aws

Guía del usuario

AWS Systems Manager Referencia del manual de automatización

AWS Systems Manager Referencia del manual de automatización: Guía del usuario

Table of Contents

Referencia del manual de procedimientos de Systems Manager Automation

Para ayudarle a empezar rápidamente, AWS Systems Manager proporciona manuales de ejecución predefinidos. Estos manuales son mantenidos por Amazon Web Services, AWS Support, y AWS Config. La referencia del manual de ejecución describe cada uno de los manuales de ejecución predefinidos proporcionados por Systems Manager AWS Support, y. AWS Config

> **Important**
>
> Si ejecuta un flujo de trabajo de automatización que invoca otros servicios mediante un rol de servicio de AWS Identity and Access Management (IAM), tenga en cuenta que el rol de servicio debe configurarse con el permiso necesario para invocar dichos servicios. Este requisito se aplica a todos los manuales de procedimientos de Automatización de AWS (manuales de `AWS-*`), como los manuales de procedimientos `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup` y `AWS-RestartEC2Instance`, por nombrar algunos. Este requisito también se aplica a todos los manuales de automatización personalizados que cree y que invoquen otros AWS servicios mediante acciones que llamen a otros servicios. Por ejemplo, si utiliza las acciones `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, debe configurar el rol de servicio con el permiso necesario para invocar esos servicios. Puedes habilitar los permisos para otros AWS servicios añadiendo una política integrada de IAM al rol. Para obtener más información, consulte Añadir una política integrada de automatización para invocar otros servicios. AWS

Esta referencia incluye temas que describen cada uno de los manuales de ejecución de Systems Manager propiedad de AWS AWS Support, y AWS Config. Los manuales están organizados por los correspondientes. Servicio de AWS Cada página proporciona una explicación de los parámetros obligatorios y opcionales que se pueden especificar al utilizar el manual de procedimientos. Cada página también muestra una lista de los pasos que se indican en el manual de procedimientos y la salida de la automatización, si la hay.

Esta referencia no incluye una página separada para los manuales que requieren aprobación, como el manual de procedimientos `AWS-CreateManagedLinuxInstanceWithApproval` o `AWS-StopEC2InstanceWithApproval`. Cualquier nombre de manual de procedimientos que incluya

`WithApproval` significa que el manual de procedimientos incluye la acción `aws:approve`. Esta acción detiene temporalmente una automatización hasta que las entidades principales designadas aprueben o rechacen la acción. Después de que se alcanza el número necesario de aprobaciones, se reanuda la automatización.

Para obtener información acerca de la ejecución de las automatizaciones, consulte Ejecución de una automatización sencilla. Para obtener información sobre cómo ejecutar automatizaciones en varios objetivos, consulte Running automations that use targets and rate controls.

Temas

- Cómo ver contenido del manual de procedimientos
- API Gateway
- AWS Batch
- AWS CloudFormation
- CloudFront
- CloudTrail
- CloudWatch
- Amazon DocumentDB
- CodeBuild
- AWS CodeDeploy
- AWS Config
- Amazon Connect
- AWS Directory Service
- AWS AppSync
- Amazon Athena
- DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Elastic Beanstalk

- Elastic Load Balancing
- Amazon EMR
- OpenSearch Servicio Amazon
- EventBridge
- GuardDuty
- IAM
- Amazon Kinesis Data Streams
- AWS KMS
- Lambda
- Amazon Managed Workflows para Apache Airflow
- Neptune
- Amazon RDS
- Amazon Redshift
- Amazon S3
- SageMaker
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- De terceros
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

Cómo ver contenido del manual de procedimientos

Puede ver el contenido de los manuales de procedimientos en la consola de Systems Manager.

Cómo ver el contenido del manual de procedimientos

1. Abra la AWS Systems Manager consola en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.

   -o bien-

   Si la página de AWS Systems Manager inicio se abre primero, elija el icono de menú (☰) para abrir el panel de navegación y, a continuación, elija Documentos en el panel de navegación.
3. En la sección Categorías, seleccione Documentos de automatización.
4. Elija un manual de procedimientos y, a continuación, elija View details (Ver detalles).
5. Elija la pestaña Content.

API Gateway

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon API Gateway. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

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

AWSConfigRemediation-DeleteAPIGatewayStage

Descripción

El `AWSConfigRemediation-DeleteAPIGatewayStage`runbook elimina una etapa de Amazon API Gateway (API Gateway). AWS Configdebe estar habilitado en el Región de AWSlugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- Stagearn

  Tipo: String

  Descripción: (Obligatorio) El nombre de recurso de Amazon (ARN) de la etapa API Gateway que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Elimina la etapa de API Gateway especificada en el `StageArn`parámetro.

`AWSConfigRemediation-EