema Nitro.
7. `aws:branch`: garante que o tipo de volume raiz da instância do Amazon EC2 seja um volume do Amazon Elastic Block Store (Amazon EBS).
8. `aws:assertAwsResourceProperty`: confirma se o comportamento de desligamento da instância é `stop`, e não `terminate`.
9. `aws:branch`: garante que a instância do Amazon EC2 não seja uma instância spot.
10. `aws:branch`: garante que a locação da instância do Amazon EC2 seja padrão e não um host dedicado ou uma instância dedicada.
11. `aws:executeScript`: confirma que há apenas uma automação desse runbook direcionada ao ID da instância atual. Se outra automação já estiver em andamento visando a mesma instância, a automação retornará um erro e terminará.
12. `aws:branch`: ramifica a automação com base no estado da instância do Amazon EC2.
    a. Se `stopped` ou `stopping`, a automação executa `aws:waitForAwsResourceProperty` até que a instância do Amazon EC2 seja totalmente interrompida.
    b. Se `running` ou `pending`, a automação executa `aws:waitForAwsResourceProperty` até que a instância do Amazon EC2 passe as verificações de status.
13. `aws:assertAwsResourceProperty`: confirma que a instância do Amazon EC2 não faz parte de um grupo do Auto Scaling chamando a operação da API `DescribeAutoScalingInstances`. Se a instância faz parte de um grupo do Auto Scaling, garante que a instância do Amazon EC2 esteja no modo `standby`.
14. `aws:branch`: ramifica a automação dependendo se você deseja que a automação verifique se a instância do Amazon EC2 faz parte de uma pilha do AWS CloudFormation.
    a. `aws:executeScript`: garante que a instância do Amazon EC2 não faça parte de uma pilha do AWS CloudFormation chamando a operação da API `DescribeStackResources`.

15. `aws:executeAwsApi`: retorna uma lista de tipos de instância com o mesmo tipo de arquitetura de processador, tipo de virtualização, e que suporta o número de interfaces de rede atualmente conectadas à instância de destino.
16. `aws:executeAwsApi`: obtém o valor do tipo de instância de destino da chave de tag especificada no parâmetro `TargetInstanceTypeFromTagValue`.
17. `aws:executeScript`: confirma que os tipos de instâncias atual e de destino são compatíveis. Garante que o tipo de instância de destino esteja disponível na mesma sub-rede. Verifica se a entidade principal que iniciou o runbook tem permissões para alterar o tipo de instância e parar e iniciar a instância se ela estiver em execução.
18. `aws:branch`: ramifica a automação com base no valor do parâmetro `DryRun` estar definido como `yes`. Se `yes`, a automação termina.
19. `aws:branch`: verifica se o tipo de instância original e de destino são iguais. Se forem iguais, a automação termina.
20. `aws:executeAwsApi`: obtém o estado atual da instância.
21. `aws:changeInstanceState`: interrompe a instância do Amazon EC2.
22. `aws:changeInstanceState`: força a instância a parar se ela estiver presa no estado `stopping`.
23. `aws:executeAwsApi`: altera o tipo de instância para o tipo de instância de destino.
24. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
25. `aws:branch`: ramifica a automação com base no estado anterior da instância. Se foi `running`, a instância é iniciada.
    a. `aws:changeInstanceState`: inicia a instância do Amazon EC2 se ela estava em execução antes de alterar o tipo de instância.
    b. `aws:waitForAwsResourceProperty`: espera que a instância do Amazon EC2 passe nas verificações de status. Se a instância não passar nas verificações de status, altere-a de volta para seu tipo original.
        i. `aws:changeInstanceState`: interrompe a instância do Amazon EC2 antes de alterá-la para seu tipo original.
        ii. `aws:changeInstanceState`: força a instância do Amazon EC2 a parar antes de alterá-la para o tipo de instância original, caso ela fique presa em um estado de parada.
        iii. `aws:executeAwsApi`: altera a instância do Amazon EC2 para seu tipo original.

iv. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.

v. `aws:changeInstanceState`: inicia a instância do Amazon EC2 se ela estava em execução antes de alterar o tipo de instância.

vi. `aws:waitForAwsResourceProperty`: espera que a instância do Amazon EC2 passe nas verificações de status.

26.`aws:sleep`: espera antes de terminar o runbook.

AWSSupport-RestoreEC2InstanceFromSnapshot

Descrição

O runbook `AWSSupport-RestoreEC2InstanceFromSnapshot` ajuda você a identificar e restaurar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) a partir de um instantâneo do Amazon Elastic Block Store (Amazon EBS) do volume raiz.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EndDate

  Tipo: sequência

  Descrição: (opcional) A última data em que você deseja que a automação procure um snapshot.

- InplaceSwap

  Tipo: booliano

  Valores válidos: verdadeiro | falso

  Descrição: (opcional) se o valor desse parâmetro for definido como `true`, o volume recém-criado do snapshot substituirá o volume raiz existente anexado à sua instância.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância de banco de dados do que você deseja reinicializar.

- LookForInstanceStatusCheck

  Tipo: booliano

  Valores válidos: verdadeiro | falso

  Padrão: true

  Descrição: (opcional) se o valor desse parâmetro for definido como `true`, a automação verificará se as verificações de status da instância falham nas instâncias de teste iniciadas a partir dos snapshots.

- SkipSnapshotsBy

  Tipo: sequência

  Descrição: (opcional) o intervalo em que os snapshots são ignorados ao pesquisar snapshots para restaurar sua instância. Por exemplo, se houver 100 snapshots disponíveis e você especificar um valor de 2 para esse parâmetro, cada terceiro snapshot será revisado.

  Padrão: 0

- SnapshotId

Tipo: sequência

Descrição: (opcional) o ID de um snapshot do qual você deseja restaurar a instância.

- StartDate

  Tipo: sequência

  Descrição: (opcional) a primeira data em que você deseja que a automação procure um snapshot.

- TotalSnapshotsToLook

  Tipo: sequência

  Descrição: (opcional) o número de snapshots que a automação analisa.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:executeAwsApi: reúne detalhes sobre a instância de destino.
2. aws:assertAwsResourceProperty: verifica se a instância de destino existe.
3. aws:assertAwsResourceProperty: verifica se o volume raiz é um volume do Amazon EBS.
4. aws:assertAwsResourceProperty: verifica se ainda não está em execução outra automação que tenha como destino essa instância.
5. aws:executeAwsApi: marca a instância de destino.
6. aws:executeAwsApi: cria uma AMI da instância.
7. aws:executeAwsApi: reúne detalhes sobre a AMI criada na etapa anterior.
8. aws:waitForAwsResourceProperty: espera que o estado da AMI se torne available antes de prosseguir.
9. aws:executeScript: inicia uma nova instância a partir da AMI recém-criada.
10. aws:assertAwsResourceProperty: verifica se o estado da instância é available.
11. aws:executeAwsApi: reúne detalhes sobre a instância recém-iniciada.
12. aws:branch: ramifica com base no fato de ter fornecido um valor para o parâmetro SnapshotId.
13. aws:executeScript: retorna uma lista de snapshots dentro do período especificado.
14. aws:executeAwsApi: interrompe a instância.
15. aws:waitForAwsResourceProperty: espera que o estado do volume seja available.
16. aws:waitForAwsResourceProperty: espera que o estado da instância seja stopped.
17. aws:executeAwsApi: separa o volume de raiz.
18. aws:waitForAwsResourceProperty: espera que o volume raiz seja desanexado.
19. aws:executeAwsApi: anexa o novo volume raiz.
20. aws:waitForAwsResourceProperty: espera que o novo volume seja anexado.
21. aws:executeAwsApi: inicia a instância.

22. `aws:waitForAwsResourceProperty`: espera que o estado da instância seja `available`.
23. `aws:waitForAwsResourceProperty`: espera que as verificações de status do sistema e da instância sejam aprovadas na instância.
24. `aws:executeScript`: executa um script para encontrar um snapshot que possa ser usado para criar um volume com êxito.
25. `aws:executeScript`: executa um script para recuperar a instância usando o volume recém-criado a partir do snapshot identificado pela automação ou usando o volume criado a partir do snapshot que você especificou no parâmetro `SnapshotId`.
26. `aws:executeScript`: exclui recursos criados pela automação.

Saídas

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

Descrição

O runbook `AWSSupport-SendLogBundleToS3Bucket` carrega um pacote de logs gerado pela ferramenta EC2Rescue da instância de destino para o bucket do S3 especificado. O runbook instala a versão específica de plataforma do EC2Rescue com base na plataforma da instância de destino. O EC2Rescue é, então, usado para coletar todos os logs de sistema operacional (SO) disponíveis.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID da instância gerenciada Windows ou Linux das quais você deseja coletar os logs.
- S3BucketName

  Tipo: sequência

  Descrição: (Obrigatório) Bucket do S3 para os quais carregar os logs.
- S3Path

  Tipo: sequência

  Padrão: `AWSSupport-SendLogBundleToS3Bucket/`

  Descrição: (Opcional) Caminho do S3 para os logs coletados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a instância do EC2 que recebe o comando tenha uma função do IAM com a política gerenciada pela Amazon AmazonSSMManagedInstanceCore anexada. O usuário deve ter pelo menos ssm:StartAutomationExecution e ssm:SendCommand para executar a automação e

enviar o comando para a instância, além de ssm:GetAutomationExecution para poder ler a saída de automação.

Etapas do documento

1. `aws:runCommand`: instala o EC2Rescue via `AWS-ConfigureAWSPackage`.
2. `aws:runCommand`: executa o script do PowerShell para coletar os logs de solução de problemas do Windows com o EC2Rescue.
3. `aws:runCommand`: executa o script bash para coletar os logs de solução de problemas do Linux com o EC2Rescue.

Saídas

collectAndUploadWindowsLogBundle.Output

collectAndUploadLinuxLogBundle.Output

`AWSSupport-StartEC2RescueWorkflow`

Descrição

O `AWSSupport-StartEC2RescueWorkflow` runbook executa o script codificado em base64 fornecido (Bash ou Powershell) em uma instância auxiliar criada para salvar sua instância. O volume raiz de sua instância está anexado e anexado à instância auxiliar, também conhecida como instância EC2Rescue. Se sua instância for Windows, forneça um script do Powershell. Caso contrário, use Bash. O runbook define algumas variáveis de ambiente que você pode usar em seu script. As variáveis de ambiente contêm informações sobre a entrada que você forneceu, bem como informações sobre o volume raiz offline. O volume offline já está instalado e pronto para uso. Por exemplo, você pode salvar um arquivo de configuração de estado desejado para um volume raiz do Windows offline, ou chroot para um volume raiz do Linux offline, e executar uma correção offline.

Execute esta automação (console)

> **Important**
>
> As instâncias do Amazon EC2 criadas pelas imagens de máquina da Amazon (AMIs) do Marketplace não são compatíveis com essa automação.

Informações adicionais

Para codificar um script em base64, você pode usar Powershell ou Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::Rea
```

Bash:

```
base64 PATH_TO_FILE
```

Esta é uma lista de variáveis de ambiente que você pode usar em seus scripts offline, dependendo do sistema operacional de destino

Windows:

Variável	Descrição	Valor de exemplo
$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 para caminho de instalação do Windows	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EC2RW_DIR	EC2Rescue para caminho de instalação do Windows	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	Caminho definido de controle atual do Windows offline	`HKLM:\AWSTempSystem\ControlSet001`
$env:EC2RESCUE_OFFLINE_DRIVE	Letra de unidade offline do Windows	D:\

Variável	Descrição	Valor de exemplo
$env:EC2RESCUE_OFFLINE_EBS_DEVICE	Dispositivo EBS do volume raiz offline	xvdf
$env:EC2RESCUE_OFFLINE_KERNEL_VER	Versão de kernel do Windows offline	6.1.7601.24214
$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	Arquitetura do Windows offline	AMD64
$env:EC2RESCUE_OFFLINE_OS_CAPTION	Legenda off-line do Windows	Datacenter do Windows Server 2008 R2
$env:EC2RESCUE_OFFLINE_OS_TYPE	Tipo de sistema operacional Windows offline	de aplicativos
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	Caminho de diretório de arquivos de programa do Windows offline	D:\Program Files
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	Caminho de diretório x86 de arquivos de programa do Windows offline	D:\Program Files (x86)
$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	Caminho de diretório de registro do Windows offline	D:\Windows\System32\config
$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT	Caminho de diretório de raiz do sistema do Windows offline	D:\Windows
$env:EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket
$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/

Variável	Descrição	Valor de exemplo
$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	Metadados de instalação do Windows offline	Objeto Powershell do cliente

Linux

Variável	Descrição	Valor de exemplo
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 para caminho de instalação do Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	Nome do dispositivo offline	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	Dispositivo EBS do volume raiz offline	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Ponto de montagem de volume raiz offline	/mnt/mount
EC2RESCUE_PYTHON	Versão do Python	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket

Variável	Descrição	Valor de exemplo
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AMIPrefix

  Tipo: sequência

  Padrão: `AWSSupport-EC2Rescue`

  Descrição: (Opcional) Um prefixo para o nome de backup da AMI.
- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CreatePostEC2RescueBackup

  Tipo: sequência

  Valores válidos: verdadeiro | falso

Padrão: falso

Descrição: (opcional) defina como `true` para criar uma AMI de InstanceId depois de executar o script, antes de iniciá-la. A AMI persistirá depois da conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la.

- CreatePreEC2RescueBackup

  Tipo: sequência

  Valores válidos: verdadeiro | falso

  Padrão: falso

  Descrição: (opcional) defina como `true` para criar uma AMI de InstanceId antes de executar o script. A AMI persistirá depois da conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la.

- EC2RescueInstanceType

  Tipo: sequência

  Valores permitidos: t2.small | t2.medium | t2.large

  Padrão: t2.small

  Descrição: (Opcional) O tipo de instância do EC2 para a instância EC2Rescue.

- InstanceId

  Tipo: sequência

  Descrição: (Obrigatório) ID de sua instância do EC2. IMPORTANTE: a Automação do AWS Systems Manager interrompe essa instância. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- OfflineScript

  Tipo: sequência

  Descrição: (obrigatório) Script codificado em Base64 a ser executado contra a instância auxiliar. Use Bash se sua instância de origem for Linux; use PowerShell se for Windows.

- S3BucketName

  Tipo: sequência

  Descrição: (Opcional) Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.
- S3Prefix

  Tipo: sequência

  Padrão: `AWSSupport-EC2Rescue`

  Descrição: (Opcional) Um prefixo para os logs da S3.
- SubnetId

  Tipo: sequência

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) O ID de sub-rede para a instância EC2Rescue. Por padrão, é usada a mesma sub-rede na qual a instância fornecida reside. IMPORTANTE: se você fornecer uma sub-rede personalizada, ela deve estar na mesma zona de disponibilidade que o InstanceId, e deve permitir acesso aos endpoints SSM.
- UniqueId

  Tipo: sequência

  Padrão: {{ automation:EXECUTION_ID }}

  Descrição: (opcional) um identificador exclusivo para o fluxo de trabalho.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que o usuário que executa a automação tenha a política gerenciada do IAM AmazonSSMAutomationRole anexada. Além dessa política, o usuário deve ter:

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

Etapas do documento

1. `aws:executeAwsApi`: descreve a instância fornecida
2. `aws:executeAwsApi`: descreve o volume raiz da instância fornecida
3. `aws:assertAwsResourceProperty`: verifica se o tipo de dispositivo de volume raiz é EBS
4. `aws:assertAwsResourceProperty`: verifica se o volume raiz não está criptografado
5. `aws:assertAwsResourceProperty`: verifica o ID de sub-rede fornecido
   a. (Usar sub-rede da instância atual) - se * SubnetId = SelectedInstanceSubnet*, execute `aws:createStack` para implantar a pilha do CloudFormation EC2Rescue

b. (Criar nova VPC) - Se* SubnetId = CreateNewVPC*, execute `aws:createStack` para implantar a pilha do CloudFormation EC2Rescue

c. (Usar sub-rede personalizada) - em todos os demais casos:

`aws:assertAwsResourceProperty`: verifique se a sub-rede fornecida está na mesma zona de disponibilidade da instância fornecida

`aws:createStack`: implante a pilha do CloudFormation EC2Rescue

6. `aws:invokeLambdaFunction`: execute validação adicional de entrada
7. `aws:executeAwsApi`: atualize a pilha do CloudFormation EC2Rescue para criar a instância auxiliar EC2Rescue
8. `aws:waitForAwsResourceProperty`: aguarde a atualização completa da pilha do CloudFormation EC2Rescue
9. `aws:executeAwsApi`: descreva a saída da pilha do CloudFormation EC2Rescue para obter o ID de instância auxiliar EC2Rescue
10. `aws:waitForAwsResourceProperty`: aguarde que a instância auxiliar EC2Rescue se torne uma instância gerenciada.
11. `aws:changeInstanceState`: interrompe a instância fornecida
12. `aws:changeInstanceState`: interrompe a instância fornecida
13. `aws:changeInstanceState`: força a parada da instância fornecida
14. `aws:assertAwsResourceProperty`: verifica o valor de entrada CreatePreEC2RescueBackup
    a. (Criar um backup pre-EC2Rescue) - Se *CreatePreEC2RescueBackup = true*
    b. `aws:executeAwsApi`: crie uma AMI de backup da instância fornecida
    c. `aws:createTags`: marca o backup da AMI
15. `aws:runCommand`: instala o EC2Rescue na instância auxiliar EC2Rescue
16. `aws:executeAwsApi`: desanexa o volume raiz da instância fornecida
17. `aws:assertAwsResourceProperty`: verifica a plataforma da instância fornecida
    a. (Instância é Windows):

    `aws:executeAwsApi`: anexa o volume raiz à instância auxiliar EC2Rescue como *xvdf*

    `aws:sleep`: repousa por 10 segundos

    `aws:runCommand`: executa o script offline fornecido no Powershell

b. (Instância é Linux):

`aws:executeAwsApi`: anexa o volume raiz à instância auxiliar EC2Rescue como */dev/sdf*

`aws:sleep`: repousa por 10 segundos

`aws:runCommand`: executa o script offline fornecido no Bash

18. `aws:changeInstanceState`: interrompe a instância auxiliar do EC2Rescue
19. `aws:changeInstanceState`: força a parada da instância auxiliar do EC2Rescue
20. `aws:executeAwsApi`: desanexa o volume raiz da instância auxiliar EC2Rescue
21. `aws:executeAwsApi`: anexa o volume raiz novamente à instância fornecida
22. `aws:assertAwsResourceProperty`: verifica o valor de entrada CreatePostEC2RescueBackup
    a. (Criar um backup post-EC2Rescue) - Se *CreatePostEC2RescueBackup = true*
    b. `aws:executeAwsApi`: crie uma AMI de backup da instância fornecida
    c. `aws:createTags`: marca o backup da AMI
23. `aws:executeAwsApi`: restaura a exclusão inicial no estado de encerramento para o volume raiz da instância fornecida
24. `aws:changeInstanceState`: restaura o estado inicial da instância fornecida (em execução/parado)
25. `aws:deleteStack`: exclua a pilha do CloudFormation EC2Rescue

Saídas

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descrição

O runbook `AWSPremiumSupport-TroubleshootEC2DiskUsage` ajuda você a investigar e potencialmente corrigir problemas com o uso de disco raiz e não raiz de instâncias do Amazon

Elastic Compute Cloud (Amazon EC2). Se possível, o runbook tenta corrigir os problemas estendendo o volume e seu sistema de arquivos. Para realizar essas tarefas, esse runbook orquestra a execução de vários runbooks com base no sistema operacional da instância afetada.

O primeiro runbook, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` ou `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, determina se os problemas de disco podem ser atenuados com a expansão do volume.

O segundo runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` ou `AWSPremiumSupport-ExtendVolumesOnLinux`, usa a saída do primeiro runbook para executar o código Python que modifica o volume. Depois que o volume for modificado, o runbook estende a partição e o sistema de arquivos dos volumes afetados.

> **Important**
>
> O acesso aos runbooks `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar PlanosAWS Support.

Este documento foi criado em colaboração com o AWS Managed Services (AMS). O AMS ajuda você a gerenciar sua infraestrutura da AWS com mais eficiência e segurança. O AMS também oferece flexibilidade operacional, segurança e conformidade aprimoradas, otimização de capacidade e identificação de economia de custos. Para obter mais informações, consulte AWS Managed Services.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- InstanceId

  Tipo: sequência

  Valores permitidos: ^i-[a-z0-9]{8,17}$

  Descrição: (obrigatório) ID de sua instância do Amazon EC2.
- VolumeExpansionEnabled

  Tipo: booliano

  Descrição: (opcional) sinalize para controlar se o documento estenderá os volumes e partições afetados.

  Padrão: true
- VolumeExpansionUsageTrigger

  Tipo: sequência

  Descrição: (opcional) uso mínimo do espaço de partição necessário para acionar a extensão (em porcentagem).

  Valores permitidos: ^[0-9]{1,2}$

  Padrão: 85
- VolumeExpansionCapSize

  Tipo: sequência

  Descrição: (opcional) o tamanho máximo para o qual o volume do Amazon Elastic Block Store (Amazon EBS) será aumentado (em GiB).

  Valores permitidos: ^[0-9]{1,4}$

  Padrão: 2048
- VolumeExpansionGibIncrease

  Tipo: sequência

  Descrição: (opcional) aumento do volume em GiB. O maior aumento líquido entre VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease será usado.

Valores permitidos: ^[0-9]{1,4}$

Padrão: 20

- VolumeExpansionPercentageIncrease

  Tipo: sequência

  Descrição: (opcional) aumento do volume em porcentagem. O maior aumento líquido entre VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease será usado.

  Valores permitidos: ^[0-9]{1,2}$

  Padrão: 20

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:assertAwsResourceProperty: verifica se a instância é gerenciada pelo Systems Manager
2. aws:executeAwsApi: descreve a instância para obter a plataforma.
3. aws:branch: ramifica a automação com base na plataforma da instância.
   a. Se a instância for Windows:
      i. aws:executeAutomation: executa o runbook AWSPremiumSupport-DiagnoseDiskUsageOnWindows para diagnosticar problemas de uso de disco na instância.
      ii. aws:executeAwsApi: obtém a saída da automação anterior.
      iii. aws:branch: ramifica com base na saída do diagnóstico e se houver volumes que possam ser expandidos para mitigar o alerta.
         A. Não há volumes que precisem ser expandidos: terminar a automação.
         B. Há volumes que precisam ser expandidos:
            I. aws:executeAwsApi: cria uma Amazon Machine Image (AMI) da instância.
            II. aws:waitForAwsResourceProperty: espera que o estado da AMI seja available.
            III. aws:executeAutomation: executa o runbook AWSPremiumSupport-ExtendVolumesOnWindows para realizar a modificação do volume, bem como as etapas necessárias no sistema operacional (SO) para disponibilizar o novo espaço.
   b. (A plataforma não é Windows) Se a instância de entrada não for Windows:
      i. aws:executeAutomation: executa o runbook AWSPremiumSupport-DiagnoseDiskUsageOnLinux para diagnosticar problemas de uso de disco na instância.

ii. `aws:executeAwsApi`: obtém a saída da automação anterior.

iii. `aws:branch`: ramifica com base na saída do diagnóstico e se houver volumes que possam ser expandidos para mitigar o alerta.

A. Não há volumes que precisem ser expandidos: terminar a automação.

B. Há volumes que precisam ser expandidos:

I. `aws:executeAwsApi`: cria uma AMI da instância.

II. `aws:waitForAwsResourceProperty`: espera que o estado da AMI seja `available`.

III. `aws:executeAutomation`: executa o runbook `AWSPremiumSupport-ExtendVolumesOnLinux` para realizar a modificação do volume, bem como as etapas necessárias no OS para disponibilizar o novo espaço.

Saídas

diagnoseDiskUsageAlertOnWindows.Output

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Output

extendVolumesOnLinux.Output

BackupAMILinux.ImageId

BackupAMIWindows.ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Descrição

`AWSSupport-TroubleshootEC2InstanceConnect`a automação ajuda a analisar e detectar erros que impedem a conexão com uma instância do Amazon Elastic Compute Cloud (Amazon EC2) usando o Amazon EC2 Instance Connect. Ele identifica problemas causados por uma Amazon Machine Image (AMI) não suportada, falta de instalação ou configuração de pacotes no nível do sistema operacional, permissões ausentes AWS Identity and Access Management (IAM) ou problemas de configuração de rede.

Como funciona?

O runbook usa o ID da instância do Amazon EC2, o nome de usuário, o modo de conexão, o CIDR IP de origem, a porta SSH e o Amazon Resource Name (ARN) para a função do IAM ou o usuário com problemas com o Amazon EC2 Instance Connect. Em seguida, ele verifica os pré-requisitos para se conectar a uma instância do Amazon EC2 usando o Amazon EC2 Instance Connect:

- A instância está em execução e em um estado íntegro.
- A instância está localizada em uma AWS região suportada pelo Amazon EC2 Instance Connect.
- A AMI da instância é suportada pelo Amazon EC2 Instance Connect.
- A instância pode acessar o Instance Metadata Service (IMDSv2).
- O pacote Amazon EC2 Instance Connect está devidamente instalado e configurado no nível do sistema operacional.
- A configuração da rede (grupos de segurança, ACL de rede e regras da tabela de rotas) permite a conexão com a instância por meio do Amazon EC2 Instance Connect.
- A função ou o usuário do IAM que é usado para aproveitar o Amazon EC2 Instance Connect tem acesso às chaves push para a instância do Amazon EC2.

Important

- Para verificar a AMI da instância, a acessibilidade do IMDSv2 e a instalação do pacote Amazon EC2 Instance Connect, a instância deve ser gerenciada por SSM. Caso contrário, ele pula essas etapas. Para obter mais informações, consulte Por que minha instância do Amazon EC2 não está sendo exibida como um nó gerenciado.
- A verificação de rede detectará somente se o grupo de segurança e as regras de ACL de rede bloquearem o tráfego quando o SourceIp CIDR for fornecido como um parâmetro de entrada. Caso contrário, ele exibirá apenas regras relacionadas ao SSH.
- As conexões usando o Amazon EC2 Instance Connect Endpoint não são validadas neste runbook.
- Para conexões privadas, a automação não verifica se o cliente SSH está instalado na máquina de origem e se ele pode acessar o endereço IP privado da instância.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-TroubleshootEC2InstanceConnect`no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId (Obrigatório):

     O ID da instância de destino do Amazon EC2 à qual você não conseguiu se conectar usando o Amazon EC2 Instance Connect.
   - AutomationAssumeRole (Opcional):

O ARN da função do IAM que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- Nome de usuário (obrigatório):

  O nome de usuário usado para se conectar à instância do Amazon EC2 usando o Amazon EC2 Instance Connect. Ele é usado para avaliar se o acesso do IAM foi concedido para esse usuário específico.

- EC2 InstanceConnectRoleOrUser (obrigatório):

  O ARN da função ou usuário do IAM que está utilizando o Amazon EC2 Instance Connect para enviar chaves para a instância.

- Porta SSH (opcional):

  A porta SSH configurada na instância do Amazon EC2. O valor padrão é `22`. O número da porta deve estar entre`1-65535`.

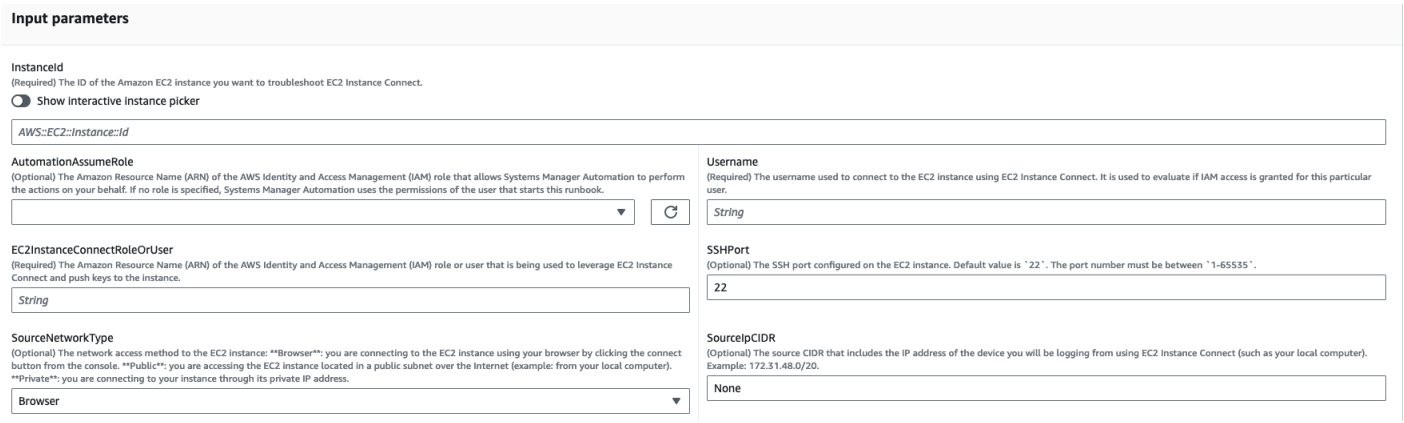
- SourceNetworkType (Opcional):

  O método de acesso à rede para a instância do Amazon EC2:

  - Navegador: você se conecta a partir do AWS Management Console.
  - Público: você se conecta à instância localizada em uma sub-rede pública pela Internet (por exemplo, seu computador local).
  - Privado: você se conecta por meio do endereço IP privado da instância.

- SourceIpCIDR (opcional):

  O CIDR de origem que inclui o endereço IP do dispositivo (como seu computador local) do qual você fará login usando o Amazon EC2 Instance Connect. Exemplo: 172.31.48.6/32. Se nenhum valor for fornecido com o modo de acesso público ou privado, o runbook não avaliará se o grupo de segurança da instância do Amazon EC2 e as regras de ACL de rede permitem tráfego SSH. Em vez disso, ele exibirá regras relacionadas ao SSH.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - AssertInitialState:

     Garante que o status da instância do Amazon EC2 esteja em execução. Caso contrário, a automação termina.
   - GetInstanceProperties:

     Obtém as propriedades atuais da instância do Amazon EC2 (PlatformDetails, PublicIpAddress VpcId, SubnetId e MetadataHttpEndpoint).
   - GatherInstanceInformationFromSMS:

     Obtém o status de ping da instância do Systems Manager e os detalhes do sistema operacional se a instância for gerenciada por SSM.
   - CheckIfAWSRegionSupported:

     Verifica se a instância do Amazon EC2 está localizada em uma região compatível com o Amazon EC2 Instance ConnectAWS.
   - BranchOnIfAWSRegionSupported:

     Continua a execução se a AWS região for suportada pelo Amazon EC2 Instance Connect. Caso contrário, ele cria a saída e sai da automação.
   - CheckIfInstanceAMIIsSupported:

     Verifica se a AMI associada à instância é compatível com o Amazon EC2 Instance Connect.
   - BranchOnIfInstanceAMIIsSupported:

Se a AMI da instância for compatível, ela executa as verificações no nível do sistema operacional, como a acessibilidade dos metadados e a instalação e configuração do pacote Amazon EC2 Instance Connect. Caso contrário, ele verifica se os metadados HTTP estão habilitados usando a AWS API e, em seguida, avança para a etapa de verificação de rede.

- Verifique IMDsReachabilityFromOs:

  Executa um script Bash na instância Linux do Amazon EC2 de destino para verificar se ela é capaz de acessar o IMDSv2.

- Verifique o ID: PackageInstallation

  Executa um script Bash na instância Linux do Amazon EC2 de destino para verificar se o pacote Amazon EC2 Instance Connect está instalado e configurado corretamente.

- Verifique o SSHConfigFromOs:

  Executa um script Bash na instância Linux do Amazon EC2 de destino para verificar se a porta SSH configurada corresponde ao parâmetro de entrada `SSHport. `

- CheckMetadataHTTPEndpointIsEnabled:

  Verifica se o endpoint HTTP do serviço de metadados da instância está ativado.

- Verifique o ID: NetworkAccess

  Verifica se a configuração da rede (grupos de segurança, ACL de rede e regras da tabela de rotas) permite a conexão com a instância por meio do Amazon EC2 Instance Connect.

- Verifique se eu sou: RoleOrUserPermissions

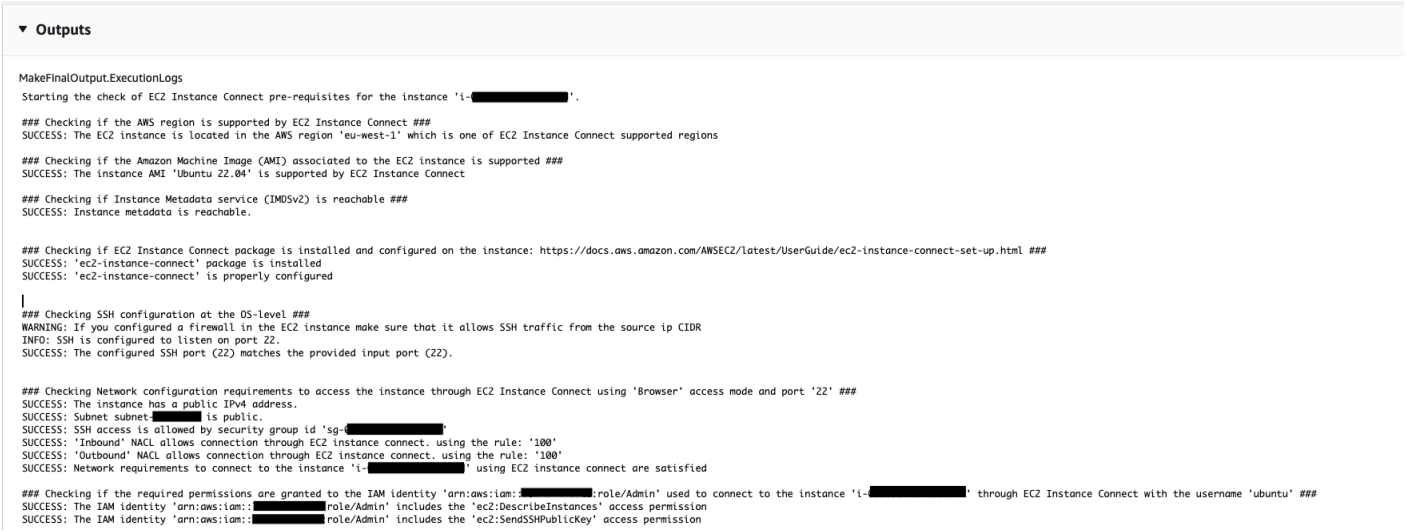
  Verifica se a função do IAM ou o usuário usado para utilizar o Amazon EC2 Instance Connect tem acesso às chaves push para a instância do Amazon EC2 usando o nome de usuário fornecido.

- MakeFinalOutput:

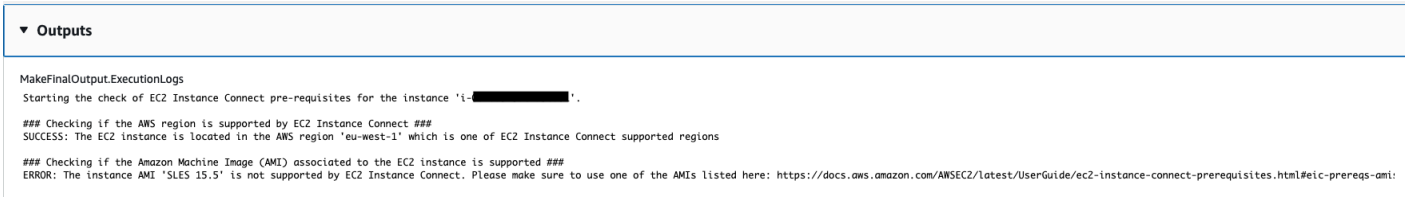
  Consolida a saída de todas as etapas anteriores.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   Execução em que a instância de destino tem todos os pré-requisitos necessários:



Execução em que a AMI da instância de destino não é suportada:



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSDocumentação do serviço

- Como soluciono problemas de conexão com minha instância do Amazon EC2 usando o Amazon EC2 Instance Connect?

AWSSupport-TroubleshootRDP

Descrição

O runbook `AWSSupport-TroubleshootRDP` permite ao usuário verificar ou modificar configurações comuns na instância de destino que possam afetar as conexões Remote Desktop Protocol (RDP), como os perfis RDP port, Network Layer Authentication (NLA) e Windows Firewall. Opcionalmente, as alterações podem ser aplicadas offline ao interromper e iniciar a instância, se o usuário explicitamente permitir a correção offline. Por padrão, o runbook lê e exibe os valores das configurações.

> **Important**
>
> As alterações nas configurações RDP, serviço RDP e perfis de Firewall do Windows devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- Ação

  Tipo: sequência

  Valores válidos: CheckAll | FixAll | Custom

  Padrão: Custom

  Descrição: (opcional) [personalizado] use os valores do Firewall, RDPServiceStartupType, RDPServiceAction, RDPportAction, NLASettingAction e RemoteConnections para gerenciar as configurações. [CheckAll] Leia os valores das configurações sem alterá-las. [FixAll] Restaure as configurações padrão RDP e desabilitar todos os perfis de firewall do Windows.
- AllowOffline

Tipo: sequência

Valores válidos: verdadeiro | falso

Padrão: falso

Descrição: (opcional) apenas correção - Defina como verdadeiro se você permitir a correção do RDP offline, caso a solução de problemas online falhe ou caso a instância fornecida não seja uma instância gerenciada. Observação: para a correção offline, a Automação do SSM interrompe a instância e cria uma AMI antes de tentar qualquer operação.

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Firewall

  Tipo: sequência

  Valores válidos: Check | Disable

  Padrão: Check

  Descrição: (Opcional) Marque ou desabilite o firewall do Windows (todos os perfis).

- InstanceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID da instância que vai solucionar os problemas das configurações de RDP.

- NLASettingAction

  Tipo: sequência

  Valores válidos: Check | Disable

  Padrão: Check

Descrição: (Opcional) Marque ou desabilite o Network Layer Authentication (NLA).

- RDPPortAction

  Tipo: sequência

  Valores válidos: Check | Modify

  Padrão: Check

  Descrição: (Opcional) Marque a porta atual usada para conexões RDP, ou modifique a porta RDP de volta para 3389 e reinicie o serviço.

- RDPServiceAction

  Tipo: sequência

  Valores válidos: Check | Start | Restart | Force-Restart

  Padrão: Check

  Descrição: (Opcional) Verifique, inicie, reinicie ou reinicie à força o serviço do RDP (TermService).

- RDPServiceStartupType

  Tipo: sequência

  Valores válidos: Check | Auto

  Padrão: Check

  Descrição: (Opcional) Marque ou defina o serviço RDP para iniciar automaticamente quando o Windows é inicializado.

- RemoteConnections

  Tipo: sequência

  Valores válidos: Check | Enable

  Padrão: Check

  Descrição: (Opcional) Uma ação para executar na configuração fDenyTSConnections: Check, Enable.

- S3BucketName

  Tipo: sequência

  Descrição: (Opcional) Apenas offline - Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- SubnetId

  Tipo: sequência

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Apenas offline - O ID de sub-rede para a instância EC2Rescue usado para executar a solução de problemas offline. Se nenhum ID de sub-rede for especificado, a Automação do AWS Systems Manager criará uma nova VPC. IMPORTANTE: a sub-rede deve estar na mesma zona de disponibilidade que o InstanceId, e deve permitir acesso aos endpoints SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a instância do EC2 que recebe o comando tenha uma função do IAM com a política gerenciada pela Amazon AmazonSSMManagedInstanceCore anexada. Para a correção online, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution e ssm:SendCommand para executar a automação e enviar o comando para a instância, além de ssm:GetAutomationExecution para poder ler a saída da automação. Para a correção offline, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances, além de ssm:GetAutomationExecution para poder ler a saída de automação. `AWSSupport-TroubleshootRDP` chama `AWSSupport-ExecuteEC2Rescue` para realizar a correção offline - revise as permissões para `AWSSupport-ExecuteEC2Rescue` para garantir que você possa executar a automação com êxito.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância é uma instância Windows Server
2. `aws:assertAwsResourceProperty`: verifica se a instância é uma instância gerenciada
3. (Solução de problemas online) Se a instância é uma instância gerenciada, então:

a. `aws:assertAwsResourceProperty`: verifica o valor da ação fornecido

b. (Verificação online) Se Action = CheckAll, então:

`aws:runPowerShellScript`: executa o script do PowerShell para obter o status de perfis de firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para obter o status do serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para obter as configurações do RDP.

c. (Correção online) Se Action = FixAll, então:

`aws:runPowerShellScript`: executa o script do PowerShell para desabilitar todos os perfis de firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para iniciar o serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para ativar conexões remotas e desativar o NLA.

d. (Gerenciamento online) Se Action = Custom, então:

`aws:runPowerShellScript`: executa o script do PowerShell para gerenciar os perfis de firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para gerenciar o serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para gerenciar as configurações do RDP.

4. (Correção offline) Se a instância não for uma instância gerenciada, então:

a. `aws:assertAwsResourceProperty` declara AllowOffline = true

b. `aws:assertAwsResourceProperty` declara Action = FixAll

c. `aws:assertAwsResourceProperty`: declara o valor de SubnetId

(Use a sub-rede da instância fornecida) Se SubnetId for SELECTED_INSTANCE_SUBNET

`aws:executeAwsApi`: recupera a sub-rede da instância atual.

`aws:executeAutomation`: executa `AWSSupport-ExecuteEC2Rescue` com a sub-rede da instância fornecida.

d. (Use a sub-rede personalizada fornecida) Se SubnetId não for SELECTED_INSTANCE_SUBNET

`aws:executeAutomation`: executa `AWSSupport-ExecuteEC2Rescue` com o valor SubnetId fornecido.

Saídas

manageFirewallProfiles.Output

manageRDPServiceSettings.Output

manageRDPSettings.Output

checkFirewallProfiles.Output

checkRDPServiceSettings.Output

checkRDPSettings.Output

disableFirewallProfiles.Output

restoreDefaultRDPServiceSettings.Output

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

Descrição

O runbook `AWSSupport-TroubleshootSSH` instala o Amazon EC2Rescue para Linux e, em seguida, usa a ferramenta EC2Rescue para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Opcionalmente, as alterações podem

ser aplicadas offline ao interromper e iniciar a instância, se o usuário explicitamente permitir a correção offline. Por padrão, o runbook opera em modo somente leitura.

Execute esta automação (console)

Para obter informações sobre como trabalhar com o runbook `AWSSupport-TroubleshootSSH`, consulte este `AWSSupport-TroubleshootSSH`tópico de solução de problemas do AWS Premium Support.

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- Ação

  Tipo: sequência

  Valores válidos: checkAll | FixAll

  Padrão: CheckAll

  Descrição: (Obrigatório) Especifique se deseja verificar se há problemas sem corrigi-los ou verificar e corrigir automaticamente todos os problemas detectados.
- AllowOffline

  Tipo: sequência

  Valores válidos: verdadeiro | falso

  Padrão: falso

  Descrição: (Opcional) Apenas correção - Defina como verdadeiro se você permitir a correção do SSH offline, caso a solução de problemas online falhe ou caso a instância fornecida não seja uma

instância gerenciada. Observação: Para a correção offline, a Automação do SSM interrompe a instância e cria uma AMI antes de tentar qualquer operação.

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: sequência

  Descrição: (obrigatória) o ID de sua instância do EC2 para o Linux.

- S3BucketName

  Tipo: sequência

  Descrição: (Opcional) Apenas offline - Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- SubnetId

  Tipo: sequência

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Apenas offline - O ID de sub-rede para a instância EC2Rescue usado para executar a solução de problemas offline. Se nenhum ID de sub-rede for especificado, a Automação do AWS Systems Manager criará uma nova VPC.

  > **Important**
  >
  > A sub-rede deve estar na mesma zona de disponibilidade que o InstanceId, e deve permitir acesso aos endpoints SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a instância do EC2 que recebe o comando tenha uma função do IAM com a política gerenciada pela Amazon AmazonSSMManagedInstanceCore anexada. Para a correção online, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution e ssm:SendCommand para executar a automação e enviar o comando para a instância, além de ssm:GetAutomationExecution para poder ler a saída da automação. Para a correção offline, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances, além de ssm:GetAutomationExecution para poder ler a saída de automação. `AWSSupport-TroubleshootSSH` chama `AWSSupport-ExecuteEC2Rescue` para realizar a correção offline - revise as permissões para `AWSSupport-ExecuteEC2Rescue` para garantir que você possa executar a automação com êxito.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância é uma instância gerenciada
   a. (Correção online) Se a instância não for uma instância gerenciada, então:
      i. `aws:configurePackage`: instalar o EC2Rescue para Linux via `AWS-ConfigureAWSPackage`.
      ii. `aws:runCommand`: executar o script bash para executar o EC2Rescue para Linux.
   b. (Correção offline) Se a instância não for uma instância gerenciada, então:
      i. `aws:assertAwsResourceProperty` declara AllowOffline = true
      ii. `aws:assertAwsResourceProperty` declara Action = FixAll
      iii. `aws:assertAwsResourceProperty`: declara o valor de SubnetId
      iv. (Use a sub-rede da instância fornecida) Se a SubnetId for SelectedInstanceSubnet use `aws:executeAutomation` para executar `AWSSupport-ExecuteEC2Rescue` com a sub-rede da instância fornecida.
      v. (Use a sub-rede da instância fornecida) Se a SubnetId for SelectedInstanceSubnet use `aws:executeAutomation` para executar `AWSSupport-ExecuteEC2Rescue` com o valor SubnetId fornecido.

Saídas

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSSupport-TroubleshootSUSERegistration

Descrição

O runbook `AWSSupport-TroubleshootSUSERegistration` ajuda você a identificar por que o registro de uma instância SUSE Linux Enterprise Server do Amazon Elastic Compute Cloud (Amazon EC2) com infraestrutura de atualização SUSE falhou. A saída de automação fornece etapas para resolver ou ajuda você a solucionar o problema, a questão. Se a instância passar por todas as verificações durante a automação, ela será registrada na infraestrutura de atualização SUSE.

Execute esta automação (console)

Tipo de documento

Automation

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: sequência

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: sequência

  Descrição: (obrigatório) o ID da instância do Amazon EC2 cujo problema você deseja solucionar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Etapas do documento

- `aws:assertAwsResourceProperty`: verifica se a instância do Amazon EC2 é gerenciada pelo AWS Systems Manager.
- `aws:runCommand`: verifica se a plataforma de instância do Amazon EC2 é SLES.
- `aws:runCommand`: verifica se a versão `cloud-regionsrv-client` do pacote é superior ou igual à versão 9.0.10 necessária.
- `aws:runCommand`: verifica se o link simbólico do produto base está quebrado e corrige o link se ele estiver quebrado.
- `aws:runCommand`: verifica se o arquivo hosts (`/etc/hosts`) contém registros de `smt-ec2-suscloud.net`. A automação remove todas as entradas duplicadas.
- `aws:runCommand`: verifica se o comando `curl` está instalado.
- `aws:runCommand`: verifica se a instância do Amazon EC2 pode acessar o endereço do serviço de metadados de instância (IMDS) 169.254.169.254.
- `aws:runCommand`: verifica se a instância do Amazon EC2 tem um código de cobrança ou código de produto AWS Marketplace.
- `aws:runCommand`: verifica se a instância do Amazon EC2 pode alcançar pelo menos um servidor regional via HTTPS.
- `aws:runCommand`: verifica se a instância do Amazon EC2 pode acessar os servidores da ferramenta de gerenciamento de sistema (SMT) via HTTP.
- `aws:runCommand`: verifica se a instância do Amazon EC2 pode acessar os servidores da ferramenta de gerenciamento de sistema (SMT) via HTTPS.

- `aws:runCommand`: verifica se a instância do Amazon EC2 pode acessar o endereço `smt-ec2.susecloud.net`via HTTPS.
- `aws:runCommand`: registra a instância do Amazon EC2 com infraestrutura de atualização SUSE.
- `aws:executeScript`: reúne e gera a saída de todas as etapas anteriores.

`AWSSupport-TroubleshootWindowsPerformance`

Descrição

O runbook `AWSSupport-TroubleshootWindowsPerformance` ajuda a solucionar problemas contínuos de desempenho na instância Windows do Amazon Elastic Compute Cloud (Amazon EC2). O runbook captura registros da instância de destino e analisa as métricas de desempenho de CPU, memória, disco e rede. Opcionalmente, a automação pode capturar um despejo do processo para ajudá-lo a determinar a causa potencial da degradação do desempenho. A automação também captura os registros de eventos e do sistema usando a `EC2Rescue`ferramenta mais recente, se você permitir que esse runbook a instale.

Como funciona?

O runbook executa as seguintes etapas:

- Verifica os pré-requisitos na instância do Amazon EC2.
- Gera registros de desempenho no disco raiz da instância Windows do Amazon EC2
- Armazena os registros capturados na pasta `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Se um bucket do Amazon Simple Storage Service (Amazon S3) for fornecido e a função de assumir a automação tiver as permissões necessárias, os logs capturados serão enviados para o bucket do Amazon S3.
- Instala a `EC2Rescue` ferramenta mais recente na instância Windows do Amazon EC2 para capturar eventos e registros do sistema se você optar por instalá-la, mas ela não analisa o despejo do processo e os registros capturados por. `EC2Rescue`

Important

- Para executar esse runbook, a instância Windows do Amazon EC2 deve ser gerenciada pelo. AWS Systems Manager Para obter mais informações, consulte Por que minha instância do Amazon EC2 não está sendo exibida como um nó gerenciado.
- Para executar esse runbook, a instância Windows do Amazon EC2 deve estar em execução nas versões Windows 8.1/Windows Server 2012 R2 (6.3) ou mais recentes PowerShell com 4.0 ou superior. Para obter mais informações, consulte a versão do sistema operacional Windows.
- Para a geração de registros de desempenho, é necessário pelo menos 10 GB de espaço livre no dispositivo raiz. Se o disco raiz for maior que 100 GB, o espaço livre deverá ser maior que 10% do tamanho do disco. Se você despejar um processo durante a execução, o espaço livre deverá ser maior que 10 GB mais o tamanho total da memória consumida pelo processo quando o processo consumir mais de 10 GB de memória.
- Os registros gerados no dispositivo raiz não são excluídos automaticamente.
- O runbook não desinstala a `EC2Rescue` ferramenta. Para obter mais informações, consulte Usar `EC2Rescue` para Windows Server.
- É uma prática recomendada executar essa automação durante um impacto no desempenho. Você também pode executá-lo periodicamente usando uma associação AWS Systems Manager do State Manager ou agendando janelas de AWS Systems Manager manutenção.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

(Opcional) A função do IAM anexada ao perfil da instância ou ao usuário do IAM configurado na instância exige as seguintes ações para carregar os registros no bucket do Amazon S3 especificado para o parâmetro: *`LogUploadBucketName`*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até `AWSSupport-TroubleshootWindowsPerformance`em Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).

3. Para os parâmetros de entrada, insira o seguinte:

- AutomationAssumeRole (Opcional):

  O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- InstanceId (Obrigatório):

  O ID da instância Windows de destino do Amazon EC2 em que você deseja executar a automação. A instância deve ser gerenciada pelo Systems Manager para executar a automação.

- CaptureProcessDump (Opcional):

  O tipo de despejo do processo a ser capturado. A automação pode capturar um despejo de processo para o processo que está potencialmente causando o impacto no desempenho no início da automação. O volume raiz da instância requer pelo menos 10 GB de espaço livre (maior que 10% do tamanho do disco quando o tamanho do volume raiz é maior que 100 GB e 10 GB mais o tamanho total da memória consumida pelo processo quando o processo consome mais de 10 GB de memória).

- LogCaptureDuration (Opcional):

  O número de minutos, entre `1` e`15`, em que essa automação capturará os registros enquanto o problema estiver presente. O padrão é`5`.

- LogUploadBucketName (Opcional):

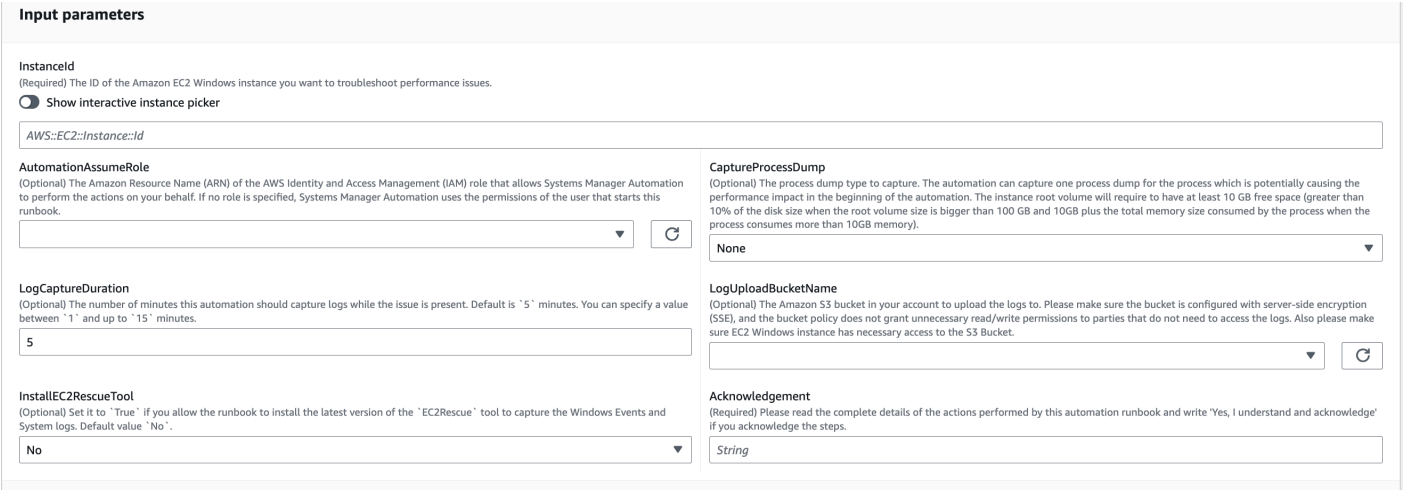
  O bucket do Amazon S3 na sua conta em que você deseja fazer o upload dos registros. O bucket deve ser configurado com criptografia do lado do servidor (SSE), e a política do bucket não deve conceder permissões desnecessárias de leitura/gravação a partes que não precisam acessar os registros capturados. A instância Windows do Amazon EC2 deve ter acesso ao bucket do Amazon S3.

- Instale o EC2 RescueTool (opcional):

  Defina `Yes` para permitir que o runbook instale a versão mais recente da `EC2Rescue` ferramenta para capturar os registros de eventos e do sistema do Windows. O padrão é`No`.

- Reconhecimento (obrigatório):

Leia os detalhes completos das ações realizadas por esse runbook de automação e, se concordar, digite`Yes, I understand and acknowledge`.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - **`CheckConcurrency:`**

     Garante que haja apenas uma execução desse runbook direcionada à instância. Se o runbook encontrar outra execução direcionada à mesma instância, ele retornará um erro e terminará.

   - **`AssertInstanceIsWindows:`**

     Afirma que a instância do Amazon EC2 está sendo executada no sistema operacional Windows. Caso contrário, a automação termina.

   - **`AssertInstanceIsManagedInstance:`**

     Afirma que a instância do Amazon EC2 é gerenciada por. AWS Systems Manager Caso contrário, a automação termina.

   - **`VerifyPrerequisites:`**

     Verifica a PowerShell versão no sistema operacional da instância e garante que a instância possa ser conectada por meio do Systems Manager para executar PowerShell comandos. Essa automação oferece suporte à PowerShell versão 4.0 e superior em execução nas versões Windows 8.1/Server 2012 R2 (6.3) ou mais recentes. Se a versão for mais antiga, a automação falhará. Quando você opta por fazer o upload de registros para o bucket do Amazon S3, essa

automação verifica se o PowerShell módulo AWS Tools for está disponível. Caso contrário, a automação termina.

- **BranchOnProcessDump:**

  Ramifica com base em se você o configurou para capturar o despejo de processos que afetaram o desempenho.

- **CaptureProcessDump:**

  Verifica se a instância tem espaço suficiente para executar essa automação (quando você escolhe CPU/Memória mais alta).

- **CapturePerformanceLogs:**

  Verifica o espaço em disco novamente e executa o PowerShell script na instância para criar contadores perfmon e iniciar o registro do Monitor de Desempenho e do Gravador de Desempenho do Windows. O script é interrompido depois que o definido `LogCaptureDuration` é atendido.

- **SummarizePerformanceLogs:**

  Resume o relatório XML gerado na etapa anterior,`CapturePerformanceLogs`, para encontrar o processo responsável que consome mais WorkingSet 64 (memória) e% de tempo de processador (CPU) mostrados como saída na automação. Ele gera informações semelhantes para uso de Interface de Rede LogicalDisk, Memória, TCPv4, IPv4 e UDPv4 e as salva na pasta de saída. `analysis_output.log`

- **BranchOnInstallEC2Rescue:**

  Ramifica se você configurá-lo para instalar a `EC2Rescue` ferramenta mais recente na instância do Amazon EC2.

- **InstallEC2RescueTool:**

  Instala a `EC2Rescue` ferramenta no sistema operacional da instância para capturar `EC2Rescue` registros usando`AWS-ConfigureAWSPackage`.

- **RunEC2RescueTool:**

  Executa a `EC2Rescue` ferramenta no sistema operacional da instância para capturar todos os registros necessários. `EC2Rescue`captura somente os registros necessários para economizar espaço.

- **BranchOnIfS3BucketProvided:**

Ramifica com base na entrada do usuário de `LogUploadBucketName` para ver se há um nome de bucket disponível para fazer upload de registros.

- **`GetS3BucketPublicStatus:`**

  Determina se um bucket do Amazon S3 é fornecido e, em caso afirmativo, confirma que o bucket do Amazon S3 não é público e está configurado com SSE.

- **`UploadLogResult:`**

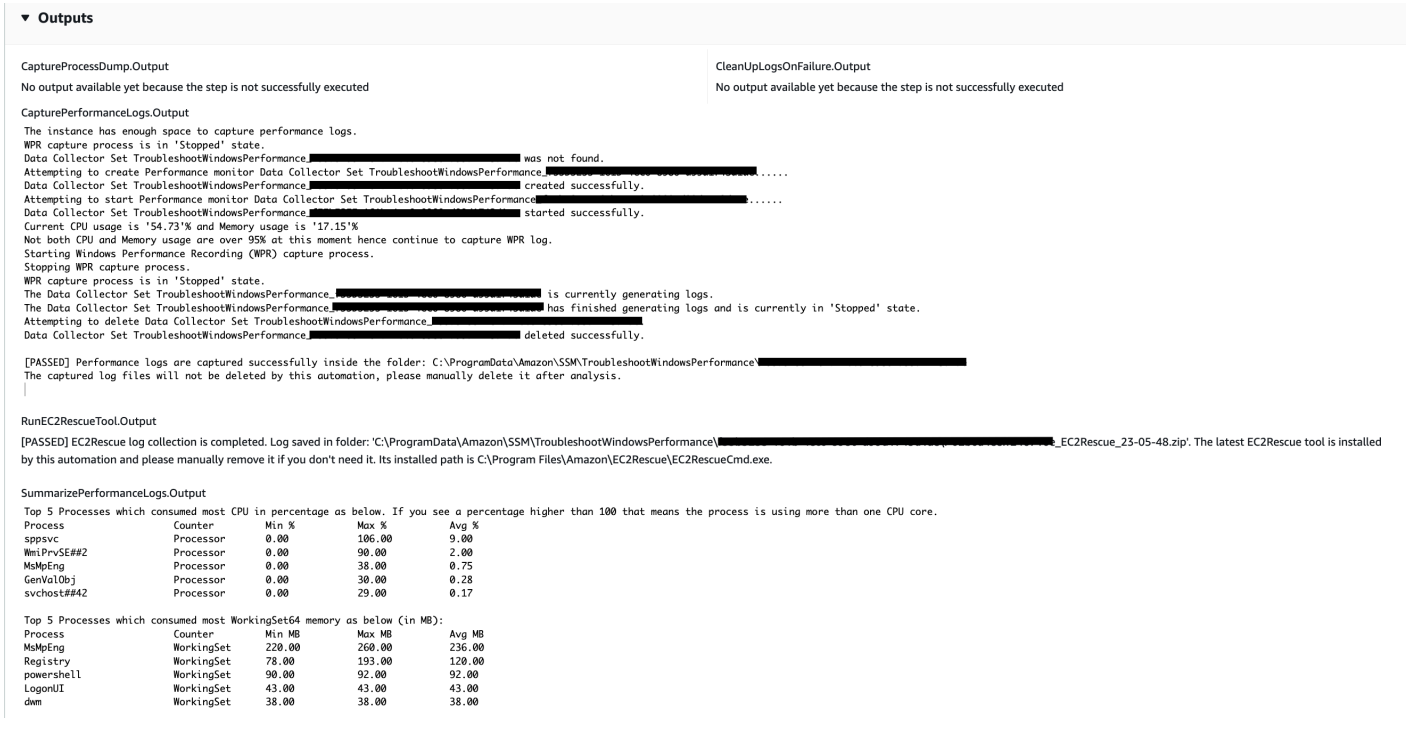
  Carrega os registros no bucket Amazon S3 fornecido. Se a PowerShell versão for 5.0 ou superior, ela compactará os registros em um arquivo ZIP e os carregará. Ele exclui o arquivo ZIP após a conclusão do upload. Se a PowerShell versão estiver abaixo de 5.0, ele carregará os arquivos diretamente para uma pasta.

- **`CleanUpLogsOnFailure:`**

  Limpa todos os registros gerados pela `CapturePerformanceLogs` etapa quando ela falha. A `CleanUpLogsOnFailure` etapa pode falhar ou atingir o tempo limite se o SSM Agent não estiver funcionando corretamente ou se o sistema Windows não estiver respondendo.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   Execução em que a instância de destino tem todos os pré-requisitos necessários.



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

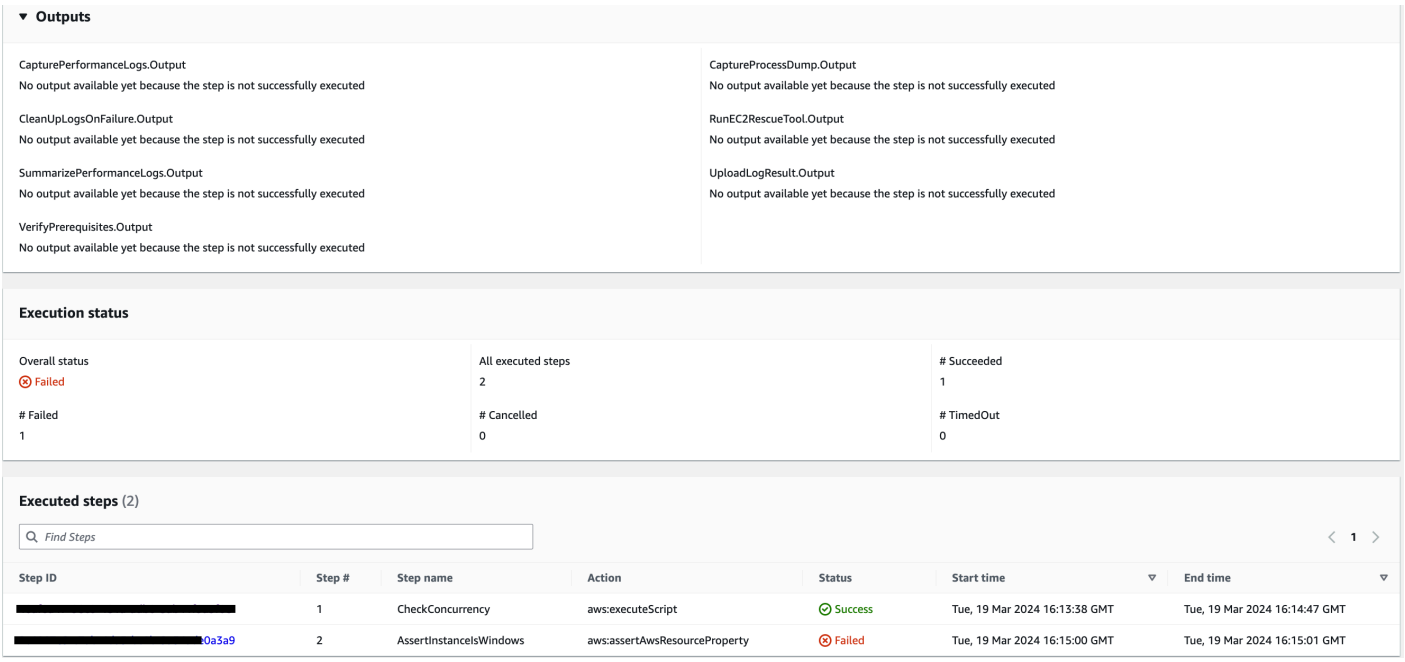
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]_EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

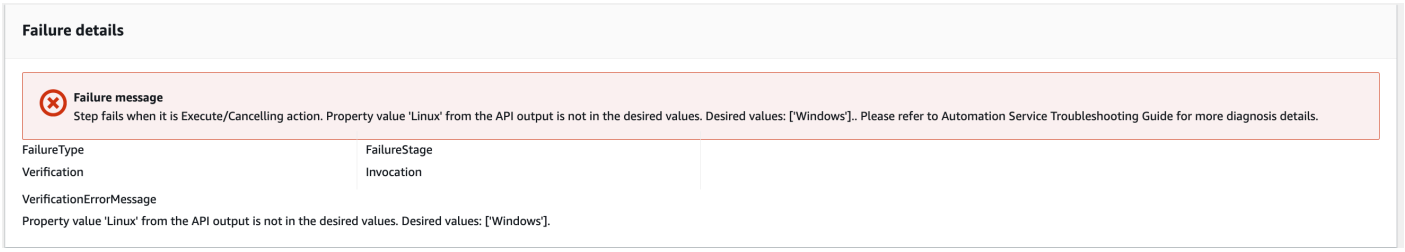
```
Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.
Process                 Counter         Min %           Max %           Avg %
sppsvc                  Processor       0.00            106.00          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
```

Execução em que a instância de destino está na plataforma Linux e a execução falhou. Você selecionaria o ID da etapa para ver os detalhes da falha.



Os detalhes da falha da etapa`AssertInstanceIsWindows`.



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

`AWSSupport-TroubleshootWindowsUpdate`

Descrição

O `AWSSupport-TroubleshootWindowsUpdate` runbook é usado para identificar problemas que podem falhar nas atualizações do Windows para instâncias Windows do Amazon Elastic Compute Cloud (Amazon EC2).

Como funciona?

O runbook executa as seguintes etapas:

- Verifica se a instância de destino do Amazon EC2 é gerenciada pelo. AWS Systems Manager
- Verifica se as versões AWS Systems Manager Agent (SSM Agent) e Windows Server são compatíveis com as operações de patch do Systems Manager.
- Verifica o espaço em disco disponível recomendado para atualizações do Windows e se a reinicialização está pendente. Uma reinicialização pendente normalmente indica que as atualizações estão pendentes, e uma reinicialização é necessária antes de realizar atualizações adicionais.
- Define as configurações de proxy no nível do sistema operacional, o que pode ajudar a solucionar problemas de conectividade.
- Executa um teste de conectividade de endpoint do Amazon Simple Storage Service (Amazon S3) e chama a operação de API para recuperar `GetDeployablePatchSnapshotForInstance`o snapshot atual da linha de base do patch que o nó gerenciado usa.
- Se a conexão falhar, oferece a opção de executar o `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analisar a conectividade da instância com os endpoints do Amazon S3.
- Valida a configuração das atualizações do Windows e testa o Windows Server Update Services (WSUS) (se aplicável).

Important

- Não há suporte para controladores de domínio do Active Directory.
- Não há suporte para a versão 2008 R2 do Windows Server ou versões anteriores.
- O SSM Agent 1.2.371 ou versões anteriores não são compatíveis.
- O `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook é usado `VPC Reachability Analyzer`para analisar a conectividade de rede entre uma fonte e um ponto final de serviço. Você é cobrado por análise executada entre a origem e o destino. Para obter mais detalhes, consulte Preço da Amazon VPC.

- O `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook não está disponível em todas as regiões em que o Systems Manager é suportado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Para executar o runbook secundárioAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2, adicione as permissões listadas neste documento.

Instruções

Siga estas etapas para configurar a automação:

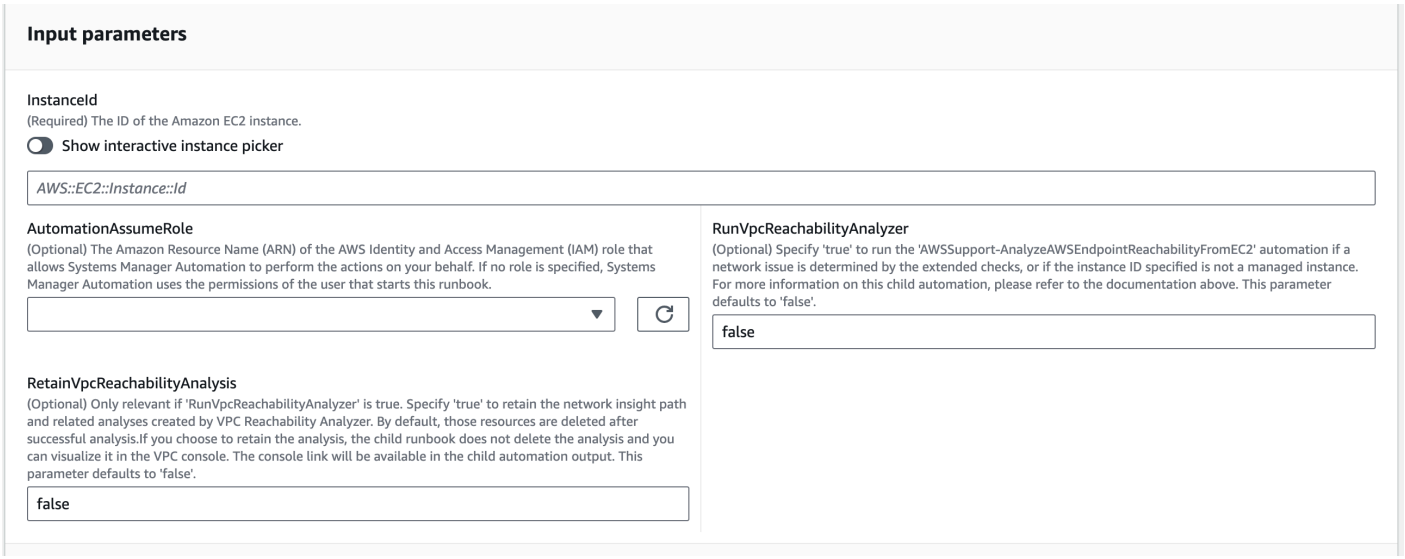
1. Navegue até AWSSupport-TroubleshootWindowsUpdateem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - InstanceId (Obrigatório):

     Insira o ID da instância do Amazon EC2 em que a atualização do Windows falhou.
   - RunVpcReachabilityAnalyzer(Opcional):

     Especifique `true` a execução da `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` automação se um problema de rede for determinado pelas verificações estendidas ou se o ID da instância especificado não for uma instância gerenciada. Para obter mais informações sobre essa automação infantil, consulte a documentação. O valor padrão é `false`.
   - RetainVpcReachabilityAnalysis(Opcional):

     Só é relevante se `RunVpcReachabilityAnalyzer` for`true`. Especifique `true` para manter o caminho do insight da rede e as análises relacionadas criadas por`Reachability Analyzer`. Por padrão, esses recursos são excluídos após uma análise bem-sucedida. Se você optar por manter a análise, o runbook secundário não excluirá a análise e você poderá visualizá-la no console da Amazon VPC. O link do console estará disponível na saída de automação infantil. O valor padrão`false`.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`getWindowsServerAndSSMAgentVersion:`**

     Verifica se a instância de destino é gerenciada AWS Systems Manager e obtém detalhes sobre a versão do SSM Agent e a versão do Windows.
   - **`assertifInstanceIsSsmManaged:`**

     Garante que a instância do Amazon EC2 seja gerenciada pelo AWS Systems Manager (SSM), caso contrário, a automação termina.
   - **`CheckProxy:`**

     Verifica todos os tipos de proxy para a instância do Windows.
   - **`CheckPrerequisites:`**

     Obtém a versão do SSM Agent e a versão do Windows e determina se é um controlador de domínio (DC) do Active Directory. Se a instância for um DC ou se o SSM Agent ou a versão do Windows não for suportada, o runbook será interrompido.
   - **`CheckDiskSpace:`**

     Obtém e valida o espaço em disco disponível na instância do Windows se for suficiente para realizar a atualização do Windows.
   - **`CheckPendingReboot:`**

Verifica se há alguma reinicialização pendente na instância do Windows.

- **CheckS3Connectivity:**

  Verifica se a instância pode alcançar os endpoints do Amazon S3 para. `Patchbaseline`

- **branchOnRunVpcReachabilityAnalyzer:**

  Se `RunVpcReachabilityAnalyzer` for verdade, ele ramifica a automação para executar uma análise mais profunda da depuração da conectividade do Amazon S3.

- **GenerateEndpoints:**

  Gera um endpoint para ter uma verificação de conectividade estendida para o endpoint Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

  Chama o runbook de automação,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. para verificar a acessibilidade da instância selecionada aos endpoints necessários.

- **CheckWindowsUpdateServices:**

  Verifica o status do serviço Windows Update e o tipo de início.

- **CheckWindowsUpdateSettings:**

  Verifica as políticas do Windows Update configuradas na instância do Windows.

- **CheckWSUSSettings:**

  Verifica se a atualização do Windows está configurada com o WSUS ou o Microsoft Update Catalog e verifica a conectividade.

- **CheckWUGlobalSettings:**

  Verifica as configurações globais do Windows Update definidas na instância do Windows.

- **GenerateLogs:**

  Faz o download dos registros do Windows Update e do CBS na área de trabalho da instância e verifica se há falhas nos registros de eventos do Windows.

- **FinalReport:**

  Gera um relatório completo de todas as etapas.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

```
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
"
```

Referências

Automação do Systems Manager

- Execute esta automação (console)

- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Documentação relacionada ao AWS serviço

- Consulte o artigo TroubleShoot Windows Update para obter mais informações.

AWSSupport-UpgradeWindowsAWSDrivers

Descrição

O `AWSSupport-UpgradeWindowsAWSDrivers` runbook atualiza ou repara os drivers AWS de armazenamento e rede na instância do EC2 especificada. O runbook tenta instalar as versões mais recentes dos drivers AWS on-line chamando o agente SSM. Se o SSM atendente não puder ser conectado, o runbook poderá executar uma instalação offline dos drivers da AWS caso solicitado explicitamente.

> **Note**
>
> Observação: tanto a atualização online e offline criará uma AMI antes de tentar quaisquer operações, que persistem após a conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la. O método online reinicia a instância como parte do processo de atualização, enquanto o método offline requer que a instância do EC2 seja interrompida e depois iniciada.

> **Important**
>
> Se suas instâncias se conectarem ao AWS Systems Manager usando endpoints da VPC, este runbook falhará, a menos que seja usado na região us-east-1. Este runbook também falhará em um controlador de domínio. Para atualizar drivers do AWS PV em um controlador de domínio, consulte Atualizar um controlador de domínio (upgrade do AWS PV).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AllowOffline

  Tipo: string

  Valores válidos: True | False

  Padrão: False

  Descrição: (Opcional) Defina como verdadeiro se você permitir uma atualização de drivers offline, caso a instalação online não possa ser realizada. Observação: O método offline requer que a instância do EC2 fornecida seja interrompida e, em seguida, iniciada. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.
- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ForceUpgrade

  Tipo: string

  Valores válidos: True | False

  Padrão: False

Descrição: (opcional) apenas offline: defina como verdadeiro se você permitir que a atualização de drivers offline prossiga, mesmo que sua instância já tenha os drivers mais recentes instalados.

- InstanceId

  Tipo: string

  Descrição: (obrigatória) o ID de sua instância do EC2 para o Windows Server.

- SubnetId

  Tipo: string

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Apenas offline - O ID de sub-rede para a instância EC2Rescue usado para executar a atualização de drivers offline. Se nenhum ID de sub-rede for especificado, o Systems Manager Automation criará uma nova VPC.

  > **Important**
  >
  > A sub-rede deve estar na mesma InstanceId zona de disponibilidade e deve permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

A instância EC2 que recebe o comando deve ter, no mínimo, uma função do IAM que inclua permissões para ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação. Você pode anexar a política `AmazonSSMManagedInstanceCore` gerenciada pela Amazon à sua função do IAM para fornecer essas permissões. No entanto, recomendamos usar a função do IAM `AmazonSSMAutomationRole` de automação para essa finalidade. Para obter mais informações, consulte Usar o IAM para configurar perfis para o Automation.

Se você estiver executando uma atualização offline, consulte as permissões necessárias por `AWSSupport-StartEC2RescueWorkflow`.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância de entrada é Windows.
2. `aws:assertAwsResourceProperty`: verifica se a instância de entrada é uma instância gerenciada. Se esse for o caso, a atualização online é iniciada; caso contrário, a atualização offline é avaliada.
   a. (Atualização online) Se a instância de entrada for uma instância gerenciada:
      i. `aws:createImage`: cria um backup da AMI.
      ii. `aws:createTags`: marca o backup da AMI.
      iii. `aws:runCommand`: instala o driver de rede ENA via `AWS-ConfigureAWSPackage`.
      iv. `aws:runCommand`: instala o driver de NVMe via `AWS-ConfigureAWSPackage`.
      v. `aws:runCommand`: instala o driver AWS PV via `AWS-ConfigureAWSPackage`.
   b. (Atualização offline) Se a instância de entrada não for uma instância gerenciada:
      i. `aws:assertAwsResourceProperty`: verifica se o sinalizador AllowOffline está definido como `true`. Se esse for o caso, a atualização offline é iniciada; caso contrário, a automação termina.
      ii. `aws:changeInstanceState`: interrompe a parada da instância
      iii. `aws:changeInstanceState`: força a parada da instância de origem.
      iv. `aws:createImage`: cria uma AMI de backup da instância de origem.
      v. `aws:createTags`: marca uma AMI de backup da instância de origem.
      vi. `aws:executeAwsApi`: ativa o ENA para a instância
      vii. `aws:assertAwsResourceProperty`- Afirme a ForceUpgrade bandeira.
      viii (Forçar atualização offline) Se ForceUpgrade = true, execute `aws:executeAutomation` para invocar `AWSSupport-StartEC2RescueWorkflow` com o script de atualização forçada do driver. Isso instala os drivers independentemente da versão atual instalada
      ix. (Atualização offline) Se ForceUpgrade = false, execute `aws:executeAutomation` para invocar `AWSSupport-StartEC2RescueWorkflow` com o script de atualização de drivers.

Saídas

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Saída

forceUpgradeDriversOffline. Saída

Amazon ECS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Container Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

Descrição

O runbook `AWSSupport-CollectECSInstanceLogs` coleta arquivos de log relacionados ao sistema operacional e ao Amazon Elastic Container Service (Amazon ECS) de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para ajudá-lo a solucionar problemas comuns do Amazon ECS. Enquanto a automação coleta os arquivos de log associados, são feitas alterações no sistema de arquivos. Essas mudanças incluem a criação de diretórios temporários e um diretório de log, a cópia de arquivos de log para esses diretórios e a compactação dos arquivos de log em um arquivo.

Se você especificar um valor para o parâmetro `LogDestination`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos logs coletados da sua instância do Amazon EC2, se o status da

política `isPublic` estiver definido como `true`, ou se a lista de controle de acesso (ACL) conceder permissões de `READ|WRITE` ao grupo predefinido `All Users` do Amazon S3, os logs não serão carregados. Além disso, se o bucket fornecido não estiver disponível em sua conta, os logs não serão carregados. Para mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ECS InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância da qual deseja coletar os logs. A instância especificada deve ser gerenciada pelo Systems Manager.
- LogDestination

  Tipo: string

  Descrição: (Opcional) O bucket do Amazon S3 em seu local Conta da AWS para fazer o upload dos registros arquivados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Recomendamos que a instância do Amazon EC2 especificada no parâmetro `ECSInstanceId` tenha um perfil do IAM com a política `AmazonSSMManagedInstanceCore` gerenciada pela Amazon anexada. Para fazer o upload do arquivo de log para o bucket do Amazon S3 que foi especificado no parâmetro `LogDestination`, as seguintes permissões devem ser adicionadas:

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

Etapas do documento

- `assertInstanceIsManaged` :Verifica se a instância especificada no parâmetro `ECSInstanceId` é gerenciada pelo Systems Manager.
- `getInstancePlatform` :Obtém informações sobre a plataforma do sistema operacional (OS) da instância especificada no parâmetro `ECSInstanceId`.
- `verifyInstancePlatform` :Ramifica a automação com base na plataforma do sistema operacional.
- `runLogCollectionScriptOnLinux` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon ECS em instâncias do Linux e cria um arquivo de arquivamento no diretório `/var/log/collectECSlogs`.
- `runLogCollectionScriptOnWindows` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon ECS em instâncias do Windows e cria um arquivo de arquivamento no diretório `C:\ProgramData\collectECSlogs`.
- `verifyIfS3BucketProvided` :Verifica se um valor foi especificado para o parâmetro `LogDestination`.

- `runUploadScript` :Ramifica a etapa de automação com base na plataforma do sistema operacional.
- `runUploadScriptOnLinux` :Carrega o arquivo de log no bucket do Amazon S3 especificado no parâmetro `LogDestination` e exclui o arquivo de log arquivado do sistema operacional.
- `runUploadScriptOnWindows` :Carrega o arquivo de log no bucket do Amazon S3 especificado no parâmetro `LogDestination` e exclui o arquivo de log arquivado do sistema operacional.

AWS-InstallAmazonECSAgent

Descrição

O runbook `AWS-InstallAmazonECSAgent` instala o atendente do Amazon Elastic Container Service (Amazon ECS) na instância do Amazon Elastic Compute Cloud (Amazon EC2) que for especificado. Este runbook oferece compatibilidade apenas com instâncias do Amazon Linux e do Amazon Linux 2.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceIds

Tipo: StringList

Descrição: (obrigatório) Os IDs das instâncias do Amazon EC2 nas quais deseja instalar o atendente do Amazon ECS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Etapas do documento

`aws:executeScript` :Instala o atendente do Amazon ECS nas instâncias do Amazon EC2 especificadas no parâmetro de `InstanceIds`.

Saídas

InstallAmazonAgente ECS. SuccessfulInstances - O ID da instância em que a instalação do agente Amazon ECS foi bem-sucedida.

InstallAmazonAgente ECS. FailedInstances - O ID da instância em que a instalação do agente do Amazon ECS falhou.

InstallAmazonAgente ECS. InProgressInstances - O ID da instância em que a instalação do agente Amazon ECS está em andamento.

AWS-ECSRunTask

Descrição

O `AWS-ECSRunTask` runbook executa a tarefa do Amazon Elastic Container Service (Amazon ECS) especificada por você.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- capacityProviderStrategy

  Tipo: string

  Descrição: (Opcional) A estratégia do provedor de capacidade a ser usada para a tarefa.
- cluster

  Tipo: string

  Descrição: (Opcional) O nome abreviado ou ARN do cluster no qual executar sua tarefa. Se você não especificar um cluster, o cluster padrão será usado.
- contagem

  Tipo: string

  Descrição: (Opcional) O número de instanciações da tarefa especificada a serem colocadas em seu cluster. Você pode especificar até 10 tarefas para cada solicitação.

- Habilitar o ECS ManagedTags

  Tipo: booliano

  Descrição: (Opcional) Especifica se as tags gerenciadas do Amazon ECS devem ser usadas para a tarefa. Para obter mais informações, consulte Marcar seus recursos do Amazon ECS, no Guia do Desenvolvedor do Amazon Elastic Container Service.

- enableExecuteCommand

  Tipo: booliano

  Descrição: (Opcional) Determina se a funcionalidade de execução do comando deve ser ativada para os contêineres nessa tarefa. Se verdadeiro, isso ativa a funcionalidade de execução do comando em todos os contêineres da tarefa.

- group

  Tipo: string

  Descrição: (Opcional) O nome do grupo de tarefas a ser associado à tarefa. O valor padrão é o nome da família da definição da tarefa. Por exemplo, `family:my-family-name`.

- Tipo de lançamento

  Tipo: string

  Valores válidos: EC2 | FARGATE | EXTERNAL

  Descrição: (Opcional) A infraestrutura na qual executar sua tarefa autônoma.

- networkConfiguration

  Tipo: string

  Descrição: (Opcional) A configuração de rede para a tarefa. Esse parâmetro é necessário para definições de tarefas que usam o modo de `awsvpc` rede para receber sua própria interface de rede elástica e não é compatível com outros modos de rede.

- substituições

  Tipo: string

  Descrição: (Opcional) Uma lista de substituições de contêiner no formato JSON que especificam o nome de um contêiner na definição de tarefa especificada e as substituições que ele deve receber.

Você pode substituir o comando padrão de um contêiner especificado na definição da tarefa ou na imagem do Docker com uma substituição de comando. Você também pode substituir as variáveis de ambiente existentes que são especificadas na definição da tarefa ou na imagem do Docker em um contêiner. Além disso, você pode adicionar novas variáveis de ambiente com uma substituição de ambiente.

- Restrições de posicionamento

  Tipo: string

  Descrição: (Opcional) Uma matriz de objetos de restrição de posicionamento para usar na tarefa. Você pode especificar até 10 restrições para cada tarefa, incluindo restrições na definição da tarefa e aquelas especificadas em tempo de execução.

- Estratégia de colocação

  Tipo: string

  Descrição: (Opcional) Os objetos da estratégia de posicionamento a serem usados na tarefa. Você pode especificar no máximo 5 regras de estratégia para cada tarefa.

- platformVersion

  Tipo: string

  Descrição: (Opcional) A versão da plataforma que a tarefa usa. Uma versão da plataforma é especificada somente para tarefas hospedadas no Fargate. Se não for especificada uma versão da plataforma, a versão da plataforma `LATEST` será usada.

- propagateTags

  Tipo: string

  Descrição: (Opcional) Determina se as tags se propagam da definição da tarefa para a tarefa. Se nenhum valor for especificado, as tags não serão propagadas. As tags só podem ser propagadas para a tarefa durante sua criação.

- referenceId

  Tipo: string

  Descrição: (Opcional) O ID de referência a ser usado para a tarefa. O ID de referência pode ter um tamanho máximo de 1024 caracteres.

- Iniciado por

Tipo: string

Descrição: (Opcional) Uma tag opcional especificada quando uma tarefa é iniciada. Isso ajuda você a identificar quais tarefas pertencem a um trabalho específico filtrando os resultados de uma operação de `ListTasks` API. São permitidos até 36 letras (maiúsculas e minúsculas), números, hífens (-) e sublinhados (_).

- tags

  Tipo: string

  Descrição: (Opcional) Metadados que você deseja aplicar à tarefa para ajudá-lo a categorizar e organizar tarefas. Cada tag consiste em uma chave e um valor definidos pelo usuário.

- Definição de tarefa

  Tipo: string

  Descrição: (Opcional) O `family` e `revision` (`family:revision`) ou o ARN completo da definição da tarefa a ser executada. Se uma revisão não for especificada, a `ACTIVE` revisão mais recente será usada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ecs:RunTask`

Etapas do documento

`aws:executeScript`- Executa a tarefa do Amazon ECS com base nos valores que você especifica para os parâmetros de entrada do runbook.

AWSSupport-TroubleshootECSContainerInstance

Descrição

O runbook `AWSSupport-TroubleshootECSContainerInstance` ajuda a solucionar problemas de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que não consegue se registrar em um cluster do Amazon ECS. Essa automação analisa se os dados do usuário da

instância contêm as informações corretas do cluster, se o perfil de instância contém as permissões necessárias e problemas de configuração de rede.

> **Important**
>
> Para executar essa automação com sucesso, o estado da instância do Amazon EC2 deve ser `running`, e o estado do cluster do Amazon ECS deve ser `ACTIVE`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon ECS no qual a instância não conseguiu se registrar.
- InstanceId

Tipo: string

Descrição: (obrigatório) o ID da instância do Amazon EC2 cujo problema você deseja solucionar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

aws:executeScript: Analisa se a instância do Amazon EC2 atende aos pré-requisitos necessários para se registrar em um cluster do Amazon ECS.

AWSSupport-TroubleshootECSTaskFailedToStart

Descrição

O runbook `AWSSupport-TroubleshootECSTaskFailedToStart` ajuda a solucionar o motivo pelo qual uma tarefa do Amazon Elastic Container Service (Amazon ECS) em um cluster do Amazon ECS não foi iniciada. Você deve executar esse runbook da Região da AWS mesma forma que sua

tarefa que falhou ao iniciar. O runbook analisa os seguintes problemas comuns que podem impedir o início de uma tarefa:

- Conectividade de rede com o registro de contêiner configurado
- Permissões do IAM ausentes exigidas pela função de execução da tarefa
- Conectividade do serviço de endpoint da VPC
- Configuração de regras do grupo de segurança
- AWS Secrets Manager referências de segredos
- Configuração de registro em log

> **Note**
>
> Se a análise determinar que a conectividade de rede precisa ser testada, uma função do Lambda e o perfil do IAM necessário serão criados em sua conta. Esses atributos são usados para simular a conectividade de rede da tarefa que falhou. A automação exclui esses atributos quando eles não são mais necessários. No entanto, se a automação não conseguir excluir os atributos, isso deverá ser feito manualmente.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon ECS em que a tarefa não foi iniciada.

- CloudwatchRetentionPeriod

  Tipo: inteiro

  Descrição: (Opcional) O período de retenção, em dias, para que os registros da função Lambda sejam armazenados no Amazon CloudWatch Logs. Isso só é necessário se a análise determinar que a conectividade de rede precisa ser testada.

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Padrão: 30

- TaskId

  Tipo: string

  Descrição: (obrigatório) O ID da tarefa que falhou. Use a tarefa que falhou mais recentemente.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript` :Verifica se o usuário ou a função que iniciou a automação tem as permissões necessárias do IAM. Se não tiver permissões suficientes para usar esse runbook, as permissões necessárias ausentes serão incluídas na saída da automação.
- `aws:branch` :Ramificações com base no fato de você ter permissões para todas as ações necessárias para o runbook.
- `aws:executeScript` :Cria uma função do Lambda em sua VPC se a análise determinar que a conectividade de rede precisa ser testada.
- `aws:branch` :Ramificações com base nos resultados da etapa anterior.
- `aws:executeScript` :Analisa as possíveis causas da falha em iniciar a tarefa.
- `aws:executeScript` :Exclui atributos criados por essa automação.
- `aws:executeScript` :Formata a saída da automação para retornar os resultados da análise ao console. Você pode revisar a análise depois dessa etapa antes que a automação seja concluída.
- `aws:branch` :Ramifica com base no fato de a função do Lambda e os recursos associados terem sido criados e precisarem ser excluídos.
- `aws:sleep` :Permanece em repouso por 30 minutos para que a interface de rede elástica da função do Lambda possa ser excluída.
- `aws:executeScript` :Exclui a interface de rede da função do Lambda.
- `aws:executeScript` :Formata a saída da etapa de exclusão da interface de rede da função do Lambda.

AWS-UpdateAmazonECSAgent

Descrição

O runbook `AWS-UpdateAmazonECSAgent` atualiza o atendente do Amazon Elastic Container Service (Amazon ECS) na instância do Amazon Elastic Compute Cloud (Amazon EC2) especificada. Este runbook oferece compatibilidade apenas com instâncias do Amazon Linux e do Amazon Linux 2.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterARN

  Tipo: StringList

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do cluster do Amazon ECS no qual as instâncias de contêineres estão registradas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Etapas do documento

`aws:executeScript` :Atualiza o atendente do Amazon ECS no cluster do Amazon ECS especificado nos parâmetros de `ClusterARN`.

Saídas

UpdateAmazonAgente ECS. UpdatedContainers - O ID da instância em que a atualização do agente do Amazon ECS foi bem-sucedida.

UpdateAmazonAgente ECS. FailedContainers - O ID da instância em que a atualização do agente do Amazon ECS falhou.

UpdateAmazonAgente ECS. InProgressContainers - O ID da instância em que a atualização do agente do Amazon ECS está em andamento.

Amazon EFS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic File System. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CheckAndMountEFS

`AWSSupport-CheckAndMountEFS`

Descrição

O runbook `AWSSupport-CheckAndMountEFS` verifica os pré-requisitos para montar seu sistema de arquivos do Amazon Elastic File System (Amazon EFS) e monta o sistema de arquivos na instância do Amazon Elastic Compute Cloud (Amazon EC2) especificado. Esse runbook oferece suporte à montagem do sistema de arquivos Amazon EFS com o nome DNS ou com o endereço IP do destino de montagem.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Ação

  Tipo: string

  Valores válidos: Verifique | CheckAndMount

  Descrição: (obrigatório) Determina se o runbook verifica os pré-requisitos ou verifica os pré-requisitos e monta o sistema de arquivos.
- EfsId

  Tipo: string

Descrição: (obrigatório) O ID do sistema de arquivos que deseja montar.

- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância do Amazon EC2 na qual deseja montar o sistema de arquivos.

- MountOptions

  Tipo: string

  Descrição: (opcional) As opções suportadas pelo auxiliar de montagem do Amazon EFS que deseja usar ao montar o sistema de arquivos. Se a opção `tls` for especificada, verifique se o stunnel foi atualizado na instância de destino.

- MountPoint

  Tipo: string

  Descrição: (opcional) O diretório em que deseja montar o sistema de arquivos. Se você especificar o valor `Check` para o parâmetro `Action`, esse parâmetro não deverá ser especificado.

- MountTargetIP

  Tipo: string

  Descrição: (opcional) O endereço IP do alvo de montagem. A montagem por endereço IP funciona em ambientes em que o DNS está desabilitado, como nuvens privadas virtuais (VPCs) com nomes de host DNS desativados. Além disso, você pode usar essa opção se seu ambiente usar um provedor de DNS diferente do Amazon Route 53 (Route 53).

- Região

  Tipo: string

  Descrição: (Obrigatório) Região da AWS Onde a instância e o sistema de arquivos do Amazon EC2 estão localizados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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:*

Etapas do documento

- aws:executeScript :Reúne detalhes sobre a instância do Amazon EC2 especificada no parâmetro InstanceId.
- aws:executeScript :Reúne detalhes sobre o sistema de arquivos especificado no parâmetro EfsId.
- aws:executeScript :Verifica se o grupo de segurança associado ao sistema de arquivos permite tráfego na porta 2049 a partir da instância do Amazon EC2 especificada no parâmetro InstanceId.
- aws:assertAwsResourceProperty :Verifica se a instância do Amazon EC2 especificada no parâmetro InstanceId é gerenciada pelo Systems Manager e se o status é Online.

- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Action`.
- `aws:runCommand` :Verifica os pré-requisitos para montar o sistema de arquivos especificado no parâmetro `EfsId`.
- `aws:runCommand` :Verifica os pré-requisitos para montar o sistema de arquivos especificado no parâmetro `EfsId` e monta o sistema de arquivos na instância do Amazon EC2 especificada no parâmetro `InstanceId`.

Amazon EKS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Kubernetes Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups

`AWSSupport-CollectEKSInstanceLogs`

Descrição

O runbook `AWSSupport-CollectEKSInstanceLogs` reúne arquivos de log relacionados ao sistema operacional e ao Amazon Elastic Kubernetes Service (Amazon EKS) de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para ajudar a solucionar problemas comuns.

Enquanto a automação reúne os arquivos de log associados, são feitas alterações na estrutura do sistema de arquivos, incluindo a criação de diretórios temporários, a cópia dos arquivos de log nos diretórios temporários e a compactação dos arquivos de log em um arquivamento. Essa atividade pode resultar em aumento de `CPUUtilization` na instância do EC2. Para obter mais informações sobre`CPUUtilization`, consulte Métricas de instância no Guia CloudWatch do usuário da Amazon.

Se você especificar um valor para o parâmetro `LogDestination`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos logs coletados da sua instância do EC2, se o status da política `isPublic` estiver definido como `true` ou se a lista de controle de acesso (ACL) conceder permissões de `READ|WRITE` ao grupo predefinido `All Users` do Amazon S3, os logs não serão carregados. Para mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Essa automação requer pelo menos 10% do espaço em disco disponível no volume raiz do Amazon Elastic Block Store (Amazon EBS) anexado à instância do EC2. Se não houver espaço em disco disponível suficiente no volume raiz, a automação será interrompida.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EKS InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância do Amazon EKS EC2 das quais deseja coletar os logs.

- LogDestination

  Tipo: string

  Descrição: (opcional) O bucket do S3 em sua conta para fazer o upload dos logs arquivados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Recomendamos que a instância do EC2 que recebe o comando tenha uma função do IAM com a política gerenciada da ManagedInstanceCore Amazon do AmazonSSM anexada. Para carregar o arquivo de log no bucket do S3 especificado no parâmetro `LogDestination`, a permissão `s3:PutObject` deve ser adicionada.

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma se o sistema operacional do valor especificado no parâmetro `EKSInstanceId` é Linux.
- `aws:runCommand` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon EKS, compactando-os em um arquivo no diretório `/var/log`.
- `aws:branch` :Confirma se um valor foi especificado para o parâmetro de `LogDestination`.
- `aws:runCommand` :Carrega o arquivo de log no bucket do S3 especificado no parâmetro `LogDestination`.

AWS-CreateEKSClusterWithFargateProfile

Descrição

O `AWS-CreateEKSClusterWithFargateProfile` runbook cria um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando um. AWS Fargate

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (Obrigatório) Um nome exclusivo para o cluster.
- ClusterRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM que fornece permissões para o plano de controle do Kubernetes fazer chamadas para operações de AWS API em seu nome.

- FargateProfileName

  Tipo: string

  Descrição: (Obrigatório) O nome do perfil do Fargate.

- FargateProfileRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função IAM de execução do Amazon EKS Pod.

- FargateProfileSelectors

  Tipo: string

  Descrição: (Obrigatório) Os seletores para combinar os pods com o perfil do Fargate.

- SubnetIds

  Tipo: StringList

  Descrição: (Obrigatório) Os IDs das sub-redes que você deseja usar para seu cluster Amazon EKS. O Amazon EKS cria interfaces de rede elásticas nessas sub-redes para comunicação entre seus nós e o plano de controle do Kubernetes. Você deve especificar pelo menos dois IDs de sub-rede.

- EKS EndpointPrivateAccess

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Defina esse valor para permitir acesso privado `True` ao endpoint do servidor da API Kubernetes do seu cluster. Se você habilitar o acesso privado, as solicitações de API do Kubernetes originadas da VPC do cluster usarão o endpoint da VPC privada. Se você desabilitar o acesso privado e tiver nós ou AWS Fargate pods no cluster, certifique-se de `publicAccessCidrs` incluir os blocos CIDR necessários para comunicação com os nós ou pods Fargate.

- EKS EndpointPublicAccess

  Tipo: booliano

  Padrão: False

Descrição: (Opcional) Defina esse valor para desativar `False` o acesso público ao endpoint do servidor da API Kubernetes do seu cluster. Se você desativar o acesso público, o servidor da API Kubernetes do seu cluster só poderá receber solicitações de dentro da VPC em que foi lançado.

- PublicAccessCIDRs

  Tipo: StringList

  Descrição: (Opcional) Os blocos CIDR que têm acesso permitido ao endpoint público do servidor da API Kubernetes do seu cluster. A comunicação com o endpoint em endereços fora dos blocos CIDR especificados é negada. Se você desativou o acesso privado ao endpoint e tem nós ou pods Fargate no cluster, certifique-se de especificar os blocos CIDR necessários.

- SecurityGroupIds

  Tipo: StringList

  Descrição: (Opcional) Especifique um ou mais grupos de segurança para associar às interfaces de rede elástica criadas em sua conta pelo Amazon EKS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- CreateEksCluster (aws:executeAwsApi) - Cria um cluster Amazon EKS.
- VerifyEks ClusterIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do cluster é. `ACTIVE`
- CreateFargateProfile (aws:executeAwsApi) - Cria um Fargate para o cluster.
- VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do perfil Fargate é. `ACTIVE`

Saídas

`CreateEKSCluster.CreateClusterResponse`

Descrição: Resposta recebida da chamada `CreateCluster` da API.

`CreateFargateProfile.CreateFargateProfileResponse`

Descrição: Resposta recebida da chamada `CreateFargateProfile` da API.

AWS-CreateEKSClusterWithNodegroup

Descrição

O `AWS-CreateEKSClusterWithNodegroup` runbook cria um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando um grupo de nós para capacidade.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (Obrigatório) Um nome exclusivo para o cluster.
- ClusterRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM que fornece permissões para o plano de controle do Kubernetes fazer chamadas para operações de AWS API em seu nome.
- NodegroupName

  Tipo: string

  Descrição: (Obrigatório) Um nome exclusivo para o grupo de nós.
- NodegroupRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM a ser associada ao seu grupo de nós. O daemon kubelet do node worker node do Amazon EKS faz chamadas para AWS APIs em seu nome. Os nós recebem permissões para essas chamadas de API por meio de um perfil de instância do IAM e políticas associadas. Antes de iniciar os nós e registrá-los em um cluster, você deve criar um perfil do IAM para uso desses nós quando eles forem iniciados.
- SubnetIds

  Tipo: StringList

Descrição: (Obrigatório) Os IDs das sub-redes que você deseja usar para seu cluster Amazon EKS. O Amazon EKS cria interfaces de rede elásticas nessas sub-redes para comunicação entre seus nós e o plano de controle do Kubernetes. Você deve especificar pelo menos dois IDs de sub-rede.

- EKS EndpointPrivateAccess

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Defina esse valor para permitir acesso privado `True` ao endpoint do servidor da API Kubernetes do seu cluster. Se você habilitar o acesso privado, as solicitações de API do Kubernetes originadas da VPC do cluster usarão o endpoint da VPC privada. Se você desabilitar o acesso privado e tiver nós ou AWS Fargate pods no cluster, certifique-se de `publicAccessCidrs` incluir os blocos CIDR necessários para comunicação com os nós ou pods Fargate.

- EKS EndpointPublicAccess

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Defina esse valor para desativar `False` o acesso público ao endpoint do servidor da API Kubernetes do seu cluster. Se você desativar o acesso público, o servidor da API Kubernetes do seu cluster só poderá receber solicitações de dentro da VPC em que foi lançado.

- PublicAccessCIDRs

  Tipo: StringList

  Descrição: (Opcional) Os blocos CIDR que têm acesso permitido ao endpoint público do servidor da API Kubernetes do seu cluster. A comunicação com o endpoint em endereços fora dos blocos CIDR especificados é negada. Se você desativou o acesso privado ao endpoint e tem nós ou pods Fargate no cluster, certifique-se de especificar os blocos CIDR necessários.

- SecurityGroupIds

  Tipo: StringList

Descrição: (Opcional) Especifique um ou mais grupos de segurança para associar às interfaces de rede elástica criadas em sua conta pelo Amazon EKS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Etapas do documento

- CreateEksCluster (aws:executeAwsApi) - Cria um cluster Amazon EKS.
- VerifyEks ClusterIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do cluster é. `ACTIVE`
- CreateNodegroup (aws:executeAwsApi) - Cria um grupo de nós para o cluster.
- VerifyNodegroupIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do grupo de nós é`ACTIVE`.

Saídas

- `CreateEKSCluster.CreateClusterResponse`: resposta recebida da chamada `CreateCluster` da API.

- `CreateNodegroup.CreateNodegroupResponse`: resposta recebida da chamada `CreateNodegroup` da API.

AWS-DeleteEKSCluster

Descrição

Esse runbook exclui os atributos associados a um cluster do Amazon EKS, incluindo grupos de nós e perfis do Fargate. Opcionalmente, você pode optar por excluir todos os nós autogerenciados, as AWS CloudFormation pilhas usadas para criar os nós e a pilha de VPC CloudFormation do seu cluster. Para obter mais informações sobre como excluir um cluster do ECS, consulte Excluir um cluster no Guia do usuário do Amazon EKS.

> **Note**
>
> Se tiver serviços ativos no cluster associados a um balanceador de carga, você deve excluir esses serviços antes de excluir o cluster. Caso contrário, o sistema não poderá excluir os balanceadores de carga. Utilizar o procedimento a seguir para localizar e excluir serviços antes de executar o runbook `AWS-DeleteEKSCluster`.

Para localizar e excluir serviços no cluster

1. Instalar o utilitário de linha de comando Kubernetes, `kubectl`. Para obter mais informações, consulte Instalar o kubectl no Manual do usuário do Amazon EKS.
2. Executar o comando a seguir para listar todos os serviços em execução no cluster.

```
kubectl get svc --all-namespaces
```

3. Executar o comando a seguir para excluir todos os serviços que tenham um valor de IP EXTERNO associado. Esses serviços são liderados por um balanceador de carga e devem ser excluídos no Kubernetes para permitir que o balanceador de carga e os atributos associados sejam liberados corretamente.

```
kubectl delete svc
service-name
```

Agora você pode executar o runbook `AWS-DeleteEKSCluster`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EKS ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon EKS a ser excluído.
- VPC CloudFormationStack

  Tipo: string

  Descrição: nome da AWS CloudFormation pilha (opcional) para VPC para o cluster EKS que está sendo excluído. Isso exclui a AWS CloudFormation pilha da VPC e todos os recursos criados pela pilha.
- VPC CloudFormationStackRole

  Tipo: string

Descrição: (Opcional) O ARN de uma função do IAM que AWS CloudFormation pressupõe a exclusão da pilha de VPC. CloudFormation AWS CloudFormation usa as credenciais da função para fazer chamadas em seu nome.

- SelfManagedNodeStacks

  Tipo: string

  Descrição: (Opcional) Lista separada por vírgulas de nomes de AWS CloudFormation pilha para nós autogerenciados. Isso excluirá as AWS CloudFormation pilhas para nós autogerenciados.

- SelfManagedNodeStacksRole

  Tipo: string

  Descrição: (Opcional) O ARN de uma função do IAM que AWS CloudFormation pressupõe a exclusão dos Node Stacks autogerenciados. AWS CloudFormation usa as credenciais da função para fazer chamadas em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn:DeleteStack`

Etapas do documento

- `aws:executeScript`- DeleteNodeGroups: Encontre e exclua todos os grupos de nós no cluster EKS.
- `aws:executeScript`- DeleteFargateProfiles: Encontre e exclua todos os perfis do Fargate no cluster EKS.

- `aws:executeScript`- DeleteSelfManagedNodes: Exclua todos os nós autogerenciados e as CloudFormation pilhas usadas para criar os nós.
- `aws:executeScript` :DeleteEKSCluster: Excluir o cluster EKS.
- `aws:executeScript`- DeleteVPCCloudFormationStack: exclua a pilha de VPC. CloudFormation

AWS-MigrateToNewEKSSelfManagedNodeGroup

Descrição

O `AWS-MigrateToNewEKSSelfManagedNodeGroup` runbook ajuda você a criar um novo grupo de nós Linux do Amazon Elastic Kubernetes Service (Amazon EKS) para o qual migrar seu aplicativo existente. Para obter mais informações, consulte Migração para um novo grupo de nós no Guia do usuário do Amazon EKS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- OldStackName

Tipo: string

Descrição: (Obrigatório) O nome ou ID da pilha existente AWS CloudFormation .

- NewStackName

  Tipo: string

  Descrição: (Opcional) O nome da nova AWS CloudFormation pilha criada para seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, o nome da pilha será criado usando o formato:`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGroup

  Tipo: string

  Descrição: (Opcional) O ID do grupo de segurança que você deseja que os nós usem para se comunicar com o plano de controle do Amazon EKS. Se você não especificar um valor para esse parâmetro, o grupo de segurança especificado em sua AWS CloudFormation pilha existente será usado.

- NodeInstanceType

  Tipo: string

  Descrição: (Opcional) O tipo de instância que você deseja usar para o novo grupo de nós. Se você não especificar um valor para esse parâmetro, o tipo de instância especificado na sua AWS CloudFormation pilha existente será usado.

- NodeGroupName

  Tipo: string

  Descrição: (Opcional) O nome do seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, o nome do grupo de nós especificado na AWS CloudFormation pilha existente será usado.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: string

  Descrição: (Opcional) O número desejado de nós para escalar quando sua nova pilha for criada. Esse número deve ser maior ou igual ao `NodeAutoScalingGroupMinSize` valor e menor

ou igual aoNodeAutoScalingGroupMaxSize. Se você não especificar um valor para esse parâmetro, a capacidade desejada do grupo de nós especificada em sua AWS CloudFormation pilha existente será usada.

- NodeAutoScalingGroupMaxSize

  Tipo: string

  Descrição: (Opcional) O número máximo de nós para os quais seu grupo de nós pode ser expandido. Se você não especificar um valor para esse parâmetro, o tamanho máximo do grupo de nós especificado em sua AWS CloudFormation pilha existente será usado.

- NodeAutoScalingGroupMinSize

  Tipo: string

  Descrição: (Opcional) O número mínimo de nós para os quais seu grupo de nós pode escalar. Se você não especificar um valor para esse parâmetro, o tamanho mínimo do grupo de nós especificado em sua AWS CloudFormation pilha existente será usado.

- NodeImageId

  Tipo: string

  Descrição: (opcional) O ID do Amazon Machine Image (AMI) a ser usado pelo grupo de nós.

- NodeImageIdParâmetro SSM

  Tipo: string

  Descrição: (opcional) O parâmetro público do Systems Manager para o AMI a ser usado pelo grupo de nós.

- NodeVolumeSize

  Tipo: string

  Descrição: (Opcional) O tamanho do volume raiz dos seus nós em GiB. Se você não especificar um valor para esse parâmetro, o tamanho do volume do nó especificado na AWS CloudFormation pilha existente será usado.

- NodeVolumeType

  Tipo: string

Descrição: (Opcional) O tipo de volume do Amazon EBS que você deseja usar para o volume raiz dos seus nós. Se você não especificar um valor para esse parâmetro, o tipo de volume especificado na AWS CloudFormation pilha existente será usado.

- KeyName

  Tipo: string

  Descrição: (Opcional) O par de chaves que você deseja atribuir aos seus nós. Se você não especificar um valor para esse parâmetro, o par de chaves especificado na AWS CloudFormation pilha existente será usado.

- Subredes

  Tipo: StringList

  Descrição: (Opcional) Uma lista separada por vírgulas dos IDs de sub-rede que você deseja usar para seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, as sub-redes especificadas na sua AWS CloudFormation pilha existente serão usadas.

- DisableIMDSv1

  Tipo: booliano

  Descrição: (Opcional) Especifique `true` para desativar o Instance Metadata Service Version 1 (IMDSv1). Por padrão, os nós oferecem suporte ao IMDSv1 e ao IMDSv2.

- BootstrapArguments

  Tipo: string

  Descrição: (Opcional) Argumentos adicionais que você deseja passar para o script de bootstrap do node.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- DetermineParameterValuesForNewNodeGroup (aws:ExecuteScript) - Reúne os valores dos parâmetros a serem usados no novo grupo de nós.
- CreateStack (aws:createStack) - Cria a AWS CloudFormation pilha para o novo grupo de nós.
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - Obtém a função da instância do nó.
- GetNewStackSecurityGroup (aws:executeAwsApi) - A etapa obtém o grupo de segurança do nó.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - Adiciona regras de entrada ao grupo de segurança recém-criado para que ele possa aceitar tráfego daquele atribuído ao seu grupo de nós anterior.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) - Adiciona regras de entrada ao grupo de segurança anterior para que ele possa aceitar tráfego daquele atribuído ao seu grupo de nós recém-criado.
- VerifyStackComplete (aws: assertAwsResource Property) - Verifica se o status da nova pilha é. CREATE_COMPLETE

Saídas

DetermineParameterValuesForNewNodeGroup. NewStackParameters - Os parâmetros usados para criar a nova pilha.

GetNewStackNodeInstanceRole. NewNodeInstanceRole - A função da instância do nó para o novo grupo de nós.

GetNewStackSecurityGroup. NewNodeSecurityGroup - O ID do grupo de segurança para o novo grupo de nós.

DetermineParameterValuesForNewNodeGroup. NewStackName - O nome da AWS CloudFormation pilha para o novo grupo de nós.

CreateStack. StackId - O ID da AWS CloudFormation pilha para o novo grupo de nós.

`AWSPremiumSupport-TroubleshootEKSCluster`

Descrição

O runbook `AWSPremiumSupport-TroubleshootEKSCluster` diagnostica problemas comuns com um cluster do Amazon Elastic Kubernetes Service (Amazon EKS), a infraestrutura subjacente, e fornece etapas de remediação recomendadas.

> **Important**
>
> O acesso aos runbooks da `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Compare AWS Support Plans.

Se você especificar um valor para o parâmetro `S3BucketName`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos logs coletados da sua instância do EC2, se o status da política `isPublic` estiver definido como `true` ou se a lista de controle de acesso (ACL) conceder permissões de `READ|WRITE` ao grupo predefinido `All Users` do Amazon S3, os logs não serão carregados. Para mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon EKS que deseja solucionar.
- S3 BucketName

  Tipo: string

  Descrição: (opcional) O nome do bucket privado do Amazon S3 em que o relatório gerado pelo runbook deve ser carregado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Além disso, a política AWS Identity and Access Management (IAM) anexada ao usuário ou à função que inicia a automação deve permitir a `ssm:GetParameter` operação com os seguintes AWS Systems Manager parâmetros públicos para obter a última recomendação do Amazon EKS Amazon Machine Image (AMI) para os nós de trabalho.

- 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

Para carregar o relatório gerado pelo runbook em um bucket do Amazon S3, as seguintes permissões são necessárias para o bucket do Amazon S3 especificado.

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

Etapas do documento

- `aws:executeAwsApi` :Reúne detalhes do cluster Amazon EKS especificado.
- `aws:executeScript` :Reúne detalhes das instâncias do Amazon Elastic Compute Cloud (Amazon EC2), grupos do Auto Scaling, AMIs e tipos de instância gráfica de GPU do Amazon EC2.
- `aws:executeScript` :Reúne detalhes da nuvem privada virtual (VPC), sub-redes, gateways de conversão de endereços de rede (NAT), rotas de sub-rede, grupos de segurança e listas de controle de acesso (ACLs) à rede do cluster do Amazon EKS.
- `aws:executeScript` :Reúne detalhes dos perfis de instância do IAM anexados e das políticas de perfis.
- `aws:executeScript` :Reúne detalhes do bucket do Amazon S3 especificado no parâmetro `S3BucketName`.
- `aws:executeScript` :Classifica as sub-redes da Amazon VPC como públicas ou privadas.
- `aws:executeScript` :Verifica as sub-redes da Amazon VPC em busca de tags que são necessárias como parte de um cluster do Amazon EKS.
- `aws:executeScript` :Verifica as sub-redes da Amazon VPC em busca das tags que são necessárias para as sub-redes do Elastic Load Balancing.
- `aws:executeScript` :Verifica se as instâncias da Amazon EC2 do nó de processamento usam a última versão otimizada das AMIs do Amazon EKS
- `aws:executeScript` :Verifica se os grupos de segurança da Amazon VPC estão conectados aos nós de processamento quanto às tags necessárias.
- `aws:executeScript` :Verifica as regras do cluster do Amazon EKS e do grupo de segurança da Amazon VPC do nó de processamento quanto às regras de entrada recomendadas para o cluster do Amazon EKS.
- `aws:executeScript` :Verifica as regras do cluster do Amazon EKS e do grupo de segurança da Amazon VPC do nó de processamento para ver as regras de saída recomendadas do cluster do Amazon EKS.
- `aws:executeScript` :Verifica a configuração de rede da ACL para as sub-redes da Amazon VPC.

- `aws:executeScript` :Verifica se as instâncias do nó de processamento do Amazon EC2 têm as políticas gerenciadas necessárias.
- `aws:executeScript` :Verifica se os grupos do Auto Scaling têm as tags necessárias para o escalonamento automático do cluster.
- `aws:executeScript` :Verifica se as instâncias do nó de processamento do Amazon EC2 estão conectadas à Internet.
- `aws:executeScript` :Gera um relatório com base nas saídas das etapas anteriores. Se um valor for especificado para o parâmetro `S3BucketName`, o relatório gerado será carregado no bucket do Amazon S3.

`AWSSupport-TroubleshootEKSWorkerNode`

Descrição

O runbook `AWSSupport-TroubleshootEKSWorkerNode` analisa um nó de processamento do Amazon Elastic Compute Cloud (Amazon EC2) e um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) para ajudar a identificar e solucionar causas comuns que impedem que os nós de processamento se juntem a um cluster. O runbook fornece orientações para ajudar a resolver quaisquer problemas identificados.

> **Important**
>
> Para executar essa automação com sucesso, o estado do nó de processamento do Amazon EC2 deve ser `running` e o estado do cluster do Amazon EKS deve ser `ACTIVE`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon EKS.
- WorkerID

  Tipo: string

  Descrição: (obrigatório) O ID do nó de processamento do Amazon EC2 que não conseguiu se juntar ao cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:assertAwsResourceProperty :Confirma que o cluster Amazon EKS especificado no parâmetro ClusterName existe e está no estado ACTIVE.
- aws:assertAwsResourceProperty :Confirma que o nó de processamento do Amazon EC2 especificado no parâmetro WorkerID existe e está no estado running.
- aws:executeScript :Executa um script Python que ajuda a identificar possíveis causas da falha do nó de processamento em ingressar no cluster.

AWS-UpdateEKSCluster

Descrição

O AWS-UpdateEKSCluster runbook ajuda você a atualizar seu cluster do Amazon Elastic Kubernetes Service (Amazon EKS) para a versão do Kubernetes que você deseja usar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (Obrigatório) O nome do seu cluster Amazon EKS.
- Version (Versão)

  Tipo: string

  Descrição: (Obrigatório) A versão do Kubernetes para a qual você deseja atualizar seu cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`- Atualiza a versão do Kubernetes que é usada pelo seu cluster Amazon EKS.
- `aws:waitForAwsResourceProperty`- Espera que o status da atualização seja`Successful`.

AWS-UpdateEKSManagedNodeGroup

Descrição

O runbook `AWS-UpdateEKSManagedNodeGroup` ajuda a atualizar um grupo de nós gerenciados do Amazon Elastic Kubernetes Service (Amazon EKS). Você pode escolher uma atualização de `Version` ou de `Configuration`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster cujo grupo de nós deseja atualizar.
- NodeGroupName

  Tipo: string

  Descrição: (obrigatório) O nome do grupo de nós a ser atualizado.

- UpdateType

  Tipo: string

  Valores válidos: Update Node Group Version | Update Node Group Configurations

  Padrão: Atualizar versão do grupo de nós

  Descrição: (obrigatório) O tipo de atualização que deseja realizar no grupo de nós.

Os parâmetros a seguir se aplicam somente ao tipo de atualização de `Version`:

- AMI ReleaseVersion

  Tipo: string

  Descrição: (opcional) A versão da AMI otimizada do Amazon EKS que deseja usar. A versão mais recente é usada por padrão.

- ForceUpgrade

  Tipo: booliano

  Descrição: (opcional) Se verdadeiro, a atualização não falhará em resposta a uma violação do orçamento de interrupção do pod.

- KubernetesVersion

  Tipo: string

  Descrição: (opcional) A versão do Kubernetes para a qual atualizar o grupo de nós.

- LaunchTemplateId

  Tipo: string

  Descrição: (opcional) O ID do modelo de execução.

- LaunchTemplateName

  Tipo: string

  Descrição: (opcional) O nome do modelo de execução.

- LaunchTemplateVersion

Tipo: string

Descrição: (opcional) A versão do modelo de lançamento do Amazon Elastic Compute Cloud (Amazon EC2). Esse parâmetro só é válido se um grupo de nós foi criado a partir de um modelo de execução.

Os parâmetros a seguir se aplicam somente ao tipo de atualização de `Configuration`:

- AddOrUpdateNodeGroupLabels

  Tipo: StringMap

  Descrição: (opcional) Rótulos do Kubernetes que deseja adicionar ou atualizar.
- AddOrUpdateKubernetesTaintsEffect

  Tipo: StringList

  Descrição: (opcional) As taints do Kubernetes que deseja adicionar ou atualizar.
- MaxUnavailableNodeGroups

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número máximo de nós indisponíveis ao mesmo tempo durante uma atualização de versão.
- MaxUnavailablePercentageNodeGroup

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) A porcentagem de nós não disponíveis durante uma atualização de versão.
- NodeGroupDesiredSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número atual de nós que o grupo de nós gerenciados deve manter.

- NodeGroupMaxSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número máximo de nós para o qual o grupo de nós gerenciados pode ser aumentado na escala horizontalmente.

- NodeGroupMinSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número mínimo de nós para o qual o grupo de nós gerenciados pode ser reduzido na escala horizontalmente.

- RemoveKubernetesTaintsEffect

  Tipo: StringList

  Descrição: (opcional) As taints do Kubernetes que deseja remover.

- RemoveNodeGroupLabels

  Tipo: StringList

  Descrição: (opcional) Uma lista separada por vírgulas dos rótulos que deseja remover.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Etapas do documento

- `aws:executeScript` :Atualiza um grupo de nós do cluster Amazon EKS de acordo com os valores especificados para os parâmetros de entrada do runbook.

- `aws:waitForAwsResourceProperty` :Espera que o status de atualização do cluster seja `Successful`.

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descrição

O runbook `AWS-UpdateEKSSelfManagedLinuxNodeGroups` atualiza grupos de nós autogerenciados em seu cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando uma pilha do AWS CloudFormation .

Se o cluster usa ajuste de escala automático, recomendamos reduzir a implantação para duas réplicas antes de usar esse runbook.

Escalar uma implantação para duas réplicas

1. Instalar o utilitário de linha de comando Kubernetes, `kubectl`. Para obter mais informações, consulte Instalar o kubectl no Manual do usuário do Amazon EKS.
2. Execute o seguinte comando .

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

3. Executar o runbook `AWS-UpdateEKSSelfManagedLinuxNodeGroups`.
4. Escalar a implantação para o número desejado de réplicas executando o comando a seguir.

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

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (obrigatório) O nome do cluster do Amazon EKS.
- NodeGroupName

  Tipo: string

  Descrição: (obrigatório) O nome do grupo de nós gerenciados.
- ClusterControlPlaneSecurityGroup

  Tipo: string

  Descrição: (obrigatório) O ID do grupo de segurança do ambiente de gerenciamento.
- DisableIMDSv1

  Tipo: Booliano

  Descrição: (opcional) Determina se deseja permitir o serviço de metadados de instância versão 1 (IMDSv1) e IMDSv2.
- KeyName

  Tipo: string

  Descrição: (opcional) O nome da chave para as instâncias.
- NodeAutoScalingGroupDesiredCapacity

Tipo: string

Descrição: (opcional) O número de nós que o grupo de nós deve manter.

- NodeAutoScalingGroupMaxSize

  Tipo: string

  Descrição: (opcional) O número máximo de nós para o qual o grupo de nós pode ser expandido.

- NodeAutoScalingGroupMinSize

  Tipo: string

  Descrição: (opcional) O número mínimo de nós para o qual o grupo de nós pode ser reduzido.

- NodeInstanceType

  Tipo: string

  Padrão: T3.large

  Descrição: (opcional) O tipo de instância a ser usado para o grupo de nós.

- NodeImageId

  Tipo: string

  Descrição: (opcional) O ID do Amazon Machine Image (AMI) a ser usado pelo grupo de nós.

- NodeImageIdParâmetro SSM

  Tipo: string

  Padrão: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Descrição: (opcional) O parâmetro público do Systems Manager para o AMI a ser usado pelo grupo de nós.

- StackName

  Tipo: string

  Descrição: (Obrigatório) O nome da AWS CloudFormation pilha usada para atualizar o grupo de nós.

- Subredes

  Tipo: string

  Descrição: (obrigatório) Uma lista separada por vírgulas dos IDs das sub-redes a serem usados pelo cluster.

- VpcId

  Tipo: string

  Padrão: Default

  Descrição: (obrigatório) A nuvem privada virtual (VPC) em que seu cluster está implantado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Etapas do documento

- `aws:executeScript` :Atualiza um grupo de nós do cluster Amazon EKS de acordo com os valores especificados para os parâmetros de entrada do runbook.
- `aws:waitForAwsResourceProperty`- Espera que o status de atualização da AWS CloudFormation pilha seja retornado.

Elastic Beanstalk

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Elastic Beanstalk Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWSSupport-CollectElasticBeanstalkLogs

Descrição

O runbook `AWSSupport-CollectElasticBeanstalkLogs` reúne arquivos de log do AWS Elastic Beanstalk relacionados de uma instância do Amazon Elastic Compute Cloud (Amazon Windows Server EC2) lançada pelo Elastic Beanstalk para ajudar a solucionar problemas comuns. Enquanto a automação reúne os arquivos de log associados, são feitas alterações na estrutura do sistema de arquivos, incluindo a criação de diretórios temporários, a cópia dos arquivos de log nos diretórios temporários e a compactação dos arquivos de log em um arquivamento. Essa atividade pode resultar em aumento da `CPUUtilization` na instância do Amazon EC2. Para obter mais informações sobre`CPUUtilization`, consulte Métricas de instância no Guia CloudWatch do usuário da Amazon.

Se você especificar um valor para o parâmetro `S3BucketName`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos logs coletados da sua instância do Amazon EC2, se o status da política `isPublic` estiver definido como `true`, ou se a lista de controle de acesso (ACL) conceder permissões de `READ|WRITE` ao grupo predefinido `All Users` do Amazon S3, os logs não serão carregados. Para mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Se não for especificado um valor para o parâmetro `S3BucketName`, a automação carrega o pacote de log para o bucket padrão do Amazon S3 do Elastic Beanstalk na Região da AWS em que a automação é executada. O diretório é nomeado de acordo com a estrutura `elasticbeanstalk-`*`region`*`-`*`accountID` a seguir. Os valores de *`region`* e *`accountID`* serão diferentes com base

na região da Conta da AWS em que a automação é executada. O pacote de logs será salvo no diretório `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* . Os valores de *`environmentID`* e *`instanceID`* serão diferentes com base no ambiente do Elastic Beanstalk e na instância do Amazon EC2 da qual os logs estão sendo coletados.

Por padrão, o perfil de instância AWS Identity and Access Management (IAM) anexado às instâncias do Amazon EC2 do ambiente do Elastic Beanstalk tem as permissões necessárias para carregar o pacote no bucket Amazon S3 padrão do Elastic Beanstalk para seu ambiente. Se especificar um valor para o parâmetro `S3BucketName`, o perfil de instância anexado à instância do Amazon EC2 deverá permitir as ações `s3:GetBucketAcl`, `s3:GetBucketPolicy`, `s3:GetBucketPolicyStatus` e `s3:PutObject` para o bucket e o caminho especificados do Amazon S3.

> **Note**
>
> Essa automação requer pelo menos 500 MB de espaço em disco disponível no volume raiz do Amazon Elastic Block Store (Amazon EBS) anexado à instância do Amazon EC2. Se não houver espaço em disco disponível suficiente no volume raiz, a automação será interrompida.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EnvironmentId

  Tipo: string

  Descrição: (obrigatório) O ID do seu ambiente do Elastic Beanstalk do qual deseja coletar o pacote de logs.

- InstanceId

  Tipo: string

  (obrigatório) O ID da instância do Amazon EC2 no ambiente do Elastic Beanstalk do qual deseja coletar o pacote de logs.

- S3 BucketName

  Tipo: string

  (opcional) O bucket do Amazon S3 para o qual deseja fazer o upload dos logs arquivados.

- S3 BucketPath

  Tipo: string

  (opcional) O caminho do bucket do Amazon S3 para o qual deseja fazer o upload do pacote de log. Esse parâmetro será ignorado se um valor para o parâmetro `S3BucketName` não for especificado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que a instância do Amazon EC2 especificada no parâmetro `InstanceId` é gerenciada pelo AWS Systems Manager.
- `aws:assertAwsResourceProperty` :Confirma que a instância do Amazon EC2 especificada no parâmetro `InstanceId` é uma instância do Windows Server.
- `aws:runCommand` :Verifica se a instância faz parte de um ambiente do Elastic Beanstalk, se há espaço em disco suficiente para agrupar os logs e se o bucket do Amazon S3 para o qual os logs seriam enviados é público.
- `aws:runCommand` :Coleta os arquivos de log e carrega o arquivo no bucket do Amazon S3 especificado no parâmetro `S3BucketName` ou no bucket padrão do seu ambiente do Elastic Beanstalk se um valor não for especificado.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Descrição

O `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` runbook permite o registro no ambiente AWS Elastic Beanstalk (Elastic Beanstalk) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- EnvironmentId

  Tipo: string

  Descrição: (obrigatório) O ID do ambiente do Elastic Beanstalk no qual deseja habilitar o log.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Etapas do documento

- `aws:executeAwsApi` :Permite o log no ambiente do Elastic Beanstalk especificado no parâmetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty` :Espera que o status do ambiente mude para `Ready`.
- `aws:executeScript` :Verifica se o log foi habilitado no ambiente do Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descrição

O `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook habilita notificações para o ambiente AWS Elastic Beanstalk (Elastic Beanstalk) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EnvironmentId

  Tipo: string

  Descrição: (obrigatório) O ID do ambiente do Elastic Beanstalk para o qual deseja habilitar notificações.
- TopicArn

  Tipo: string

  Descrição: (obrigatório) O ARN do tópico do Amazon Simple Notification Service (Amazon SNS) para o qual deseja enviar notificações.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`

- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Etapas do documento

- `aws:executeAwsApi` :Habilita notificações para o ambiente do Elastic Beanstalk especificado no parâmetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty` :Espera que o status do ambiente mude para `Ready`.
- `aws:executeScript` :Verifica se as notificações foram habilitadas para o ambiente do Elastic Beanstalk.

`AWSSupport-TroubleshootElasticBeanstalk`

Descrição

O `AWSSupport-TroubleshootElasticBeanstalk` runbook ajuda você a solucionar os possíveis motivos pelos quais seu AWS Elastic Beanstalk ambiente está em um estado `Degraded` ou`Severe`. Essa automação verifica os seguintes AWS recursos associados ao seu ambiente do Elastic Beanstalk:

- Detalhes de configuração para um balanceador de carga, AWS CloudFormation pilha, grupo Amazon EC2 Auto Scaling, instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e nuvem privada virtual (VPC).
- Problemas de configuração de rede com as regras de grupos de segurança, tabelas de rotas e lista de controle de acesso (ACL) à rede associadas às suas sub-redes.
- Verifica a conectividade com os endpoints do Elastic Beanstalk e o acesso público à Internet.
- Verifica o status do balanceador de carga.
- Verifica o status das instâncias do Amazon EC2.
- Recupera um pacote de registros do seu ambiente do Elastic Beanstalk e, opcionalmente, carrega os arquivos para o. AWS Support

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ApplicationName

  Tipo: string

  Descrição: (obrigatório) O nome da aplicação do Elastic Beanstalk.
- EnvironmentName

  Tipo: string

  Descrição: (obrigatório) O nome do seu ambiente do Elastic Beanstalk.
- AWSS3UploaderLink

  Tipo: string

  Descrição: (Opcional) Uma URL fornecida por você AWS Support para fazer o upload do pacote de registros do seu ambiente do Elastic Beanstalk para o. Essa opção está disponível somente para clientes que compraram um AWS Support plano e abriram um caso de Support.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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*

Etapas do documento

- aws:executeScript- Verifica se o diretor AWS Identity and Access Management (IAM) que iniciou a automação tem as permissões necessárias para realizar todas as ações definidas no runbook.
- aws:branch :Ramifica o fluxo de trabalho com base nos resultados da etapa anterior.
- aws:executeScript- Coleta informações sobre o ambiente do Elastic Beanstalk, incluindo o balanceador de carga, a pilha, o grupo Auto Scaling AWS CloudFormation , as instâncias do Amazon EC2 e a configuração da VPC.
- aws:executeScript :Verifica problemas de conectividade de rede com as tabelas de rotas e ACLs associadas às sub-redes na VPC.

- `aws:executeScript` :Verifica problemas de conectividade de rede com as regras do grupo de segurança associadas às suas instâncias do Amazon EC2.
- `aws:executeScript` :Verifica o status das instâncias do Amazon EC2.
- `aws:executeScript` :Gera um link para um pacote de logs do seu ambiente do Elastic Beanstalk.
- `aws:executeScript`- Carrega o pacote de registros para. AWS Support
- `aws:executeScript` :Gera um relatório de itens de ação para ajudar a solucionar problemas que estejam afetando o status do ambiente do Elastic Beanstalk.

Elastic Load Balancing

AWS Systems Manager A automação fornece runbooks predefinidos para o Elastic Load Balancing. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSConfigRemediation-DropInvalidHeadersForALB`

Descrição

O runbook `AWSConfigRemediation-DropInvalidHeadersForALB` habilita que o application load balancer especificado remova cabeçalhos HTTP com cabeçalhos inválidos.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerArn

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do balanceador de carga para o qual deseja eliminar cabeçalhos inválidos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita a definição de descartar cabeçalhos inválidos para o balanceador de carga especificado no parâmetro `LoadBalancerArn`.
- `aws:executeScript` :Verifica se a definição de descartar cabeçalhos inválidos foi habilitada para o balanceador de carga especificado no parâmetro `LoadBalancerArn`.

AWS-EnableCLBAccessLogs

Descrição

O `AWS-EnableCLBAccessLogs` runbook permite registros de acesso para um Classic Load Balancer.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EmitInterval

  Tipo: inteiro

  Valores válidos: 5 | 60

Padrão: 60

Descrição: (Opcional) O intervalo para publicar os registros de acesso em minutos.

- LoadBalancerNames

  Tipo: string

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos Classic Load Balancers para os quais você deseja habilitar os registros de acesso.

- S3 BucketName

  Tipo: string

  Descrição: (Obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) onde os registros de acesso são armazenados.

- S3 BucketPrefix

  Tipo: string

  Descrição: (Opcional) A hierarquia lógica que você criou para seu bucket do Amazon S3, por exemplo. `my-bucket-prefix/prod` Se o prefixo não for fornecido, o log será colocado no nível raiz do bucket.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi`- Habilita registros de acesso para os Classic Load Balancers que você especifica no `LoadBalancerNames` parâmetro.

Saídas

Habilitar o CLB. AccessLogs SuccessesLoadBalancers - Lista de nomes de balanceadores de carga nos quais os registros de acesso foram habilitados com sucesso.

Habilitar o CLB. AccessLogs FailedLoadBalancers - MapList dos nomes dos balanceadores de carga em que a ativação dos registros de acesso falhou e o motivo da falha.

AWS-EnableCLBConnectionDraining

Descrição

O AWS-EnableCLBConnectionDraining runbook permite a drenagem da conexão em um Classic Load Balancer (CLB) até o valor de tempo limite especificado. A drenagem da conexão permite que o CLB conclua solicitações em andamento feitas para instâncias que estão cancelando o registro ou não estão íntegras, com o tempo limite especificado sendo o tempo limite em que ele mantém as conexões ativas antes de relatar a instância como cancelada. Para obter mais informações sobre a drenagem de conexão em CLBs, consulte Configurar a drenagem de conexão para seu Classic Load Balancer no Guia do usuário para Classic Load Balancers.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LoadBalancerName

  Tipo: string

Descrição: (Obrigatório) O nome do balanceador de carga no qual você deseja ativar a drenagem da conexão.

- ConnectionTimeout

  Tipo: inteiro

  Valores válidos: 1-3600

  Padrão: 300

  Descrição: (Obrigatório) O valor do tempo limite de conexão para o balanceador de carga. O valor do tempo limite pode ser definido entre 1 e 3600 segundos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): ativa a drenagem da conexão e define o valor de tempo limite especificado para o balanceador de carga que você especificar.
- VerifyLoadBalancerConnectionDrainingEnabled(aws: assertAwsResource Propriedade): Verifica se a drenagem da conexão está habilitada para o balanceador de carga.
- VerifyLoadBalancerConnectionDrainingTimeout(aws: assertAwsResource Propriedade): verifica se o valor do tempo limite da conexão para o balanceador de carga corresponde ao valor especificado.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Descrição

O runbook `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` habilita o balanceamento de carga entre zonas para o Classic Load Balancer (CLB) especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerName

  Tipo: string

  Descrição: (obrigatório) O nome do CLB no qual deseja habilitar o balanceamento de carga entre zonas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`

- `elb:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita o uso do balanceamento de carga entre zonas para o CLB especificado no parâmetro `LoadBalancerName`.
- `aws:assertAwsResourceProperty` :Verifica se o balanceamento de carga entre zonas foi habilitado no CLB.

AWSConfigRemediation-EnableELBDeletionProtection

Descrição

O runbook `AWSConfigRemediation-EnableELBDeletionProtection` habilita a proteção contra exclusão para o balanceador de carga elástico (ELB) especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerArn

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do ELB no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeScript` :Habilita a proteção contra exclusão no ELB especificado no parâmetro `LoadBalancerArn`.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descrição

O `AWSConfigRemediation-EnableLoggingForALBAndCLB` runbook permite o registro do AWS Application Load Balancer ou de um Classic Load Balancer (CLB) especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerId

  Tipo: string

  Descrição: (obrigatório) O nome do Classic Load Balancer ou o ARN do Application Load Balancer.
- S3 BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3.
- S3 BucketPrefix

  Tipo: string

  Descrição: (opcional) A hierarquia lógica criada para o bucket do Amazon Simple Storage Service (Amazon S3), por exemplo, `my-bucket-prefix/prod`. Se o prefixo não for fornecido, o log será colocado no nível raiz do bucket.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeScript` :Habilita e verifica o log do Classic Load Balancer ou do Application Load Balancer.

`AWSSupport-TroubleshootCLBConnectivity`

Descrição

O runbook `AWSSupport-TroubleshootCLBConnectivity` ajuda a solucionar problemas de conectividade entre um Classic Load Balancer (CLB) e as instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Além disso, os problemas de conectividade entre um cliente e o CLB são analisados. Este runbook também analisa as verificações de integridade do CLB, verifica se as melhores práticas estão sendo seguidas e cria um painel de solução de problemas. Opcionalmente, você pode fazer upload da saída de automação para um bucket do Amazon Simple Storage Service (Amazon S3). No entanto, esse runbook não é compatível com o upload de saída para buckets do S3 que são acessíveis ao público. Recomendamos criar um bucket do S3 temporário para essa automação.

> **Important**
>
> O uso desse runbook pode gerar cobranças pelo painel criado. Para obter mais informações, consulte Amazon CloudWatch Pricing

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InvestigationType

  Tipo: string

  Valores válidos: Best Practices | Connectivity Issues | Troubleshooting Dashboard

  Descrição: (obrigatório) As operações que deseja que o runbook execute.

- LoadBalancerName

  Tipo: string

  Descrição: (obrigatório) O nome do CLB.

- S3Location

  Tipo: string

  Descrição: (opcional) O nome do bucket do S3 para o qual enviar os resultados da automação. Não há suporte para buckets acessíveis publicamente. Se seu bucket do S3 usa criptografia do lado do servidor, o usuário ou a função que executa essa automação deve ter permissões de `kms:GenerateDataKey` para a chave AWS KMS .

- S3 LocationPrefix

  Tipo: string

  Descrição: (opcional) O prefixo de chave (subpasta) do Amazon S3 para o qual deseja fazer o upload da saída de automação. *O formato de saída é armazenado no seguinte formato: DOC-EXAMPLE-BUCKET/ S3 LocationPrefix/{{}} _ {{automation: EXECUTION_ID InvestigationType}} .txt.*

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

- `aws:executeScript` :Verifica se o CLB especificado no parâmetro `LoadBalancerName` existe.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `InvestigationType`.
- `aws:executeScript` :Executa verificações de conectividade com o CLB.
- `aws:executeScript` :Verifica se a configuração do CLB segue as melhores práticas do Elastic Load Balancing.
- `aws:executeScript`- Cria um CloudWatch painel da Amazon para seu CLB.
- `aws:executeScript` :Cria um arquivo de texto com os resultados da automação e o carrega no bucket do Amazon S3 especificado no parâmetro `S3Location`.

Saídas

RunBestPractices.Resumo

RunConnectivityChecks.Resumo

CreateTroubleshootingDashboard.Saída

UploadOutputToS3. Saída

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing`

Descrição

O runbook `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` habilita o balanceamento de carga entre zonas para o network load balancer (NLB) especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerArn

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do NLB no qual deseja habilitar o balanceamento de carga entre zonas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita o balanceamento de carga entre zonas para o NLB especificado no parâmetro `LoadBalancerArn`.
- `aws:executeScript`: Verifica se o balanceamento de carga entre zonas foi habilitado no NLB.

Laboratório de atualização da AWS DesyncMitigationMode

Descrição

O `AWS-UpdateALBDesyncMitigationMode` runbook atualizará o modo de mitigação de dessincronização em um Application Load Balancer (ALB) para o modo de mitigação especificado.

O modo de mitigação de dessincronização determina como o balanceador de carga lida com solicitações que podem representar um risco de segurança para seu aplicativo.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LoadBalancerArn

  Tipo: string

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) do ALB do qual você deseja modificar o modo de mitigação de dessincronização.
- DesyncMitigationMode

  Tipo: string

  Valores válidos: monitor | defensivo | mais rigoroso

  Descrição: (Obrigatório) O modo de mitigação que você deseja que o ALB use. Para obter informações sobre os modos de mitigação de dessincronização, consulte Modo de mitigação de dessincronização no Guia do usuário para balanceadores de carga de aplicativos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- VerifyLoadBalancerType (aws: assertAwsResource Property) - Verifica se o valor especificado para o parâmetro `LoadBalancerArn` de entrada é para um balanceador de carga do aplicativo antes de prosseguir para a próxima etapa.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Atualiza o ALB para usar o especificado`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) - Verifica se o modo de mitigação de dessincronização foi atualizado para o ALB de destino.

Saídas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil da mensagem do script verificando a modificação em seu ALB.

AWS Update CLB DesyncMitigationMode

Descrição

O `AWS-UpdateCLBDesyncMitigationMode` runbook atualizará o modo de mitigação de dessincronização em um Classic Load Balancer (CLB) para o modo de mitigação especificado. O modo de mitigação de dessincronização determina como o balanceador de carga lida com solicitações que podem representar um risco de segurança para seu aplicativo.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LoadBalancerName

  Tipo: string

  Descrição: (Obrigatório) O nome do CLB do qual você deseja modificar o modo de mitigação de dessincronização.
- DesyncMitigationMode

  Tipo: string

  Valores válidos: monitor | defensivo | mais rigoroso

  Descrição: (Obrigatório) O modo de mitigação que você deseja que o CLB use. Para obter informações sobre os modos de mitigação de dessincronização, consulte Modo de mitigação de dessincronização no Guia do usuário para balanceadores de carga de aplicativos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Atualiza o CLB para usar o especificado`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) - Verifica se o modo de mitigação de dessincronização foi atualizado para o CLB de destino.

Saídas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil da mensagem do script verificando a modificação em seu CLB.

Amazon EMR

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon EMR. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-AnalyzeEMRLogs

`AWSSupport-AnalyzeEMRLogs`

Descrição

Esse runbook ajuda a identificar erros ao executar um trabalho em um cluster do Amazon EMR. O runbook analisa uma lista de logs definidos no sistema de arquivos e procura uma lista de palavras-chave predefinidas. Essas entradas de registro são usadas para criar CloudWatch eventos da Amazon Events para que você possa realizar as ações necessárias com base nos eventos. Opcionalmente, o runbook publica entradas de registro no grupo de CloudWatch registros Amazon Logs de sua escolha. Atualmente, esse runbook procura os seguintes erros e padrões nos arquivos de log:

- container_out_of_memory :O contêiner YARN ficou sem memória, o trabalho em execução pode falhar.
- yarn_nodemanager_health: O nó de TAREFA ou CORE está com pouco espaço em disco e não poderá executar tarefas.
- node_state_change: o nó de TAREFA ou CORE não pode ser acessado pelo nó PRINCIPAL.
- step_failure: Uma etapa do EMR falhou.
- no_core_nodes_running: Nenhum nó CENTRAL está em execução no momento, o cluster não está íntegro.
- hdfs_missing_blocks: Há blocos HDFS ausentes que podem levar à perda de dados.
- hdfs_high_util: A utilização do HDFS é alta, o que pode afetar as tarefas e a integridade do cluster.
- instance_controller_restart: O processo do Instance-Controller foi reiniciado. Esse processo é essencial para a integridade do cluster.
- instance_controller_restart_legacy: O processo do Instance-Controller foi reiniciado. Esse processo é essencial para a integridade do cluster.
- high_load: A alta média de carga detectada pode afetar os relatórios de integridade do nó ou resultar em tempos limite ou lentidão.
- yarn_node_blacklisted: O nó de TAREFA ou CORE foi colocado na lista negra do YARN para executar tarefas.
- yarn_node_lost: O nó de TAREFA ou CORE foi marcado como PERDIDO pelo YARN, possíveis problemas de conectividade.

As instâncias associadas ao `ClusterID` que você especifica devem ser gerenciadas pelo AWS Systems Manager. Você pode executar essa automação uma vez, programar a automação para ser executada em um intervalo de tempo específico ou remover uma programação criada anteriormente por uma automação. Este runbook é compatível com as versões 5.20 a 6.30 do Amazon EMR.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterID

  Tipo: string

  Descrição: (obrigatório) O ID do cluster cujos logs de nós que deseja analisar.
- Operation

  Tipo: string

  Valores válidos: Run Once | Schedule | Remove Schedule

  Descrição: (obrigatório) A operação a ser executada no cluster.
- IntervalTime

  Tipo: string

  Valores válidos: 5 minutes | 10 minutes | 15 minutes

  Descrição: (opcional) A duração do tempo entre a execução da automação. Esse parâmetro só é aplicável se for especificado `Schedule` para o parâmetro `Operation`.
- LogToCloudWatchLogs

  Tipo: string

  Valores válidos: sim | não

  Descrição: (Opcional) Se você especificar `yes` o valor desse parâmetro, a automação criará um grupo de CloudWatch registros de registros com o nome especificado no `CloudWatchLogGroup` parâmetro para armazenar todas as entradas de registro correspondentes.

- CloudWatchLogGroup

  Tipo: string

  Descrição: (Opcional) O nome do grupo de CloudWatch registros de registros em que você deseja armazenar todas as entradas de registro correspondentes. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.
- CreateLogInsightsDashboard

  Tipo: string

  Valores válidos: sim | não

  Descrição: (Opcional) Se você especificar`yes`, o CloudWatch painel será criado se ainda não existir. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.
- CreateMetricFilters

  Tipo: string

  Valores válidos: sim | não

  Descrição: (Opcional) Especifique `yes` se você deseja criar filtros métricos para o grupo de CloudWatch registros de registros. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi :Coleta informações sobre o cluster do Amazon EMR especificado no parâmetro ClusterID.
- aws:branch :Ramificações com base na entrada.
  - Se a operação fornecida for Run Once ou Schedule:
    - aws:assertAwsResourceProperty :Verifica se o cluster está disponível.
    - aws:executeAwsApi :Reúne os IDs de todas as instâncias em execução no cluster.

- `aws:assertAwsResourceProperty` :Verifica se o SSM Agent está sendo executado em todas as instâncias do cluster.
- `aws:branch` :Ramificações com base na especificação de executar a automação uma vez ou em um cronograma.
  - Se a operação fornecida for `Run Once`:
    - `aws:branch` :Ramificações com base no valor especificado para o parâmetro `LogToCloudWatchLogs`.
      - Se o valor de `LogToCloudWatchLogs` for `yes`:
        - `aws:executeScript`- Verifica se `CloudWatchLogGroup` já existe um grupo de CloudWatch registros de registros com o nome especificado no parâmetro. Caso contrário, o grupo será criado com o nome especificado.
        - `aws:branch` :Ramificações com base no valor especificado para o parâmetro `CreateMetricFilters`.
          - Se o valor de `CreateMetricFilters` for `yes`:
            - `aws:executeAwsApi` :12 etapas são executadas para cada filtro métrico
            - `aws:branch` :Ramificações com base no valor especificado para o parâmetro `CreateLogInsightsDashboard`.
              - Se o valor de `CreateLogInsightsDashboard` for `yes`:
                - `aws:executeAwsApi`- Cria um CloudWatch painel com o mesmo nome especificado no `CloudWatchLogGroup` parâmetro, caso ele ainda não exista.
              - Se o valor de `CreateLogInsightsDashboard` for `no`:
                - `aws:runCommand` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.
          - Se o valor de `CreateMetricFilters` for `no`:
            - `aws:branch` :Ramificações com base no valor especificado no parâmetro `CreateLogInsightsDashboard`.
              - Se o valor de `CreateLogInsightsDashboard` for `yes`:
                - `aws:executeAwsApi`- Cria um CloudWatch painel com o mesmo nome especificado no `CloudWatchLogGroup` parâmetro, caso ele ainda não exista.
              - Se o valor de `CreateLogInsightsDashboard` for `no`:

- `aws:runCommand` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.

- Se o valor de `LogToCloudWatchLogs` for no:
  - `aws:executeAwsApi` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.

- Se a operação fornecida for `Schedule`:
  - `aws:createStack`- Cria um EventBridge evento da Amazon que tem como alvo esse runbook.

- Se a operação fornecida for `Remove Schedule`:
  - `aws:executeAwsApi` :Verifica se existe um cronograma para o cluster.
  - `aws:deleteStack` :Exclui a programação.

Saídas

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.IDs de instância

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.saída

FindLogPatternOnMerNode. CommandId

OpenSearch Serviço Amazon

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon OpenSearch Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

AWSConfigRemediation-DeleteOpenSearchDomain

Descrição

O `AWSConfigRemediation-DeleteOpenSearchDomain` runbook exclui um determinado domínio do Amazon OpenSearch Service usando a DeleteDomainAPI.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

  Tipo: string

  Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja excluir.
- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Etapas do documento

- `aws:executeScript`- Aceita o nome OpenSearch de domínio do Amazon Service como entrada, o exclui e verifica a exclusão.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descrição

O `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` runbook é ativado `EnforceHTTPS` em um determinado domínio do Amazon OpenSearch Service usando a UpdateDomainConfigAPI.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

Tipo: string

Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja usar para aplicar HTTPS.

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Etapas do documento

- `aws:executeScript`- Ativa a opção de `EnforceHTTPS` endpoint no domínio do Amazon OpenSearch Service que você especifica no `DomainName` parâmetro.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Descrição

O `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` runbook atualiza a configuração do grupo de segurança em um determinado domínio do Amazon OpenSearch Service usando a UpdateDomainConfigAPI.

> **Note**
>
> AWS Os grupos de segurança só podem ser aplicados aos domínios do Amazon OpenSearch Service configurados para acesso à Amazon Virtual Private Cloud (VPC), e não aos domínios do Amazon OpenSearch Service configurados para acesso público.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

  Tipo: string

  Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja usar para atualizar grupos de segurança.
- SecurityGroupList

  Tipo: StringList

  Descrição: (Obrigatório) Os IDs do grupo de segurança que você deseja atribuir ao domínio do Amazon OpenSearch Service.
- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Etapas do documento

- `aws:executeScript`- Atualiza a configuração do grupo de segurança no domínio do Amazon OpenSearch Service que você especifica no `DomainName` parâmetro.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Descrição

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`o runbook de automação é usado para identificar a causa do status de integridade do cluster vermelho ou amarelo e orientá-lo na alteração do cluster de volta para verde.

Como funciona?

O runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` ajuda você a solucionar a causa do cluster vermelho ou amarelo e fornece as próximas etapas para resolver esse problema analisando a configuração do cluster e a utilização de recursos.

O runbook executa as seguintes etapas:

- Chama a DescribeDomainAPI no domínio de destino para obter a configuração do cluster.
- Verifica se o domínio do OpenSearch Serviço é baseado na Internet (público) ou na Amazon Virtual Private Cloud (VPC).
- Cria uma AWS Lambda função pública ou baseada no Amazon VPC, dependendo da configuração do cluster. Observação: a função Lambda contém o código de solução de problemas que executa as APIs de OpenSearch serviço no cluster para determinar por que o cluster está no estado vermelho ou amarelo.
- Exclui a função Lambda.

- Exibe as verificações realizadas e as próximas etapas recomendadas para resolver o problema do cluster vermelho ou amarelo.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

O `LambdaExecutionRole` parâmetro requer as seguintes ações para usar o runbook com êxito:

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

Visão geral da `LambdaExecutionRole` política:

Veja a seguir um exemplo de uma função de execução AWS Identity and Access Management (função IAM) da função Lambda que concede à função permissão para acessar AWS serviços e recursos exigidos por esse runbook. Para obter mais informações, consulte Função de execução do Lambda.

> **Note**
>
> O`ec2:DescribeNetworkInterfaces`,`ec2:CreateNetworkInterface`, e só `ec2:DeleteNetworkInterface` são necessários se seu cluster de OpenSearch serviços for baseado em Amazon VPC para permitir que a função Lambda crie e gerencie as interfaces de rede Amazon VPC. Para obter mais informações, consulte Conectando redes externas a recursos em uma função de execução do Amazon VPC e do Lambda.

```
{
    "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"
                }

            ]
        }
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport- TroubleshootOpenSearchRedYellowCluster no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Você pode usar os seguintes parâmetros de entrada:

- AutomationAssumeRole (Opcional):

  O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- LambdaExecutionRole (Obrigatório):

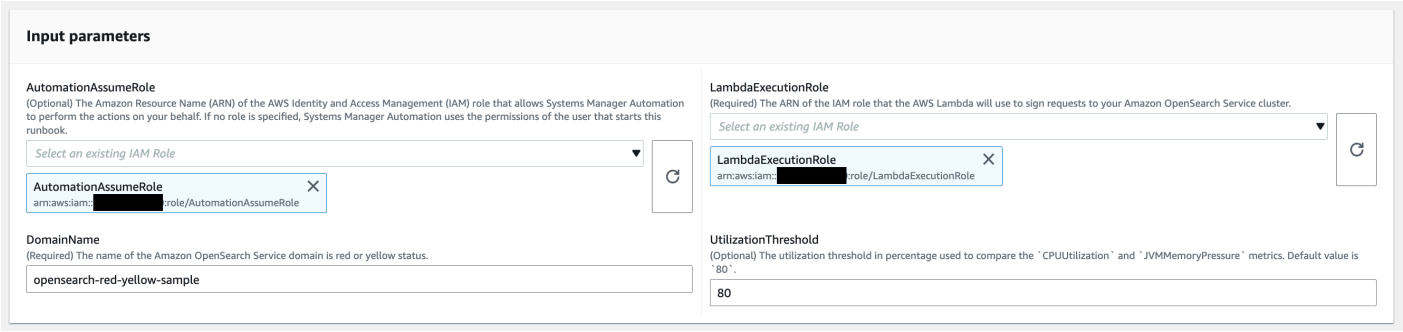
  O ARN da função do IAM que o Lambda usará para assinar solicitações no seu cluster do Amazon Service. OpenSearch

- DomainName (Obrigatório):

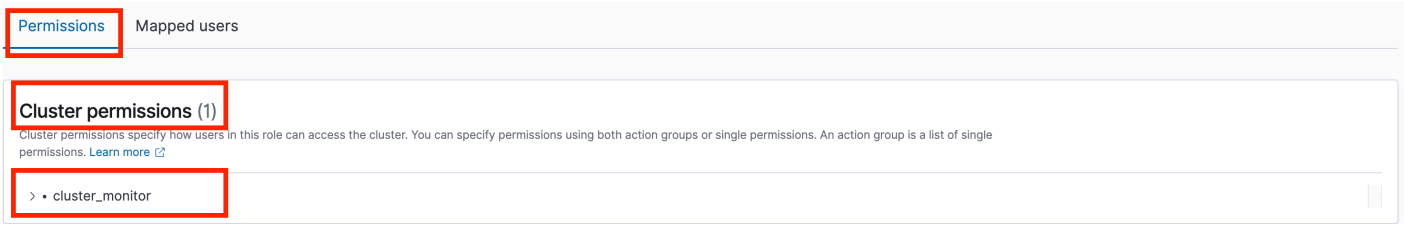
  O nome do domínio do OpenSearch serviço com o status de integridade do cluster vermelho ou amarelo.

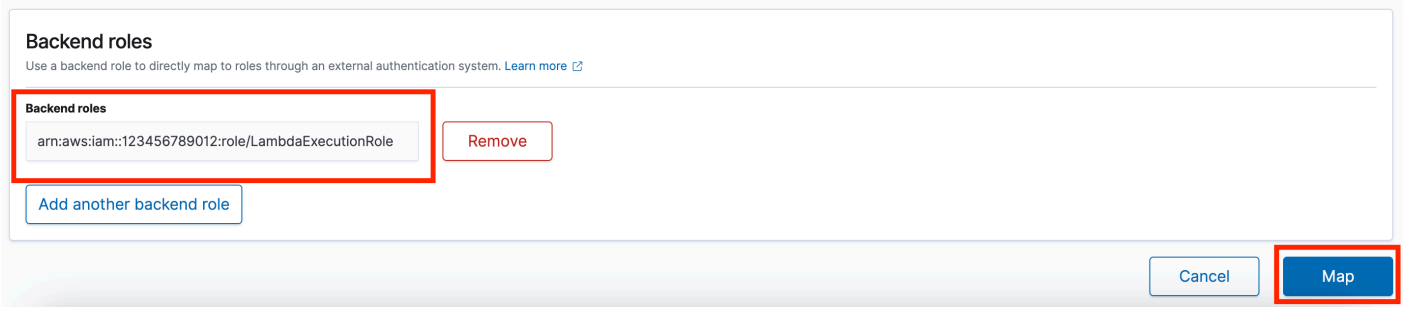
- UtilizationThreshold (Opcional):

  A porcentagem do limite de utilização usada para comparar as métricas de utilização da CPU e da JVM. MemoryPressure O valor padrão é 80.



4. Se você ativou o controle de acesso refinado em um cluster de OpenSearch serviços, certifique-se de que o arn da `LambdaExecutionRole` função esteja mapeado para uma função com pelo menos permissão. `cluster_monitor`





5. Selecione Executar.
6. A automação é iniciada.
7. O runbook de automação realiza as seguintes etapas:
   - GetClusterConfiguration:

     Busca a configuração do cluster OpenSearch de serviços.
   - CrieAWSLambdaFunctionStack:

     Cria uma função Lambda temporária em sua conta usando. AWS CloudFormation A função Lambda é usada para executar as APIs de OpenSearch serviço.
   - WaitForAWSLambdaFunctionStack:

     Espera que a CloudFormation pilha seja concluída.
   - GetClusterMetricsFromCloudWatch:

     Obtém as métricas relacionadas ao cluster Amazon CloudWatch ClusterStatus, CPUUtilization e JVM MemoryPressure OpenSearch Service e sua data de criação.
   - RunOpenSearchAPIs:

     Usa a função Lambda para chamar as APIs de OpenSearch serviço e analisar os dados das métricas do cluster para diagnosticar a causa do status do cluster vermelho ou amarelo.
   - ExcluirAWSLambdaFunctionStack:

     Exclui a função Lambda criada por essa automação em sua conta.
8. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.
   - RootCause:

     Fornece uma visão geral da causa identificada para que a integridade do cluster esteja no estado vermelho ou amarelo.

- IssueDescription:

  Fornece detalhes sobre por que o cluster está no estado vermelho ou amarelo e as possíveis etapas para retornar o cluster ao estado verde.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Consulte Solução de problemas do Amazon OpenSearch Service para obter mais informações

AWSSupport-TroubleshootOpenSearchHighCPU

Descrição

O `AWSSupport-TroubleshootOpenSearchHighCPU` runbook fornece uma solução automatizada para coletar dados de diagnóstico de um domínio do Amazon OpenSearch Service para solucionar problemas de alta CPU.

Como funciona?

O `AWSSupport-TroubleshootOpenSearchHighCPU` runbook ajuda a solucionar problemas de alta utilização da CPU no domínio do Amazon OpenSearch Service.

O runbook executa as seguintes etapas:

- Executa a DescribeDomainAPI no domínio fornecido do Amazon OpenSearch Service para obter os metadados do cluster.
- Verifica se o domínio do Amazon OpenSearch Service é público ou baseado no Amazon VPC e, com a ajuda de AWS CloudFormation, cria uma função pública ou baseada no Amazon AWS Lambda VPC.
- A função Lambda busca dados de diagnóstico dos domínios do Amazon OpenSearch Service.

- Usa uma máquina de AWS Step Functions estado para orquestrar várias execuções de funções Lambda para coletar dados mais abrangentes.
- Armazena os dados coletados em um grupo de CloudWatch registros da Amazon por 24 horas por padrão.
- Exclui os recursos criados, exceto o grupo de CloudWatch registros.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

O LambdaExecutionRole parâmetro requer as seguintes ações para usar o runbook com êxito:

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

A função de execução do Lambda concede à função permissão para acessar AWS serviços e recursos exigidos por esse runbook. Para obter mais informações, consulte Função de execução do Lambda.

> **Note**
>
> Osec2:DescribeNetworkInterfaces,ec2:CreateNetworkInterface, e só ec2:DeleteNetworkInterface são necessários se seu cluster de OpenSearch serviços for baseado em Amazon VPC para permitir que a função Lambda crie e gerencie as

interfaces de rede Amazon VPC. Para obter mais informações, consulte Conectando redes externas a recursos em uma função de execução do Amazon VPC e do Lambda.

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até a AWSSupport- TroubleshootOpenSearchHigh CPU no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

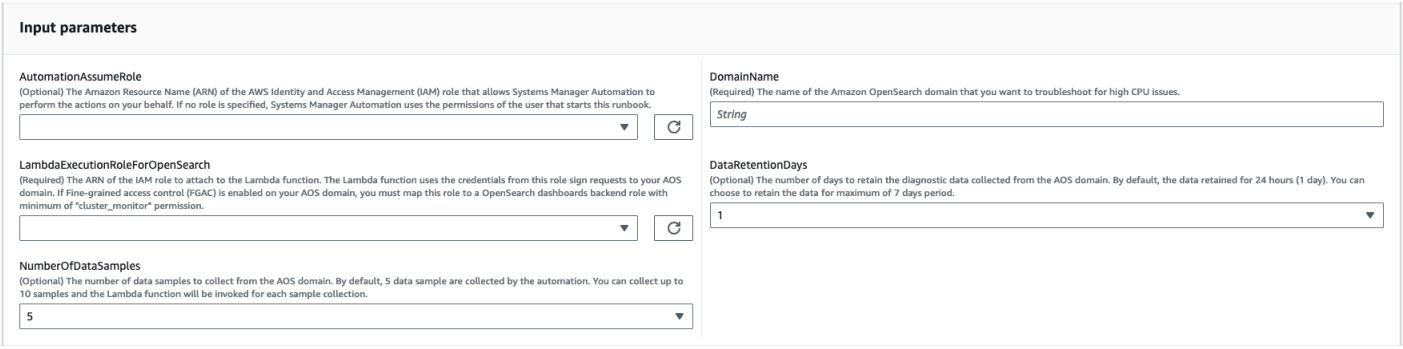
     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - DomainName (Obrigatório):

     O nome do domínio do Amazon OpenSearch Service que você deseja solucionar para problemas de alta CPU.
   - LambdaExecutionRoleForOpenSearch (Obrigatório):

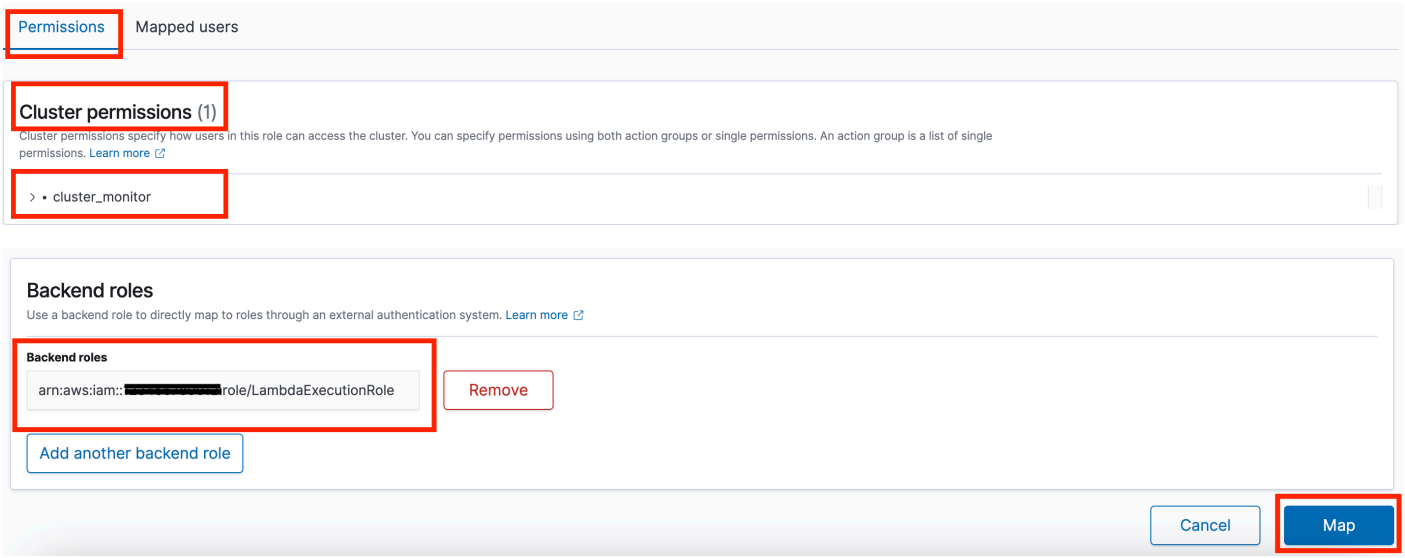
     O ARN da função do IAM a ser anexada à função Lambda. A função Lambda usa as credenciais dessa função para assinar solicitações no domínio do Amazon OpenSearch Service. Se o controle de acesso refinado estiver habilitado no domínio do Amazon OpenSearch Service, você deverá mapear essa função para uma função de back-end do OpenSearch Service Dashboards com uma permissão mínima de “cluster_monitor”.
   - DataRetentionDays (Opcional):

     O número de dias para reter os dados de diagnóstico coletados do domínio do Amazon OpenSearch Service. Por padrão, os dados são retidos por 24 horas (um dia). Você pode optar por reter os dados por no máximo 30 dias.
   - NumberOfDataSamples (Opcional):

O número de amostras de dados a serem coletadas do domínio do Amazon OpenSearch Service. Por padrão, 5 amostras de dados são coletadas. Você pode coletar até 10 amostras e a função Lambda será invocada para cada coleta de amostras.



4. Se você ativou o controle de acesso refinado em um cluster de OpenSearch serviços, certifique-se de que o arn da `LambdaExecutionRole` função esteja mapeado para uma função com pelo menos permissão. `cluster_monitor`



5. Selecione Executar.
6. A automação é iniciada.
7. O runbook de automação realiza as seguintes etapas:
   - Verifique a simultaneidade:

     Garante que haja apenas uma execução desse runbook visando o domínio especificado do Amazon OpenSearch Service. Se o runbook encontrar outra execução com o mesmo nome de domínio, ele retornará um erro e terminará.
   - getDomainConfig:

Obtém os detalhes da configuração do domínio OpenSearch de serviço de destino.

- Recursos de provisionamento:

  Provisiona os recursos para coleta de dados usando AWS CloudFormation.

- waitForStackCriação:

  Espera a conclusão da AWS CloudFormation pilha.

- describeStackResources:

  Descreve a AWS CloudFormation pilha e obtém o ARN da máquina de estado.

- runStateMachine:

  Invoca a função Lambda do coletor de dados uma ou mais vezes executando uma máquina de estado Step Functions.

- describeErrorsFromStackEvents:

  Descreve os erros da AWS CloudFormation pilha em busca de erros.

- unstageOpenSearchAlta automação de CPU:

  Exclui a `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation pilha.

- describeErrorsFromStackDeletion:

  Descreve os erros encontrados ao excluir a AWS CloudFormation pilha.

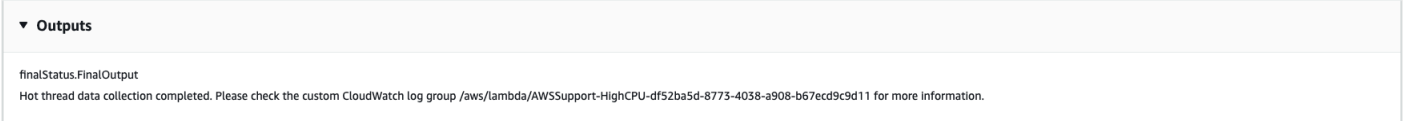
- Status final:

  Retorna a saída final do `AWSSupport-TroubleshootOpenSearchHighCPU` runbook.

8. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.

   - Status final. FinalOutput:

     Fornece o grupo de CloudWatch registros em que os dados de diagnóstico são armazenados.



Referências

- Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Consulte Solução de problemas do Amazon OpenSearch Service para obter mais informações

EventBridge

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. EventBridge Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

Descrição

O `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook adiciona uma string de desduplicação para todos os AWS Systems Manager OpsItems associados a uma regra da Amazon. EventBridge Este runbook não adicionará uma string de eliminação de duplicação se a regra já tiver uma. Para saber mais sobre cadeias de caracteres de desduplicação e OpsItems, consulte Reduzindo a duplicação OpsItems no Guia do usuário.AWS Systems Manager

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DedupString

  Tipo: string

  Descrição: (obrigatório) A string de eliminação de deduplicação que deseja adicionar à regra.
- RuleName

  Tipo: string

  Descrição: (obrigatório) O nome da regra à qual deseja adicionar a string de deduplicação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Etapas do documento

- `aws:executeScript`- Adiciona uma sequência de deduplicação à EventBridge regra especificada no `RuleName` parâmetro.

AWS-DisableEventBridgeRule

Descrição

O *AWS-DisableEventBridgeRule* runbook desativa a EventBridge regra da Amazon que você especifica. Para saber mais sobre as regras EventBridge , consulte as regras da Amazon EventBridge no Guia do usuário da Amazon. EventBridge

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EventBusName

  Tipo: string

  Padrão: Default

  Descrição: (opcional) O barramento de eventos associado à regra a ser desabilitada.
- RuleName

  Tipo: string

Descrição: (obrigatório) O nome da regra que deseja desabilitar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Etapas do documento

- `aws:executeAwsApi`- Desativa a EventBridge regra especificada no `RuleName` parâmetro.

GuardDuty

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. GuardDuty Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-CreateGuardDutyDetector

`AWSConfigRemediation-CreateGuardDutyDetector`

Descrição

O `AWSConfigRemediation-CreateGuardDutyDetector` runbook cria um detector Amazon GuardDuty (GuardDuty) no Região da AWS local onde você executa a automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Etapas do documento

- `aws:executeAwsApi`- Cria um GuardDuty detector.
- `aws:assertAwsResourceProperty` :Verifica se o `Status` do detector é `ENABLED`.

IAM

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Identity and Access Management Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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

Descrição

Anexe uma função AWS Identity and Access Management (IAM) a uma instância gerenciada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ForceReplace

  Tipo: booliano

  Descrição: (opcional) Sinalizador para especificar se deseja substituir o perfil do IAM existente ou não.

  Padrão: True

- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância a qual você deseja associar um perfil do IAM.

- RoleName

  Tipo: string

  Descrição: (obrigatório) O nome do perfil do IAM a ser adicionado à instância gerenciada.

Etapas do documento

1. `aws:executeAwsApi`- DescribeInstanceProfile - Encontre o perfil da instância do IAM anexado à instância do EC2.
2. `aws:branch`- CheckInstanceProfileAssociations - Verifique o perfil da instância do IAM anexado à instância do EC2.
   a. Se um perfil de instância do IAM estiver anexado e `ForceReplace` estiver definido como `true`:
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Desassocie o perfil da instância do IAM da instância do EC2.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Liste os perfis de instância para a função IAM fornecida.

c. `aws:branch`- CheckInstanceProfileCreated - Verifique se a função do IAM fornecida tem um perfil de instância associado.

   i. Se a o perfil do IAM tiver um perfil de instância associado:

      A. `aws:executeAwsApi`- attachiam ProfileToInstance - anexe a função de perfil da instância do IAM à instância do EC2.

   i. Se o perfil do IAM não tiver um perfil de instância associado:

      A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Crie uma função de perfil de instância para a função do IAM especificada.

      B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Anexe a função do perfil da instância à função do IAM especificada.

      C. `aws:executeAwsApi`- GetInstanceProfile - Obtenha os dados do perfil da instância para a função do IAM especificada.

      D. `aws:executeAwsApi`- attachiam ProfileToInstanceWithRetry - anexe a função de perfil da instância do IAM à instância do EC2.

Saídas

Anexo TachiamProfileToInstanceWithRetry. AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Anexo TachiamProfileToInstance. AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Descrição

O `AWS-DeleteIAMInlinePolicy` runbook exclui todas as políticas em linha AWS Identity and Access Management (IAM) anexadas às identidades do IAM que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- IamArns

  Tipo: string

  Descrição: (Obrigatório) Uma lista separada por vírgulas de ARNs para as identidades do IAM das quais você deseja excluir políticas em linha. Essa lista pode incluir usuários, grupos ou funções do IAM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Etapas do documento

- `aws:executeScript`- Exclui as políticas embutidas do IAM anexadas às identidades específicas do IAM.

`AWSConfigRemediation-DeleteIAMRole`

Descrição

O runbook `AWSConfigRemediation-DeleteIAMRole` exclui o perfil do AWS Identity and Access Management (IAM) especificado. Essa automação não exclui perfis de instância associados ao perfil do IAM ou funções vinculadas ao serviço.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAMRoleID

  Tipo: string

  Descrição: (obrigatório) O ID do perfil do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Etapas do documento

- `aws:executeScript` :Reúne o nome do perfil do IAM especificado no parâmetro `IAMRoleID`.
- `aws:executeScript` :Reúne políticas e perfis de instância associados ao perfil do IAM.
- `aws:executeScript` :Exclui as políticas anexadas.
- `aws:executeScript` :Exclui o perfil do IAM e verifica se o perfil foi excluído.

AWSConfigRemediation-DeleteIAMUser

Descrição

O runbook `AWSConfigRemediation-DeleteIAMUser` exclui o usuário do AWS Identity and Access Management (IAM) especificado. Essa automação exclui ou desanexa os seguintes atributos associados ao usuário do IAM:

- Chaves de acesso
- Políticas gerenciadas anexadas
- Credenciais do git
- Associações ao grupo IAM

- Senha de usuário do IAM
- Políticas em linha
- Dispositivos de autenticação multifator (MFA)
- Assinatura de certificados
- Chaves públicas de SSH

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAM UserId

  Tipo: string

  Descrição: (obrigatório) O ID do usuário do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeScript :Reúne o nome do usuário do IAM especificado no parâmetro IAMUserId.
- aws:executeScript :Reúne chaves de acesso, certificados, credenciais, dispositivos de MFA e chaves SSH associadas ao usuário do IAM.
- aws:executeScript :Reúne associações e políticas de grupos para o usuário do IAM.
- aws:executeScript :Exclui chaves de acesso, certificados, credenciais, dispositivos de MFA e chaves SSH associadas ao usuário do IAM.

- `aws:executeScript` :Exclui associações e políticas de grupos para o usuário do IAM.
- `aws:executeScript` :Exclui o usuário do IAM e verifica se a função foi excluída.

AWSConfigRemediation-DeleteUnusedIAMGroup

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedIAMGroup` exclui um grupo do IAM que não contém nenhum usuário.

O runbook `AWSConfigRemediation-DeleteUnusedIAMGroup` exclui um grupo do IAM que não contém nenhum usuário.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- GroupName

  Tipo: string

  Descrição: (obrigatório) O nome do grupo do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Etapas do documento

- `aws:executeScript` :Remove as políticas gerenciadas e em linha do IAM anexadas ao grupo de destino do IAM e, em seguida, exclui o grupo do IAM.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedIAMPolicy` exclui uma política do AWS Identity and Access Management (IAM) que não está anexada a nenhum usuário, grupo ou perfil.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- IAM ResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador de atributo da política do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DeletePolicy`
- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Etapas do documento

- `aws:executeScript` :Exclui a política especificada no parâmetro `IAMResourceId` e verifica se a política foi excluída.

AWSConfigRemediation-DetachIAMPolicy

Descrição

O runbook `AWSConfigRemediation-DetachIAMPolicy` desvincula a política do AWS Identity and Access Management (IAM) especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAM ResourceId

  Tipo: string

  Descrição: (obrigatório) O ID da política do IAM a ser desvinculada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Etapas do documento

- `aws:executeScript` :Desvincula a política do IAM de todos os atributos.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descrição

O `AWSConfigRemediation-EnableAccountAccessAnalyzer` runbook cria um analisador de acesso AWS Identity and Access Management (IAM) em seu. Conta da AWS Para obter mais informações sobre o analisador de acesso, consulte Utilizando o IAM Access Analyzer da AWS no Guia do usuário do IAM.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AnalyzerName

  Tipo: string

  Descrição: (obrigatório) Nome do analizador a ser criado.
- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Etapas do documento

- `aws:executeAwsApi` :Cria um analisador de acesso para sua conta.
- `aws:waitForAwsResourceProperty` :Espera que o status do analisador de acesso seja `ACTIVE`.
- `aws:assertAwsResourceProperty` :Confirma que o status do analisador de acesso é `ACTIVE`.

AWSSupport-GrantPermissionsToIAMUser

Descrição

Este runbook concede as permissões especificadas a um grupo do IAM (novo ou existente) e adiciona o usuário do IAM existente a ele. As políticas das quais você pode escolher: Faturamento ou Suporte. Para ativar o acesso de faturamento para o IAM, lembre-se de ativar o acesso do usuário do IAM e do usuário federado às páginas de Gerenciamento de custo e Faturamento.

> **Important**
>
> Se você fornecer um grupo do IAM existente, todos os usuários do IAM atualmente no grupo recebem as novas permissões.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- IAM GroupName

  Tipo: string

  Padrão: ExampleSupportAndBillingGroup

  Descrição: (Obrigatório) Pode ser um grupo novo ou existente. Deve estar em conformidade com as Limitações de nome das entidades do IAM.
- IAM UserName

  Tipo: string

  Padrão: ExampleUser

  Descrição: (Obrigatório) Deve ser um usuário existente.
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) O ARN da função assumida pelo lambda.
- Permissões

  Tipo: string

  Valores válidos: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

Padrão: SupportAndBillingFullAccess

Descrição: (obrigatório) Escolha um dos itens a seguir: `SupportFullAccess` concede acesso total à central de suporte. `BillingFullAccess` concede acesso total ao painel de faturamento. `SupportAndBillingFullAccess` concede acesso total à central de suporte e ao painel de faturamento. Mais informações sobre políticas estão em Detalhes do documento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

As permissões necessárias dependem de como o `AWSSupport-GrantPermissionsToIAMUser` é executado.

Executando como o usuário ou o perfil conectado no momento

É recomendável anexar a política gerenciada `AmazonSSMAutomationRole` da Amazon e as seguintes permissões adicionais para poder criar a função do Lambda e o perfil do IAM para passar para o Lambda:

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

```
                            "iam:GetUser"
                        ],
                        "Resource" : [
                            "arn:aws:iam::*:user/*",
                            "arn:aws:iam::*:group/*"
                        ]
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:AttachGroupPolicy"
                        ],
                        "Resource": "*",
                        "Condition": {
                            "ArnEquals": {
                                "iam:PolicyArn": [
                                    "arn:aws:iam::aws:policy/job-function/Billing",
                                    "arn:aws:iam::aws:policy/AWSSupportAccess"
                                ]
                            }
                        }
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:ListAccountAliases",
                            "iam:GetAccountSummary"
                        ],
                        "Resource" : "*"
                    }
                ]
            }
```

Usando AutomationAssumeRole e LambdaAssumeRole

O usuário deve ter as StartAutomationExecution permissões ssm: no runbook e iam: PassRole nas funções do IAM passadas como e. AutomationAssumeRoleLambdaAssumeRole Aqui estão as permissões que cada função do IAM precisa:

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

Etapas do documento

1. `aws:createStack`- Execute o AWS CloudFormation modelo para criar uma função Lambda.
2. `aws:invokeLambdaFunction` :Executar o Lambda para definir as permissões do IAM.
3. `aws:deleteStack`- Excluir CloudFormation modelo.

Saídas

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

Descrição

O runbook `AWSConfigRemediation-RemoveUserPolicies` exclui as políticas em linha do AWS Identity and Access Management (IAM) e desvincula todas as políticas gerenciadas anexadas ao usuário especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAMUserID

  Tipo: string

  Descrição: (obrigatório) O ID do usuário cujas políticas serão removidas.
- PolicyType

  Tipo: string

  Valores válidos: All | Inline | Managed

  Padrão: All

  Descrição: (obrigatório) O tipo de política do IAM a ser removida do usuário.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`

- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Etapas do documento

- `aws:executeScript` :Exclui e desvincula as políticas do IAM do usuário especificado no parâmetro `IAMUserID`.

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descrição

O `AWSConfigRemediation-ReplaceIAMInlinePolicy` runbook substitui uma política em linha AWS Identity and Access Management (IAM) por uma política de IAM gerenciada replicada. Para uma política em linha anexada a um usuário, grupo ou perfil, as permissões da política embutida são clonadas em uma política do IAM gerenciada. A política gerenciada do IAM é adicionada ao recurso e a política embutida é removida. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- InlinePolicyName

  Tipo: StringList

  Descrição: (obrigatório) A política do IAM em linha a ser substituída.

- ResourceId

  Tipo: string

  Descrição: (obrigatório) O ID do usuário, grupo ou perfil do IAM cujo a política embutida será substituída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript` :Substituir a política do IAM em linha por uma política da AWS replicada no recurso especificado.

`AWSConfigRemediation-RevokeUnusedIAMUserCredentials`

Descrição

O `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` runbook revoga senhas não utilizadas AWS Identity and Access Management (IAM) e chaves de acesso ativas. Esse runbook também desativa as chaves de acesso expiradas e exclui os perfis de login expirados. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- IAM ResourceId

  Tipo: string

  Descrição: (obrigatório) O ID do recurso do IAM cujas credenciais não utilizadas serão revogadas.

- MaxCredentialUsageAge

  Tipo: string

  Padrão: 90

  Descrição: (obrigatório) O número de dias em que a credencial deve ter sido usada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

Etapas do documento

- `aws:executeScript` :Revoga as credenciais do IAM para o usuário especificado no parâmetro `IAMResourceId`. As chaves de acesso expiradas são desativadas e os perfis de login expirados são excluídos.

> **Note**
>
> Certifique-se de configurar o `MaxCredentialUsageAge` parâmetro desta ação de remediação para corresponder ao `maxAccessKeyAge` parâmetro da AWS Config regra que você usa para acionar esta ação: access-keys-rotated.

`AWSConfigRemediation-SetIAMPasswordPolicy`

Descrição

O runbook `AWSConfigRemediation-SetIAMPasswordPolicy` define a política de senha de usuário do AWS Identity and Access Management (IAM) para sua Conta da AWS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AllowUsersToChangePassword

  Tipo: booliano

  Padrão: False

Descrição: (Opcional) Se definido como`true`, todos os usuários do IAM em Conta da AWS você podem usar o AWS Management Console para alterar suas senhas.

- HardExpiry

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definido como `true`, os usuários do IAM são impedidos de redefinir suas senhas após a expiração desta.

- MaxPasswordAge

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número de dias em que a senha de um usuário do IAM é válida.

- MinimumPasswordLength

  Tipo: inteiro

  Padrão: 6

  Descrição: (opcional) O número mínimo de caracteres que uma senha de usuário do IAM pode ter.

- PasswordReusePrevention

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número de senhas anteriores que um usuário do IAM é impedido de reutilizar.

- RequireLowercaseCharacters

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere minúsculo do alfabeto latino básico ISO (a a z).

- RequireNumbers

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere numérico (0 a 9).

- RequireSymbols

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere não alfanumérico (! @ # $ % ^ * ( ) _ + - = [ ] { } | ').

- RequireUppercaseCharacters

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere maiúsculo do alfabeto latino básico ISO (A a Z).

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Etapas do documento

- `aws:executeScript` :Define a política de senha de usuário do IAM com base nos valores especificados para os parâmetros do runbook da sua Conta da AWS.

Amazon Kinesis Data Streams

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Kinesis Data Streams. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWS-EnableKinesisStreamEncryption`

Descrição

O `AWS-EnableKinesisStreamEncryption` runbook permite a criptografia em um Amazon Kinesis Data Streams (Kinesis Data Streams). Os aplicativos produtores que gravam em um fluxo criptografado encontrarão erros se não tiverem acesso à chave AWS Key Management Service (AWS KMS).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- KinesisStreamName

  Tipo: string

  Descrição: (Obrigatório) O nome do stream no qual você deseja habilitar a criptografia.

- KeyId

  Tipo: string

  Padrão: alias/aws/kinesis

  Descrição: (Obrigatório) A AWS KMS chave gerenciada pelo cliente que você deseja usar para criptografia. Esse valor pode ser um identificador global exclusivo, um ARN para um alias ou uma chave ou um nome de alias prefixado por “alias/”. Você também pode usar a chave AWS gerenciada usando o valor padrão para o parâmetro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Etapas do documento

- VerifyKinesisStreamStatus (aws: waitforAwsResource Property) - Verifica o status do Kinesis Data Streams.
- EnableKinesisStreamEncryption (aws:executeAwsApi) - Permite a criptografia para o Kinesis Data Streams.
- VerifyKinesisStreamUpdateComplete (aws: waitForAwsResourceProperty) - Aguarda o retorno do status do Kinesis Data Streams para. `ACTIVE`

- VerifyKinesisStreamEncryption (aws: assertAwsResource Propriedade) - Verifica se a criptografia está habilitada para o Kinesis Data Streams.

AWS KMS

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Key Management Service Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

`AWSConfigRemediation-CancelKeyDeletion`

Descrição

O `AWSConfigRemediation-CancelKeyDeletion` runbook cancela a exclusão da chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) especificada por você.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KeyId

  Tipo: string

  Descrição: (obrigatório) O ID da chave gerenciada pelo cliente da qual deseja cancelar a exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Etapas do documento

- `aws:executeAwsApi` :Cancela a exclusão da chave gerenciada pelo cliente especificada no parâmetro `KeyId`.
- `aws:assertAwsResourceProperty` :Confirma que a exclusão da chave está desabilitada em sua chave gerenciada pelo cliente.

AWSConfigRemediation-EnableKeyRotation

Descrição

O `AWSConfigRemediation-EnableKeyRotation` runbook permite a rotação automática de chaves para a chave simétrica AWS Key Management Service (AWS KMS) gerenciada pelo cliente.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- KeyId

  Tipo: string

  Descrição: (obrigatório) O ID da chave gerenciada pelo cliente na qual deseja habilitar a rotação automática de chaves.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Etapas do documento

- `aws:executeAwsApi` :Permite a rotação automática da chave gerenciada pelo cliente especificada no parâmetro `KeyId`.
- `aws:assertAwsResourceProperty` :Confirma se a rotação automática de chaves está habilitada na chave gerenciada pelo cliente.

Lambda

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Lambda Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing`

Descrição

O `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` runbook permite o rastreamento AWS X-Ray ao vivo na AWS Lambda função que você especifica no `FunctionName` parâmetro.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FunctionName

  Tipo: string

  Descrição: (obrigatório) O nome ou ARN da função do Lambda para ativar o rastreamento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi` :Ativa o rastreamento de raio-X na função do Lambda especificada no parâmetro `FunctionName`.
- `aws:assertAwsResourceProperty` :Verifica se o rastreamento de X-Ray foi ativado na função do Lambda.

Saídas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Resposta da chamada `UpdateFunctionConfiguration` da API.

AWSConfigRemediation-DeleteLambdaFunction

Descrição

O runbook `AWSConfigRemediation-DeleteLambdaFunction` exclui a função AWS Lambda especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LambdaFunctionName

  Tipo: string

  Descrição: (obrigatório) O nome da função do Lambda a ser excluída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Etapas do documento

- `aws:executeAwsApi` :Exclui a função do Lambda especificada no parâmetro `LambdaFunctionName`.
- `aws:executeScript` :Verifica se a função do Lambda foi excluída.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Descrição

O `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook criptografa, em repouso, as variáveis de ambiente para a função (AWS Lambda Lambda) que você especifica usando uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS). Esse runbook só deve ser usado como uma linha de base para garantir que as variáveis de ambiente da sua função do Lambda sejam criptografadas de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar várias funções com diferentes chaves gerenciadas pelo cliente.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FunctionName

Tipo: string

Descrição: (obrigatório) O nome ou ARN da função do Lambda cujas variáveis de ambiente serão criptografadas.

- KMS KeyArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da chave gerenciada pelo AWS KMS cliente que você deseja usar para criptografar as variáveis de ambiente da função Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Espera que a propriedade `LastUpdateStatus` fique `Successful`.
- `aws:executeAwsApi`- Criptografa as variáveis de ambiente da função Lambda que você especifica `FunctionName` no parâmetro usando AWS KMS a chave gerenciada pelo cliente especificada no `KMSKeyArn` parâmetro.
- `aws:assertAwsResourceProperty` :Confirma que a criptografia está habilitada nas variáveis de ambiente da sua função do Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descrição

O runbook `AWSConfigRemediation-MoveLambdaToVPC` move uma função AWS Lambda do (Lambda) para uma Amazon Virtual Private Cloud (Amazon VPC).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FunctionName

  Tipo: string

  Descrição: (obrigatório) O nome da função do Lambda a ser movida para uma Amazon VPC.
- SecurityGroupIds

  Tipo: string

  Descrição: (obrigatório) Os IDs do grupo de segurança que serão atribuídos às interfaces de rede elástica (ENIs) associadas à sua função do Lambda.
- SubnetIds

  Tipo: string

  Descrição: (obrigatório) Os IDs de sub-rede para os quais deseja criar as interfaces de rede elástica (ENIs) associadas à sua função do Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Etapas do documento

- `aws:executeAwsApi` :Atualiza a configuração da Amazon VPC para a função do Lambda especificada no parâmetro `FunctionName`.
- `aws:waitForAwsResourceProperty` :Espera que a função do Lambda `LastUpdateStatus` seja `successful`.
- `aws:executeScript` :Verifica se a configuração da função do Lambda da Amazon VPC foi atualizada com sucesso.

`AWSSupport-RemediateLambdaS3Event`

Descrição

O `AWSSupport-TroubleshootLambdaS3Event` runbook fornece uma solução automatizada para os procedimentos descritos nos artigos do AWS Knowledge Center Por que minha notificação de eventos do Amazon S3 não aciona minha função Lambda? e Por que recebo o erro “Não é possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função Lambda? Esse runbook ajuda você a identificar e corrigir o motivo pelo qual uma notificação de evento do Amazon Simple Storage Service (Amazon S3) falhou em acionar a função especificada. AWS Lambda Se a saída do runbook sugerir a validação e a configuração da simultaneidade da função do Lambda, consulte Invocação assíncrona e escalabilidade de funções do AWS Lambda.

> **Note**
>
> O erro “Não foi possível validar as seguintes configurações de destino” também podem ocorrer devido a configurações incorretas de eventos do Amazon Simple Notification Service (Amazon SNS) e do Amazon Simple Queue Service (Amazon SQS) do Amazon

S3. Esse runbook verifica somente as configurações da função do Lambda. Se, depois de usar o runbook, você ainda estiver recebendo o erro “Não foi possível validar as seguintes configurações de destino”, revise todas as configurações de eventos existentes do Amazon SNS e do Amazon SQS Amazon S3.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaFunctionArn

  Tipo: string

  Descrição: (obrigatório) O ARN da função do Lambda.
- S3 BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cujas notificações de eventos acionam a função do Lambda.

- Ação

  Tipo: string

  Valores válidos: Troubleshoot | Remediate

  Descrição: (obrigatório) As operações que você deseja que o runbook execute. A opção `Troubleshoot` ajuda a identificar qualquer problema, mas não executa nenhuma ação de mutação para resolver o problema. A opção `Remediate` ajuda a identificar e tenta resolver problemas para você.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Etapas do documento

- `aws:branch` :Ramifica com base na entrada especificada para o parâmetro `Action`.

  Se o valor especificado for `Troubleshoot`:

  - `aws:executeAutomation` :Executa o runbook `AWSSupport-TroubleshootLambdaS3Event`.
  - `aws:executeAwsApi` :Verifica a saída do runbook `AWSSupport-TroubleshootLambdaS3Event` executado na etapa anterior.

  Se o valor especificado for `Remediate`:

- `aws:executeScript` :Executa um script para corrigir os problemas descritos na seção Por que minha notificação de eventos do Amazon S3 não aciona minha função do Lambda? e Por que recebo o erro “Não foi possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função do Lambda? Artigos do Centro de Conhecimentos.

Saídas

checkoutput.Output

remediatelambdas3event.Output

`AWSSupport-TroubleshootLambdaInternetAccess`

Descrição

O `AWSSupport-TroubleshootLambdaInternetAccess` runbook ajuda você a solucionar problemas de acesso à Internet para uma AWS Lambda função que foi lançada na Amazon Virtual Private Cloud (Amazon VPC). Recursos como rotas de sub-rede, regras de grupos de segurança e regras de lista de controle de acesso (ACL) à rede são revisados para confirmar se o acesso de saída à Internet é permitido.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- FunctionName

  Tipo: string

  Descrição: (obrigatório) O nome da função do Lambda para a qual deseja solucionar problemas de acesso à Internet.

- destinationIp

  Tipo: string

  Descrição: (obrigatório) O endereço IP de destino com o qual deseja estabelecer uma conexão de saída.

- destinationPort

  Tipo: string

  Padrão: 443

  Descrição: (opcional) A porta de destino com o qual deseja estabelecer uma conexão de saída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeScript` :Verifica a configuração de vários recursos na VPC onde a função do Lambda foi lançada.
- `aws:branch` :Ramifica com base no fato de a função do Lambda especificada estar em uma VPC ou não.
- `aws:executeScript` :Analisa as rotas da tabela de rotas da sub-rede em que a função do Lambda foi iniciada e verifica se as rotas para um gateway de conversão de endereços de rede (NAT) e um gateway da internet estão presentes. Confirma que a função do Lambda não está em uma sub-rede pública.
- `aws:executeScript` :Verifica se o grupo de segurança associado à função do Lambda permite acesso externo à Internet com base nos valores especificados para os parâmetros `destinationIp` e `destinationPort`.
- `aws:executeScript` :Verifica se as regras da ACL associadas às sub-redes da função do Lambda e o gateway NAT permitem acesso externo à Internet com base nos valores especificados para os parâmetros `destinationIp` e `destinationPort`.

Saídas

checkVpc.vpc :o ID da VPC em que a função do Lambda foi lançada.

checkVpc.subnet :os IDs das sub-redes em que a função do Lambda foi lançada.

checkVpc.securityGroups :grupos de segurança associados à função do Lambda.

checkNACL.NACL :Mensagem de análise com nomes de recursos. `LambdaIp` refere-se ao endereço IP privado da interface de rede elástica para a função do Lambda. O objeto `LambdaIpRules` é gerado somente para sub-redes que têm uma rota para um gateway NAT. O conteúdo a seguir é um exemplo de saída.

```
{
   "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"
   }
}
```

checkSecurityGroups.secgrps - Análise do grupo de segurança associado à sua função Lambda. O conteúdo a seguir é um exemplo de saída.

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets :Análise das sub-redes na VPC associadas à função do Lambda. O conteúdo a seguir é um exemplo de saída.

```
{
   "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

Descrição

O `AWSSupport-TroubleshootLambdaS3Event` runbook fornece uma solução automatizada para os procedimentos descritos nos artigos do AWS Knowledge Center Por que minha notificação de eventos do Amazon S3 não aciona minha função Lambda? e Por que recebo o erro “Não é possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função Lambda? Esse runbook ajuda você a identificar por que uma notificação de evento do Amazon Simple Storage Service (Amazon S3) falhou em acionar a função especificada. AWS Lambda Se a saída do runbook sugerir a validação e a configuração da simultaneidade da função do Lambda, consulte Invocação assíncrona e escalabilidade de funções do AWS Lambda.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaFunctionArn

  Tipo: string

Descrição: (obrigatório) O ARN da função do Lambda que a notificação de eventos do Amazon S3 aciona.

- S3 BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cujas notificações de eventos acionam a função do Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Etapas do documento

- `aws:executeScript` :Executa o script para validar as definições de configuração da notificação de eventos do Amazon S3. Valida a política do IAM baseada em recursos para sua função Lambda e gera um comando AWS Command Line Interface (AWS CLI) para adicionar as permissões necessárias se as permissões necessárias estiverem ausentes da política. Valida outras políticas de recursos de funções Lambda que fazem parte das notificações de eventos para o mesmo bucket do S3 e gera AWS CLI um comando como saída se as permissões necessárias estiverem ausentes.

Saídas

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager A automação fornece runbooks predefinidos para fluxos de trabalho gerenciados da Amazon para Apache Airflow. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWSSupport-TroubleshootMWAAEnvironmentCreation

Descrição

O `AWSSupport-TroubleshootMWAAEnvironmentCreation` runbook fornece informações para depurar problemas de criação de ambientes do Amazon Managed Workflows for Apache Airflow (Amazon MWAA) e realizar verificações, juntamente com os motivos documentados, da melhor forma possível, para ajudar a identificar a falha.

Como funciona?

O runbook executa as seguintes etapas:

- Recupera os detalhes do ambiente Amazon MWAA.
- Verifica as permissões da função de execução.
- Verifica se o ambiente tem permissões para usar a AWS KMS chave fornecida para registro e se o grupo de CloudWatch registros necessário existe.
- Analisa os registros no grupo de registros fornecido para localizar quaisquer erros.
- Verifica a configuração da rede para verificar se o ambiente Amazon MWAA tem acesso aos endpoints necessários.
- Gera um relatório com as descobertas.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- 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

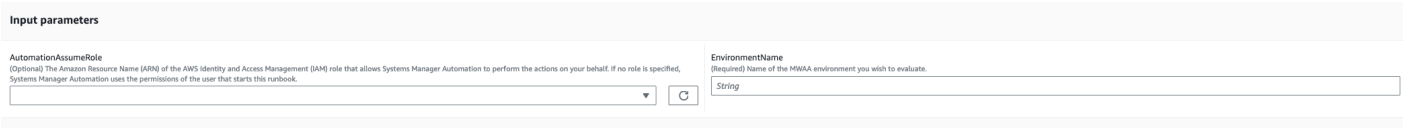
Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootMWAAEnvironmentCreationem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - EnvironmentName (Obrigatório):

     Nome do ambiente Amazon MWAA que você deseja avaliar.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`GetMWAAEnvironmentDetails:`**

     Recupera os detalhes do ambiente Amazon MWAA. Se essa etapa falhar, o processo de automação será interrompido e exibido como`Failed`.
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Verifica se a função de execução tem as permissões necessárias para os recursos do Amazon MWAA, Amazon S3, CloudWatch Logs e CloudWatch Amazon SQS. Se detectar uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS), a automação valida as permissões necessárias da chave. Essa etapa emprega a `iam:SimulateCustomPolicy` API para verificar se a função de execução da automação atende a todas as permissões necessárias.
   - **`CheckKMSPolicyOnKMSKey:`**

     Verifica se a política de AWS KMS chaves permite que o ambiente Amazon MWAA use a chave para criptografar CloudWatch registros. Se a AWS KMS chave for AWS gerenciada, a automação ignora essa verificação.

- **CheckIfRequiredLogGroupsExists:**

  Verifica se os grupos de CloudWatch log necessários para o ambiente Amazon MWAA existem. Caso contrário, a automação verifica CloudTrail `CreateLogGroup` os `DeleteLogGroup` eventos. Essa etapa também verifica a existência de `CreateLogGroup` eventos.

- **BranchOnLogGroupsFindings:**

  Ramificações com base na existência de grupos de CloudWatch registros relacionados ao ambiente Amazon MWAA. Se existir pelo menos um grupo de registros, a automação o analisará para localizar erros. Se nenhum grupo de registros estiver presente, a automação pulará a próxima etapa.

- **CheckForErrorsInLogGroups:**

  Analisa os grupos de CloudWatch registros para localizar erros.

- **GetRequiredEndPointsDetails:**

  Recupera os endpoints de serviço utilizados pelo ambiente Amazon MWAA.

- **CheckNetworkConfiguration:**

  Verifica se a configuração de rede do ambiente Amazon MWAA atende aos requisitos, incluindo verificações de grupos de segurança, ACLs de rede, sub-redes e configurações de tabelas de rotas.

- **CheckEndpointsConnectivity:**

  Invoca a automação `AWSSupport-ConnectivityTroubleshooter` secundária para validar a conectividade do Amazon MWAA com os endpoints necessários.

- **CheckS3BlockPublicAccess:**

  Verifica se o bucket Amazon S3 do ambiente Amazon MWAA `Block Public Access` foi ativado e também analisa as configurações gerais do Amazon S3 Block Public Access da conta.

- **GenerateReport:**

  Coleta informações da automação e imprime o resultado ou a saída de cada etapa.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:
   - Verificando as permissões da função de execução do ambiente Amazon MWAA:

Verifica se a função de execução tem as permissões necessárias para os recursos do Amazon MWAA, Amazon S3, CloudWatch Logs e CloudWatch Amazon SQS. Se uma AWS KMS chave gerenciada pelo cliente for detectada, a automação valida as permissões necessárias da chave.

- Verificando a política AWS KMS chave do ambiente Amazon MWAA:

  Verifica se a função de execução possui as permissões necessárias para os recursos do Amazon MWAA, Amazon S3 CloudWatch , Logs e CloudWatch Amazon SQS. Além disso, se uma AWS KMS chave gerenciada pelo cliente for detectada, a automação verificará as permissões necessárias da chave.

- Verificando os grupos de CloudWatch registros do ambiente Amazon MWAA:

  Verifica se os grupos de CloudWatch log necessários para o ambiente Amazon MWAA existem. Caso contrário, a automação verifica CloudTrail a localização `CreateLogGroup` e `DeleteLogGroup` os eventos.

- Verificando as tabelas de rotas do ambiente Amazon MWAA:

  Verifica se as tabelas de rotas da Amazon VPC no ambiente Amazon MWAA estão configuradas corretamente.

- Verificando os grupos de segurança do ambiente Amazon MWAA:

  Verifica se os grupos de segurança Amazon VPC do ambiente Amazon MWAA estão configurados corretamente.

- Verificando as ACLs de rede do ambiente Amazon MWAA:

  Verifica se os grupos de segurança da Amazon VPC no ambiente Amazon MWAA estão configurados corretamente.

- Verificando as sub-redes do ambiente Amazon MAA:

  Verifica se as sub-redes do ambiente Amazon MWAA são privadas.

- A verificação do ambiente Amazon MWAA exigia conectividade de endpoints:

  Verifica se o ambiente Amazon MWAA pode acessar os endpoints necessários. Para isso, a automação invoca a `AWSSupport-ConnectivityTroubleshooter` automação.

- Verificando o ambiente Amazon MWAA (bucket do Amazon S3):

  Verifica se o bucket Amazon S3 do ambiente Amazon MWAA `Block Public Access` foi ativado e também analisa as configurações do Amazon S3 Block Public Access da conta.

- Verificar os CloudWatch registros do ambiente Amazon MWAA agrupa erros:

  Analisa os grupos de CloudWatch log existentes do ambiente Amazon MWAA para localizar erros.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Neptune

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Neptune. Para obter mais informações sobre runbooks, consulte Trabalhando com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Descrição

O `AWS-EnableNeptuneDbAuditLogsToCloudWatch` runbook ajuda você a enviar registros de auditoria de um cluster de banco de dados Amazon Neptune para o Amazon Logs. CloudWatch

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DbClusterResourceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID do recurso do cluster de banco de dados Neptune para o qual você deseja habilitar os registros de auditoria.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property) - Verifica se o tipo de mecanismo de banco de dados Neptune é. `neptune`
- EnableNeptuneDbAuditLogs (aws:executeAwsApi) - Permite que os registros de auditoria do cluster de banco de dados Neptune recebam registros. CloudWatch
- VerifyNeptuneDbStatus (aws: waitAwsResource Property) - Verifica se o status do cluster de banco de dados Neptune é. `available`
- VerifyNeptuneDbAuditLogs (aws:ExecuteScript) — Verifica se os registros de auditoria foram configurados com sucesso para serem enviados ao Logs. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

Descrição

O AWS-EnableNeptuneDbBackupRetentionPeriod runbook ajuda você a habilitar backups automatizados com um período de retenção de backup entre 7 e 35 dias para um cluster de banco de dados Amazon Neptune.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DbClusterResourceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID do recurso do cluster de banco de dados Neptune para o qual você deseja habilitar backups.
- BackupRetentionPeriod

  Tipo: inteiro

Valores válidos: 7-35

Descrição: (Obrigatório) O número de dias em que os backups são retidos.

- PreferredBackupWindow

  Tipo: sequência

  Descrição: (Opcional) Um período diário de pelo menos 30 minutos quando os backups são feitos. O valor deve estar em Tempo Universal Coordenado (UTC) e usar o formato:`hh24:mm-hh24:mm`. O período de retenção de backup não pode entrar em conflito com a janela de manutenção preferida.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property) - Verifica se o tipo de mecanismo de banco de dados Neptune é. `neptune`
- VerifyNeptuneDbStatus (aws: waitAwsResource Property) - Verifica se o status do cluster de banco de dados Neptune é. `available`
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Define o período de retenção para o cluster de banco de dados Neptune.
- VerifyNeptuneDbBackupsEnabled (aws:ExecuteScript) — Verifica se o período de retenção e a janela de backup foram definidos com sucesso.

AWS-EnableNeptuneClusterDeletionProtection

Descrição

O AWS-EnableNeptuneClusterDeletionProtection runbook permite a proteção contra exclusão do cluster Amazon Neptune que você especificar.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DbClusterResourceId

  Tipo: sequência

  Descrição: (Obrigatório) O ID do cluster Neptune no qual você deseja ativar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- ssm:GetAutomationExecution

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property) - Verifica se o tipo de mecanismo do cluster de banco de dados especificado é `neptune`.
- VerifyNeptuneStatus (aws: waitForAwsResourceProperty) - Verifica se o status do cluster é `available`.
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi) - Ativa a proteção contra exclusão no cluster de banco de dados Neptune.
- VerifyNeptuneDbDeletionProtection (aws: assertAwsResource Property) - Verifica se a proteção contra exclusão está habilitada no cluster de banco de dados.

Saídas

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - A saída da operação da API.

Amazon RDS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Relational Database Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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

Descrição

O `AWS-CreateEncryptedRdsSnapshot` runbook cria um snapshot criptografado de uma instância não criptografada do Amazon Relational Database Service (Amazon RDS).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DB InstanceIdentifier

  Tipo: string

  Descrição: (Obrigatório) O ID da instância do Amazon RDS da qual você deseja criar um snapshot.
- DB SnapshotIdentifier

  Tipo: string

  Descrição: (Opcional) O modelo de nome para o snapshot do Amazon RDS. O modelo de nome padrão é *`DB InstanceIdentifier -yyyymmddhhmmss`*.
- Banco de dados criptografado SnapshotIdentifier

  Tipo: string

  Descrição: (Opcional) O nome do instantâneo criptografado. O nome padrão é o valor que você especifica para o `DBSnapshotIdentifier` parâmetro anexado`-encrypted`.

- InstanceTags

  Tipo: string

  Descrição: (Opcional) Tags a serem adicionadas à instância de banco de dados. (Exemplo: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '
- KmsKeyId

  Tipo: string

  Padrão: `alias/aws/rds`

  Descrição: (Opcional) O ARN, o ID da chave ou o alias da chave gerenciada pelo cliente que você deseja usar para criptografar o snapshot.
- SnapshotTags

  Tipo: string

  Descrição: (Opcional) Tags a serem adicionadas ao instantâneo. (Exemplo: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Etapas do documento

- `aws:executeScript`- Cria um instantâneo da instância de banco de dados que você especifica no `DBInstanceIdentifier` parâmetro.
- `aws:executeScript`- Verifica se o instantâneo criado na etapa anterior existe e é. `available`
- `aws:executeScript`- Copia o instantâneo criado anteriormente em um instantâneo criptografado.

- `aws:executeScript`- Verifica se o instantâneo criptografado criado na etapa anterior existe.

Saídas

CopyRdsSnapshotToEncryptedRdsSnapshot. EncryptedSnapshotId - O ID do snapshot criptografado do Amazon RDS.

AWS-CreateRdsSnapshot

Descrição

Criar um snapshot do Amazon Relational Database Service (Amazon RDS) para uma instância do Amazon RDS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DB InstanceIdentifier

  Tipo: string

Descrição: (Obrigatório) O InstanceId ID do banco de dados da instância do RDS a partir da qual criar o snapshot.

- DB SnapshotIdentifier

  Tipo: string

  Descrição: (Opcional) O SnapshotIdentifier ID do banco de dados do snapshot do RDS a ser criado.

- InstanceTags

  Tipo: string

  Descrição: (Opcional) tags a serem criadas para a instância.

- SnapshotTags

  Tipo: string

  Descrição: (Opcional) tags a serem criadas para o snapshot.

Etapas do documento

createRDSSnapshot :Cria o snapshot do RDS e retorna o ID do snapshot.

verifyRDSSnapshot :Verifica se o snapshot criado na etapa anterior existe.

Saídas

CreaterDSSnapshot. SnapshotId — O ID do instantâneo criado.

AWSConfigRemediation-DeleteRDSCluster

Descrição

O `AWSConfigRemediation-DeleteRDSCluster` runbook exclui o cluster do Amazon Relational Database Service (Amazon RDS) que você especificar. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DB ClusterId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para o cluster de banco de dados no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

Etapas do documento

- `aws:executeScript` :Exclui o cluster de banco de dados especificado no parâmetro `DBClusterId`.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descrição

O runbook `AWSConfigRemediation-DeleteRDSClusterSnapshot` exclui o snapshot do cluster do Amazon Relational Database Service (Amazon RDS) fornecido.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DB ClusterSnapshotId

  Tipo: string

  Descrição: (obrigatório) O identificador de snapshot do cluster do Amazon RDS a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DeleteDBClusterSnapshot
- rds:DescribeDBClusterSnapshots

Etapas do documento

- aws:branch :Verifica se o snapshot do cluster está no estado available. Se não estiver disponível, o fluxo termina.
- aws:executeAwsApi :Exclui o snapshot do cluster Amazon RDS fornecido usando o identificador de snapshot do cluster do banco de dados (DB).
- aws:executeScript :Verifica se o snapshot de cluster do Amazon RDS fornecido foi excluído.

AWSConfigRemediation-DeleteRDSInstance

Descrição

O runbook AWSConfigRemediation-DeleteRDSInstance exclui a instância do Amazon Relational Database Service (Amazon RDS) especificada. Quando uma instância de banco de dados (BD) é excluída, todas as cópias de segurança automatizadas para essa instância são excluídas e não podem ser recuperadas. Os snapshots manuais do BD não são excluídos. Se a instância de banco de dados que deseja excluir estiver no estado failed, incompatible-network ou incompatible-restore, o parâmetro SkipFinalSnapshot deverá ser definido como true.

> **Note**
>
> Se a instância de banco de dados que você deseja excluir estiver em um cluster de banco de dados Amazon Aurora, o runbook não excluirá a instância de banco de dados se ela for uma réplica de leitura e a única instância no cluster de banco de dados.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador de recurso da instância de banco de dados a ser excluída.
- SkipFinalSnapshot

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definido como `true`, um snapshot final não é criado antes que a instância de banco de dados seja excluída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Etapas do documento

- `aws:executeAwsApi` :Reúne o nome da instância de banco de dados a partir do valor que você especifica no parâmetro `DbiResourceId`.
- `aws:branch` :Ramifica com base no valor especificado para o parâmetro `SkipFinalSnapshot`.
- `aws:executeAwsApi` :Exclui a instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:executeAwsApi` :Exclui a instância de banco de dados que você especifica no parâmetro `DbiResourceId` após a criação do snapshot final.
- `aws:assertAwsResourceProperty` :Verifica se a instância de banco de dados foi excluída.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Descrição

O runbook `AWSConfigRemediation-DeleteRDSInstanceSnapshot` exclui o snapshot da instância do Amazon Relational Database Service (Amazon RDS) especificado. Somente os snapshots no estado `available` são excluídos. Este runbook não oferece suporte à exclusão de snapshots das instâncias do banco de dados Amazon Aurora.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbSnapshotId

  Tipo: string

  Descrição: (obrigatório) O ID do snapshot a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Etapas do documento

- `aws:executeAwsApi` :Reúne o estado do snapshot especificado no parâmetro `DbSnapshotId`.
- `aws:assertAwsResourceProperty` :Confirma o estado do snapshot como `available`.
- `aws:executeAwsApi` :Exclui o snapshot especificado no parâmetro `DbSnapshotId`.
- `aws:executeScript` :Verifica se o snapshot foi excluído.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descrição

O runbook `AWSConfigRemediation-DisablePublicAccessToRDSInstance` desabilita a acessibilidade pública da instância de banco de dados (DB) do Amazon Relational Database Service (Amazon RDS) especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados para a qual deseja desabilitar a acessibilidade pública.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Verifica se as instâncias de banco de dados estão no estado `AVAILABLE`.
- `aws:executeAwsApi` :Desabilita a acessibilidade pública em sua instância de banco de dados.
- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `MODIFYING`.

- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `AVAILABLE`.
- `aws:assertAwsResourceProperty` :Confirma que a acessibilidade pública está desabilitada na instância de banco de dados.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Descrição

O runbook `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` habilita a definição `CopyTagsToSnapshot` no cluster do Amazon Relational Database Service (Amazon RDS) especificado. Habilitar essa definição copia todas as tags do cluster do banco de dados para snapshots desse cluster. O padrão é não copiá-los. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` for especificado para esse parâmetro, as modificações feitas nesta solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona

assim que possível, independentemente da definição `PreferredMaintenanceWindow` do cluster de banco de dados.

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbClusterResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para o cluster do banco de dados no qual deseja habilitar a definição `CopyTagsToSnapshot`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador do cluster de banco de dados a partir do identificador de recursos do cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o cluster de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `CopyTagsToSnapshot` em seu cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a definição `CopyTagsToSnapshot` está habilitada no cluster de banco de dados.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Descrição

O runbook `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` habilita a definição `CopyTagsToSnapshot` na instância do Amazon Relational Database Service (Amazon RDS) especificada. Habilitar essa configuração copia todas as tags da instância do banco de dados para snapshots dessa instância. O padrão é não copiá-los. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbiResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar a definição `CopyTagsToSnapshot`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `CopyTagsToSnapshot` em sua instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a configuração `CopyTagsToSnapshot` está habilitada na instância de banco de dados.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` permite o monitoramento avançado na instância de banco de dados do Amazon RDS especificada. Para obter informações sobre o monitoramento avançado, consulte Monitoramento avançado no Guia do usuário do Amazon RDS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- MonitoringInterval

  Tipo: inteiro

  Valores válidos: 1 | 5 | 10 | 15 | 30 | 60

  Descrição: (obrigatório) O intervalo em segundos quando as métricas de monitoramento avançado são coletadas da instância de banco de dados.
- MonitoringRoleArn

  Tipo: string

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) da função do IAM que permite que o Amazon RDS envie métricas de monitoramento aprimorado para o Amazon Logs. CloudWatch

- ResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar o Enhanced Monitoring.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Permite o monitoramento avançado na instância de banco de dados.
- `aws:executeScript` :Confirma que o monitoramento avançado está habilitado na instância de banco de dados.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Descrição

O runbook `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` habilita a definição `AutoMinorVersionUpgrade` na instância de banco de dados do Amazon RDS especificada. Habilitar essa configuração significa que as atualizações secundárias das versões serão aplicadas automaticamente à instância de banco de dados durante a janela de manutenção.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja a definição `AutoMinorVersionUpgrade`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.

- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `AutoMinorVersionUpgrade` em sua instância de banco de dados.
- `aws:executeScript` :Confirma se a definição `AutoMinorVersionUpgrade` está habilitada na sua instância de banco de dados.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnableMultiAZOnRDSInstance` transforma a instância de banco de dados (DB) do Amazon Relational Database Service (Amazon RDS) para uma implantação Multi-AZ. Alterar essa configuração não resultará em uma interrupção. A alteração será aplicada durante a próxima janela de manutenção, a menos que o parâmetro `ApplyImmediately` seja definido como `true`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona

logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbiResourceId

  Tipo: string

  Descrição: (Obrigatório) O identificador Região da AWS exclusivo e imutável da instância de banco de dados para habilitar a configuração. `MultiAZ`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Etapas do documento

- `aws:executeAwsApi` :Recupera o nome da instância de banco de dados usando o valor fornecido no parâmetro `DBInstanceId`.
- `aws:executeAwsApi` :Verifica se `DBInstanceStatus` é `available`.
- `aws:branch` :Verifica se a `MultiAZ` já está definida como `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:executeAwsApi` :Altera a definição `MultiAZ` para `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:assertAwsResourceProperty` :Verifica se a `MultiAZ` está definida como `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` habilita o Performance Insights na instância de banco de dados Amazon RDS especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar o Performance Insights.
- PerformanceInsightsKMS KeyId

  Tipo: string

  Padrão: `alias/aws/rds`

Descrição: (Opcional) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente que você deseja que o Performance Insights use para criptografar todos os dados potencialmente confidenciais. Prefixe o valor com **alias/** se for inserir o alias da chave para esse parâmetro. Se você não especificar um valor para esse parâmetro, o Chave gerenciada pela AWS será usado.

- PerformanceInsightsRetentionPeriod

  Tipo: inteiro

  Valores válidos: 7, 731

  Padrão: 7

  Descrição: (opcional) O número de dias para reter dados do Performance Insights.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o status da instância de banco de dados é `available`.
- `aws:executeAwsApi`- Reúne o ARN da chave gerenciada AWS KMS pelo cliente especificada no `PerformanceInsightsKMSKeyId` parâmetro.
- `aws:branch` :Verifica se um valor já está atribuído à propriedade do `PerformanceInsightsKMSKeyId` da instância de banco de dados.

- `aws:executeAwsApi` :Habilita o Performance Insights na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:assertAwsResourceProperty` :Confirma que o valor especificado para o parâmetro `PerformanceInsightsKMSKeyId` foi usado para habilitar a criptografia para o Performance Insights na instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o Performance Insights está habilitado na instância de banco de dados.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descrição

O `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook permite a proteção contra exclusão no cluster Amazon Relational Database Service (Amazon RDS) que você especificar. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterId

Tipo: string

Descrição: (obrigatório) O identificador do recurso para o cluster de banco de dados no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- `aws:executeAwsApi` :Reúne o nome do cluster de banco de dados a partir do identificador de recursos do cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Verifica se o status do cluster de banco de dados é `available`.
- `aws:executeAwsApi` :Ativa a proteção contra exclusão no cluster de banco de dados especificada no parâmetro `ClusterId`.
- `aws:assertAwsResourceProperty` :Verifica se a proteção contra exclusão foi habilitada no cluster de banco de dados.

AWSConfigRemediation-EnableRDSInstanceBackup

Descrição

O runbook `AWSConfigRemediation-EnableRDSInstanceBackup` habilita backups para a instância de banco de dados do Amazon Relational Database Service (Amazon RDS) especificada. Este runbook não oferece suporte à habilitação de backups para instâncias de banco de dados Amazon Aurora.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BackupRetentionPeriod

  Tipo: inteiro

  Valores válidos: 1 a 35

  Descrição: (obrigatório) O número de dias que os backups são retidos.
- DbiResourceId

  Tipo: string

Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados para a qual deseja habilitar backups.

- PreferredBackupWindow

  Tipo: string

  Descrição: (opcional) O intervalo de tempo diário (em UTC) durante o qual os backups são criados.

  Restrições:

  - Deve estar no formato `hh24:mi-hh24:mi`
  - Deve estar expresso no Tempo Universal Coordenado (Coordinated Universal Time, UTC)
  - Não pode entrar em conflito com a janela de manutenção preferencial
  - Deve ser, pelo menos, 30 minutos

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeScript` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados. Habilita backups para a instância de banco de dados. Confirma que backups estão habilitados na instância de banco de dados.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descrição

O runbook `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` habilita a proteção contra exclusão na instância de banco de dados do Amazon RDS especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbInstanceResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:executeAwsApi` :Habilita a proteção contra exclusão na instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a proteção contra exclusão está habilitada na instância de banco de dados.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Descrição

O runbook `AWSConfigRemediation-ModifyRDSInstancePortNumber` modifica o número da porta na qual a instância do Amazon Relational Database Service (Amazon RDS) aceita conexões. A execução dessa automação reiniciará o banco de dados.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- PortNumber

  Tipo: string

  Descrição: (opcional) O número da porta na qual deseja que a instância de banco de dados aceite conexões.

- RDSDB InstanceResourceId

  Tipo: string

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados cujo número da porta de entrada deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Modifica o número da porta de entrada na qual sua instância de banco de dados aceita conexões.

- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `MODIFYING`.
- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `AVAILABLE`.

AWSSupport-ModifyRDSSnapshotPermission

Descrição

O runbook `AWSSupport-ModifyRDSSnapshotPermission` ajuda a modificar permissões para vários snapshots do Amazon Relational Database Service (Amazon RDS). Usando este runbook, você pode criar snapshots `Public` ou `Private` e compartilhá-los com outras Contas da AWS. Os snapshots criptografados com uma chave KMS padrão não podem ser compartilhados com outras contas usando este runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AccountIds

Tipo: StringList

Padrão: nenhum

Descrição: (opcional) Os IDs das contas com as quais deseja compartilhar os snapshots. Esse parâmetro será necessário se um valor `No` for especificado para o parâmetro `Private`.

- AccountPermissionOperation

  Tipo: string

  Valores válidos: add | remove

  Padrão: nenhum

  Descrição: (opcional) O tipo de operação a ser executada.

- Privado

  Tipo: string

  Valores válidos: sim | não

  Descrição: (obrigatório) Insira o valor `No` se quiser compartilhar snapshots com contas específicas.

- SnapshotIdentifiers

  Tipo: StringList

  Descrição: (obrigatório) Os nomes dos snapshots do Amazon RDS cuja permissão deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Etapas do documento

1. `aws:executeScript` :Verifica os IDs dos snapshots fornecidos no parâmetro `SnapshotIdentifiers`. Depois de verificar os IDs, o script verifica se há snapshots criptografados e gera uma lista, se algum for encontrado.
2. `aws:branch` :Ramifica a automação com base no valor inserido para o parâmetro `Private`.
3. `aws:executeScript` :Modifica as permissões dos snapshots especificados para compartilhá-los com as contas especificadas.
4. `aws:executeScript` :Modifica as permissões dos snapshots para alterá-los de `Public` para `Private`.

Saídas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSPremiumSupport-PostgreSQLWorkloadReview

Descrição

O runbook `AWSPremiumSupport-PostgreSQLWorkloadReview` captura vários snapshots das estatísticas de uso do banco de dados PostgreSQL do Amazon Relational Database Service (Amazon RDS). As estatísticas capturadas são necessárias para que um especialista em Serviços AWS Support Proativos realize uma análise operacional. As estatísticas são coletadas usando um conjunto de scripts SQL e shell personalizados. Esses scripts são baixados para uma instância temporária do Amazon Elastic Compute Cloud (Amazon EC2) na Conta da AWS sua, criada por este runbook. O runbook exige o fornecimento de credenciais usando um segredo do AWS Secrets Manager contendo um par de valores-chave de nome de usuário e senha. O nome de usuário deve ter permissões para consultar as visualizações e funções de estatísticas padrão do PostgreSQL.

Esse runbook cria automaticamente os seguintes AWS recursos em você Conta da AWS usando uma AWS CloudFormation pilha. Você pode monitorar a criação da pilha usando o console AWS CloudFormation .

- Uma nuvem privada virtual (VPC) e uma instância do Amazon EC2 lançadas em uma sub-rede privada da VPC com conectividade opcional à Internet usando um gateway NAT.
- Uma função AWS Identity and Access Management (IAM) anexada à instância temporária do Amazon EC2 com permissões para recuperar o valor secreto do Secrets Manager. A função também fornece permissões para fazer upload de arquivos para um bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha e, opcionalmente, para um caso. AWS Support
- Uma conexão de emparelhamento da VPC para permitir a conectividade entre sua instância de banco de dados e a instância temporária do Amazon EC2.
- Os endpoints da VPC, do Systems Manager, do Secrets Manager e do Amazon S3 que estão anexados à VPC temporária.
- Uma janela de manutenção com tarefas registradas que iniciam e interrompem periodicamente a instância temporária do Amazon EC2, executam scripts de coleta de dados e carregam arquivos em um bucket do Amazon S3. Um perfil do IAM também é criado para a janela de manutenção que fornece permissões para realizar as tarefas registradas.

Quando o runbook é concluído, a AWS CloudFormation pilha usada para criar os AWS recursos necessários é excluída e o relatório é carregado no bucket Amazon S3 de sua escolha e, opcionalmente, em um caso. AWS Support

> **Note**
>
> Por padrão, o volume raiz do Amazon EBS da instância temporária do Amazon EC2 é preservado. Você pode substituir essa opção configurando o parâmetro `EbsVolumeDeleteOnTermination` como `true`.

Pré-requisitos

- Assinatura do Enterprise Support Este runbook e os diagnósticos e análises da workload do Proactive Services exigem uma assinatura do Enterprise Support. Antes de usar este runbook, entre em contato com seu gerente técnico de contas (TAM) ou com o TAM especializado (STAM) para obter instruções. Para obter mais informações, consulte Proactive Services do AWS Support.
- Conta e Região da AWS cotas Certifique-se de não ter atingido o número máximo de instâncias ou VPCs do Amazon EC2 que você pode criar na sua conta e na região em que você usa este runbook. Para solicitar um aumento de limite, use o Formulário de aumento de limite de serviço.
- Configuração do banco de dados

1. O banco de dados especificado no parâmetro `DatabaseName` deve ter a extensão `pg_stat_statements` configurada. Se `pg_stat_statements` não estiver configurado na `shared_preload_libraries`, o valor no grupo de parâmetros do banco de dados deverá ser editado e as alterações aplicadas. As alterações no parâmetro `shared_preload_libraries` exigem que você reinicie sua instância de banco de dados. Para obter mais informações, consulte Trabalhar com grupos de parâmetros. Adicionar `pg_stat_statements` a `shared_preload_libraries` adicionará alguma sobrecarga de desempenho. No entanto, isso é útil para monitorar o desempenho de instruções individuais. Para obter mais informações sobre a extensão `pg_stat_statements`, consulte a documentação do PostgreSQL. Se a extensão `pg_stat_statements` não for configurada ou se a extensão não estiver presente no banco de dados que está sendo usado para coleta de estatísticas, a análise em nível de instrução não será apresentada na revisão operacional.
2. Verifique se os parâmetros `track_counts` e `track_activities` não estão desativados. Se esses parâmetros estiverem desativados no grupo de parâmetros do banco de dados, nenhuma estatística significativa estará disponível. A alteração desses parâmetros exigirá a reinicialização da sua instância de banco de dados. Para mais informações, consulte Trabalhar com parâmetros na instância de banco de dados do Amazon RDS para PostgreSQL.
3. Se o parâmetro `track_io_timing` estiver desativado, as estatísticas do nível de E/S não serão incluídas na análise operacional. A alteração de `track_io_timing` exigirá a reinicialização da sua instância de banco de dados e incorrerá em sobrecarga adicional de desempenho, dependendo da workload da instância de banco de dados. Apesar da sobrecarga de desempenho para workload críticas, esse parâmetro fornece informações úteis relacionadas ao tempo de E/S por consulta.

Cobrança e cobranças Você Conta da AWS será cobrado pelos custos associados à instância temporária do Amazon EC2, ao volume associado do Amazon EBS, ao gateway NAT e aos dados transferidos durante a execução dessa automação. Por padrão, esse runbook cria uma instância `t3.micro` do Amazon Linux 2 para coletar as estatísticas. O runbook inicia e interrompe a instância entre as etapas para reduzir custos.

Segurança e governança de dados Este runbook coleta estatísticas consultando as visualizações e funções de estatísticas do PostgreSQL. Verifique se as credenciais fornecidas no parâmetro `SecretId` permitem somente permissões de leitura para as visualizações e funções de estatísticas. Como parte da automação, os scripts de coleta são carregados em seu bucket do Amazon S3 e podem ser localizados em `s3://`*`DOC-EXAMPLE-BUCKET`*`/`*`automation execution id`*`/queries/`.

Esses scripts coletam dados que são usados por um AWS especialista para revisar os principais indicadores de desempenho no nível do objeto. O script coleta informações como nome da tabela, nome do esquema e nome do índice. Se alguma dessas informações contiver informações confidenciais, como indicadores de receita, nome de usuário, endereço de e-mail ou qualquer outra informação de identificação pessoal, recomendamos que essa análise da workload seja interrompida. Entre em contato com seu AWS TAM para discutir uma abordagem alternativa para a análise da carga de trabalho.

Certifique-se de ter a aprovação e a autorização necessárias para compartilhar as estatísticas e os metadados coletados por essa automação. AWS

Considerações de segurança Se o parâmetro `UpdateRdsSecurityGroup` for definido como `yes`, o runbook atualizará o grupo de segurança associado à sua instância de banco de dados para permitir tráfego de entrada do endereço IP privado da instância temporária do Amazon EC2.

Se o parâmetro `UpdateRdsRouteTable` for definido como `yes`, o runbook atualizará a tabela de rotas associada à sub-rede em que sua instância de banco de dados está sendo executada para permitir o tráfego para a instância temporária do Amazon EC2 por meio da conexão de emparelhamento da VPC.

Criação de usuário Para permitir que o script de coleta se conecte ao seu banco de dados do Amazon RDS, deve ser configurado um usuário com permissões para ler as visualizações estatísticas. Em seguida, as credenciais devem ser armazenadas no Secrets Manager. Recomendamos criar um novo usuário dedicado para essa automação. A criação de um usuário separado permite auditar e rastrear as atividades realizadas por essa automação.

1. Criar um novo usuário.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Garantir que esse usuário possa fazer conexões somente para leitura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Definir limites de nível de usuário.

```
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. Conceder permissões de `pg_monitor` ao novo usuário para que ele possa acessar as estatísticas do banco de dados. (O perfil `pg_monitor` é membro de `pg_read_all_settings`, `pg_read_all_stats` e `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Permissões adicionadas ao perfil de instância temporária do Amazon EC2 por este Systems Manager Automation As seguintes permissões são adicionadas ao perfil do IAM associado à instância temporária do Amazon EC2. A política gerenciada `AmazonSSMManagedInstanceCore` também está associada ao perfil do IAM para permitir que a instância do Amazon EC2 seja gerenciada pelo Systems Manager.

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

Permissões adicionadas à janela de manutenção temporária por essa automação do Systems Manager Automation As seguintes permissões são adicionadas automaticamente ao perfil do IAM associada às tarefas do Maintenance Windows. As tarefas do Maintenance Windows iniciam, param e enviam comandos para a instância temporária do Amazon EC2.

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

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DB InstanceIdentifier

  Tipo: string

  Descrição: (obrigatório) O ID de sua instância de banco de dados.

- DatabaseName

  Tipo: string

  Descrição: (obrigatório) O nome do banco de dados hospedado na instância de banco de dados.

- SecretId

  Tipo: string

  Descrição: (obrigatório) O ARN do segredo do Secrets Manager que contém o par de valores-chave de nome de usuário e senha. A AWS CloudFormation pilha cria uma política do IAM com permissões para a `GetSecretValue` operação desse ARN. As credenciais são usadas para permitir que a instância temporária colete as estatísticas do banco de dados. Entre em contato com seu TAM ou STAM para discutir as permissões mínimas necessárias.

- Reconhecer

  Tipo: string

  Descrição: (obrigatório) Digite **`yes`** para confirmar que esse runbook crie recursos temporários em sua conta para coletar estatísticas da sua instância de banco de dados. Recomendamos entrar em contato com seu TAM ou STAM antes de executar essa automação.

- SupportCase

  Tipo: string

Descrição: (Opcional) O número do AWS Support caso fornecido pelo seu TAM ou STAM. Se fornecido, o runbook atualiza o caso e anexa os dados coletados. Essa opção exige que a instância temporária do Amazon EC2 tenha conectividade com a Internet para acessar o endpoint da AWS Support API. O parâmetro `AllowVpcInternetAccess` deve ser definido como `true`. O assunto do caso deve conter a frase `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- S3 BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 na conta para a qual deseja fazer o upload dos dados coletados pela automação. Verificar se a política do bucket não concede permissões desnecessárias de leitura ou gravação às entidades principais que não precisam acessar o conteúdo do bucket. Recomendamos criar um novo bucket temporário do Amazon S3 para fins dessa automação. O runbook fornece permissões para a operação de `s3:PutObject` da API para o perfil do IAM anexado à instância temporária do Amazon EC2. Os arquivos enviados estarão localizados em `s3://`*`bucket name`*`/`*`automation execution id`*`/`.

- InstanceType

  Tipo: string

  Descrição: (opcional) O tipo da instância temporária do Amazon EC2 que executará os scripts SQL e shell personalizados.

  Valores válidos: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Padrão: t3.micro

- VpcCidr

  Tipo: string

  Descrição: (opcional) O intervalo de endereço IP na notação CIDR para a nova VPC (por exemplo, `172.31.0.0/16`). Verificar se selecionou um CIDR que não se sobreponha ou corresponda a nenhuma VPC existente com conectividade com a instância de banco de dados. A menor VPC que você pode criar usa uma máscara de sub-rede /28 e a maior VPC usa uma máscara de sub-rede /16.

  Padrão: 172.31.0.0/16

- StackResourcesNamePrefix

Tipo: string

Descrição: (Opcional) O prefixo e a tag do nome dos recursos da AWS CloudFormation pilha. O runbook cria os recursos da AWS CloudFormation pilha usando esse prefixo como parte do nome e da tag aplicados aos recursos. A estrutura do par chave/valor da tag é *StackResourcesNamePrefix*`:{{automation:EXECUTION_ID}}`.

Padrão: AWSPostgreSQLWorkloadReview

- Schedule

  Tipo: string

  Descrição: (opcional) O cronograma da janela de manutenção. Especifica com que frequência a janela de manutenção executa as tarefas. O valor padrão é a cada `1 hour`.

  Valores válidos: 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 12 hours | 1 day | 2 days | 4 days

  Padrão: 1 hour

- Duração

  Tipo: Inteiro

  Descrição: (opcional) A duração máxima, em minutos, que deseja permitir que a automação seja executada. A duração máxima suportada é de 8.640 minutos (seis dias). O valor padrão é de 4.320 minutos (três dias).

  Valores válidos: 30 a 8640

  Padrão: 4320

- UpdateRdsRouteTable

  Tipo: string

  Descrição: (opcional) Se definido como `true`, o runbook atualiza a tabela de rotas associada à sub-rede em que a instância de banco de dados é executada. Uma rota IPv4 é adicionada para rotear o tráfego para o endereço IPV4 privado temporário da instância da Amazon EC2 por meio da conexão de emparelhamento da VPC recém-criada.

  Valores válidos: True | False

Padrão: False

- AllowVpcInternetAccess

  Tipo: string

  Descrição: (Opcional) Se definido como`true`, o runbook cria um gateway NAT para fornecer conectividade com a Internet à instância temporária do Amazon EC2 para se comunicar com AWS Support o endpoint da API. Você pode deixar esse parâmetro como `false` se quiser apenas que o runbook faça o upload da saída para o seu bucket do Amazon S3.

  Valores válidos: true | false

  Padrão: False
- UpdateRdsSecurityGroup

  Tipo: string

  Descrição: (opcional) Se definido como `true`, o runbook atualiza o grupo de segurança associado à sua instância de banco de dados para permitir o tráfego do endereço IP privado da instância temporária.

  Valores válidos: false | true

  Padrão: False
- EbsVolumeDeleteOnTermination

  Tipo: string

  Descrição: (Opcional) Se definido como`true`, o volume raiz da instância temporária do Amazon EC2 é excluído após a conclusão do runbook e a exclusão da pilha. AWS CloudFormation

  Valores válidos: false | true

  Padrão: False

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:assertAwsResourceProperty :Confirma que a instância de banco de dados está no estado available.
2. aws:executeAwsApi :Reúne detalhes sobre a instância de banco de dados.
3. aws:executeScript :Verifica se o bucket do Amazon S3 especificado em S3BucketName concede permissões de acesso anônimo ou público de leitura ou gravação.
4. aws:executeScript- Obtém o conteúdo do AWS CloudFormation modelo do anexo do Automation runbook que é usado para criar os AWS recursos temporários em seu Conta da AWS.

5. `aws:createStack`- Cria os recursos da AWS CloudFormation pilha.
6. `aws:waitForAwsResourceProperty`- Espera até que a instância do Amazon EC2 criada pelo modelo esteja em AWS CloudFormation execução.
7. `aws:executeAwsApi` :Obtém os IDs da instância temporária do Amazon EC2 e da conexão de emparelhamento da VPC criada pelo AWS CloudFormation.
8. `aws:executeAwsApi` :Obtém o endereço IP da instância temporária do Amazon EC2 para configurar a conectividade com sua instância de banco de dados.
9. `aws:executeAwsApi` :Marca o volume do Amazon EBS anexado à instância temporária do Amazon EC2.
10. `aws:waitForAwsResourceProperty` :Espera até que a instância temporária do Amazon EC2 passe pelas verificações de status.
11. `aws:waitForAwsResourceProperty` :Espera até que a instância temporária do Amazon EC2 seja gerenciada pelo Systems Manager. Se essa etapa expirar ou falhar, o runbook reinicializa a instância.
    a. `aws:executeAwsApi` :Reinicializa a instância temporária do Amazon EC2 se a etapa anterior falhar ou atingir o tempo limite.
    b. `aws:waitForAwsResourceProperty` :Espera até que a instância temporária do Amazon EC2 seja gerenciada pelo Systems Manager após reiniciar.
12. `aws:runCommand` :Instala os requisitos do aplicativo coletor de metadados na instância temporária do Amazon EC2.
13. `aws:runCommand` :Configura o acesso à sua instância de banco de dados criando um arquivo de configuração na instância temporária do Amazon EC2.
14. `aws:executeAwsApi` :Cria uma janela de manutenção para executar periodicamente o aplicativo coletor de metadados usando o comando Executar. A janela de manutenção inicia e interrompe a instância entre os comandos.
15. `aws:waitForAwsResourceProperty`- Espera até que a janela de manutenção criada pelo AWS CloudFormation modelo esteja pronta.
16. `aws:executeAwsApi`- Obtém os IDs da janela de manutenção e do calendário de alterações criado por AWS CloudFormation.
17. `aws:sleep` :Espera até a data de término da janela de manutenção.
18. `aws:executeAwsApi` :Desliga a janela de manutenção.
19. `aws:executeScript` :Obtém os resultados das tarefas executadas durante a janela de manutenção.

20. `aws:waitForAwsResourceProperty` :Espera que a janela de manutenção conclua a última tarefa antes de continuar.
21. `aws:branch` :Ramifica o fluxo de trabalho com base no fato de ter fornecido um valor para o parâmetro `SupportCase`.
    a. `aws:changeInstanceState` :Inicia a instância temporária do Amazon EC2 e aguarda a aprovação das verificações de status antes de fazer o upload do relatório.
    b. `aws:waitForAwsResourceProperty` :Espera até que a instância temporária do Amazon EC2 seja gerenciada pelo Systems Manager. Se essa etapa atingir o tempo limite ou falhar, o runbook reinicializa a instância.
        i. `aws:executeAwsApi` :Reinicializa a instância temporária do Amazon EC2 se a etapa anterior falhar ou atingir o tempo limite.
        ii. `aws:waitForAwsResourceProperty` :Espera até que a instância temporária do Amazon EC2 seja gerenciada pelo Systems Manager após reiniciar.
    c. `aws:runCommand` :Anexa o relatório de metadados ao caso do AWS Support se foi fornecido um valor para o parâmetro `SupportCase`. O script compacta e divide o relatório em arquivos de 5 MB. O número máximo de arquivos que o script anexa a um caso do AWS Support é 12.
22. `aws:changeInstanceState`- Interrompe a instância temporária do Amazon EC2 caso a AWS CloudFormation pilha não seja excluída.
23. `aws:executeAwsApi`- Descreve os eventos da AWS CloudFormation pilha se os runbooks falharem em criar ou atualizar a AWS CloudFormation pilha.
24. `aws:waitForAwsResourceProperty`- Espera até que a AWS CloudFormation pilha esteja em um status de terminal antes de excluí-la.
25. `aws:executeAwsApi`- Exclui a AWS CloudFormation pilha, excluindo a janela de manutenção. O volume raiz do Amazon EBS associado à instância temporária do Amazon EC2 é preservado se o valor do parâmetro `EbsVolumeDeleteOnTermination` tiver sido definido como `false`.

AWS-RebootRdsInstance

Descrição

O runbook `AWS-RebootRdsInstance` reinicializa uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS), caso esta ainda não esteja sendo reinicializada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância de banco de dados do Amazon RDS que você deseja reinicializar.

Etapas do documento

RebootInstance - Reinicializa a instância de banco de dados se ela ainda não estiver sendo reinicializada.

WaitForAvailableState - Espera que a instância de banco de dados conclua o processo de reinicialização.

Saídas

Essa automação não tem saídas.

AWSSupport-ShareRDSSnapshot

Descrição

O runbook `AWSSupport-ShareRDSSnapshot` fornece uma solução automatizada para o procedimento descrito no artigo do centro de conhecimentos Como posso compartilhar um snapshot criptografado do banco de dados do Amazon RDS com outra conta? Se seu snapshot do Amazon Relational Database Service (Amazon RDS) foi criptografado usando o Chave gerenciada pela AWS padrão, você não poderá compartilhar o snapshot. Nesse caso, o snapshot deve ser copiado usando uma chave gerenciada pelo cliente para, em seguida, compartilhá-lo com a conta de destino. Essa automação executa essas etapas usando o valor especificado no parâmetro `SnapshotName` ou o último snapshot encontrado para o cluster ou instância de banco de dados selecionado do Amazon RDS.

> **Note**
>
> Se você não especificar um valor para o `KMSKey` parâmetro, a automação cria uma nova chave gerenciada pelo AWS KMS cliente em sua conta que é usada para criptografar o instantâneo.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AccountIds

  Tipo: StringList

  Descrição: (obrigatório) Lista separada por vírgulas de IDs de conta com a qual compartilhar o snapshot.
- AutomationAssumeRole

Tipo: string

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Banco de dados

  Tipo: string

  Descrição: (obrigatório) O nome do cluster ou instância de banco de dados do Amazon RDS cujo snapshot deseja compartilhar. Esse parâmetro será necessário se for especificado um valor para o parâmetro `SnapshotName`.

- KMSKey

  Tipo: string

  Descrição: (opcional) O nome do recurso da Amazon (ARN) completo da chave gerenciada pelo cliente do AWS KMS a ser usada para criptografar o snapshot.

- SnapshotName

  Tipo: string

  Descrição: (opcional) O ID do snapshot do cluster ou instância de banco de dados que deseja usar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

O `AutomationAssumeRole` requer as seguintes ações para iniciar com êxito o runbook de um cluster de banco de dados.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

O perfil do IAM usado para executar a automação deve ser adicionado como um usuário chave para usar a chave KMS especificada no parâmetro `ARNKmsKey`. Para obter informações sobre como adicionar usuários de chave à uma chave KMS, consulte Alterar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service .

O `AutomationAssumeRole` requer as seguintes ações adicionais para iniciar com êxito o runbook se não for especificado um valor para o parâmetro de `KMSKey`.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`

Etapas do documento

1. `aws:executeScript`- Verifica se um valor foi fornecido para o `KMSKey` parâmetro e cria uma chave gerenciada pelo AWS KMS cliente se nenhum valor for encontrado.
2. `aws:branch` :Verifica se um valor foi fornecido para o parâmetro de `SnapshotName` e ramifica de acordo.
3. `aws:executeAwsApi` :Verifica se o snapshot fornecido é de uma instância de banco de dados.
4. `aws:executeScript` :Formata o parâmetro de `SnapshotName` substituindo dois pontos por um hífen.
5. `aws:executeAwsApi` :Copia o snapshot usando a `KMSKey` especificada.
6. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
7. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
8. `aws:executeAwsApi` :Verifica se o snapshot fornecido é de um cluster de banco de dados.

9. `aws:executeScript` :Formata o parâmetro de `SnapshotName` substituindo dois pontos por um hífen.
10. `aws:executeAwsApi` :Copia o snapshot usando a `KMSKey` especificada.
11. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
12. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
13. `aws:executeAwsApi` :Verifica se o valor fornecido para o parâmetro do `Database` é uma instância de banco de dados.
14. `aws:executeAwsApi` :Verifica se o valor fornecido para o parâmetro do `Database` é um cluster de banco de dados.
15. `aws:executeAwsApi` :Recupera uma lista de snapshots para o `Database` especificado.
16. `aws:executeScript` :Determina o último snapshot disponível na lista montada na etapa anterior.
17. `aws:executeAwsApi` :Copia o snapshot da instância de banco de dados usando a `KMSKey` especificada.
18. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
19. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
20. `aws:executeAwsApi` :Recupera uma lista de snapshots para o `Database` especificado.
21. `aws:executeScript` :Determina o último snapshot disponível na lista montada na etapa anterior.
22. `aws:executeAwsApi` :Copia o snapshot da instância de banco de dados usando a `KMSKey` especificada.
23. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
24. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
25. `aws:executeScript`- Exclui a chave gerenciada pelo AWS KMS cliente criada pela automação se você não especificar um valor para o `KMSKey` parâmetro e a automação falhar.

AWS-StartRdsInstance

Descrição

Iniciar uma instância do Amazon Relational Database Service (Amazon RDS)

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância do Amazon RDS a ser iniciado.

AWS-StartStopAuroraCluster

Descrição

Esse runbook inicia ou interrompe um cluster Amazon Aurora.

> **Note**
>
> Para iniciar um cluster, ele deve estar em um `stopped` status. Para parar um cluster, ele deve estar em um `available` status. Esse runbook não pode ser usado para iniciar ou

interromper um cluster que seja um cluster Aurora Serverless, um cluster multimaster do Aurora, parte de um banco de dados global do Aurora ou um cluster que usa a consulta paralela do Aurora.

[Execute esta automação (console)]

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: string

  Descrição: (Obrigatório) O nome do cluster Aurora que você deseja interromper ou iniciar.
- Ação

  Tipo: string

  Valores válidos: Iniciar | Parar

  Padrão: Iniciar

Descrição: (Obrigatório) O nome do cluster Aurora que você deseja interromper ou iniciar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

Etapas do documento

- `aws:executeScript`- Inicia ou interrompe o cluster com base nos valores que você especifica para o.

Saídas

StartStopAuroraCluster. ClusterName - O nome do cluster Aurora

StartStopAuroraCluster. CurrentStatus - O status atual do cluster Aurora

StartStopAuroraCluster.Message - Detalhes da automação

AWS-StopRdsInstance

Descrição

Interrompa uma instância do Amazon Relational Database Service (Amazon RDS).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: ID (obrigatório) da instância do Amazon RDS a ser interrompida.

AWSSupport-TroubleshootConnectivityToRDS

Descrição

O runbook `AWSSupport-TroubleshootConnectivityToRDS` diagnostica problemas de conectividade entre uma instância do EC2 e uma instância do Serviço de banco de dados relacional da Amazon. A automação garante que a instância de banco de dados esteja disponível e verifica as regras do grupo de segurança associadas, as listas de controle de acesso à rede (ACLs de rede) e as tabelas de rotas para verificar possíveis problemas de conectividade.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DB InstanceIdentifier

  Tipo: string

  Descrição: (obrigatória) o ID da instância de banco de dados com a qual testar a conectividade.
- SourceInstance

  Tipo: string

  Padrão permitido: ^i-[a-z0-9]{8,17}$

  Descrição: (obrigatória) o ID da instância do EC2 para testar a conectividade.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o status da instância de banco de dados é `available`.

- `aws:executeAwsApi` :Obtém informações resumidas sobre a instância do banco de dados.
- `aws:executeAwsApi` :Obtém informações sobre as ACLs de rede da instância de banco de dados.
- `aws:executeAwsApi` :Obtém o CIDR da sub-rede da instância de banco de dados.
- `aws:executeAwsApi` :Obtém informações resumidas sobre a instância do EC2
- `aws:executeAwsApi` :Obtém informações sobre as ACLs de rede da instância do EC2.
- `aws:executeAwsApi` :Obtém informações sobre os grupos de segurança associados à instância do EC2.
- `aws:executeAwsApi` :Obtém informações sobre os grupos de segurança associados à instância do banco de dados.
- `aws:executeAwsApi` :Obtém informações sobre as tabelas de rotas associadas à instância do EC2.
- `aws:executeAwsApi` :Obtém informações sobre a tabela de rotas principal associada à Amazon VPC para a instância do EC2.
- `aws:executeAwsApi` :Obtém informações sobre as tabelas de rotas associadas à instância do banco de dados.
- `aws:executeAwsApi` :Obtém informações sobre a tabela de rotas principal associada à Amazon VPC para a instância do banco de dados.
- `aws:executeScript`: avalia as regras do grupo de segurança.
- `aws:executeScript`: avalia ACLs de rede.
- `aws:executeScript` :Avalia as tabelas de rotas.
- `aws:sleep` :Encerra a automação.

Saídas

GetRDS InstanceProperties .DB InstanceIdentifier - A instância de banco de dados usada na automação.

GetRDS InstanceProperties .DB InstanceStatus - O status atual da instância de banco de dados.

evalSecurityGroupRegras. SecurityGroupEvaluation - Resultados da comparação das regras do grupo `SourceInstance` de segurança com as regras do grupo de segurança da instância de banco de dados.

evalNetworkAclRegras. NetworkAclEvaluation - Resultados da comparação das ACLs de `SourceInstance` rede com as ACLs de rede da instância de banco de dados.

evalRouteTableInscrições. RouteTableEvaluation - Resultados da comparação da tabela de `SourceInstance` rotas com as rotas da instância de banco de dados.

`AWSSupport-TroubleshootRDSIAMAuthentication`

Descrição

`AWSSupport-TroubleshootRDSIAMAuthentication`Isso ajuda a solucionar problemas de autenticação AWS Identity and Access Management (IAM) para instâncias do Amazon RDS para PostgreSQL, Amazon RDS para MySQL, Amazon RDS para MariaDB, Amazon Aurora PostgreSQL e Amazon Aurora MySQL. Use esse runbook para verificar a configuração necessária para a autenticação do IAM com uma instância do Amazon RDS ou Aurora Cluster. Ele também fornece etapas para corrigir os problemas de conectividade com a Instância do Amazon RDS ou o Aurora Cluster.

> **Important**
>
> Este runbook não é compatível com Amazon RDS para Oracle ou Amazon RDS para Microsoft SQL Server.

> **Important**
>
> Se uma instância do Amazon EC2 de origem for fornecida e o banco de dados de destino for o Amazon RDS, uma automação secundária `AWSSupport-TroubleshootConnectivityToRDS` será invocada para solucionar problemas de conectividade TCP. A saída também fornece comandos que você pode executar em sua instância do Amazon EC2 ou máquina de origem para se conectar às instâncias do Amazon RDS usando a autenticação do IAM.

Como funciona?

Este runbook consiste em seis etapas:

- Etapa 1: ValidateInputs: valida as entradas para a automação.

- Etapa 2: branchOnSource Fornecido pelo EC2: verifica se uma ID de instância do Amazon EC2 de origem é fornecida nos parâmetros de entrada.
- Etapa 3: ValidateRDSConnectivity: valida a conectividade do Amazon RDS a partir da instância de origem do Amazon EC2, se fornecida.
- Etapa 4: ValidateRDSIAMAuthentication: valida se o recurso de autenticação do IAM está ativado.
- Etapa 5: ValidateIAMPolicies: verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM fornecido.
- Etapa 6: Gerar relatório: gera um relatório dos resultados das etapas executadas anteriormente.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Tipo RDS

  Tipo: string

  Descrição: (Obrigatório): Selecione o tipo de banco de dados relacional ao qual você está tentando se conectar e autenticar.

Valores permitidos: `Amazon RDS` ou `Amazon Aurora Cluster.`

- DB InstanceIdentifier

  Tipo: string

  Descrição: (Obrigatório) O identificador da instância de banco de dados Amazon RDS de destino ou do cluster de banco de dados Aurora.

  Allowed-pattern: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  Número máximo de caracteres: 63

- SourceEc2 InstanceIdentifier

  Tipo: `AWS::EC2::Instance::Id`

  Descrição: (Opcional) O ID da instância do Amazon EC2 se você estiver se conectando à instância de banco de dados do Amazon RDS a partir de uma instância do Amazon EC2 em execução na mesma conta e região. Não especifique esse parâmetro se a origem não for uma instância do Amazon EC2 ou se o tipo de destino do Amazon RDS for um cluster de banco de dados Aurora.

  Padrão: `""`

- DBIAM RoleName

  Tipo: string

  Descrição: (Opcional) O nome da função do IAM que está sendo usado para autenticação baseada em IAM. Forneça somente se o parâmetro não `DBIAMUserName` for fornecido, caso contrário, deixe-o vazio. `DBIAMRoleName`Ou `DBIAMUserName` deve ser fornecido.

  Allowed-pattern: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Número máximo de caracteres: 64

  Padrão: `""`

- DBIAM UserName

  Tipo: string

Descrição: (Opcional) O nome de usuário do IAM usado para autenticação baseada em IAM. Forneça somente se o `DBIAMRoleName` parâmetro não for fornecido, caso contrário, deixe-o vazio. `DBIAMRoleNameOu DBIAMUserName` deve ser fornecido.

Allowed-pattern: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

Número máximo de caracteres: 64

Padrão: `""`

- DB UserName

  Tipo: string

  Descrição: (Opcional) O nome de usuário do banco de dados mapeado para uma função/usuário do IAM para autenticação baseada em IAM no banco de dados. A opção padrão `*` avalia se a `rds-db:connect` permissão é permitida para todos os usuários no banco de dados.

  Allowed-pattern: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Número máximo de caracteres: 64

  Padrão: `*`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Instruções

1. Navegue até a autenticação AWSSupport-TroubleshootRDSIAM no console. AWS Systems Manager
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - Tipo de RDS (obrigatório):

     Selecione o tipo de Amazon RDS ao qual você está tentando se conectar e autenticar. Escolha entre os dois valores permitidos: `Amazon RDS` ou `Amazon Aurora Cluster.`
   - DB InstanceIdentifier (obrigatório):

     Insira o identificador da Instância de Banco de Dados Amazon RDS de destino ou do Aurora Cluster ao qual você está tentando se conectar e usar as credenciais do IAM para autenticação.
   - SourceEc2 InstanceIdentifier (opcional):

     Forneça o ID da instância do Amazon EC2 se você estiver se conectando à instância de banco de dados do Amazon RDS a partir de uma instância do Amazon EC2 presente na mesma conta e região. Deixe em branco se a origem não for o Amazon EC2 ou se o tipo de Amazon RDS de destino for um Aurora Cluster.

- DBIAM RoleName (opcional):

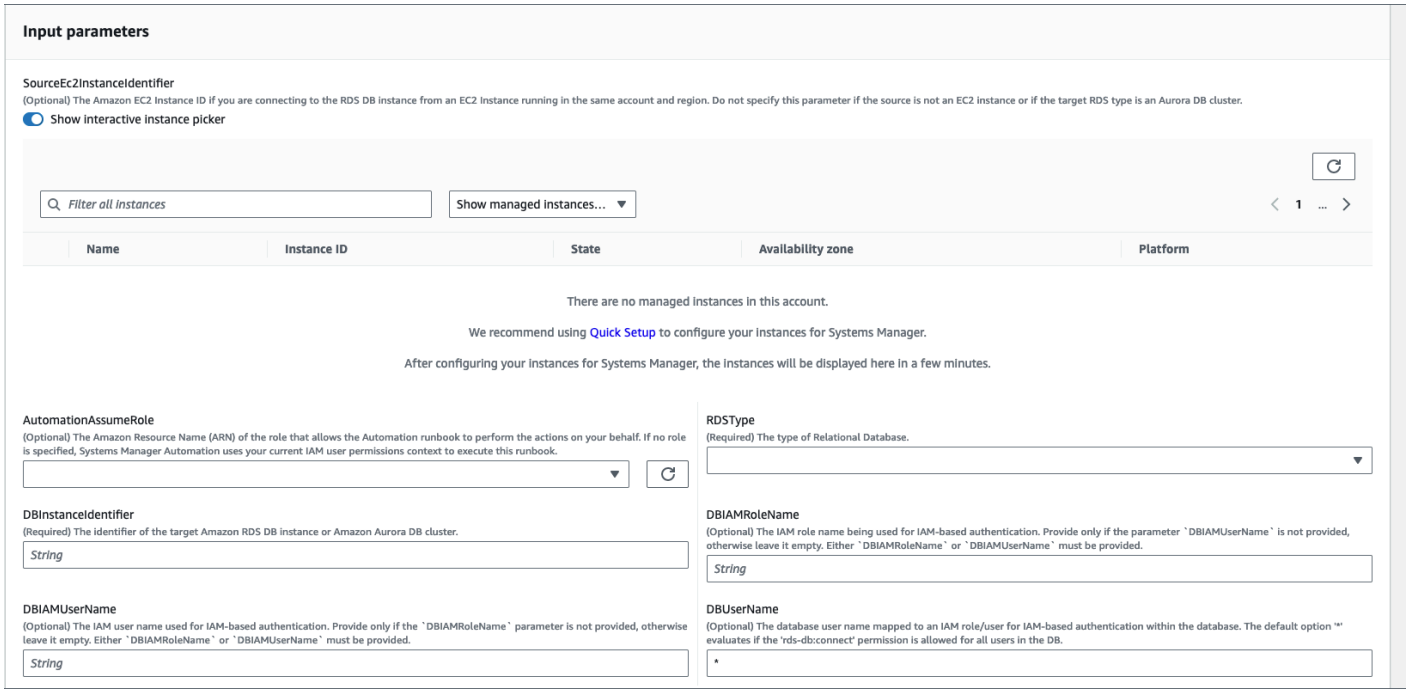
  Insira o nome da função do IAM usado para autenticação baseada em IAM. Forneça somente se não `DBIAMUserName` for fornecido; caso contrário, deixe em branco. `DBIAMRoleNameOu` `DBIAMUserName` deve ser fornecido.

- DBIAM UserName (opcional):

  Insira o usuário do IAM usado para a autenticação baseada em IAM. Forneça somente se não `DBIAMRoleName` for fornecido, caso contrário, deixe em branco. `DBIAMRoleNameOu` `DBIAMUserName` deve ser fornecido.

- DB UserName (opcional):

  Insira o usuário do banco de dados mapeado para uma função/usuário do IAM para autenticação baseada em IAM no banco de dados. A opção padrão * é usada para avaliar; nada é fornecido nesse campo.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - Etapa 1: validar as entradas:

     Valida as entradas para a automação - `SourceEC2InstanceIdentifier` (opcional), `DBInstanceIdentifier` ou`ClusterID`, e `DBIAMRoleName` ou. `DBIAMUserName` Ele

verifica se os parâmetros de entrada inseridos estão presentes em sua conta e região. Também verifica se o usuário inseriu um dos parâmetros do IAM (por exemplo, `DBIAMRoleName` ou`DBIAMUserName`). Além disso, ele executa outras verificações, como se o banco de dados mencionado estiver no status Disponível.

- Etapa 2: o branchOnSource EC2 forneceu:

  Verifica se o Amazon EC2 de origem é fornecido nos parâmetros de entrada e se o banco de dados é o Amazon RDS. Se sim, prossegue para a etapa 3. Caso contrário, ele pula a etapa 3, que é a validação da conectividade Amazon EC2-Amazon RDS, e prossegue para a etapa 4.

- Etapa 3: Validar a conectividade RDS:

  Se a origem do Amazon EC2 for fornecida nos parâmetros de entrada e o banco de dados for o Amazon RDS, a etapa 2 iniciará a etapa 3. Nesta etapa, a automação secundária `AWSSupport-TroubleshootConnectivityToRDS` é invocada para validar a conectividade do Amazon RDS a partir da origem do Amazon EC2. O runbook de automação infantil `AWSSupport-TroubleshootConnectivityToRDS` verifica se as configurações de rede necessárias (Amazon Virtual Private Cloud [Amazon VPC], grupos de segurança, lista de controle de acesso à rede [NACL], disponibilidade do Amazon RDS) estão em vigor para que você possa se conectar da instância do Amazon EC2 à instância do Amazon RDS.

- Etapa 4: validar a autenticação RDSIAM:

  Valida se o recurso de autenticação do IAM está ativado na instância do Amazon RDS ou no Aurora Cluster.

- Etapa 5: validar as políticas do IAM:

  Verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM passado para permitir que as credenciais do IAM sejam autenticadas na instância do Amazon RDS para o usuário de banco de dados especificado (se houver).

- Etapa 6: Gerar relatório:

  Obtém todas as informações das etapas anteriores e imprime o resultado ou a saída de cada etapa. Ele também lista as etapas a serem consultadas e executadas para se conectar à instância do Amazon RDS usando as credenciais do IAM.

7. Quando a automação estiver concluída, revise a seção Saídas para obter os resultados detalhados:

   - Verificando a permissão de usuário/função do IAM para se conectar ao banco de dados:

Verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM passado para permitir que as credenciais do IAM sejam autenticadas na instância do Amazon RDS para o usuário de banco de dados especificado (se houver).

- Verificando o atributo de autenticação baseado em IAM para o banco de dados:

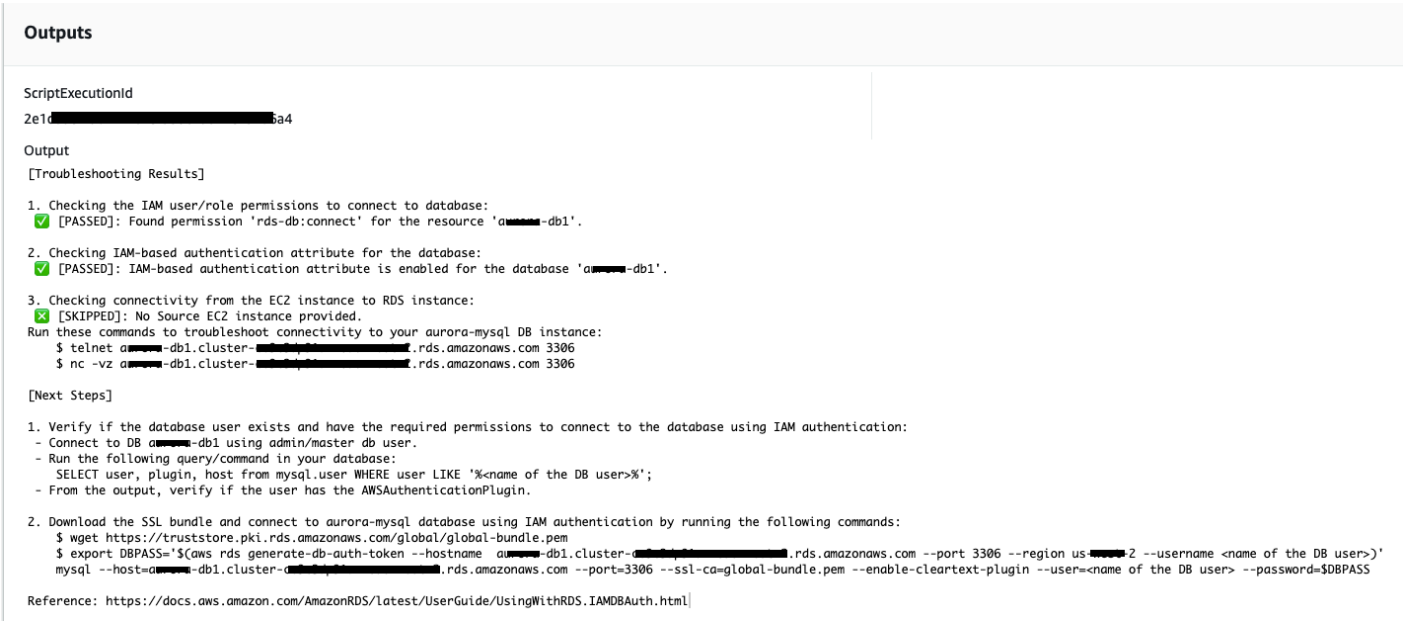
  Verifica se o recurso da autenticação do IAM está habilitado para o banco de dados Amazon RDS/cluster Aurora especificado.

- Verificando a conectividade da instância do Amazon EC2 com a instância do Amazon RDS:

  Verifica se as configurações de rede necessárias (Amazon VPC, grupos de segurança, NACL, disponibilidade do Amazon RDS) estão em vigor para que você possa se conectar da instância do Amazon EC2 à instância do Amazon RDS.

- Próximas etapas:

  Lista os comandos e as etapas a serem consultados e executados para se conectar à instância do Amazon RDS usando as credenciais do IAM.



Outputs

ScriptExecutionId

2e1d[redacted]6a4

Output

```
[Troubleshooting Results]

1. Checking the IAM user/role permissions to connect to database:
 ✅ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[redacted]-db1'.

2. Checking IAM-based authentication attribute for the database:
 ✅ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[redacted]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:
 ❎ [SKIPPED]: No Source EC2 instance provided.
Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:
    $ telnet a[redacted]-db1.cluster-[redacted].rds.amazonaws.com 3306
    $ nc -vz a[redacted]-db1.cluster-[redacted].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:
 - Connect to DB a[redacted]-db1 using admin/master db user.
 - Run the following query/command in your database:
    SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';
 - From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:
    $ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
    $ export DBPASS='$(aws rds generate-db-auth-token --hostname  a[redacted]-db1.cluster-[redacted].rds.amazonaws.com --port 3306 --region us-[redacted]2 --username <name of the DB user>)'
    mysql --host=a[redacted]-db1.cluster-[redacted].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=$DBPASS

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html
```

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação

- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-ValidateRdsNetworkConfiguration

Descrição

`AWSSupport-ValidateRdsNetworkConfiguration`a automação ajuda a evitar um estado de rede incompatível para sua instância existente do Amazon Relational Database Service (Amazon RDS) /Amazon Aurora /Amazon DocumentDB antes de você executar ou operar. `ModifyDBInstance` `StartDBInstance` Se a instância já estiver em um estado de rede incompatível, o runbook fornecerá o motivo.

Como funciona?

Este runbook determina se sua instância de banco de dados do Amazon RDS entrará em um estado de rede incompatível ou, se estiver, determina o motivo pelo qual está em um estado de rede incompatível.

O runbook executa as seguintes verificações em relação à sua instância de banco de dados Amazon RDS:

- Cota da Amazon Elastic Network Interface (ENI) por região.
- Todas as sub-redes no grupo de sub-redes do banco de dados existem.
- Há endereços IP gratuitos suficientes disponíveis para a (s) sub-rede (s).
- (Para instâncias do Amazon RDS acessíveis publicamente) Configurações de atributos de VPC `enableDnsSupport` (`enableDnsHostnamese`).

> **Important**
>
> Ao usar este documento em clusters Amazon Aurora/Amazon DocumentDB, certifique-se de usar em vez de. `DBInstanceIdentifier` `ClusterIdentifier` Caso contrário, o documento falhará na primeira etapa.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Política de amostra:

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

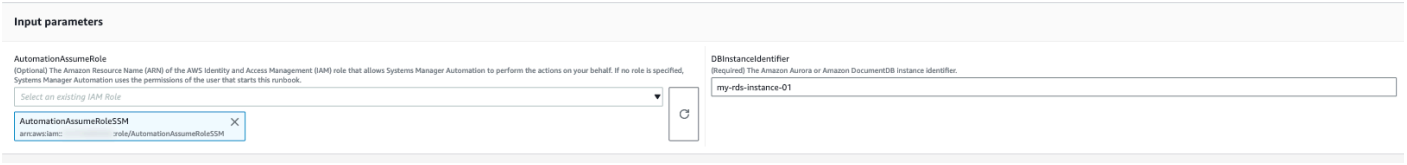
```
            ]
        }
```

Instruções

1. Navegue até AWSSupport- ValidateRdsNetworkConfiguration no AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - DB InstanceIdentifier (obrigatório):

     Insira o identificador de instância do Amazon Relational Database Service.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - Etapa 1 assertRdsState:

     Verifica se o identificador de instância fornecido existe e tem algum dos seguintes estados:`available`,`stopped`, ou`incompatible-network`.
   - Etapa 2 gatherRdsInformation:

     Coleta as informações necessárias sobre a instância do Amazon RDS para uso posterior na automação.
   - Etapa 3 checkEniQuota:

     Verifica a cota atual disponível do Amazon ENI para a região.
   - Etapa 4 validateVpcAttributes:

Valida se os parâmetros de DNS (`enableDnsSupporteenableDnsHostnames`) da Amazon VPC estão definidos como verdadeiros (ou não, se a instância do Amazon RDS estiver). `PubliclyAccessible`

- Etapa 5 validateSubnetAttributes:

  Valida a existência de sub-redes no `DBSubnetGroup` e verifica os IPs disponíveis para cada sub-rede.

- Etapa 6: Gerar relatório:

  Obtém todas as informações das etapas anteriores e imprime o resultado ou a saída de cada etapa. Ele também lista as etapas a serem consultadas e executadas para se conectar à instância do Amazon RDS usando as credenciais do IAM.

7. Quando a automação estiver concluída, revise a seção Saídas para obter os resultados detalhados:

   Instância do Amazon RDS com configuração de rede válida:

▼ 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.
```

Instância do Amazon RDS com configuração de rede incorreta (o enableDnsHostnames atributo VPC está definido como false):

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.
```

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSDocumentação do serviço

- Como resolvo problemas com um banco de dados do Amazon RDS que está em um estado de rede incompatível?
- Como resolvo problemas com uma instância do Amazon DocumentDB que está em um estado de rede incompatível?

Amazon Redshift

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Redshift. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSConfigRemediation-DeleteRedshiftCluster`

Descrição

O runbook `AWSConfigRemediation-DeleteRedshiftCluster` exclui o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O ID do cluster do Amazon Redshift que deseja excluir.
- SkipFinalClusterSnapshot

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `false`, a automação cria um snapshot antes de excluir o cluster do Amazon Redshift. Se definido como `true`, um snapshot final do cluster não será criado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Etapas do documento

- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `SkipFinalClusterSnapshot`.
- `aws:executeAwsApi` :Exclui o cluster do Amazon Redshift especificado no parâmetro `ClusterIdentifier`.

- `aws:assertAwsResourceProperty` :Verifica se o cluster do Amazon Redshift foi excluído.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descrição

O runbook `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` desabilita a acessibilidade pública para o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster para o qual deseja desabilitar a acessibilidade pública.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Desabilita a acessibilidade pública para o cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty` :Espera que o estado do cluster mude para `available`.
- `aws:assertAwsResourceProperty` :Confirma que a definição de acessibilidade pública está desabilitada no cluster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` habilita o log de auditoria para o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) para o qual deseja fazer upload de logs.

- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o log de auditoria.

- S3 KeyPrefix

  Tipo: string

  Descrição: (opcional) O prefixo de chave (subpasta) do Amazon S3 para o qual deseja fazer o upload dos logs.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Etapas do documento

- `aws:branch` :Ramifica com base no fato de um valor ter sido especificado para o parâmetro `S3KeyPrefix`.
- `aws:executeAwsApi` :Permite o log de auditoria no cluster especificado no `ClusterIdentifier` parâmetro.
- `aws:assertAwsResourceProperty` :Verifica se o log de auditoria foi habilitado no cluster.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` habilita snapshots automatizados para o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AutomatedSnapshotRetentionPeriod

  Tipo: inteiro

Valores válidos: 1 a 35

Descrição: (obrigatório) O número de dias que os snapshots automatizados são retidos.

- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual você deseja ativar os snapshots automatizados

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita snapshots de automação no cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty` :Espera que o estado do cluster mude para `available`.
- `aws:executeScript` :Confirma que os snapshots automatizados foram habilitados no cluster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descrição

O `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook permite a criptografia no cluster do Amazon Redshift que você especifica usando AWS Key Management Service uma chave AWS KMS() gerenciada pelo cliente. Esse runbook só deve ser usado como uma linha de base para garantir que os clusters do Amazon Redshift sejam criptografados de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar vários clusters com diferentes chaves gerenciadas pelo cliente. Esse runbook não pode alterar a

chave gerenciada pelo AWS KMS cliente usada em um cluster já criptografado. Para alterar a chave gerenciada pelo AWS KMS cliente usada para criptografar um cluster, primeiro você deve desativar a criptografia no cluster.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual você deseja habilitar a criptografia.
- KMSKeyARN

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da chave gerenciada pelo cliente do AWS KMS que deseja usar para criptografar os dados do cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita a criptografia no cluster do Amazon Redshift especificado no parâmetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty` :Verifica se a criptografia foi habilitada no cluster.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` habilita um roteamento avançado da nuvem privada virtual (VPC) para o cluster do Amazon Redshift especificado. Para obter mais informações sobre o roteamento avançado da Amazon VPC, consulte Roteamento avançado da VPC do Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita o roteamento avançado da VPC no cluster especificado no parâmetro `ClusterIdentifier`.
- `assertAwsResourceProperty` :Confirma que o roteamento avançado da VPC foi habilitado no cluster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descrição

O runbook `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` exige que as conexões de entrada usem SSL para o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Etapas do documento

- `aws:executeAwsApi` :Reúne os detalhes dos parâmetros do cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:executeAwsApi`: Habilita a definição de `require_ssl` no cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty` :Confirma que a definição de `require_ssl` está habilitada no cluster .
- `aws:executeScript` :Verifica a definição de `require_ssl` do cluster.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Descrição

O runbook `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` modifica as definições de manutenção do cluster Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AllowVersionUpgrade

  Tipo: booliano

  Descrição: (obrigatório) Se definido como `true`, as atualizações da versão principal serão aplicadas automaticamente ao cluster durante a janela de manutenção.
- AutomationAssumeRole

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- AutomatedSnapshotRetentionPeriod

  Tipo: inteiro

  Valores válidos: 1 a 35

  Descrição: (obrigatório) O número de dias que os snapshots automatizados são retidos.
- ClusterIdentifier

  Tipo: string

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.
- PreferredMaintenanceWindow

  Tipo: string

  Descrição: (obrigatório) O intervalo de tempo semanal (em UTC) durante o qual pode ocorrer manutenção do sistema.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Modifica as definições de manutenção do cluster especificado no parâmetro `ClusterIdentifier`.

- `aws:assertAwsResourceProperty` :Confirma que as definições de manutenção modificadas foram configuradas para o cluster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descrição

O runbook `AWSConfigRemediation-ModifyRedshiftClusterNodeType` modifica o tipo de nó e o número de nós para o cluster do Amazon Redshift especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- Clássica

  Tipo: Booliano

  Descrição: (opcional) Se definida como `true`, a operação de redimensionamento usa o processo de redimensionamento clássico.
- ClusterIdentifier

  Tipo: string

Descrição: (obrigatório) O identificador exclusivo do cluster cujo tipo de nó deseja modificar.

- ClusterType

  Tipo: string

  Valores válidos: single-node | multi-node

  Descrição: (obrigatório) O tipo de cluster que deseja atribuir ao seu cluster.

- NodeType

  Tipo: string

  Valores válidos: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  Descrição: (obrigatório) O tipo de nó que você deseja atribuir ao seu cluster.

- NumberOfNodes

  Tipo: inteiro

  Valores válidos: 2 a 100

  Descrição: (opcional) O número de nós que deseja atribuir ao seu cluster. Se o cluster for do tipo `single-node`, não especifique um valor para esse parâmetro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Etapas do documento

- `aws:executeScript` :Modifica o tipo de nó e o número de nós do cluster especificado no parâmetro `ClusterIdentifier`.

Amazon S3

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Storage Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWS-ArchiveS3BucketToIntelligentTiering`

Descrição

O `AWS-ArchiveS3BucketToIntelligentTiering` runbook cria ou substitui uma configuração de classificação por níveis inteligente para o bucket do Amazon Simple Storage Service (Amazon S3) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (Obrigatório) O nome do bucket do S3 para o qual você deseja criar uma configuração de hierarquização inteligente.
- ConfigurationId

  Tipo: string

  Descrição: (Obrigatório) O ID da configuração inteligente de camadas. Isso pode ser um novo ID de configuração ou o ID de uma configuração existente.
- NumberOfDaysToArchive

  Tipo: string

  Valores válidos: 90-730

  Descrição: (Obrigatório) O número de dias consecutivos após um objeto em seu bucket estar qualificado para ser transferido para o nível Archive Access.
- NumberOfDaysToDeepArchive

  Tipo: string

Valores válidos: 180-730

Descrição: (Obrigatório) O número de dias consecutivos após um objeto em seu bucket estar qualificado para ser transferido para o nível de acesso ao Deep Archive.

- S3Prefix

  Tipo: string

  Descrição: (Opcional) O prefixo do nome da chave dos objetos aos quais você deseja aplicar a configuração.

- Tags

  Tipo: MapList

  Descrição: (Opcional) Metadados atribuídos aos objetos aos quais você deseja aplicar a configuração. As tags consistem em uma chave e um valor definidos pelo usuário.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Etapas do documento

- PutsBucketIntelligentTieringConfiguration (aws:ExecuteScript) — Cria ou atualiza uma configuração do Amazon S3 Intelligent-Tiering para o bucket especificado.
- VerifyBucketIntelligentTieringConfiguration(aws: assertAwsResource Property) - Verifica se a configuração inteligente do bucket do S3 foi aplicada ao bucket especificado.

AWS-ConfigureS3BucketLogging

Descrição

Habilitar o log do bucket do Amazon Simple Storage Service (Amazon S3).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 para o qual você deseja configurar o log.
- GrantedPermission

  Tipo: string

  Valores permitidos: FULL_CONTROL | READ | WRITE

  Descrição: (obrigatório) Registrar permissões atribuídas ao usuário autorizado para o bucket.
- GranteeEmailAddress

  Tipo: string

(Opcional) O endereço de e-mail do favorecido.

- GranteeId

  Tipo: string

  Descrição: (opcional) O ID de usuário canônico do favorecido.

- GranteeType

  Tipo: string

  Valores válidos: CanonicalUser | AmazonCustomerByEmail | Grupo

  Descrição: (obrigatório) Tipo de favorecido.

- GranteeUri

  Tipo: string

  Descrição: (opcional) URI do grupo de favorecidos.

- TargetBucket

  Tipo: string

  Descrição: (obrigatório) Especifica o bucket em que você deseja que o Amazon S3 armazene os logs de acesso do servidor. Os logs podem ser entregues em qualquer bucket de sua propriedade. Você também pode configurar vários buckets para entregar seus logs para o mesmo bucket de destino. Nesse caso, você deve escolher um diferente TargetPrefix para cada bucket de origem para que os arquivos de log entregues possam ser diferenciados por chave.

- TargetPrefix

  Tipo: string

  Padrão: /

  Descrição: (opcional) Especifica um prefixo para as chaves em que os arquivos de log serão armazenados.

AWS-ConfigureS3BucketVersioning

Descrição

Configurar o versionamento de um bucket do Amazon Simple Storage Service (Amazon S3).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 para o qual você deseja configurar o versionamento.
- VersioningState

  Tipo: string

  Valores permitidos: Enabled | Suspended

  Padrão: Habilitado

  Descrição: (Opcional) Aplicada ao VersioningConfiguration .Status. Quando definido como "Enabled", esse processo permite o versionamento de objetos no bucket; todos os objetos

adicionados ao bucket recebem um ID de versão exclusivo. Quando definido como `Suspended`, esse processo desabilita o versionamento dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null`.

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Descrição

O runbook `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` define as configurações do bloco de acesso público do Amazon Simple Storage Service (Amazon S3) para um bucket do Amazon S3 com base nos valores especificados nos parâmetros do runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BlockPublicAcls

  Tipo: booleano

  Padrão: True

Descrição: (opcional) Se definido como `true`, o listas de controle (ACLs) do Bloqueio de Acesso Público do Amazon S3 para o bucket do S3 e os objetos armazenados no bucket do S3 especificado no parâmetro `BucketName`.

- BlockPublicPolicy

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Se definido como `true`, o Amazon S3 bloqueia políticas públicas de bucket para o bucket S3 especificado no parâmetro `BucketName`.

- BucketName

  Tipo: string

  Descrição: (obrigatória) O nome do bucket do S3 onde você deseja configurar.

- IgnorePublicAcls

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Se definido como `true`, o Amazon S3 ignora todas as ACLs públicas do bucket do S3 especificadas no parâmetro `BucketName`.

- RestrictPublicBuckets

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Se definido como `true`, o Amazon S3 restringe as políticas públicas de bucket para o bucket do S3 especificado no parâmetro `BucketName`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Etapas do documento

- `aws:executeAwsApi` :Cria ou modifica a configuração de `PublicAccessBlock` do bucket do S3 especificado no parâmetro `BucketName`.
- `aws:executeScript` :Retorna a configuração de `PublicAccessBlock` do bucket do S3 especificado no parâmetro `BucketName` e verifica se as alterações foram feitas com sucesso com base nos valores especificados nos parâmetros do runbook.

AWSConfigRemediation-ConfigureS3PublicAccessBlock

Descrição

O `AWSConfigRemediation-ConfigureS3PublicAccessBlock` runbook configura as configurações de um bloco de acesso público do Conta da AWS Amazon Simple Storage Service (Amazon S3) com base nos valores que você especifica nos parâmetros do runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AccountId

  Tipo: string

Descrição: (Obrigatório) O ID do proprietário do bucket S3 Conta da AWS que você está configurando.

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BlockPublicAcls

  Tipo: booleano

  Padrão: True

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 bloqueia listas públicas de controle de acesso (ACLs) para buckets do S3 pertencentes ao Conta da AWS que você especifica no parâmetro. `AccountId`

- BlockPublicPolicy

  Tipo: booleano

  Padrão: True

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 bloqueia políticas públicas de bucket para buckets do S3 de propriedade do Conta da AWS que você especifica no parâmetro. `AccountId`

- IgnorePublicAcls

  Tipo: booleano

  Padrão: True

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 ignora todas as ACLs públicas para buckets do S3 pertencentes aos que você especificou no Conta da AWS parâmetro. `AccountId`

- RestrictPublicBuckets

  Tipo: booleano

Padrão: True

Descrição: (Opcional) Se definido como`true`, o Amazon S3 restringe as políticas públicas de bucket para buckets do S3 de propriedade do que Conta da AWS você especifica no parâmetro. `AccountId`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Etapas do documento

- `aws:executeAwsApi` :Cria ou modifica a configuração `PublicAccessBlock` para a Conta da AWS especificada no parâmetro `AccountId`.
- `aws:executeScript`- Retorna a `PublicAccessBlock` configuração Conta da AWS especificada no `AccountId` parâmetro e verifica se as alterações foram feitas com sucesso com base nos valores especificados nos parâmetros do runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descrição

O `AWS-CreateS3PolicyToExpireMultipartUploads` runbook cria uma política de ciclo de vida para um bucket específico que expira os uploads incompletos de várias partes em andamento após um número definido de dias. Esse runbook mescla a nova política de ciclo de vida com qualquer política de bucket de ciclo de vida existente que já exista.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (obrigatória) O nome do bucket do S3 onde você deseja configurar.
- DaysUntilExpire

  Tipo: inteiro

  Descrição: (Obrigatório) O número de dias que o Amazon S3 espera antes de remover permanentemente todas as partes do upload.
- RuleId

  Tipo: string

  Descrição: (Obrigatório) O ID usado para identificar a regra do intervalo de ciclo de vida. Esse deve ser um valor exclusivo.
- S3Prefix

  Tipo: string

  Descrição: (Opcional) O prefixo do nome da chave dos objetos aos quais você deseja aplicar a configuração.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Etapas do documento

- ConfigureExpireMultipartUploads (aws:ExecuteScript) — Configura a política de ciclo de vida do bucket.
- VerifyExpireMultipartUploads (aws:ExecuteScript) — Verifica se a política de ciclo de vida foi configurada para o bucket.

Saídas

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

AWS-DisableS3BucketPublicReadWrite

Descrição

Usar o `Block Public Access` do Amazon Simple Storage Service (Amazon S3) para desabilitar o acesso de leitura e gravação para um bucket público do S3. Para obter mais informações, consulte Usar o bloqueio de acesso público do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- S3 BucketName

  Tipo: string

  Descrição: (obrigatória) o bucket do S3 no qual você deseja restringir o acesso.

AWS-EnableS3BucketEncryption

Descrição

Configura o bucket Amazon Simple Storage Service (Amazon S3) para criptografia padrão.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- BucketName

  Tipo: string

  Descrição: (obrigatória) o nome do bucket do S3 onde você deseja criptografar o conteúdo.

- SSEAlgorithm

  Tipo: string

  Padrão: AES256

  Descrição: (Opcional) Algoritmo de criptografia do lado do servidor a ser usado para a criptografia padrão.

AWS-EnableS3BucketKeys

Descrição

O `AWS-EnableS3BucketKeys` runbook habilita Bucket Keys no bucket do Amazon Simple Storage Service (Amazon S3) especificado por você. Essa chave em nível de bucket cria chaves de dados para novos objetos durante seu ciclo de vida. Se você não especificar um valor para o `KmsKeyId` parâmetro, a criptografia do lado do servidor usando as chaves gerenciadas do Amazon S3 (SSE-S3) será usada para a configuração de criptografia padrão.

> **Note**
>
> As chaves de bucket do Amazon S3 não são compatíveis com criptografia de duas camadas no lado do servidor com AWS Key Management Service chaves () (DSSE-KMS).AWS KMS

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (Obrigatório) O nome do bucket do S3 para o qual você deseja habilitar o Bucket Keys.
- KMS KeyId

  Tipo: string

  Descrição: (Opcional) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente que você deseja usar para criptografia no lado do servidor.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Etapas do documento

- ChooseEncryptionType (aws:branch) - Avalia o valor fornecido para o `KmsKeyId` parâmetro para determinar se o SSE-S3 (AES256) ou o SSE-KMS serão usados.
- PutBucketKeysKMS (aws:executeAwsApi) - Define a `BucketKeyEnabled` propriedade `true` para o bucket S3 especificado usando o especificado. `KmsKeyId`
- PutBucketKeysAES256 (aws:executeAwsApi) - Define a `BucketKeyEnabled` propriedade `true` para o bucket S3 especificado com criptografia AES256.
- VerifyS3 BucketKeysEnabled (aws: assertAwsResource Property) - Verifica se as chaves de bucket estão habilitadas no bucket S3 de destino.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Descrição

O runbook `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` remove as instruções de política da entidade principal que têm curingas (`Principal: *` ou `Principal: "AWS": *`) para ações de `Allow` de sua política de bucket do Amazon Simple Storage Service (Amazon S3). As instruções de política com condições também são removidas.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cuja política deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Etapas do documento

- `aws:executeScript` :Modifica a política do bucket e verifica se as instruções de política da entidade principal com curingas foram removidas do bucket do Amazon S3 especificado no parâmetro `BucketName`.

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Descrição

O runbook `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` cria uma instrução de política de bucket do Amazon Simple Storage Service (Amazon S3) que nega explicitamente solicitações HTTP para o bucket do Amazon S3 especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BucketName

  Tipo: string

  Descrição: (obrigatório) O nome do bucket do S3 cujas solicitações HTTP serão negadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Etapas do documento

- `aws:executeScript` :Cria uma política de bucket para o bucket do S3 especificado no parâmetro `BucketName` que nega explicitamente as solicitações HTTP.

AWSSupport-TroubleshootS3PublicRead

Descrição

O runbook `AWSSupport-TroubleshootS3PublicRead` diagnostica problemas de leitura de objetos do bucket público do Amazon Simple Storage Service (Amazon S3) especificado no parâmetro `S3BucketName`. Um subconjunto de definições também é analisado para objetos no bucket do S3.

Execute esta automação (console)

Limitações

- Essa automação não verifica os pontos de acesso que permitem o acesso público aos objetos.
- Essa automação não avalia as chaves de condição na política de bucket do S3.
- Se você estiver usando AWS Organizations, essa automação não avalia as políticas de controle de serviços para confirmar se o acesso ao Amazon S3 é permitido.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- CloudWatchLogGroupName

  Tipo: string

  Descrição: (Opcional) O grupo de CloudWatch registros do Amazon Logs para o qual você deseja enviar a saída de automação. Se não for encontrado um grupo de logs que corresponda ao valor especificado, a automação criará um grupo de logs usando esse valor de parâmetro. O período de retenção do grupo de logs criado por essa automação é de 14 dias.

- CloudWatchLogStreamName

  Tipo: string

  Descrição: (Opcional) O fluxo de CloudWatch registros para o qual você deseja enviar a saída de automação. Se não for encontrado um fluxo de logs que corresponda ao valor especificado, a automação criará um fluxo de logs usando esse valor de parâmetro. Se um valor para esse parâmetro não for especificado, a automação usará o `ExecutionId` para o nome do fluxo de logs.

- HttpGet

  Tipo: booliano

  Valores válidos: True | False

  Padrão: True

  Descrição: (opcional) Se esse parâmetro for definido como `true`, a automação fará uma solicitação HTTP parcial aos objetos do `S3BucketName` que forem especificados. Somente o primeiro byte do objeto é retornado usando o cabeçalho HTTP Range.

- IgnoreBlockPublicAccess

  Tipo: booliano

  Valores válidos: True | False

  Padrão: False

  Descrição: (opcional) Se esse parâmetro for definido como `true`, a automação ignorará as definições do bloco de acesso público do bucket do S3 especificado no parâmetro `S3BucketName`. Não é recomendável alterar o valor do este parâmetro padrão.

- MaxObjects

Tipo: inteiro

Valores válidos: 1 a 25

Padrão: 5

Descrição: (opcional) O número de objetos a serem analisados no bucket do S3 especificado no parâmetro `S3BucketName`.

- S3 BucketName

  Tipo: string

  Descrição: (obrigatória) O ID do bucket do S3 para solução de problemas.

- S3 PrefixName

  Tipo: string

  Descrição: (opcional) O prefixo do nome da chave dos objetos que você quer analisar em seu bucket do S3. Para ter mais informações, consulte Chaves do objeto no Guia do usuário do Amazon Simple Storage Service.

- StartAfter

  Tipo: string

  Descrição: (opcional) O nome da chave do objeto em que a automação deve começar a analisar os objetos em seu bucket do S3.

- ResourcePartition

  Tipo: string

  Valores válidos: `aws` | `aws-us-gov` | `aws-cn`

  Padrão: `aws`

  Descrição: (obrigatório) A partição em que o bucket do S3 está localizado.

- Detalhado

  Tipo: Booliano

  Valores válidos: True | False

Padrão: False

Descrição: (opcional) Para retornar informações mais detalhadas durante a automação, defina esse parâmetro como `true`. Somente mensagens de aviso e erro serão retornadas se o parâmetro estiver definido como `false`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

As `logs:PutLogEvents` permissões `logs:CreateLogGrouplogs:CreateLogStream`, e só são necessárias se você quiser que a automação envie dados de registro para o CloudWatch Logs.

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

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o bucket do S3 existe e está acessível.
- `aws:executeScript` :Retorna a localização do bucket do S3 e seu ID de usuário canônico.
- `aws:executeScript` :Retorna as definições do bloco de acesso público de sua conta e do bucket do S3.
- `aws:assertAwsResourceProperty` :Confirma que o pagador do bucket do S3 está configurado como `BucketOwner`. Se `Requester Pays` estiver habilitado no bucket do S3, a automação será encerrada.
- `aws:executeScript` :Retorna o status da política do bucket do S3 e determina se ela é considerada pública. Para obter mais informações sobre buckets públicos do S3, consulte O significado de “público” no Guia do desenvolvedor do Amazon Simple Storage Service.
- `aws:executeAwsApi` :Retorna a política de bucket do S3.
- `aws:executeAwsApi` :Retorna todas as chaves de contexto encontradas na política de bucket do S3.
- `aws:assertAwsResourceProperty` :Confirma se há uma negação explícita na política de bucket do S3 para a ação `GetObject` da API.
- `aws:executeAwsApi` :Retorna a lista de controle de acesso (ACL) do bucket do S3.
- `aws:executeScript`- Cria um grupo de CloudWatch registros e um fluxo de registros se você especificar um valor para o `CloudWatchLogGroupName` parâmetro.
- `aws:executeScript` :Com base nos valores especificados nos parâmetros de entrada do runbook, avalia se alguma das definições do bucket do S3 coletadas durante a automação está impedindo que os objetos sejam acessados pelo público. Esse script executa as seguintes funções:

- Avalia as definições de bloqueio de acesso público
- Retorna objetos do bucket do S3 com base nos valores especificados nos parâmetros `MaxObjects`, `S3PrefixName` e `StartAfter`.
- Retorna a política do bucket do S3 para simular uma política do IAM personalizada para os objetos retornados do bucket do S3.
- Executa uma solicitação HTTP parcial para os objetos retornados se o parâmetro `HttpGet` estiver definido como `true`. Somente o primeiro byte do objeto é retornado usando o cabeçalho HTTP Range.
- Verifica o nome da chave do objeto retornado para confirmar se ele termina com um ou dois pontos. Os nomes de chaves de objetos que terminam em pontos não podem ser baixados do console do Amazon S3.
- Verifica se o proprietário do objeto retornado corresponde ao proprietário do bucket do S3.
- Verifica se a ACL do objeto concede permissões de `READ` ou `FULL_CONTROL` a usuários anônimos.
- Retorna tags associadas ao objeto.
- Usa a política do IAM simulada para confirmar se há uma negação explícita desse objeto na política de bucket do S3 para a ação `GetObject` da API.
- Retorna os metadados do objeto para confirmar que a classe de armazenamento é compatível.
- Verifica as configurações de criptografia do lado do servidor do objeto para confirmar se o objeto está criptografado usando uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente.

Saídas

AnalyzeObjects.balde

AnalyzeObjects.objeto

SageMaker

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. SageMaker Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-DisableSageMakerNotebookRootAccess

AWS-DisableSageMakerNotebookRootAccess

Descrição

O AWS-DisableSageMakerNotebookRootAccess runbook desativa o acesso root em uma instância de SageMaker notebook da Amazon. Durante a automação, a instância do notebook é interrompida para fazer as alterações necessárias. SageMaker As instâncias do notebook Studio não são suportadas.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- NotebookInstanceName

  Tipo: string

  Descrição: (Obrigatório) O nome da instância do SageMaker notebook na qual desabilitar o acesso root.

- StartInstanceAfterUpdate

  Tipo: booleano

  Padrão: True

  Descrição: (Opcional) Determina se a instância do notebook é iniciada após a desativação do acesso root. A configuração padrão para esse parâmetro é`true`. Se definido como`true`, a instância será iniciada após a desativação do acesso root. Se definido como`false`, a instância permanece no `stopped` estado após a desativação do acesso root.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Etapas do documento

- CheckNotebookInstanceStatus (aws:executeAwsApi): Verifica o status atual da instância do notebook.
- StopOrUpdateNotebookInstance (aws:branch): ramificações com base no status da instância do notebook.
- StopNotebookInstance (aws:executeAwsApi): inicia a instância se o status for`stopped`.
- WaitForInstanceToStop (aws: waitForAwsResourceProperty): Verifica se a instância é`stopped`.
- UpdateNotebookInstance (aws:executeAwsApi): desativa o acesso root na instância do notebook.
- WaitForNotebookUpdate (aws: waitForAwsResourceProperty): Verifica se o acesso root foi desativado e se a instância tem um `stopped` status.
- ChooseInstanceStart (aws:branch): ramificação com base na necessidade de iniciar a instância.
- StartNotebookInstance (aws:executeAwsApi): inicia a instância do notebook.

- VerifyNotebookInstanceStatus (aws: waitForAwsResourceProperty): Verifica se a instância está `available` antes de desativar o acesso root.
- VerifyNotebookInstanceRootAccess (aws: assertAwsResource Propriedade): Verifica se a configuração de acesso raiz da instância do notebook foi desativada com sucesso.

Secrets Manager

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Secrets Manager Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

`AWSConfigRemediation-DeleteSecret`

Descrição

O `AWSConfigRemediation-DeleteSecret` runbook exclui um segredo e todas as versões armazenadas nele. AWS Secrets Manager Opcionalmente, você pode especificar a janela de recuperação durante a qual o segredo pode ser restaurado. Se não for especificado um valor para o parâmetro `RecoveryWindowInDays`, o padrão da operação será 30 dias.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- RecoveryWindowInDays

  Tipo: Inteiro

  Valores válidos: 7 a 30

  Padrão: 30

  Descrição: (opcional) O número de dias em que você pode restaurar o segredo.

- SecretId

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do segredo que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

Etapas do documento

- `aws:executeAwsApi` :Exclui o segredo especificado no parâmetro `SecretId`.
- `aws:executeScript` :Verifica se o segredo foi agendado para exclusão.

AWSConfigRemediation-RotateSecret

Descrição

O AWSConfigRemediation-RotateSecret runbook gira um segredo armazenado em. AWS Secrets Manager

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- RotationInterval

  Tipo: Intervalo

  Valores válidos: 1 a 365

  Descrição: (obrigatório) O número de dias entre as alternâncias do segredo.
- RotationLambdaArn

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da função AWS Lambda que pode alternar o segredo.

- SecretId

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do segredo que deseja alternar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Etapas do documento

- `aws:executeAwsApi` :Alterna o segredo especificado no parâmetro `SecretId`.
- `aws:executeScript` :Verifica se a rotação foi habilitada no segredo.

Security Hub

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Security Hub Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

Descrição

O `AWSConfigRemediation-EnableSecurityHub` runbook habilita AWS Security Hub (Security Hub) para Conta da AWS e Região da AWS onde você executa a automação. Para obter

informações sobre o Security Hub, consulte O que é AWS Security Hub? no Guia do AWS Security Hub usuário.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EnableDefaultStandards

  Tipo: booleano

  Padrão: True

  Descrição: (obrigatório) Se definido como `true`, os padrões de segurança padrão designados pelo Security Hub serão habilitados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`

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

Etapas do documento

- `aws:executeAwsApi` :Habilita o Security Hub na região e na conta atual.
- `aws:executeAwsApi` :Verifica se o Security Hub foi habilitado.

AWS Shield

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Shield Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSPremiumSupport-DDoSResiliencyAssessment

`AWSPremiumSupport-DDoSResiliencyAssessment`

Descrição

O `AWSPremiumSupport-DDoSResiliencyAssessment`, runbook de automação AWS Systems Manager ajuda você a verificar as vulnerabilidades de DDoS e a configuração de recursos de acordo com a proteção AWS Shield Advanced de sua Conta da AWS. Ele fornece um relatório de configurações para recursos vulneráveis a ataques do tipo negação de serviço distribuída (Distributed Denial of Service, DDoS). Ele é usado para coletar, analisar e avaliar os seguintes recursos: Amazon Route 53, Amazon Load Balancers, CloudFront distribuições da Amazon AWS Global Accelerator e AWS Elastic IPs para suas definições de configuração, de acordo com as melhores práticas recomendadas de proteção. AWS Shield Advanced O relatório de configuração final está disponível em um bucket do Amazon S3 de sua escolha como um arquivo HTML.

Como funciona?

Este runbook contém uma série de verificações dos vários tipos de recursos que estão ativados para acesso público e se eles têm proteções configuradas de acordo com as recomendações do Whitepaper Melhores Práticas de DDoS da AWS. O runbook executa o seguinte:

- Verifica se a assinatura do AWS Shield Advanced está ativada.
- Se ativada, ele descobre se há algum recurso protegido do Shield Advanced.
- Ele encontra todos os recursos globais e regionais na Conta da AWS e verifica se eles estão protegidos pelo Shield.
- Ela exige os parâmetros do tipo de recurso para avaliação, o nome do bucket do Amazon S3 e o ID do Conta da AWS bucket do Amazon S3 (S3). BucketOwner
- Ele retorna as descobertas como um relatório HTML armazenado no bucket do Amazon S3 fornecido.

O `AssessmentType` dos parâmetros de entrada decide se as verificações em todos os recursos serão realizadas. Por padrão, o runbook verifica todos os tipos de recursos. Somente se o parâmetro `GlobalResources` ou `RegionalResources` for selecionado, o runbook executará verificações somente nos tipos de recursos selecionados.

> **Important**
>
> - O acesso aos runbooks `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar os planos do AWS Support.
> - Este runbook requer uma assinatura `ACTIVE` do AWS Shield Advanced.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AssessmentType

  Tipo: string

  Descrição: (opcional) determina o tipo de recursos a serem avaliados para a avaliação da resiliência de DDoS. Por padrão, o runbook avaliará os recursos globais e regionais. Para recursos regionais, o runbook descreve todos os balanceadores de carga de aplicativo (ALB) e rede (NLB), bem como todo o grupo do Auto Scaling em sua Conta da AWS/região.

  Valores válidos: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  Padrão: recursos globais e regionais

- S3 BucketName

  Tipo: `AWS::S3::Bucket::Name`

  Descrição: (obrigatório) o nome do bucket do Amazon S3 onde o relatório será carregado.

  Allowed-pattern: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  Tipo: string

  Descrição: (opcional) a Conta da AWS que é proprietária do bucket do Amazon S3. Especifique esse parâmetro se o bucket do Amazon S3 pertencer a outraConta da AWS, caso contrário, você pode deixar esse parâmetro vazio.

  Allowed-pattern: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  Tipo: `AWS::IAM::Role::Arn`

Descrição: (opcional) o ARN do perfil do IAM com permissões para descrever o bucket do Amazon S3 e Conta da AWS bloqueia a configuração de acesso público se o bucket estiver em outra Conta da AWS. Se esse parâmetro não for especificado, o runbook usa o `AutomationAssumeRole` ou o usuário do IAM que inicia esse runbook (se `AutomationAssumeRole` não for especificado). Consulte a seção de permissões necessárias na descrição do runbook.

Allowed-pattern: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

  Tipo: string

  Descrição: (opcional) o prefixo do caminho dentro do Amazon S3 para armazenar os resultados.

  Allowed-pattern: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Exemplo de política do IAM para a função Automation Assume

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

Instruções

1. Navegue até o AWSPremiumSupport-DDoS ResiliencyAssessment no AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

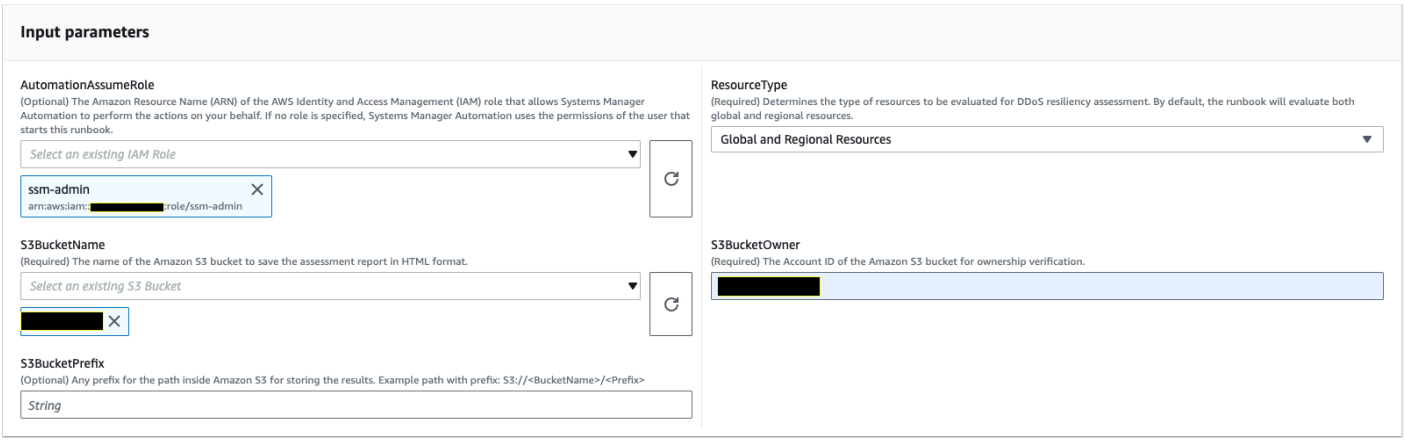
     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - AssessmentType (Opcional):

     Determina o tipo de recursos a avaliar para a avaliação da resiliência de DDoS. Por padrão, o runbook avalia os recursos globais e regionais.
   - S3 BucketName (obrigatório):

     O nome do bucket do Amazon S3 para salvar o relatório de avaliação no formato HTML.
   - S3 BucketOwner (opcional):

     O ID da Conta da AWS do bucket do Amazon S3 para verificação de propriedade. O ID da Conta da AWS é obrigatório se o relatório precisar ser publicado em um bucket do Amazon S3 com várias contas e opcional se o bucket do Amazon S3 estiver no mesmo nível do início da automação da Conta da AWS.
   - S3 BucketPrefix (opcional):

     Qualquer prefixo do caminho dentro do Amazon S3 para armazenar os resultados.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - CheckShieldAdvancedState:

     Verifica se o bucket do Amazon S3 especificado no “S3BucketName” permite permissões de acesso anônimo ou público de leitura ou gravação, se o bucket tem a criptografia em repouso ativada e se o Conta da AWS ID fornecido no “S3BucketOwner” é o proprietário do bucket do Amazon S3.
   - S3: BucketSecurityChecks

     Verifica se o bucket do Amazon S3 especificado no “S3BucketName” permite permissões de acesso anônimo ou público de leitura ou gravação, se o bucket tem a criptografia em repouso ativada e se o Conta da AWS ID fornecido no “S3BucketOwner” é o proprietário do bucket do Amazon S3.
   - BranchOnShieldAdvancedStatus:

     Ramifica etapas do documento com base no status da assinatura do AWS Shield Advanced e/ou no status de propriedade do Amazon S3 Bucket.
   - ShieldAdvancedConfigurationReview:

     Analisa as configurações do Shield Advanced para garantir que os detalhes mínimos necessários estejam presentes. Por exemplo: acesso IAM para equipe de resposta AWS Shield (SRT), detalhes da lista de contatos e status de engajamento proativo do SRT.
   - ListShieldAdvancedProtections:

Lista os recursos protegidos pelo Shield e cria um grupo de recursos protegidos para cada serviço.

- BranchOnResourceTypeAndCount:

  Ramifica etapas do documento com base no valor do parâmetro Tipo de recurso e no número de recursos globais protegidos pelo Shield.

- ReviewGlobalResources:

  Analisa os recursos globais protegidos pelo Shield Advanced, como zonas hospedadas, CloudFront distribuições e aceleradores globais do Route 53.

- BranchOnResourceType:

  Ramifica etapas do documento com base nas seleções do tipo de recurso, se global, regional ou ambas.

- ReviewRegionalResources:

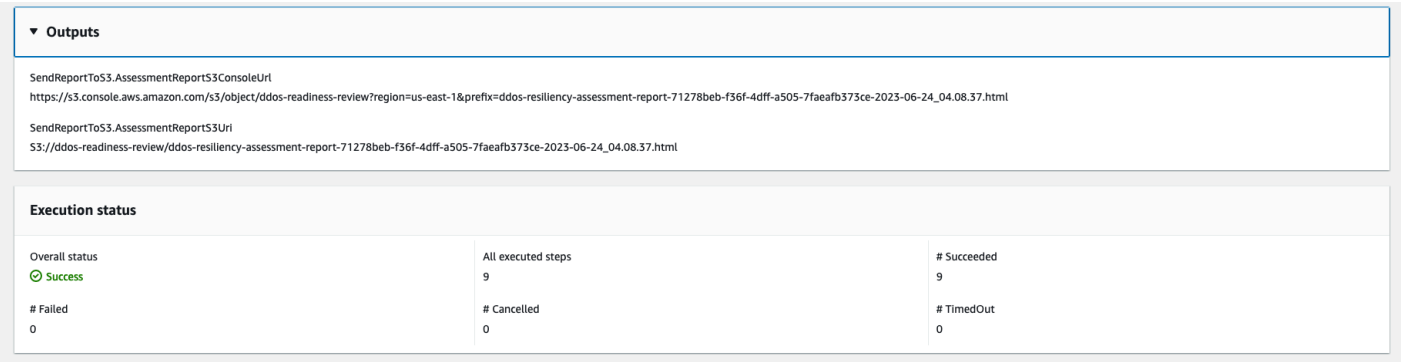
  Analisa os recursos regionais protegidos pelo Shield Advanced, como Application Load Balancers, Network Load Balancers, Classic Load Balancers e instâncias do Amazon Elastic Compute Cloud (Amazon EC2) (IPs elásticos).

- SendReportToS3:

  Carrega os detalhes do relatório de avaliação do tipo DDoS para o bucket do Amazon S3.

7. Depois de concluído, o URI do arquivo HTML do relatório de avaliação é fornecido no bucket do Amazon S3:

   Link do console S3 e URI do Amazon S3 para o relatório sobre a execução bem-sucedida do runbook



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSDocumentação do serviço

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Notification Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

`AWS-EnableSNSTopicDeliveryStatusLogging`

Descrição

O `AWS-EnableSNSTopicDeliveryStatusLogging` runbook configura o registro do status de entrega para um HTTP endpoint Amazon Data Firehose, Lambda ou Amazon Simple `Platform application` Queue Service (Amazon SQS). Isso permite que o Amazon SNS registre alertas com falha e uma porcentagem amostral de notificações de alerta bem-sucedidas na Amazon. CloudWatch Se o registro do status de entrega já estiver configurado para o tópico, o runbook substituirá a configuração existente pelos novos valores que você especificar para os parâmetros de entrada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EndpointType

  Tipo: string

  Valores válidos:
  - HTTP
  - Firehose
  - Lambda
  - Aplicativo
  - SQS

  Descrição: (Obrigatório) O tipo de endpoint de tópico do Amazon SNS para o qual você deseja registrar as mensagens de notificação de status de entrega.
- TopicArn

  Tipo: string

  Descrição: (Obrigatório) O ARN do tópico do Amazon SNS para o qual você deseja configurar o registro do status de entrega.

- SuccessFeedbackRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM que o Amazon SNS usa para enviar registros de mensagens de notificação bem-sucedidas. CloudWatch

- SuccessFeedbackSampleRate

  Tipo: string

  Valores válidos: 0-100

  Descrição: (Obrigatório) A porcentagem de mensagens bem-sucedidas a serem amostradas para o tópico especificado do Amazon SNS.

- FailureFeedbackRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM que o Amazon SNS usa para enviar registros de mensagens de notificação de falha. CloudWatch

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Etapas do documento

- `aws:executeAwsApi`- Aplica o valor do `SuccessFeedbackRoleArn` parâmetro ao tópico do Amazon SNS.
- `aws:executeAwsApi`- Aplica o valor do `SuccessFeedbackSampleRate` parâmetro ao tópico do Amazon SNS.

- `aws:executeAwsApi`- Aplica o valor do `FailureFeedbackRoleArn` parâmetro ao tópico do Amazon SNS.
- `aws:executeScript`- Confirma que o registro do status de entrega está ativado no tópico Amazon SNS.

Saídas

VerifyDeliveryStatusLoggingEnabled. GetTopicAttributesResponse - Resposta das operações `GetTopicAttributes` da API.

VerifyDeliveryStatusLoggingEnabled. VerifyDeliveryStatusLoggingEnabled - Mensagem indicando a verificação bem-sucedida do registro do status de entrega.

`AWSConfigRemediation-EncryptSNSTopic`

Descrição

O `AWSConfigRemediation-EncryptSNSTopic` runbook permite a criptografia no tópico do Amazon Simple Notification Service (Amazon SNS) que você especifica usando uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente. Esse runbook só deve ser usado como uma linha de base para garantir que os tópicos do Amazon SNS sejam criptografados de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar vários tópicos com diferentes chaves gerenciadas pelo cliente.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KmsKeyArn

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da chave gerenciada pelo cliente do AWS KMS que deseja usar para criptografar o tópico do Amazon SNS.

- TopicArn

  Tipo: string

  Descrição: (obrigatório) O ARN do tópico do Amazon SNS a ser criptografado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Etapas do documento

- `aws:executeAwsApi` :Criptografa o tópico do Amazon SNS especificado no parâmetro `TopicArn`.
- `aws:assertAwsResourceProperty` :Confirma que a criptografia está habilitada no tópico do Amazon SNS.

AWS-PublishSNSNotification

Descrição

Publicar uma notificação no Amazon SNS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Message

  Tipo: string

  Descrição: (obrigatório) A mensagem a ser incluída na notificação do SNS.
- TopicArn

  Tipo: string

  Descrição: (obrigatório) O ARN do tópico do SNS no qual publicar a notificação.

Amazon SQS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Queue Service (Amazon SQS). Para obter informações sobre como usar runbooks, consulte Trabalhado

com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWS-EnableSQSEncryption

Descrição

O `AWS-EnableSQSEncryption` runbook permite a criptografia em repouso para uma fila do Amazon Simple Queue Service (Amazon SQS). Uma fila do Amazon SQS pode ser criptografada com chaves gerenciadas do Amazon SQS (SSE-SQS) ou com AWS Key Management Service () chaves gerenciadas (SSE-KMS). AWS KMS A chave que você atribui à sua fila deve ter uma política de chaves que inclua permissões para todos os diretores autorizados a usar a fila. Com a criptografia ativada, as `ReceiveMessage` solicitações anônimas `SendMessage` e para a fila criptografada são rejeitadas.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- QueueUrl

  Tipo: string

  Descrição: (Obrigatório) A URL da fila do Amazon SQS na qual você deseja habilitar a criptografia.

- KmsKeyId

  Tipo: string

  Descrição: (Opcional) A AWS KMS chave a ser usada para criptografia. Esse valor pode ser um identificador global exclusivo, um ARN para um alias ou uma chave ou um nome de alias prefixado por “alias/”. Você também pode usar a chave AWS gerenciada especificando o alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

  Tipo: string

  Valores válidos: 60-86400

  Padrão: 300

  Descrição: (Opcional) O período de tempo, em segundos, em que uma fila do Amazon SQS pode reutilizar uma chave de dados para criptografar ou descriptografar mensagens antes de ligar novamente. AWS KMS

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Etapas do documento

- SelectKeyType (aws:branch): ramificações com base na chave especificada.

- PutAttributeSseKms (aws:executeAwsApi) - Atualiza a fila do Amazon SQS para usar a AWS KMS chave especificada para criptografia.
- PutAttributeSseSqs (aws:executeAwsApi) - Atualiza a fila do Amazon SQS para usar a chave padrão para criptografia.
- VerifySqsEncryptionKms (aws: assertAwsResource Propriedade) - Verifica se a criptografia está habilitada na fila do Amazon SQS.
- VerifySqsEncryptionDefault (aws: assertAwsResource Propriedade) - Verifica se a criptografia está habilitada na fila do Amazon SQS.

Step Functions

AWS Systems Manager A automação fornece runbooks predefinidos para AWS Step Functions (Step Functions). Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableStepFunctionsStateMachineLogging

AWS-EnableStepFunctionsStateMachineLogging

Descrição

O `AWS-EnableStepFunctionsStateMachineLogging` runbook ativa ou atualiza o registro na máquina de AWS Step Functions estado que você especificar. O nível mínimo de registro deve ser definido como`ALL`,`ERROR`, ou`FATAL`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Nível

  Tipo: string

  Valores válidos: ALL | ERROR | FATAL

  Descrição: (Obrigatório) A URL da fila do Amazon SQS na qual você deseja habilitar a criptografia.

- LogGroupArn

  Tipo: string

  Descrição: (Obrigatório) O ARN do grupo de CloudWatch logs do Amazon Logs para o qual você deseja enviar os registros da máquina de estado.

- StateMachineArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da máquina de estado na qual você deseja ativar o login.

- IncludeExecutionData

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Determina se os dados de execução estão incluídos nos registros.

- TracingConfiguration

  Tipo: booliano

Padrão: False

Descrição: (Opcional) Determina se AWS X-Ray o rastreamento está ativado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Etapas do documento

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- Atualiza a máquina de estado especificada com a configuração de registro especificada.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- Verifica se o registro foi ativado para a máquina de estado especificada.

Saídas

- EnableStepFunctionsStateMachineLogging.Response - Resposta da chamada da UpdateStateMachine API.

Systems Manager

AWS Systems Manager A automação fornece runbooks predefinidos para o Systems Manager. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-BulkDeleteAssociation
- AWS-BulkEditOpsItems

- AWS-BulkResolveOpsItems
- AWS-ConfigureMaintenanceWindows
- AWS-CreateManagedLinuxInstance
- AWS-CreateManagedWindowsInstance
- AWSConfigRemediation-EnableCWLoggingForSessionManager
- AWS-ExportOpsDataToS3
- AWS-ExportPatchReportToS3
- AWS-SetupInventory
- AWS-SetupManagedInstance
- AWS-SetupManagedRoleOnEC2Instance
- AWSSupport-TroubleshootManagedInstance
- AWSSupport-TroubleshootPatchManagerLinux
- AWSSupport-TroubleshootSessionManager

AWS-BulkDeleteAssociation

Descrição

O runbook `AWS-BulkDeleteAssociation` ajuda você a excluir até 50 associações do State Manager do Systems Manager por vez.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AssociationIds

  Tipo: StringList

  Descrição: (obrigatório): Uma lista separada por vírgulas de todos os IDs das associações que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:DeleteAssociation`

Etapas do documento

- `aws:executeScript` :Exclui as associações especificadas no parâmetro `AssociationIds`.

AWS-BulkEditOpsItems

Descrição

O `AWS-BulkEditOpsItems` runbook ajuda você a editar o status, a gravidade, a categoria ou a prioridade do AWS Systems Manager OpsItems. Essa automação pode editar OpsItems no máximo 50 por vez.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Categoria

  Tipo: string

  Valores válidos:

  - Disponibilidade
  - Custo
  - Nenhuma alteração
  - Performance
  - Recuperação
  - Segurança

  Padrão: No change

  Descrição: (Opcional) A nova categoria que você deseja especificar para os editados OpsItems.

- OpsItemIds

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos OpsItems IDs que você deseja editar (por exemplo, OI-xxxxxxxxxxxx, OI-xxxxxxxxxxxx).

- Prioridade

Tipo: string

Valores válidos:

- Nenhuma alteração
- 1
- 2
- 3
- 4
- 5

Padrão: No change

Descrição: (Opcional) A importância do editado OpsItems em relação aos outros OpsItems no sistema.

- Gravidade

  Tipo: string

  Valores válidos:

  - Nenhuma alteração
  - 1
  - 2
  - 3
  - 4

  Padrão: No change

  Descrição: (Opcional) A severidade da edição OpsItems.

- WaitTimeBetweenEditsInSecs

  Tipo: string

  Valores válidos: 0,0 a 2,0

  Padrão: 0.8

Descrição: (opcional) O tempo que a automação espera entre chamar a operação de `UpdateOpsItems`.

- Status

  Tipo: string

  Valores válidos:

  - InProgress
  - Nenhuma alteração
  - Abra o
  - Resolvido

  Padrão: No change

  Descrição: (Opcional) O novo status do editado OpsItems.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Etapas do documento

- `aws:executeScript`- Edita o OpsItems que você especificou no `OpsItemIds` parâmetro com base nos valores que você especifica para os `Status` parâmetros `Category` `PrioritySeverity`,, e.

AWS-BulkResolveOpsItems

Descrição

O `AWS-BulkResolveOpsItems` runbook resolve o AWS Systems Manager OpsItems que corresponde ao filtro que você especificou. Você também pode especificar um OpsItemId para

adicionar ao resolvido OpsItems usando o `OpsInsightsId` parâmetro. Se um valor para o parâmetro `S3BucketName` for especificado, um resumo do resultado será enviado para o bucket do Amazon Simple Storage Service (Amazon S3). Para receber uma notificação após o envio do resumo do resultado para o bucket do Amazon S3, especifique um valor para o parâmetro `SnsTopicArn`. Essa automação resolverá OpsItems no máximo 1.000 por vez.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Filtros

  Tipo: string

  Descrição: (Obrigatório) Os pares de filtros de valores-chave para retornar o OpsItems que você deseja resolver. Por exemplo, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Para saber mais sobre as opções disponíveis para filtrar OpsItems respostas, consulte OpsItemFiltersa Referência da AWS Systems Manager API.
- OpsInsightId

  Tipo: string

Descrição: (Opcional) O identificador de recurso relacionado que você deseja adicionar ao resolvido OpsItems.

- S3 BucketName

  Tipo: string

  Descrição: (opcional) O nome do bucket do Amazon S3 para o qual deseja enviar o resumo do resultado.

- SnsMessage

  Tipo: string

  Descrição: (opcional) A notificação que o Amazon Simple Notification Service (Amazon SNS) deverá enviar quando a automação for concluída.

- SnsTopicArn

  Tipo: string

  Descrição: (opcional) O ARN do tópico do Amazon SNS que deseja notificar quando o resumo do resultado for enviado para o Amazon S3.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Etapas do documento

- `aws:executeScript`- Reúne e resolve o problema OpsItems com base nos filtros que você especifica. Se um valor para o parâmetro `OpsInsightId` for especificado, o valor será adicionado como um recurso relacionado.
- `aws:executeScript` - Se você especificar um valor para o parâmetro `S3BucketName`, um resumo do resultado será enviado para o bucket do Amazon Simple Storage Service (Amazon S3).
- `aws:executeScript` :Se um valor para o parâmetro `SnsTopicArn` for especificado, uma notificação será enviada ao tópico do Amazon SNS após o envio do resumo do resultado para o Amazon S3, incluindo o valor do parâmetro `SnsMessage`, se especificado.

AWS-ConfigureMaintenanceWindows

Descrição

O runbook `AWS-ConfigureMaintenanceWindows` ajuda a habilitar ou desabilitar várias janelas de manutenção do Systems Manager.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- MaintenanceWindows

Tipo: StringList

Descrição: (obrigatório) Uma lista separada por vírgulas dos IDs das janelas de manutenção que deseja habilitar ou desabilitar.

- MaintenanceWindowsStatus

  Tipo: string

  Valores válidos: True | False

  Padrão: "False"

  Descrição: (obrigatório) Determina se as janelas de manutenção estão habilitadas ou desabilitadas. Especifique “True” para habilitar as janelas de manutenção e “False” para desabilitá-las.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Etapas do documento

- `aws:executeScript` :Reúne o status das janelas de manutenção especificadas no parâmetro `MaintenanceWindows` e habilita ou desabilita as janelas de manutenção.

AWS-CreateManagedLinuxInstance

Descrição

Criar uma instância do EC2 para o Linux que esteja configurada para o Systems Manager.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AmiId

  Tipo: string

  Descrição: (obrigatório) ID da AMI a ser usada para iniciar a instância.
- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- GroupName

  Tipo: string

  Padrão: SSM SecurityGroupForLinuxInstances

  Descrição: (obrigatório) Nome do grupo de segurança a ser criado.
- HttpTokens

  Tipo: string

  Valores válidos: optional | required

  Padrão: Optional

  Descrição: (opcional) O IMDSv2 usa sessões com token. Defina o uso de tokens HTTP como `optional` ou `required` para determinar se o IMDSv2 é opcional ou obrigatório.
- InstanceType

Tipo: string

Padrão: t2.medium

Descrição: (obrigatório) Tipo de instância a ser executada. O padrão é t2.medium.

- KeyPairName

  Tipo: string

  Descrição: (obrigatório) Par de chaves a ser usado ao criar a instância.

- RemoteAccessCidr

  Tipo: string

  Padrão: 0.0.0.0/0

  Descrição: (obrigatório) Cria grupo de segurança com porta para SSH (Intervalo de portas 22) aberta para IPs especificados pelo CIDR (o padrão é 0.0.0.0/0). Se o grupo de segurança já existe, ele não será modificado e regras não serão alteradas.

- RoleName

  Tipo: string

  Padrão: SSM ManagedInstanceProfileRole

  Descrição: (obrigatório) Nome da função a ser criada.

- StackName

  Tipo: string

  Padrão: CreateManagedInstanceStack {{automation:execution_id}}

  Descrição: (opcional) Especificar o nome da pilha usado por este runbook

- SubnetId

  Tipo: string

  Padrão: Default

Descrição: (obrigatório) A nova instância será implantada nessa sub-rede ou na sub-rede padrão se não for especificada.

- VpcId

  Tipo: string

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa Amazon Virtual Private Cloud (Amazon VPC) ou na Amazon VPC padrão se não for especificada.

AWS-CreateManagedWindowsInstance

Descrição

Criar uma instância do EC2 para o Windows Server que está configurado para o Systems Manager.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Parâmetros

- AmiId

  Tipo: string

  Padrão: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

Descrição: (obrigatório) ID da AMI a ser usada para iniciar a instância.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- GroupName

  Tipo: string

  Padrão: SSM SecurityGroupForLinuxInstances

  Descrição: (obrigatório) Nome do grupo de segurança a ser criado.

- HttpTokens

  Tipo: string

  Valores válidos: optional | required

  Padrão: Optional

  Descrição: (opcional) O IMDSv2 usa sessões com token. Defina o uso de tokens HTTP como `optional` ou `required` para determinar se o IMDSv2 é opcional ou obrigatório.

- InstanceType

  Tipo: string

  Padrão: t2.medium

  Descrição: (obrigatório) Tipo de instância a ser executada. O padrão é t2.medium.

- KeyPairName

  Tipo: string

  Descrição: (obrigatório) Par de chaves a ser usado ao criar a instância.

- RemoteAccessCidr

Tipo: string

Padrão: 0.0.0.0/0

Descrição: (obrigatório) Cria grupo de segurança com porta para RDP (Intervalo de portas 3389) aberta para IPs especificados pelo CIDR (o padrão é 0.0.0.0/0). Se o grupo de segurança já existe, ele não será modificado e regras não serão alteradas.

- RoleName

  Tipo: string

  Padrão: SSM ManagedInstanceProfileRole

  Descrição: (obrigatório) Nome da função a ser criada.

- StackName

  Tipo: string

  Padrão: CreateManagedInstanceStack {{automation:execution_id}}

  Descrição: (opcional) Especificar o nome da pilha usado por este runbook

- SubnetId

  Tipo: string

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa sub-rede ou na sub-rede padrão se não for especificada.

- VpcId

  Tipo: string

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa Amazon Virtual Private Cloud (Amazon VPC) ou na Amazon VPC padrão se não for especificada.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descrição

O AWSConfigRemediation-EnableCWLoggingForSessionManager runbook permite que as sessões do AWS Systems Manager Session Manager (Session Manager) armazenem os registros de saída em um grupo de registros da Amazon CloudWatch (CloudWatch).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DestinationLogGroup

  Tipo: string

  Descrição: (Obrigatório) O nome do grupo de CloudWatch registros.

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Etapas do documento

- `aws:executeScript`- Aceita o grupo de CloudWatch registros para atualizar o documento que armazena as preferências de registros de saída da sessão do Gerenciador de Sessões ou cria um caso ele não exista.

AWS-ExportOpsDataToS3

Descrição

Esse runbook recupera uma lista de OpsData resumos no AWS Systems Manager Explorer e os exporta para um objeto em um bucket específico do Amazon Simple Storage Service (Amazon S3).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- columnFields

  Tipo: StringList

  Descrição: (Obrigatório) campos de coluna a serem gravados no arquivo de saída.

- filtros

  Tipo: string

  Descrição: (Opcional) Filtros para a getOpsSummary solicitação.

- resultAttribute

  Tipo: string

  Descrição: (Opcional) O atributo de resultado da getOpsSummary solicitação.

- s3 BucketName

  Tipo: string

  Descrição: (obrigatória) o bucket do S3 onde deseja fazer download do arquivo de saída.

- snsSuccessMessage

  Tipo: string

  Descrição: (opcional) Mensagem a ser enviada quando o runbook terminar.

- snsTopicArn

  Tipo: string

  Descrição: (obrigatório) ARN do tópico do Amazon Simple Notification Service (Amazon SNS) a ser notificado quando o download for concluído.

- syncName

  Tipo: string

  Descrição: (Opcional) o nome da sincronização de dados do recurso.

Etapas do documento

getOpsSummaryEtapa — Recupera até 5.000 resumos de operações para exportar em um arquivo CSV agora.

Saídas

OpsData object — Se o runbook for executado com êxito, você encontrará o OpsData objeto exportado no bucket do S3 de destino.

AWS-ExportPatchReportToS3

Descrição

Esse runbook recupera listas de dados de resumo de patches e detalhes de patches no Patch Manager do AWS Systems Manager e as exporta para arquivos .csv em um bucket específico do Amazon Simple Storage Service (Amazon S3).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- assumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhuma função for especificada, a Automação do Systems Manager usará as permissões do usuário que executar esse documento.
- s3 BucketName

Tipo: string

Descrição: (obrigatório) O bucket do S3 onde deseja fazer download do arquivo de saída.

- snsTopicArn

  Tipo: string

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do tópico do Amazon Simple Notification Service (Amazon SNS) a ser notificado quando o download for concluído.

- snsSuccessMessage

  Tipo: string

  Descrição: (opcional) Texto da mensagem a ser enviada quando o runbook terminar.

- destinos

  Tipo: string

  Descrição: (obrigatório) O ID da instância ou um caractere curinga (*) para indicar se os dados de patch devem ser reportados para uma instância específica ou para todas as instâncias.

Etapas do documento

ExportReportStep — A ação dessa etapa depende do valor do `targets` parâmetro. Se os `targets` estiverem no formato de `instanceids=*`, a etapa recupera até 10.000 resumos de patches para instâncias em sua conta e exporta os dados para um arquivo .csv.

Se os `targets` estiverem no formato `instanceids=<instance-id>`, a etapa recupera o resumo do patch e todos os patches da instância especificada em sua conta e os exporta para um arquivo .csv.

Saídas

PatchSummaryObjeto /Patches — Se o runbook for executado com êxito, o objeto do relatório de patch exportado será baixado para o bucket do S3 de destino.

AWS-SetupInventory

Descrição

Criar uma associação de inventário do Systems Manager Inventory para uma ou mais instâncias gerenciadas. O sistema coleta metadados de suas instâncias de acordo com a programação na associação. Para obter mais informações, consulte AWS Systems Manager Inventário.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- Aplicações

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados sobre aplicativos instalados.
- AssociatedDocName

  Tipo: string

  Padrão: `AWS-GatherSoftwareInventory`

  Descrição: (opcional) O nome do runbook do SSM usado para coletar o inventário da instância gerenciada.
- AssociationName

  Tipo: string

  Descrição: (Opcional) Um nome para a associação de Inventário que será atribuído à instância.
- AssocWaitTime

Tipo: string

Padrão: PT5M

Descrição: (Opcional) A quantidade de tempo que deve pausar a coleta de inventário quando o horário de início da associação de Inventário for atingido. O tempo usa o formato ISO 8601.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- `AwsComponents`

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados para AWS componentes como amazon-ssm-agent.

- CustomInventory

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados de inventário personalizados.

- Arquivos

  Tipo: string

  Descrição: (Opcional) Colete metadados sobre arquivos em suas instâncias. Para obter mais informações sobre como coletar esse tipo de dados de inventário, consulte Trabalhando com arquivo e inventário de registro do Windows. Requer SSMAgent versão 2.2.64.0 ou posterior. Exemplo do Linux: `[{"Path":"/usr/bin", "Pattern": ["aws*", "*ssm*"],"Recursive":false},{"Path":"/var/log", "Pattern": ["amazon*.*"], "Recursive":true, "DirScanLimit":1000}]` Windows example: `[{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]`

- InstanceDetailedInformation

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete informações adicionais sobre a instância, incluindo o modelo da CPU, velocidade e o número de núcleos, entre outros.

- InstanceIds

  Tipo: string

  Padrão: *

  Descrição: (obrigatória) instâncias do EC2 que você deseja inventariar.

- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

- NetworkConfig

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados sobre configurações de rede.

- Saídas 3 BucketName

  Tipo: string

  Descrição: (opcional) O nome de um bucket Amazon S3 em que você deseja gravar dados de log de inventário.

- Saídas 3 KeyPrefix

  Tipo: string

Descrição: (opcional) Um prefixo de chaves do Amazon S3 (subpasta) em que você deseja gravar dados de log de inventário.

- OutputS3Region

  Tipo: string

  Descrição: (Opcional) O nome do Região da AWS local onde o Amazon S3 existe.

- Schedule

  Tipo: string

  Padrão: cron(0 */30 * * * ? *)

  Descrição: (Opcional) Uma expressão cron para a programação da associação de inventário. O padrão é a cada 30 minutos.

- Serviços

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional, somente sistema operacional Windows, requer SSMAgent versão 2.2.64.0 e posterior) Colete dados para configurações de serviço.

- WindowsRegistry

  Tipo: string

  Descrição: (Opcional) Colete metadados sobre as chaves de registro do Microsoft Windows. Para obter mais informações sobre como coletar esse tipo de dados de inventário, consulte Trabalhando com arquivo e inventário de registro do Windows. Requer SSM Agent versão 2.2.64.0 ou posterior. Exemplo: [{"Path” :"HKEY_CURRENT_CONFIG\ System”, "Recursive” :true}, {"Path” :"HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ “," “: [" amiName "]}] MachineImage ValueNames

- WindowsRoles

  Tipo: string

  Padrão: Habilitado

Descrição: (Opcional) Colete informações sobre funções do Windows na instância. Aplica-se apenas a sistemas operacionais Windows. Requer SSMAgent versão 2.2.64.0 ou posterior.

- WindowsUpdates

  Tipo: string

  Padrão: Habilitado

  Descrição: (Opcional) Colete dados sobre todas as atualizações do Windows na instância.

AWS-SetupManagedInstance

Descrição

Configure uma instância com uma função AWS Identity and Access Management (IAM) para acesso ao Systems Manager.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (obrigatória) o ID da instância do EC2 a ser configurada

- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

- RoleName

  Tipo: string

  Padrão: SSM RoleForManagedInstance

  Descrição: (opcional) o nome da função do IAM para a instância do EC2. Se essa função não existir, ela será criada. Ao especificar esse valor, verifique se a função contém a política gerenciada do AmazonSSM ManagedInstanceCore.

AWS-SetupManagedRoleOnEC2Instance

Descrição

Configure uma instância com a função IAM RoleForManagedInstance gerenciada por SSM para acesso ao Systems Manager.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (obrigatória) o ID da instância do EC2 a ser configurada
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- RoleName

  Tipo: string

  Padrão: SSM RoleForManagedInstance

  Descrição: (opcional) o nome da função do IAM para a instância do EC2. Se essa função não existir, ela será criada. Ao especificar esse valor, verifique se a função contém a política gerenciada do AmazonSSM ManagedInstanceCore.

AWSSupport-TroubleshootManagedInstance

Descrição

O runbook `AWSSupport-TroubleshootManagedInstance` ajuda a determinar por que uma instância do Amazon Elastic Compute Cloud (Amazon EC2) não reporta como gerenciada pelo AWS

Systems Manager. Este runbook analisa a configuração da VPC para a instância, incluindo regras de grupo de segurança, endpoints da VPC, regras de lista de controle de acesso (ACL) à rede e tabelas de rotas. Ele também confirma que um perfil de instância no AWS Identity and Access Management (IAM) que contém as permissões necessárias está anexado à instância.

> **Important**
>
> Esse runbook de automação não avalia as regras de IPv6.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância do Amazon EC2 que não está reportando como gerenciada pelo Systems Manager.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript` :Reúne o `PingStatus` da instância.
- `aws:branch` :Ramifica com base no fato de a instância já estar reportando conforme gerenciado pelo Systems Manager.
- `aws:executeAwsApi` :Reúne detalhes sobre a instância, incluindo a configuração da VPC.
- `aws:executeScript` :Se aplicável, reúne detalhes adicionais relacionados aos endpoints da VPC que foram implantados para uso com o Systems Manager e confirma que os grupos de segurança anexados ao endpoint da VPC permitem tráfego de entrada na porta TCP 443 da instância.

- `aws:executeScript` :Verifica se a tabela de rotas permite tráfego para o endpoint da VPC ou endpoints públicos do Systems Manager.
- `aws:executeScript` :Verifica se as regras de network ACL permite tráfego para o endpoint da VPC ou endpoints públicos do Systems Manager.
- `aws:executeScript` :Verifica se o tráfego de saída para o endpoint da VPC ou para os endpoints públicos do Systems Manager é permitido pelo grupo de segurança associado à instância.
- `aws:executeScript` :Verifica se o perfil de instância anexado à instância inclui uma política gerenciada que fornece as permissões necessárias.
- `aws:branch` :Ramifica com base no sistema operacional da instância.
- `aws:executeScript` :Fornece referência ao shell script do `ssmagent-toolkit-linux`.
- `aws:executeScript`- Fornece referência ao `ssmagent-toolkit-windows` PowerShell script.
- `aws:executeScript` :Gera a saída final para a automação.
- `aws:executeScript` :Se o `PingStatus` da instância for `Online`, retorna que a instância já é gerenciada pelo Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descrição

O `AWSSupport-TroubleshootPatchManagerLinux` runbook soluciona problemas comuns que podem causar uma falha de patch em nós gerenciados baseados em Linux usando o AWS Systems Manager recurso “Gerenciador de patches”. O objetivo principal desse runbook é identificar a causa raiz da falha do comando patch e sugerir um plano de remediação.

Como funciona?

O `AWSSupport-TroubleshootPatchManagerLinux` runbook considera o ID da instância/ID do comando do casal fornecido por você para a solução de problemas. Se nenhum ID de comando for fornecido, ele selecionará o último comando de patch com falha nos últimos 30 dias na instância fornecida. Depois de verificar o status do comando, o cumprimento dos pré-requisitos e a distribuição do sistema operacional, o runbook baixa e executa um pacote de análise de log. A saída inclui a causa raiz do problema, bem como a ação necessária para corrigir o problema.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

- Amazon Linux 2 e 2023
- Red Hat Enterprise Linux 8.X e 9.X
- Centos 8.X e 9.X
- USO 15.X

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-TroubleshootPatchManagerLinux`no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId (Obrigatório):

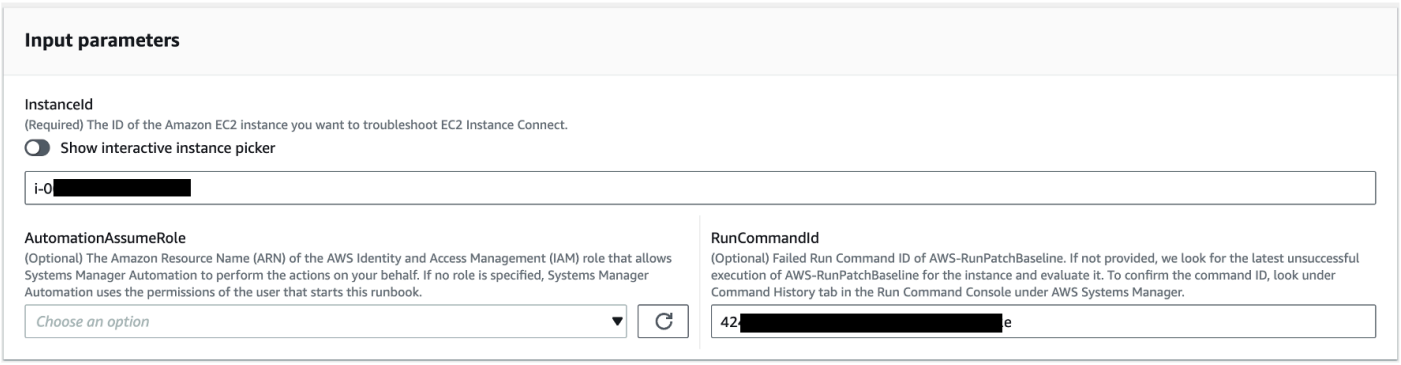
Use o seletor de instância interativo para escolher o ID do nó gerenciado SSM baseado em Linux (Amazon Elastic Compute Cloud (Amazon EC2) ou servidor Hybrid Activated) no qual o comando patch falhou, ou insira manualmente o ID da instância gerenciada do SSM.

- AutomationAssumeRole (Opcional):

  Insira o ARN da função do IAM que permite que a Automation execute ações em seu nome. Se uma função não for especificada, a automação usa as permissões do usuário que inicia esse runbook.

- RunCommandId (Opcional):

  Insira o ID do comando Failed Run do `AWS-RunPatchBaseline` documento. Se você não fornecer uma ID de comando, o runbook procurará o comando de patch com falha mais recente nos últimos 30 dias na instância selecionada.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckConcurrency:

     Garante que haja apenas uma execução desse runbook direcionada à mesma instância. Se o runbook encontrar outra execução em andamento visando a mesma instância, ele retornará um erro e terminará.

   - ValidateCommandID:

     Valida se o ID do comando fornecido, como parâmetro de entrada, foi executado para o documento `AWS-RunPatchBaseline` SSM. Se nenhum ID de comando for fornecido, o runbook considerará a última falha de execução dos `AWS-RunPatchBaseline` últimos 30 dias na instância selecionada.

- BranchOnCommandStatus:

  Confirma que o status do comando fornecido falhou. Caso contrário, o runbook encerra a execução e gera um relatório informando que o comando fornecido foi executado com sucesso.

- VerifyPrerequistes:

  Confirma que os pré-requisitos mencionados acima foram cumpridos.

- GetPlatformDetails:

  Recupera a distribuição e a versão do sistema operacional (OS).

- GetDownloadURL:

  Recupera a URL de download do pacote PatchManager Log Analyzer.

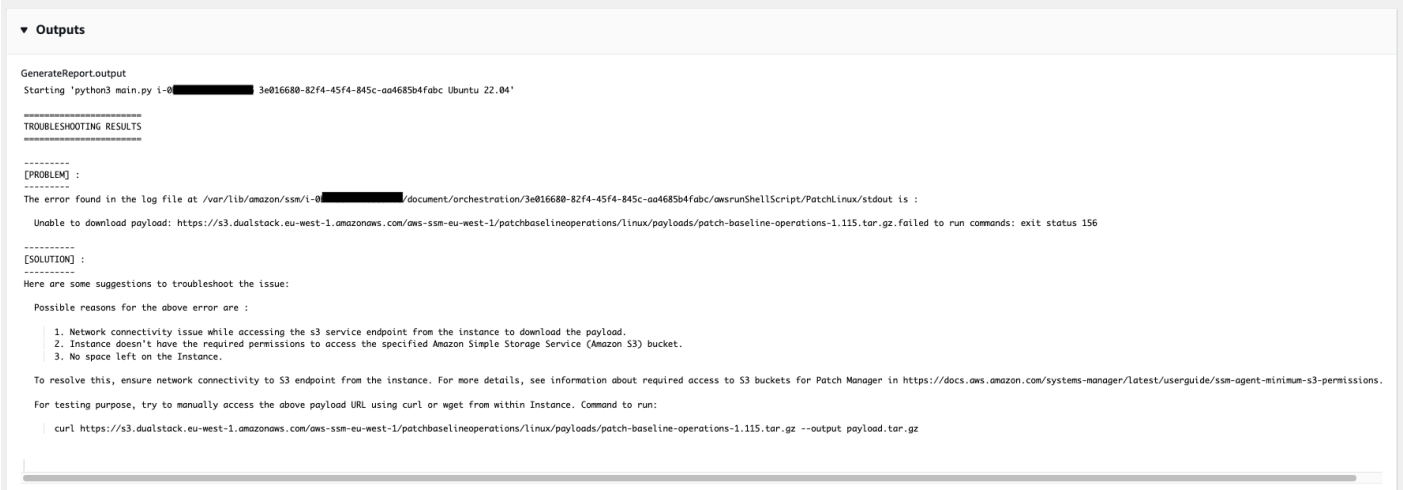
- EvaluatePatchManagerLogs:

  Faz o download e executa o pacote python do PatchManager Log Analyzer na instância para avaliar o arquivo de log.

- GenerateReport:

  Gera um relatório final da execução do runbook que inclui o problema identificado e a solução sugerida.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-TroubleshootSessionManager

Descrição

O runbook `AWSSupport-TroubleshootSessionManager` ajuda a solucionar problemas comuns que impedem a conexão com instâncias gerenciadas do Amazon Elastic Compute Cloud (Amazon EC2) usando o Session Manager. O Gerenciador de Sessões é um recurso de AWS Systems Manager. Este runbook verifica o seguinte:

- Verifica se a instância está sendo executada e reportada como gerenciada pelo Systems Manager.
- Executa o runbook `AWSSupport-TroubleshootManagedInstance` se a instância não estiver reportando como gerenciada pelo Systems Manager.
- Verifica a versão do SSM Agent instalado na instância.
- Verifica se um perfil de instância contendo uma política recomendada do AWS Identity and Access Management (IAM) para o Session Manager está anexado à instância do Amazon EC2.
- Coleta os logs do SSM Agent da instância.
- Analisa suas preferências do Session Manager.
- Executa o `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analisar a conectividade da instância com os endpoints do Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) e Amazon CloudWatch Logs (Logs). CloudWatch

Considerações

- Não há suporte para nós gerenciados híbridos.
- Esse runbook só verifica se uma política do IAM gerenciada recomendada está anexada ao perfil de instância. Ele não analisa o IAM nem as permissões do AWS KMS contidas no perfil de instância.

> **Important**
>
> O runbook `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` usa o VPC Reachability Analyzer para analisar a conectividade de rede entre uma fonte e um endpoint de serviço. Você é cobrado por análise executada entre a origem e o destino. Para obter mais detalhes, consulte Preço da Amazon VPC.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (obrigatório) O ID da instância do Amazon EC2 à qual não consegue se conectar com o Session Manager.
- SessionPreferenceDocument

  Tipo: string

Padrão: SSM- SessionManagerRunShell

Descrição: (opcional) O nome do seu documento de preferências de sessão. Se não for especificado um documento de preferências de sessão personalizado ao iniciar sessões, use o valor padrão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:waitForAwsResourceProperty: espera até 6 minutos para que sua instância de destino passe pelas verificações de status.
2. aws:executeScript: analisa o documento de preferência da sessão.
3. aws:executeAwsApi: obtém o ARN do perfil de instância anexado à sua instância.
4. aws:executeAwsApi: verifica se a instância está sendo executada e reportada como gerenciada pelo Systems Manager.
5. aws:branch: ramifica com base no fato de sua instância estar reportando como sendo gerenciada pelo Systems Manager.
6. aws:executeScript: verifica se o SSM agent instalado na sua instância é compatível com o Session Manager.
7. aws:branch: ramifica com base na plataforma da sua instância para coletar logs da ssm-cli.
8. aws:runCommand: coleta a saída de logs da ssm-cli de uma instância do Linux or macOS.
9. aws:runCommand: coleta a saída de logs da ssm-cli de uma instância do Windows.
10. aws:executeScript: analisa os logs da ssm-cli .
11. aws:executeScript: Esse runbook só verifica se uma política do IAM gerenciada recomendada está anexada ao perfil de instância.
12. aws:branch: determina se a conectividade do endpoint do ssmmessages deve ser avaliada com base nos logs da ssm-cli.
13. aws:executeAutomation: avalia se a instância pode se conectar a um endpoint do ssmmessages.
14. aws:branch: determina se a conectividade do endpoint Amazon S3 deve ser avaliada com base nos logs da ssm-cli e nas suas preferências de sessão.

15 `aws:executeAutomation`: avalia se a instância pode se conectar a um endpoint do Amazon S3.

16 `aws:branch`: determina se a conectividade do AWS KMS endpoint deve ser avaliada com base nos `ssm-cli` registros e nas suas preferências de sessão.

17 `aws:executeAutomation`: avalia se a instância pode se conectar a um AWS KMS endpoint.

18 `aws:branch`: determina se a conectividade do endpoint do CloudWatch Logs deve ser avaliada com base nos `ssm-cli` registros e nas suas preferências de sessão.

19 `aws:executeAutomation`: avalia se a instância pode se conectar a um endpoint do CloudWatch Logs.

20 `aws:executeAutomation`: executa o runbook `AWSSupport-TroubleshootManagedInstance`.

21 `aws:executeScript`: compila a saída das etapas anteriores e gera um relatório.

Saídas

- `generateReport.EvalReport` :Os resultados das verificações realizadas pelo runbook em texto simples.

Terceiros

AWS Systems Manager A automação fornece runbooks predefinidos para produtos e serviços de terceiros. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

`AWS-CreateJiraIssue`

Descrição

Cria um problema no Jira.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AssigneeName

  Tipo: string

  Descrição: (opcional) O nome de usuário da pessoa à qual o problema deve ser atribuído.
- DueDate

  Tipo: string

  Descrição: (Opcional) A data de vencimento da edição em yyyy-mm-dd formato.
- IssueDescription

  Tipo: string

  Descrição: (obrigatório) Uma descrição detalhada do problema.
- IssueSummary

  Tipo: string

  Descrição: (obrigatório) Um breve resumo do problema.
- IssueTypeName

  Tipo: string

  Descrição: (obrigatório) O nome do tipo do problema que você deseja criar (por exemplo, Tarefa, Subtarefa, Bug, etc.).

- JiraURL

  Tipo: string

  Descrição: (obrigatório) O URL da instância do Jira.
- JiraUsername

  Tipo: string

  Descrição: (obrigatório) O nome do usuário com o qual o problema será criado.
- PriorityName

  Tipo: string

  Descrição: (opcional) O nome da prioridade do problema.
- ProjectKey

  Tipo: string

  Descrição: (obrigatório) A chave do projeto no qual o problema deve ser criado.
- SSM ParameterName

  Tipo: string

  Descrição: (obrigatório) O nome de um parâmetro do SSM criptografado que contém a chave de API ou senha do usuário do Jira.

Etapas do documento

`aws:createStack`- Crie uma CloudFormation pilha para criar a função e a função do Lambda IAM.

`aws:invokeLambdaFunction` :Invocar a função do Lambda para criar o problema do Jira

`aws:deleteStack`- Exclua a CloudFormation pilha criada.

Saídas

IssueId: ID da edição recém-criada do Jira

AWS-CreateServiceNowIncident

Descrição

Crie um incidente na tabela de ServiceNow incidentes.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Categoria

  Tipo: string

  Descrição: (opcional) a categoria do incidente.

  Valores válidos: None | Inquiry/Help | Software | Hardware | Network | Database

  Valor padrão: None
- Descrição

  Tipo: string

  Descrição: (obrigatório) uma explicação detalhada sobre o incidente.
- Impacto

  Tipo: string

Descrição: (opcional) o efeito que um incidente tem sobre os negócios.

Valores válidos: High | Medium | Low

Valor padrão: Low

- ServiceNowInstanceUsername

  Tipo: string

  Descrição: (obrigatório) o nome do usuário com o qual o incidente será criado.

- ServiceNowInstancePassword

  Tipo: string

  Descrição: (Obrigatório) O nome de um parâmetro SSM criptografado contendo a senha do ServiceNow usuário.

- ServiceNowInstanceURL

  Tipo: string

  Descrição: (Obrigatório) O URL da ServiceNow instância

- ShortDescription

  Tipo: string

  Descrição: (obrigatório) uma breve descrição do incidente.

- Subcategory

  Tipo: string

  Descrição: (opcional) a subcategoria do incidente.

  Valores válidos: None | Antivirus | Email | Internal Application | Operating System | CPU | Disk | Keyboard | Hardware | Memory | Monitor | Mouse | DHCP | DNS | IP Address | VPN | Wireless | DB2 | MS SQL Server | Oracle

  Valor padrão: None

Etapas do documento

Push_incident — Envia as informações do incidente para. ServiceNow

Saídas

Push_incident.incidentID :O ID de incidente criado.

AWS-RunPacker

Descrição

Esse runbook usa a ferramenta HashiCorp Packer para validar, corrigir ou criar modelos de empacotador que são usados para criar imagens de máquina. Este runbook está usando o Packer v1.7.2.

> **Note**
>
> Se você especificar um valor de `vpc_id`, especifique também o valor de `subnet_id` de uma sub-rede pública. A menos que você modifique o atributo de endereçamento público IPv4 da sub-rede, defina `associate_public_ip_address` como true também.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Force

  Tipo: Booliano

  Descrição: uma opção da Packer para forçar um compilador a ser executado quando artefatos de uma compilação anterior impedirem que uma compilação seja executada.

- Modo

  Tipo: string

  Descrição: o modo, ou comando, no qual usar o Packer ao validar em relação ao modelo. As opções incluem `Build`, `Validate` e `Fix`.

- TemplateFileName

  Tipo: string

  Descrição: o nome ou a chave do arquivo de modelo no bucket do S3.

- Templates3 BucketName

  Tipo: string

  Descrição: o nome do bucket do S3 que contém o modelo do empacotador.

Etapas do documento

RunPackerProcessTemplate — Executa o modo selecionado em relação ao modelo usando a ferramenta Packer.

Saídas

RunPackerProcessTemplate.output — O stdout da ferramenta Packer.

RunPackerProcessTemplate.fixed_template_key — O nome do modelo armazenado em um bucket do S3 para ser usado somente quando executado no modo “Fix”.

RunPackerProcessTemplate.s3_bucket — O nome do bucket do S3 que contém o modelo fixo a ser usado somente quando executado no modo “Fix”.

Amazon VPC

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon Virtual Private Cloud. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

AWS-CloseSecurityGroup

Descrição

Esse runbook remove todas as regras de entrada e saída do grupo de segurança especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- SecurityGroupId

  Tipo: string

  Descrição: (Obrigatório) O ID do grupo de segurança que você deseja fechar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`

- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeScript`- Remove todas as regras de entrada e saída do grupo de segurança especificado no `SecurityGroupId` parâmetro.

AWSSupport-ConfigureDNSQueryLogging

Descrição

O runbook `AWSSupport-ConfigureDNSQueryLogging` configura o registro em log para consultas ao DNS que se originam em sua nuvem privada virtual (VPC) ou em zonas hospedadas do Amazon Route 53. Você pode optar por publicar registros de consulta no Amazon CloudWatch Logs, no Amazon Simple Storage Service (Amazon S3) ou no Amazon Data Firehose. Para obter mais informações sobre logs de consultas e logs de consultas do resolvedor, consulte log público de consultas ao DNS e log de consultas do resolvedor.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- LogDestinationArn

  Tipo: string

  Descrição: (Opcional) O ARN do grupo CloudWatch Logs, bucket do Amazon S3 ou stream do Firehose para o qual você deseja enviar registros de consulta. Observe que o registro de consultas DNS públicas do Route 53 só oferece suporte a grupos de CloudWatch registros. Se você não especificar um valor para esse parâmetro, a automação cria um grupo de CloudWatch registros com o formato `AWSSupport-ConfigureDNSQueryLogging-{automation:EXECUTION_ID}` e uma política de recursos do IAM para publicar os registros de consulta. O grupo de CloudWatch registros criado pela automação tem um período de retenção de 14 dias.

- QueryLogType

  Tipo: string

  Descrição: (opcional) Os tipos de consultas que deseja fazer o log.

  Valores válidos: Public | Resolver/Private

  Padrão: Public

- ResourceId

  Tipo: string

  Descrição: (obrigatório) O ID do recurso cujas consultas deseja fazer o log. Se `Public` for especificado para o parâmetro `QueryLogType`, o recurso deverá ser o ID de uma zona hospedada privada do Route 53. Se você especificar `Resolver/Private` para o parâmetro `QueryLogType`, o recurso deverá ser o ID de uma VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript` :Verifica se o recurso especificado para o parâmetro `ResourceId` existe e se o tipo de recurso corresponde à opção `QueryLogType` obrigatória.
- `aws:executeScript` :Verifica se o valor especificado para o parâmetro `LogDestinationArn` corresponde ao `QueryLogType` obrigatório.
- `aws:executeScript`- Verifica as permissões necessárias para o Route 53 publicar registros no grupo de CloudWatch registros de registros e cria a política de recursos do IAM necessária, caso ela não exista.
- `aws:executeScript` :Habilita o log de consultas ao DNS no destino selecionado.

AWSSupport-ConfigureTrafficMirroring

Descrição

O runbook `AWSSupport-ConfigureTrafficMirroring` configura o espelhamento de tráfego para ajudar a solucionar problemas de conectividade entre um balanceador de carga e as instâncias do Amazon Elastic Compute Cloud (Amazon EC2). O espelhamento de tráfego copia o tráfego de entrada e saída das interfaces de rede anexadas às suas instâncias. Para configurar o espelhamento de tráfego, esse runbook cria os destinos, filtros e sessões obrigatórios. Por padrão, o runbook configura o espelhamento para todo o tráfego de entrada e saída de todos os protocolos, exceto o Amazon DNS. Se quiser espelhar o tráfego de origens e destinos específicos, você pode modificar as regras de entrada e saída depois da conclusão da automação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- SourceENI

  Tipo: string

  Descrição: (obrigatório) A interface de rede elástica para a qual deseja configurar o espelhamento de tráfego.

- Destino

  Tipo: string

  Descrição: (obrigatório) O destino do tráfego espelhado. Você deve especificar o ID de uma interface de rede, um Network Load Balancer ou um endpoint do balanceador de carga de gateway. Se um Network Load Balancer for especificado, deverá haver receptores UDP na porta 4789.

- SessionNumber

  Tipo: string

  Valores válidos: 1 a 32766

  Descrição: (obrigatório) O número de sessão do espelho que deseja usar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:CreateTrafficMirrorTarget`

- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilter
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

Etapas do documento

- aws:executeScript :Executa um script para criar um destino.
- aws:executeAwsApi :Cria uma regra de filtro.
- aws:executeAwsApi :Cria uma regra de filtro do espelho para todo o tráfego de entrada.
- aws:executeAwsApi :Cria uma regra de filtro do espelho para todo o tráfego de saída.
- aws:executeAwsApi :Cria uma sessão do espelho de tráfego.
- aws:executeAwsApi :Exclui o filtro se a criação do filtro ou da sessão falhar.
- aws:executeAwsApi :Exclui o destino se a criação do filtro ou da sessão falhar.

Saídas

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget. Saída de ID de destino

AWSSupport-ConnectivityTroubleshooter

Descrição

O runbook AWSSupport-ConnectivityTroubleshooter diagnostica problemas de conectividade entre os seguintes:

- AWS recursos em uma Amazon Virtual Private Cloud (Amazon VPC)
- AWS recursos em diferentes Amazon VPCs dentro da mesma Região da AWS que estão conectados usando emparelhamento de VPC
- AWS recursos em uma Amazon VPC e um recurso da Internet usando um gateway da Internet
- AWS recursos em uma Amazon VPC e um recurso da Internet usando um gateway de tradução de endereços de rede (NAT)

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DestinationIP

  Tipo: string

  Descrição: (obrigatório) O endereço IPv4 do recurso ao qual deseja se conectar.
- DestinationPort

  Tipo: string

  Padrão: True

Descrição: (obrigatório) O número da porta à qual deseja se conectar no recurso de destino.

- DestinationVpc

  Tipo: string

  Padrão: All

  Descrição: (opcional) O ID da Amazon VPC com o qual deseja testar a conectividade.

- SourceIP

  Tipo: string

  Descrição: (Obrigatório) O endereço IPv4 privado do AWS recurso em sua Amazon VPC a partir do qual você deseja testar a conectividade.

- SourcePortRange

  Tipo: string

  Descrição: (Opcional) O intervalo de portas usado pelo AWS recurso em sua Amazon VPC a partir do qual você deseja testar a conectividade.

- SourceVpc

  Tipo: string

  Padrão: All

  Descrição: (opcional) O ID da Amazon VPC do qual deseja testar a conectividade.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Reúne detalhes sobre o AWS recurso que você especifica no `SourceIP` parâmetro.
- `aws:executeScript`- Determina o destino do tráfego de rede do AWS recurso usando as rotas coletadas na etapa anterior.
- `aws:branch` :Ramifica com base no destino do tráfego de rede.
- `aws:executeAwsApi` :Reúne detalhes sobre o recurso de destino.
- `aws:executeScript` :Confirma se o ID retornado para a Amazon VPC de destino corresponde ao valor especificado, se houver, no parâmetro `DestinationVpc`.
- `aws:executeAwsApi` :Reúne as regras de grupo de segurança para os recursos de origem e destino.
- `aws:executeScript` :Confirma se as regras de grupo de segurança permitem o tráfego necessário entre os recursos de origem e destino.
- `aws:executeAwsApi` :Reúne as listas de controle de acesso à rede (NACLs) associadas às sub-redes para os recursos de origem e destino.
- `aws:executeScript` - Confirma se as regras de grupo de segurança permitem o tráfego necessário entre os recursos de origem e destino.
- `aws:executeScript` :Confirma se a fonte tem um endereço IP público associado ao recurso, se o destino da rota for um gateway da internet.
- `aws:executeAwsApi` :Reúne as regras de grupo de segurança para os recursos de origem.
- `aws:executeScript` :Confirma se as regras de grupo de segurança permitem o tráfego necessário do recurso de origem para o destino.
- `aws:executeAwsApi` :Reúne as NACLs associadas à sub-rede para o recurso de origem.
- `aws:executeScript` :Confirma se as regras de grupo de segurança permitem o tráfego necessário do recurso de origem.
- `aws:executeAwsApi` :Reúne detalhes sobre o gateway NAT.
- `aws:executeAwsApi` :Reúne as NACLs associadas à sub-rede para o gateway NAT.
- `aws:executeScript` :Confirma se as NACLs permitem o tráfego necessário da sub-rede para o gateway NAT.
- `aws:executeScript` :Reúne as rotas associadas à sub-rede para o gateway NAT.
- `aws:executeScript` :Confirma se o gateway NAT tem uma rota para um gateway da Internet.

- `aws:executeAwsApi` :Reúne detalhes sobre a conexão de emparelhamento da VPC.
- `aws:executeScript` :Confirma se ambos os VPCs estão na mesma região e se o ID retornado para o VPC de destino corresponde ao valor especificado, se houver, no parâmetro `DestinationVpc`.
- `aws:executeAwsApi` :Retorna a sub-rede do recurso de destino.
- `aws:executeScript` :Reúne as rotas associadas à sub-rede para a VPC emparelhada.
- `aws:executeScript` :Confirma se a VPC emparelhada tem uma rota para a conexão de emparelhamento.
- `aws:executeScript` :Confirma se o tráfego é permitido a partir do recurso de origem se o destino não for suportado pela automação.

AWSSupport-TroubleshootVPN

Descrição

O runbook `AWSSupport-TroubleshootVPN` ajuda você a rastrear e resolver erros em uma conexão AWS Site-to-Site VPN. A automação inclui várias verificações automatizadas projetadas para rastrear erros `IKEv1` ou `IKEv2` relacionados aos túneis de conexão AWS Site-to-Site VPN. A automação tenta combinar erros específicos e sua resolução correspondente forma uma lista de problemas comuns.

Observação: esta automação não corrige os erros. Ele é executado no intervalo de tempo mencionado e verifica o grupo de registros em busca de erros no grupo de CloudWatch registros de VPN.

Como funciona?

O runbook executa uma validação de parâmetros para confirmar se o grupo de CloudWatch log da Amazon incluído no parâmetro de entrada existe, se há algum fluxo de log no grupo de log que corresponde ao registro de túneis VPN, se o ID de conexão VPN existe e se o endereço IP do túnel existe. Ele faz chamadas à API Logs Insights em seu grupo de CloudWatch registros que estão configuradas para registro de VPN.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LogGroupName

  Tipo: string

  Descrição: (Obrigatório) O nome do grupo de CloudWatch log da Amazon configurado para registro de AWS Site-to-Site VPN conexão

  Allowed-pattern: `^[\.\-_/#A-Za-z0-9]{1,512}`
- VpnConnectionId

  Tipo: string

  Descrição: (obrigatória) o ID da conexão do AWS Site-to-Site VPN para solução de problemas.

  Allowed-pattern: `^vpn-[0-9a-f]{8,17}$`
- TunnelAIPAddress

  Tipo: string

  Descrição: (obrigatório) o endereço IPv4 número 1 do túnel associado ao seu AWS Site-to-Site VPN.

  Allowed-pattern: `^((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

Tipo: string

Descrição: (opcional) o endereço IPv4 do túnel número 2 associado ao seu AWS Site-to-Site VPN.

Allowed-pattern: `^((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

  Tipo: string

  Descrição: (obrigatório) selecione a versão do IKE que você está usando. Valores permitidos: IKEv1, IKEv2

  Valores válidos: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  Tipo: string

  Descrição: (opcional) horário de início da análise de logs. Você pode usar StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod para análise de registros

  Allowed-pattern: `^\d{10}|^$`

- EndTimeinEpoch

  Tipo: string

  Descrição: (opcional) horário de término da análise de logs. Você pode usar StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod para análise de registros. Se for fornecido tanto StartTimeinEpoch/EndTimeinEpoch quanto LookBackPeriod , em seguida, LookBackPeriod tem precedência

  Allowed-pattern: `^\d{10}|^$`

- LookBackPeriod

  Tipo: string

  Descrição: (opcional) tempo de dois dígitos em horas para analisar o log. Intervalo válido: de 01 a 99 Esse valor tem precedência se você também fornecer StartTimeinEpoch e EndTime

  Allowed-pattern: `^(\d?[1-9]|[1-9]0)|^$`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Instruções

Observação: essa automação funciona nos grupos de CloudWatch registros configurados para o registro de túneis VPN, quando o formato de saída do registro é JSON.

Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-TroubleshootVPN no console. AWS Systems Manager
2. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - LogGroupName (Obrigatório):

     O nome do grupo de CloudWatch registros da Amazon a ser validado. Esse deve ser o grupo de CloudWatch registros configurado para o envio de registros pela VPN.
   - VpnConnectionId (Obrigatório):

     O ID de conexão AWS Site-to-Site VPN cujo grupo de logs é rastreado em busca de erro de VPN.
   - TunnelAIPAddress (obrigatório):

     O endereço IP do túnel A associado à sua conexão AWS Site-to-Site VPN.
   - TunnelBIPAddress (opcional):

O endereço IP do túnel B associado à sua conexão AWS Site-to-Site VPN.

- IKEVersion (obrigatório):

  Selecione qual versão de IKE você está usando. Valores permitidos: IKEv1, IKEv2.

- StartTimeinEpoch (Opcional):

  O início do intervalo de tempo a ser consultado em busca de erros. O intervalo é inclusivo, portanto, o horário de início especificado é incluído na consulta. Especificado como horário epoch, o número de segundos desde 1º de janeiro de 1970, 00:00:00 UTC.

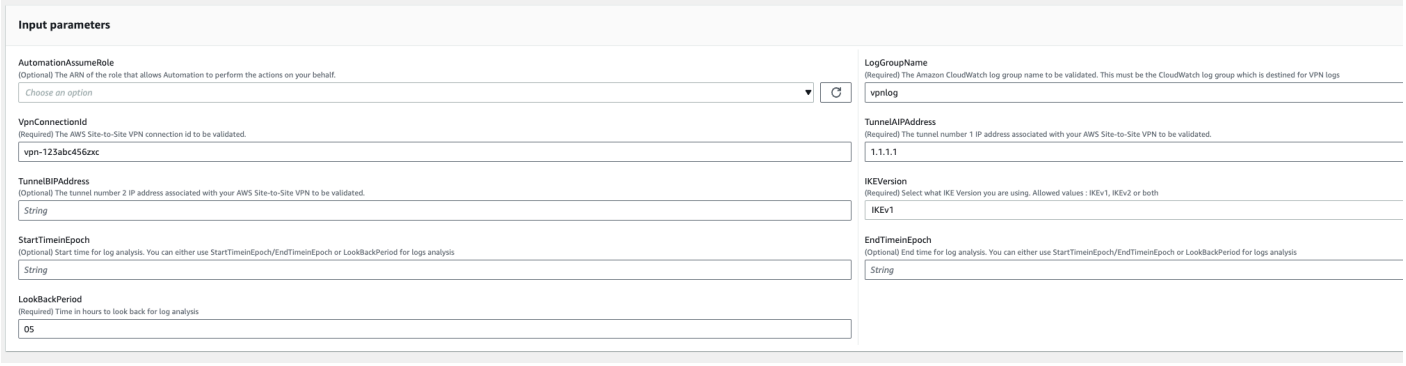
- EndTimeinEpoch (Opcional):

  O final do intervalo de tempo a ser consultado em busca de erros. O intervalo é inclusivo, portanto, o horário final especificado é incluído na consulta. Especificado como horário epoch, o número de segundos desde 1º de janeiro de 1970, 00:00:00 UTC.

- LookBackPeriod (Obrigatório):

  Tempo em horas para analisar a consulta em busca de erros.

Nota: Configure um StartTimeinEpoch, EndTimeinEpoch, ou LookBackPeriod para fixar o intervalo de tempo para análise de log. Forneça um número de dois dígitos em horas para verificar se há erros no passado a partir do horário de início da automação. Ou, se o erro estiver no passado dentro de um intervalo de tempo específico, inclua StartTimeinEpoch e EndTimeinEpoch, em vez de LookBackPeriod.



3. Selecione Executar.
4. A automação é iniciada.
5. O runbook de automação realiza as seguintes etapas:

   - parameterValidation:

Executa uma série de validações nos parâmetros de entrada incluídos na automação.

- branchOnValidationOfLogGroup:

  Verifica se o grupo de logs mencionado no parâmetro é válido. Se inválido, ele interrompe o início adicional das etapas de automação.

- branchOnValidationOfLogStream:

  Verifica se o fluxo de log existe no grupo de CloudWatch log incluído. Se inválido, ele interrompe o início adicional das etapas de automação.

- branchOnValidationOfVpnConnectionId:

  Verifica se o ID de conexão VPN incluído no parâmetro é válido. Se inválido, ele interrompe o início adicional das etapas de automação.

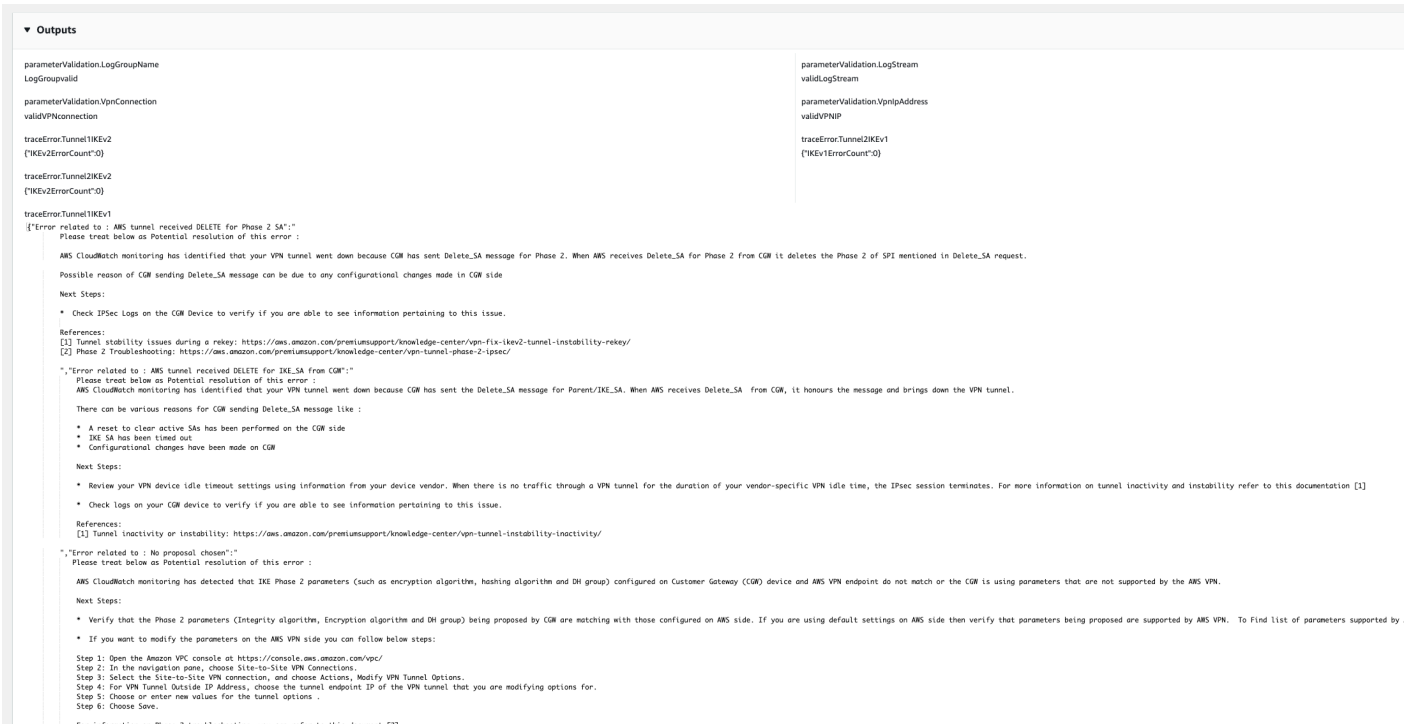
- branchOnValidationOfVpnIp:

  Verifica se o endereço IP do túnel mencionado no parâmetro é válido ou não. Se inválido, ele interrompe a execução adicional das etapas de automação.

- traceError:

  Faz uma chamada à API Logs Insight em seu grupo de CloudWatch registros incluído e pesquisa o erro relacionado a IKEv1/IKEv2 junto com uma sugestão de resolução relacionada.

6. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSDocumentação do serviço

- Conteúdo dos logs do Site-to-Site VPN

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descrição

O runbook `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` exclui o gateway da Internet somente de saída especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EgressOnlyInternetGatewayId

  Tipo: string

  Descrição: (obrigatório) O ID do Gateway da Internet somente de saída que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Etapas do documento

- `aws:executeScript` - Exclui o gateway da Internet de somente saída especificado no parâmetro `EgressOnlyInternetGatewayId`.

- `aws:executeScript` :Verifica se o gateway da Internet somente de saída foi excluído.

AWSConfigRemediation-DeleteUnusedENI

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedENI` exclui uma interface de rede elástica (ENI) que tem o status de anexo como `detached`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- NetworkInterfaceId

  Tipo: string

  Descrição: (obrigatório) O ID do ENI que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

Etapas do documento

- aws:executeAwsApi :Exclui a ENI especificada no parâmetro de NetworkInterfaceId.
- aws:executeScript - Verifica se o ENI foi excluído.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descrição

O runbook AWSConfigRemediation-DeleteUnusedSecurityGroup exclui o grupo de segurança especificado no parâmetro GroupId. Se você tentar excluir um grupo de segurança associado a uma instância Amazon Elastic Compute Cloud (Amazon EC2) ou referenciado por outro grupo de segurança, ocorrerá uma falha na operação. Essa automação não exclui um grupo de segurança padrão.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- GroupId

  Tipo: string

  Descrição: (obrigatório) O ID do grupo de segurança que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Etapas do documento

- `aws:executeAwsApi` :Retorna o nome do grupo de segurança usando o valor fornecido no parâmetro `GroupId`.
- `aws:branch` :Confirma que o nome do grupo não é “padrão”.
- `aws:executeAwsApi` - O runbook exclui o grupo de segurança especificado no parâmetro `GroupId`.
- `aws:executeScript` :Confirma que o grupo de segurança foi excluído.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` exclui uma lista de controle de acesso (ACL) de rede que não está associada a uma sub-rede.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- NetworkAclId

  Tipo: string

  Descrição: (obrigatório) O ID da ACL de rede que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeAwsApi` :Exclui a ACL de rede especificada no parâmetro `NetworkAclId`.
- `aws:executeScript`: confirma a rede ACL de rede especificada no parâmetro `NetworkAclId`.

AWSConfigRemediation-DeleteVPCFlowLog

Descrição

O runbook `AWSConfigRemediation-DeleteVPCFlowLog` exclui o log de fluxo da nuvem privada virtual (VPC) especificado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FlowLogId

  Tipo: string

  Descrição: (obrigatório) O ID do log do fluxo que você deseja reinicializar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Exclui o log de fluxo especificado no parâmetro `FlowLogId`.
- `aws:executeScript`- Verifica se o log de fluxo foi excluído.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Descrição

O runbook `AWSConfigRemediation-DetachAndDeleteInternetGateway` separa e exclui o gateway da internet especificado. Se alguma instância do Amazon EC2 em sua nuvem privada virtual (VPC) tiver endereços IP elásticos ou endereços IPv4 públicos associados, o runbook falhará.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- InternetGatewayId

Tipo: string

Descrição: (obrigatório) O ID do gateway da Internet que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Aceita a ID do gateway privado virtual e espera até que a propriedade de estado do gateway privado virtual mude para `available` ou expire o tempo limite.
- `aws:executeAwsApi` :Recupera uma configuração de gateway privado virtual especificada.
- `aws:branch`- Ramificações com base no valor do VpcAttachments parâmetro.state.

- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `attached` ou expire.
- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual e o ID da Amazon VPC como entrada e separa o gateway privado virtual da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `detached` ou expire.

- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual como entrada e o exclui.

- `aws:waitForAwsResourceProperty` :Aceita o ID do gateway privado virtual como entrada e verifica sua exclusão.

  `aws:executeAwsApi` :Reúne a ID da VPC a partir da ID do gateway da Internet.

- `aws:executeAwsApi` :Separa o ID do gateway da internet da VPC.
- `aws:executeAwsApi` :Exclui o gateway da Internet.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Descrição

O runbook `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` separa e exclui um determinado gateway privado virtual do Amazon Elastic Compute Cloud (Amazon EC2) anexada a uma nuvem privada virtual (VPC) criada com o Amazon Virtual Private Cloud (Amazon VPC).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- VpnGatewayId

  Tipo: string

  Descrição: (obrigatório) O ID do gateway privado virtual a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Aceita a ID do gateway privado virtual e espera até que a propriedade de estado do gateway privado virtual mude para `available` ou expire o tempo limite.
- `aws:executeAwsApi` :Recupera uma configuração de gateway privado virtual especificada.
- `aws:branch`- Ramificações com base no valor do VpcAttachments parâmetro.state.

- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `attached` ou expire.
- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual e o ID da Amazon VPC como entrada e separa o gateway privado virtual da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `detached` ou expire.

- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual como entrada e o exclui.

- `aws:waitForAwsResourceProperty` :Aceita o ID do gateway privado virtual como entrada e verifica sua exclusão.

AWS-DisableIncomingSSHOnPort22

Descrição

O `AWS-DisableIncomingSSHOnPort22` runbook remove regras que permitem tráfego SSH de entrada irrestrito na porta TCP 22 para grupos de segurança.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- SecurityGroupIds

  Tipo: string

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos IDs dos grupos de segurança para os quais você deseja restringir o tráfego SSH.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeAwsApi`- Remove todas as regras que permitem o tráfego SSH de entrada na porta TCP 22 dos grupos de segurança que você especifica no parâmetro. `SecurityGroupIds`

Saídas

DisableIncomingModelo SSH. RestrictedSecurityGroupIds - Uma lista dos IDs dos grupos de segurança que tiveram as regras SSH de entrada removidas.

`AWS-DisablePublicAccessForSecurityGroup`

Descrição

Esse runbook desabilita as portas SSH e RDP padrão que são abertas para todos os endereços IP.

> **Important**
>
> Este runbook falha com um "InvalidPermission. NotFound"erro para grupos de segurança que atendem aos dois critérios a seguir: 1) O grupo de segurança está localizado em uma VPC não padrão; e 2) As regras de entrada do grupo de segurança não especificam portas abertas usando todos os quatro padrões a seguir:
>
> - `0.0.0.0/0`
> - `::/0`
> - `SSH or RDP port + 0.0.0.0/0`
> - `SSH or RDP port + ::/0`

> **Note**
>
> Este runbook não está disponível na Regiões da AWS China.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- GroupId

  Tipo: string

  Descrição: (obrigatório) O ID do grupo de segurança para o qual as portas devem ser desabilitadas.
- IpAddressToBlock

  Tipo: string

  Descrição: (opcional) endereços IPv4 adicionais a partir dos quais o acesso deve ser bloqueado, no formato `1.2.3.4/32`.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descrição

O runbook `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` desabilita o atributo de endereçamento público IPv4 para a sub-rede especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- SubnetId

  Tipo: string

  Descrição: (obrigatório) O ID da sub-rede na qual deseja desabilitar o atributo de endereço IPv4 público de atribuição automática.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Etapas do documento

- `aws:executeAwsApi` :Desabilita a atribuição automática do atributo de endereço IPv4 público para a sub-rede especificada no parâmetro `SubnetId`.
- `aws:assertAwsResourceProperty` :Verifica se o atributo foi desabilitado.

AWSSupport-EnableVPCFlowLogs

Descrição

O runbook `AWSSupport-EnableVPCFlowLogs` cria logs de fluxo da Amazon Virtual Private Cloud (Amazon VPC) para sub-redes, interfaces de rede e VPCs em sua Conta da AWS. Se você criar um log de fluxo para uma sub-rede ou VPC, toda interface de rede na sub-rede ou Amazon VPC será monitorada. Os dados do log de fluxo são publicados no grupo de CloudWatch logs Amazon Logs ou no bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para obter mais informações sobre logs de fluxo, consulte Logs de fluxo no Guia do usuário da Amazon VPC.

> **Important**
>
> As taxas de ingestão e arquivamento de dados para registros vendidos se aplicam quando você publica registros de fluxo no Logs ou no CloudWatch Amazon S3. Para obter mais informações, consulte Precificação de logs de fluxo do .

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DeliverLogsPermissionArn

  Tipo: string

  Descrição: (Opcional) O ARN para a função do IAM que permite que o Amazon Elastic Compute Cloud (Amazon EC2) publique registros de fluxo no grupo de registros de registros CloudWatch em sua conta. Se especificar `s3` para o parâmetro `LogDestinationType`, não forneça um valor para esse parâmetro. Para obter mais informações, consulte Publicar registros de fluxo em CloudWatch registros no Guia do usuário da Amazon VPC.

- LogDestinationARN

  Tipo: string

  Descrição: (opcional) O ARN do recurso no qual os dados de log de fluxo são publicados. Se `cloud-watch-logs` for especificado para o `LogDestinationType` parâmetro, forneça o ARN do grupo de CloudWatch registros no qual você deseja publicar os dados do registro de fluxo. Como alternativa, use `LogGroupName`. Se `s3` for especificado para o parâmetro `LogDestinationType`, você deverá especificar o ARN do bucket do Amazon S3 no qual deseja publicar dados de log de fluxo para esse parâmetro. Você também pode especificar uma pasta no bucket.

- LogDestinationType

  Tipo: string

  Valores válidos: cloud-watch-logs | s3

  Descrição: (obrigatório) Determina onde os dados do log de fluxo são publicados. Se você especificar `LogDestinationType` como `s3`, não especifique `DeliverLogsPermissionArn` ou `LogGroupName`.

- LogFormat

  Tipo: string

  Descrição: (opcional) os campos a serem incluídos no log de fluxo e a ordem na qual eles devem aparecer no registro. Para obter uma lista de campos disponíveis, consulte Registros de logs de fluxo no Guia do usuário da Amazon VPC. Se não fornecer um valor para esse parâmetro, o log de fluxo será criado usando o formato padrão. Se você especificar esse parâmetro, deverá especificar pelo menos um campo.

- LogGroupName

Tipo: string

Descrição: (Opcional) O nome do grupo de registros de CloudWatch registros em que os dados do registro de fluxo são publicados. Se especificar `s3` para o parâmetro `LogDestinationType`, não forneça um valor para esse parâmetro.

- ResourceIds

  Tipo: StringList

  Descrição: (obrigatório) Uma lista separada por vírgulas dos IDs das sub-redes, interfaces de rede elástica ou VPC para a qual deseja criar um log de fluxo.

- TrafficType

  Tipo: string

  Valores válidos: ACCEPT | REJECT | ALL

  Descrição: (obrigatório) O tipo de tráfego para o log. Você pode registrar em log o tráfego que o recurso aceita ou rejeita ou todo o tráfego.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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:GetBucketAcl

Etapas do documento

- aws:branch :Ramificações com base no valor especificado para o parâmetro LogDestinationType.
- aws:executeScript :Cria um grupo de logs se nenhum valor for especificado para o parâmetro LogDestinationARN e for especificado cloud-watch-logs para o parâmetro LogDestinationType.
- aws:executeScript :Cria logs de fluxo com base nos valores especificados nos parâmetros do runbook.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Descrição

O AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch runbook substitui um log de fluxo existente do Amazon VPC que publica dados do log de fluxo no Amazon Simple Storage Service (Amazon S3) por um log de fluxo que publica dados do log de fluxo no grupo de log Amazon CloudWatch Logs (Logs) que você especificar. CloudWatch

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DestinationLogGroup

  Tipo: string

  Descrição: (Obrigatório) O nome do grupo de CloudWatch registros de registros no qual você deseja publicar os dados do registro de fluxo.
- DeliverLogsPermissionArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função AWS Identity and Access Management (IAM) que você deseja usar e que fornece ao Amazon Elastic Compute Cloud (Amazon EC2) as permissões necessárias para publicar dados de log de fluxo no Logs. CloudWatch
- FlowLogId

  Tipo: string

  Descrição: (obrigatório) O ID do log de fluxo publicado no Amazon S3 que deseja substituir.
- MaxAggregationInterval

  Tipo: inteiro

  Valores válidos: 60 | 600

Descrição: (opcional) o intervalo máximo de tempo, em segundos, durante o qual um fluxo de pacotes é capturado e agregado em um registro de log de fluxo.

- TrafficType

  Tipo: string

  Valores válidos: ACCEPT | REJECT | ALL

  Descrição: (obrigatório) O tipo de dados de log de fluxo que deseja registrar e publicar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Reúne detalhes sobre sua VPC a partir do valor especificado no parâmetro `FlowLogId`.
- `aws:executeAwsApi` :Cria um log de fluxo com base nos valores que especificados para os parâmetros do runbook.
- `aws:assertAwsResourceProperty`- Verifica se o registro de fluxo recém-criado é publicado no Logs. CloudWatch
- `aws:executeAwsApi` :Exclui o log de fluxo para publicação no Amazon S3.
- `aws:executeScript` :Confirma que o log de fluxo publicado no Amazon S3 foi excluído.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Descrição

O `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook substitui um log de fluxo existente da Amazon VPC que publica dados do log de fluxo no Amazon CloudWatch Logs (CloudWatch Logs) por um log de fluxo que publica dados do log de fluxo no bucket do Amazon Simple Storage Service (Amazon S3) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- Destinos 3 BucketArn

  Tipo: string

  Descrição: (obrigatório) O ARN do bucket do Amazon S3 no qual deseja publicar dados de log de fluxo.
- FlowLogId

  Tipo: string

  Descrição: (Obrigatório) O ID do registro de fluxo que é publicado nos CloudWatch registros que você deseja substituir.
- MaxAggregationInterval

Tipo: inteiro

Valores válidos: 60 | 600

Descrição: (opcional) o intervalo máximo de tempo, em segundos, durante o qual um fluxo de pacotes é capturado e agregado em um registro de log de fluxo.

- TrafficType

  Tipo: string

  Valores válidos: ACCEPT | REJECT | ALL

  Descrição: (obrigatório) O tipo de dados de log de fluxo que deseja registrar e publicar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Reúne detalhes sobre sua VPC a partir do valor especificado no parâmetro `FlowLogId`.
- `aws:executeAwsApi` :Cria um log de fluxo com base nos valores que especificados para os parâmetros do runbook.
- `aws:assertAwsResourceProperty` - Verifica se o log de fluxo recém-criado é publicado no Amazon S3.
- `aws:executeAwsApi`- Exclui o registro de fluxo que é publicado no Logs. CloudWatch
- `aws:executeScript`- Confirma que o registro de fluxo publicado no CloudWatch Logs foi excluído.

AWS-ReleaseElasticIP

Descrição

Libere o endereço IP elástico especificado usando o ID da alocação.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AllocationId

  Tipo: string

  Descrição: (obrigatório) O ID de alocação do endereço IP elástico.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descrição

O `AWS-RemoveNetworkACLUnrestrictedSSHRDP` runbook remove todas as regras da lista de controle de acesso (ACL) de rede da ACL de rede especificada que permitem o tráfego de

entrada de todos os endereços de origem para as portas SSH e RDP padrão. As regras que incluem intervalos de portas que se sobrepõem às portas SSH e RDP padrão não são removidas.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- NetworkAclId

  Tipo: string

  Descrição: (Obrigatório) A ID da ACL de rede da qual você deseja remover regras irrestritas que permitem o tráfego de entrada de todos os endereços de origem para as portas SSH e RDP padrão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeScript` :Remove todas as regras de entrada que permitem o tráfego de todos os endereços de origem do grupo de segurança especificado no parâmetro `SecurityGroupId`.

Saídas

RemoveNaclEntriesAndVerify. VerificationMessage - Mensagens de verificação das regras de ACL de rede excluídas com sucesso.

RemoveNaclEntriesAndVerify. RulesDeletedAndApiResponses - As regras de ACL de rede que foram excluídas e as respostas da operação `DeleteNetworkAclEntry` da API.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Descrição

O runbook `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` remove todas as regras de entrada do grupo de segurança especificado que permitem o tráfego de todos os endereços de origem.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- SecurityGroupId

  Tipo: string

  Descrição: (obrigatório) O ID do grupo de segurança do qual deseja remover as regras de entrada que permitem o tráfego de todos os endereços de origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeScript` :Remove todas as regras de entrada que permitem o tráfego de todos os endereços de origem do grupo de segurança especificado no parâmetro `SecurityGroupId`.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Descrição

O runbook `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` remove todas as regras do grupo de segurança padrão da nuvem privada virtual (VPC) especificada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- GroupId

  Tipo: string

  Descrição: (obrigatório) O ID do grupo de segurança do qual deseja remover todas as regras.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o grupo de segurança especificado no parâmetro `GroupId` tem o nome padrão.

- `aws:executeScript`: remove todas as regras do grupo de segurança que você especificou no parâmetro `GroupId`.

AWSSupport-SetupIPMonitoringFromVPC

Descrição

`AWSSupport-SetupIPMonitoringFromVPC` cria uma instância do Amazon Elastic Compute Cloud (Amazon EC2) na sub-rede especificada e monitora os IPs de destino selecionados (IPv4 ou IPv6) executando continuamente testes de ping, MTR, traceroute e tracetcp. Os resultados são armazenados nos CloudWatch registros do Amazon Logs e filtros métricos são aplicados para visualizar rapidamente as estatísticas de latência e perda de pacotes em um painel. CloudWatch

Informações adicionais

Os dados de CloudWatch registros podem ser usados para solução de problemas de rede e análise de padrões/tendências. Além disso, você pode configurar CloudWatch alarmes com notificações do Amazon SNS quando a perda e/ou a latência do pacote atingirem um limite. Os dados também podem ser usados ao abrir um caso com AWS Support, para ajudar a isolar um problema rapidamente e reduzir o tempo de resolução ao investigar um problema de rede.

> **Note**
>
> Para limpar os recursos criados pelo `AWSSupport-SetupIPMonitoringFromVPC`, é possível usar o runbook`AWSSupport-TerminateIPMonitoringFromVPC`. Para obter mais informações, consulte`AWSSupport-TerminateIPMonitoringFromVPC`

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CloudWatchLogGroupNamePrefix

  Tipo: string

  Padrão: / `AWSSupport-SetupIPMonitoringFromVPC`

  Descrição: (Opcional) Prefixo usado para cada grupo de CloudWatch registros criado para os resultados do teste.
- CloudWatchLogGroupRetentionInDays

  Tipo: string

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  Padrão: 7

  Descrição: (Opcional) O número de dias que você deseja manter os resultados de monitoramento de rede.
- InstanceType

  Tipo: string

  Valores válidos: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

  Padrão: t2.micro

  Descrição: (Opcional) O tipo de instância do EC2 para a instância EC2Rescue. Tamanho recomendado: t2.micro.

- SubnetId

  Tipo: string

  Descrição: (Obrigatório) O ID de sub-rede para a instância do monitor. Lembre-se de que, se você especificar uma sub-rede privada, deverá garantir que haja acesso à Internet para permitir que a instância do monitor configure o teste (ou seja, instale o agente CloudWatch Logs, interaja com o Systems Manager e CloudWatch).

- TargetIPs

  Tipo: string

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos IPv4s e/ou IPv6s a serem monitorados. Espaços não são permitidos. O tamanho máximo é de 255 caracteres. Lembre-se de que, se você fornecer um IP inválido, a automação falhará e reverterá a configuração de teste.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que o usuário que executa a automação tenha a política gerenciada do AutomationRole IAM do AmazonSSM anexada. Além disso, o usuário deve ter a política a seguir anexada à sua conta de usuário, grupo ou função:

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

Etapas do documento

1. **`aws:executeAwsApi`** :descreve a sub-rede fornecida.
2. **`aws:branch`**: avaliar a entrada TargetIPs.

   (IPv6) Se TargetIPs contém um IPv6:

   `aws:assertAwsResourceProperty`: verificar se a sub-rede fornecida tem um grupo de IPv6 associado
3. **`aws:executeScript`** :obtenha a arquitetura do tipo de instância e do caminho do parâmetro público para o AMI do Amazon Linux 2 mais recente.
4. **`aws:executeAwsApi`** :obtenha o AMI do Amazon Linux 2 mais recente na Parameter Store.
5. **`aws:executeAwsApi`**: criar um grupo de segurança para o teste na VPC da sub-rede.

   (Limpeza) Se a criação do grupo de segurança falhar:

aws:executeAwsApi - excluir o grupo de segurança criado pela automação, se existir.

6. **aws:executeAwsApi**: permitir a entrada de todo o tráfego de saída no grupo de segurança de teste.

   (Limpeza) Se a criação da regra de saída do grupo de segurança falhar:

   aws:executeAwsApi - excluir o grupo de segurança criado pela automação, se existir.

7. **aws:executeAwsApi** - criar um perfil do IAM para a instância do EC2 de teste

   (Limpeza) Se a criação da função falhar:

   a. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação, se existir.

   b. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

8. **aws:executeAwsApi**- anexar a política gerenciada do AmazonSSM ManagedInstanceCore

   (Limpeza) Se a anexação da política falhar:

   a. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação, se anexada.

   b. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

   c. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

9. **aws:executeAwsApi**- anexe uma política embutida para permitir a configuração de retenções de grupos de CloudWatch registros e a criação de um painel CloudWatch

   (Limpeza) Se a anexação da política em linha falhar:

   a. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação, se criada.

   b. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

   c. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

   d. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

10. **aws:executeAwsApi**: criar um perfil de instância do IAM

    (Limpeza) Se a criação do perfil de instância falhar:

    a. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação, se existir.

b. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

c. **aws:executeAwsApi**- exclua a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

d. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

e. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

11 **aws:executeAwsApi** - anexe o perfil de instância do IAM ao perfil do IAM.

(Limpeza) Se a associação do perfil de instância e da função falhar:

a. **aws:executeAwsApi** - remova o perfil de instância do IAM da função, se associado.

b. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

c. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

d. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

e. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

f. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

12 **aws:sleep** - aguarde que o perfil de instância fique disponível.

13 **aws:runInstances** - crie a instância de teste na sub-rede especificada e com o perfil de instância criada anteriormente anexado.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

14 **aws:branch**: avaliar a entrada TargetIPs.

(IPv6) Se TargetIPs contém um IPv6:

aws:executeAwsApi :atribua um IPv6 à instância de teste.

15 **aws:waitForAwsResourceProperty** :aguarde até que a instância de teste se torne uma instância gerenciada.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

16 **aws:runCommand** :instale os pré-requisitos de teste:

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

17 **aws:runCommand** - verifique se os IPs fornecidos estão sintaticamente corretos IPv4 e/ou endereços IPv6:

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

18 **aws:runCommand** - defina o teste MTR para cada um dos IPs fornecidos.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

19 **aws:runCommand** - defina o primeiro teste ping para cada um dos IPs fornecidos.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

20 **aws:runCommand** - defina o segundo teste ping para cada um dos IPs fornecidos.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

21 **aws:runCommand** - defina o teste tracepath para cada um dos IPs fornecidos.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

22 **aws:runCommand** - defina o teste traceroute para cada um dos IPs fornecidos.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

23 **aws:runCommand**- configurar CloudWatch registros.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

24 **aws:runCommand** - programe cronjobs para executar cada teste a cada minuto.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

25 **aws:sleep** - aguarde até que os testes gerem alguns dados.

26 **aws:runCommand**- defina as retenções de grupos de CloudWatch registros desejadas.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

27 **aws:runCommand**- defina os filtros métricos do grupo de CloudWatch registros.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

28 **aws:runCommand**- crie o CloudWatch painel.

(Limpeza) Se a etapa falhar:

a. **aws:executeAwsApi**- exclua o CloudWatch painel, se ele existir.

b. **aws:changeInstanceState** :encerre a instância de teste.

c. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

d. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

e. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

f. **aws:executeAwsApi**- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.

g. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

h. **`aws:executeAwsApi`** - excluir o grupo de segurança criado pela automação, se existir.

Saídas

createCloudWatchDashboards.Output - o URL do painel. CloudWatch

createManagedInstance. InstanceIds - o ID da instância de teste.

`AWSSupport-TerminateIPMonitoringFromVPC`

Descrição

O `AWSSupport-TerminateIPMonitoringFromVPC` encerra um teste de monitoramento de IP iniciado anteriormente pelo `AWSSupport-SetupIPMonitoringFromVPC`. Dados relacionados ao ID de teste especificado serão excluídos.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AutomationExecutionId

  Tipo: string

Descrição: (obrigatório) O ID de execução da automação de quando o runbook `AWSSupport-SetupIPMonitoringFromVPC` foi executado anteriormente. Todos os recursos associados a essa ID de execução são excluídos.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID de instância para a instância do monitor.

- SubnetId

  Tipo: string

  Descrição: (Obrigatório) O ID de sub-rede para a instância do monitor.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que o usuário que executa a automação tenha a política gerenciada do AutomationRole IAM do AmazonSSM anexada. Além disso, o usuário deve ter a política a seguir anexada ao seu usuário, grupo ou função:

```
{
"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"
    ]
}
```

Etapas do documento

1. `aws:assertAwsResourceProperty`- InstanceId verificam AutomationExecutionId e estão relacionados ao mesmo teste.
2. `aws:assertAwsResourceProperty`- InstanceId verificam SubnetId e estão relacionados ao mesmo teste.
3. `aws:executeAwsApi` :recupere o grupo de segurança do teste.
4. `aws:executeAwsApi`- exclua o CloudWatch painel.

5. `aws:changeInstanceState` :encerre a instância de teste.
6. `aws:executeAwsApi`: remover o perfil de instância do IAM da função.
7. `aws:executeAwsApi`: excluir o perfil de instância do IAM criado pela automação.
8. `aws:executeAwsApi`- exclua a política CloudWatch embutida da função criada pela automação.
9. `aws:executeAwsApi`- separe a política ManagedInstanceCore gerenciada do AmazonSSM da função criada pela automação.
10. `aws:executeAwsApi`: excluir o perfil do IAM criado pela automação.
11. `aws:executeAwsApi`: excluir o grupo de segurança criado pela automação, se existir.

Saídas

Nenhum

AWS WAF

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS WAF Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Descrição

O `AWS-AddWAFRegionalRuleToRuleGroup` runbook adiciona uma regra AWS WAF regional existente a um grupo de regras AWS WAF regionais. Somente grupos de regras regionais AWS WAF clássicos são suportados. AWS WAF Os grupos de regras regionais clássicos podem ter no máximo 10 regras.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- RuleGroupId

  Tipo: string

  Descrição: (Obrigatório) O ID do grupo de regras que você deseja atualizar.
- RulePriority

  Tipo: inteiro

  Descrição: (Obrigatório) A prioridade da nova regra. A prioridade da regra determina a ordem na qual as regras em um grupo regional são avaliadas. As regras com um valor menor têm maior prioridade do que as regras com um valor maior. O valor deve ser um inteiro exclusivo. Se você adicionar várias regras a um grupo de regras regional, os valores não precisarão ser consecutivos.
- RuleId

  Tipo: string

  Descrição: (Obrigatório) O ID da regra que você deseja adicionar ao seu grupo de regras regional.
- RuleAction

Tipo: string

Descrição: (Obrigatório) Especifica a ação que é AWS WAF executada quando uma solicitação da web corresponde às condições da regra.

Valores válidos: ALLOW | BLOCK | COUNT

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Etapas do documento

- GetWaf ChangeToken (aws:executeAwsApi) - Recupera um token de AWS WAF alteração para garantir que o runbook não envie solicitações conflitantes ao serviço.
- addWAF RuleTo WAF RegionalRuleGroup (aws:ExecuteScript) - Adiciona a regra especificada ao grupo de regras regional. AWS WAF
- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty) - Verifica se o token de alteração tem um status de `PENDING` ou`INSYNC`.
- VerifyRuleAddedToRuleGroup (aws:ExecuteScript) - Verifica se a AWS WAF regra especificada foi adicionada ao grupo de regras regionais de destino.

Saídas

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Saída da etapa de verificação de que a nova regra foi adicionada ao grupo de regras regional.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Saída da operação `ListActivatedRulesInRuleGroup` da API.

AWS-AddWAFRegionalRuleToWebAcl

Descrição

O AWS-AddWAFRegionalRuleToWebAcl runbook adiciona uma regra AWS WAF regional existente, um grupo de regras ou uma regra baseada em taxas a uma lista regional AWS WAF clássica de controle de acesso à web (ACL). Este runbook não atualiza as ACLs web regionais AWS WAF clássicas existentes que são gerenciadas pelo. AWS Firewall Manager

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- WebACLId

  Tipo: string

  Descrição: (Obrigatório) O ID da ACL da web que você deseja atualizar.
- ActivatedRulePriority

  Tipo: inteiro

Descrição: (Obrigatório) A prioridade da nova regra. A prioridade da regra determina a ordem na qual as regras em uma ACL da web são avaliadas. As regras com um valor menor têm maior prioridade do que as regras com um valor maior. O valor deve ser um inteiro exclusivo. Se você adicionar várias regras a uma ACL da web regional, os valores não precisarão ser consecutivos.

- ActivatedRuleRuleId

  Tipo: string

  Descrição: (Obrigatório) O ID da regra regular, regra baseada em taxa ou grupo que você deseja adicionar à Web ACL.

- ActivatedRuleAction

  Tipo: string

  Valores válidos: ALLOW | BLOCK | COUNT

  Descrição: (Opcional) Especifica a ação que é AWS WAF executada quando uma solicitação da web corresponde às condições da regra.

- ActivatedRuleType

  Tipo: string

  Valores válidos: REGULAR | RATE_BASED | GROUP

  Padrão: REGULAR

  Descrição: (Opcional) O tipo de regra que você está adicionando à ACL da web. Embora esse campo seja opcional, observe que, se você tentar adicionar uma `RATE_BASED` regra a uma ACL da web sem definir o tipo, a solicitação falhará porque a solicitação usa como padrão uma regra. `REGULAR`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`

- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Etapas do documento

- DetermineWebACL NotIn FMS AndRulePriority (aws:ExecuteScript) - Verifica se a AWS WAF ACL da web está em uma política de segurança do Firewall Manager e verifica se a ID de prioridade não está em conflito com uma ACL existente.
- AddRuleOrRuleGroupToWebACL (aws:ExecuteScript) - Adiciona a regra especificada à ACL da web. AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:ExecuteScript) - Verifica se a AWS WAF regra especificada foi adicionada à ACL da web de destino.

Saídas

- DetermineWebACL NotIn AndRulePriority FMS. PrereqResponse: Saída da `DetermineWebACLNotInFMSAndRulePriority` etapa.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Saída da `AddRuleOrRuleGroupToWebACL` etapa.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Saída da `VerifyRuleOrRuleGroupAddedToWebAcl` etapa.

AWSConfigRemediation-EnableWAFClassicLogging

Descrição

O `AWSConfigRemediation-EnableWAFClassicLogging` runbook permite registrar no Amazon Data Firehose (Firehose) a lista de controle de acesso AWS WAF à web (web ACL) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DeliveryStreamName

  Tipo: string

  Descrição: (Obrigatório) O nome do stream de entrega do Firehose para o qual você deseja enviar registros.
- WebACLId

  Tipo: string

  Descrição: (Obrigatório) A ID da ACL AWS WAF da web na qual você deseja ativar o login.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Etapas do documento

- `aws:executeAwsApi` :Confirma que o fluxo de entrega especificado no `DeliveryStreamName` existe.
- `aws:executeAwsApi`- Reúne o ARN da ACL AWS WAF da web especificada no parâmetro. `WebACLId`
- `aws:executeAwsApi` :Habilita o log da ACL da web.
- `aws:assertAwsResourceProperty`- Verifica se o registro foi ativado na ACL da AWS WAF web.

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Descrição

O `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook permite registrar no Amazon Data Firehose (Firehose) a lista de controle de acesso AWS WAF à web (ACL) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LogDestinationConfigs

Tipo: string

Descrição: (Obrigatório) O Amazon Resource Name (ARN) do stream de entrega do Firehose para o qual você deseja enviar registros.

- WebACLId

  Tipo: string

  Descrição: (Obrigatório) A ID da ACL AWS WAF da web na qual você deseja ativar o login.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Etapas do documento

- `aws:executeAwsApi`- Reúne o ARN da ACL AWS WAF da web especificada no parâmetro. `WebACLId`
- `aws:executeAwsApi` :Habilita o log da ACL da web.
- `aws:assertAwsResourceProperty`- Verifica se o registro foi ativado na ACL da AWS WAF web.

AWSConfigRemediation-EnableWAFV2Logging

Descrição

O `AWSConfigRemediation-EnableWAFV2Logging` runbook permite o registro de uma lista de controle de acesso à web AWS WAF (Web ACL) (AWS WAF V2) com o stream de entrega especificado do Amazon Data Firehose (Firehose).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LogDestinationConfigs

  Tipo: string

  Descrição: (Obrigatório) O ARN do stream de entrega do Firehose que você deseja associar à Web ACL.

  > **Note**
  >
  > O ARN do stream de entrega do Firehose deve começar com o prefixo. `aws-waf-logs-` Por exemplo, `aws-waf-logs-us-east-2-analytics`. Para obter mais informações, consulte Amazon Data Firehose.

- WebAclArn

  Tipo: string

  Descrição: (obrigatório) ARN da ACL da web para a qual o log será habilitado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Etapas do documento

- `aws:executeScript`- Ativa o registro para a ACL da web AWS WAF V2 e verifica se o registro tem a configuração especificada.

Amazon WorkSpaces

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. WorkSpaces Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

`AWS-CreateWorkSpace`

Descrição

O `AWS-CreateWorkSpace` runbook cria um novo desktop WorkSpaces virtual da Amazon, conhecido como a WorkSpace, com base nos valores que você especifica para os parâmetros de entrada. Para obter informações sobre WorkSpaces, consulte O que é a Amazon WorkSpaces? no Guia de WorkSpaces administração da Amazon.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BundleId

  Tipo: string

  Descrição: (Obrigatório) O ID do pacote a ser usado para o. WorkSpace
- ComputeTypeName

  Tipo: string

  Valores válidos: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  Descrição: (Opcional) O tipo de computação para o seu WorkSpace.
- DirectoryId

  Tipo: string

  Descrição: (Obrigatório) O ID do diretório ao qual você WorkSpace deve ser adicionado.
- RootVolumeEncryptionEnabled

Tipo: booliano

Valores válidos: True | False

Padrão: False

Descrição: (Opcional) Determina se o volume raiz do WorkSpace está criptografado.

- RootVolumeSizeGib

  Tipo: inteiro

  Descrição: (Obrigatório) O tamanho do volume raiz do WorkSpace.

- RunningMode

  Tipo: string

  Valores válidos: ALWAYS_ON | AUTO_STOP

  Descrição: (Obrigatório) O modo de execução do WorkSpace.

- RunningModeAutoStopTimeoutInMinutes

  Tipo: inteiro

  Descrição: (Opcional) O tempo após o usuário se desconectar quando WorkSpaces ele para. Especifique um valor em intervalos de 60 minutos.

- Tags

  Tipo: string

  Descrição: (Opcional) Tags que você deseja aplicar ao WorkSpace.

- UserName

  Tipo: string

  Descrição: (Obrigatório) O nome de usuário a ser associado ao WorkSpace.

- UserVolumeEncryptionEnabled

  Tipo: booliano

  Valores válidos: True | False

Padrão: False

Descrição: (Opcional) Determina se o volume do usuário do WorkSpace está criptografado.

- UserVolumeSizeGib

  Tipo: inteiro

  Descrição: (Obrigatório) O tamanho do volume do usuário para WorkSpace o.

- VolumeEncryptionKey

  Tipo: string

  Descrição: (Opcional) A AWS Key Management Service chave simétrica que você deseja usar para criptografar dados armazenados no seu. WorkSpace

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Etapas do documento

- `aws:executeScript`- Cria um WorkSpace com base nos valores que você especifica para os parâmetros de entrada.
- `aws:waitForAwsResourceProperty`- Verifica o estado do WorkSpace é`AVAILABLE`.

Saídas

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

Descrição

O `AWSSupport-RecoverWorkSpace` runbook executa etapas de recuperação no desktop WorkSpaces virtual da Amazon, conhecido como WorkSpace, que você especifica. O runbook

reinicia o e WorkSpace, se o estado persistirUNHEALTHY, restaura ou reconstrói o WorkSpace com base nos valores que você especifica para os parâmetros de entrada. Antes de usar este runbook, recomendamos revisar a solução de WorkSpaces problemas no Guia de WorkSpaces administração da Amazon.

> **Important**
>
> Restaurar ou reconstruir um WorkSpace é uma ação potencialmente destrutiva que pode resultar na perda de dados. Isso ocorre porque o WorkSpace é restaurado a partir do último instantâneo disponível e os dados recuperados dos instantâneos podem ter até 12 horas. A opção de restauração recria o volume raiz e o volume do usuário com base nos snapshots mais recentes. A opção de reconstrução recria o volume do usuário a partir do snapshot mais recente e o recria da imagem associada ao pacote a WorkSpace partir do qual foi criado. WorkSpace Os aplicativos que foram instalados ou as configurações do sistema que foram alteradas após a WorkSpace criação são perdidos. Para obter mais informações sobre restauração e reconstrução WorkSpaces, consulte Restore a WorkSpace e Rebuild WorkSpace a no Amazon WorkSpaces Administration Guide.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Reconhecer

  Tipo: string

  Valores válidos: yes

  Descrição: (Obrigatório) Digitar sim significa que você entende que as ações de restauração e reconstrução tentarão recuperar o WorkSpace do instantâneo mais recente e que os dados restaurados desses instantâneos podem ter até 12 horas.

- Reinicializar

  Tipo: string

  Valores válidos: sim | não

  Padrão: sim

  Descrição: (Obrigatório) Determina se o WorkSpace é reinicializado.

- Rebuild

  Tipo: string

  Valores válidos: sim | não

  Padrão: não

  Descrição: (Obrigatório) Determina WorkSpace se o foi reconstruído.

- Restaurar

  Tipo: string

  Valores válidos: sim | não

  Padrão: não

  Descrição: (Obrigatório) Determina se o WorkSpace é restaurado.

- WorkspaceId

  Tipo: string

Descrição: (Obrigatório) O ID do WorkSpace que você deseja recuperar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Etapas do documento

- `aws:executeAwsApi`- Reúne o estado do WorkSpace que você especifica no `WorkspaceId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica o estado do WorkSpace é`AVAILABLE`,`ERROR`, `IMPAIREDSTOPPED`, ou`UNHEALTHY`.
- `aws:branch`- Filiais com base no estado do WorkSpace.
- `aws:executeAwsApi`- Inicia WorkSpace o.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Action`.
- `aws:waitForAwsResourceProperty`- Aguarda o WorkSpace status após ser iniciado.
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para`AVAILABLE`, `ERRORIMPAIRED`, ou `UNHEALTHY` depois de ser iniciado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após o início.
- `aws:branch`- Filiais com base no estado do WorkSpace após o início.
- `aws:executeAwsApi`- Reúne os instantâneos disponíveis para restaurar ou reconstruir o. WorkSpace
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Reboot`.

- `aws:executeAwsApi`- Reinicia o. WorkSpace
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após o início.
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `REBOOTING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE` `ERROR`, ou `UNHEALTHY` depois de ser reinicializado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após a reinicialização.
- `aws:branch`- Ramificações com base no estado WorkSpace após a reinicialização.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Restore`.
- `aws:executeAwsApi`- Restaura o. WorkSpace Se a restauração falhar, o runbook tentará reconstruir o. WorkSpace
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `RESTORING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE` `ERROR`, ou `UNHEALTHY` depois de ser restaurado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após ser restaurado.
- `aws:branch`- Filiais com base no estado da restauração WorkSpace após a restauração.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Rebuild`.
- `aws:executeAwsApi`- Reconstrói o. WorkSpace
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE` `ERROR`, ou `UNHEALTHY` depois de ser reconstruído.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após a reconstrução.
- `aws:assertAwsResourceProperty`- Confirma o estado do WorkSpace é`AVAILABLE`.

X-Ray

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS X-Ray Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

Descrição

O `AWSConfigRemediation-UpdateXRayKMSKey` runbook permite a criptografia em seus AWS X-Ray dados usando uma chave AWS Key Management Service (AWS KMS). Esse runbook só deve ser usado como base para garantir que seus AWS X-Ray dados sejam criptografados de acordo com as melhores práticas mínimas de segurança recomendadas. Recomendamos criptografar vários conjuntos de dados com chaves KMS diferentes.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- KeyId

  Tipo: string

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave KMS que você deseja usar AWS X-Ray para criptografar dados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Etapas do documento

- `aws:executeAwsApi` :Habilita a criptografia em seus dados do X-Ray usando a chave do KMS especificada no parâmetro `KeyId`.
- `aws:waitForAwsResourceProperty` :Espera que o status da configuração da criptografia do X-Ray seja `ACTIVE`.
- `aws:executeAwsApi` :Reúne o ARN da chave especificada no parâmetro `KeyId`.
- `aws:assertAwsResourceProperty` :Verifica se a criptografia foi habilitada no seu X-Ray.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.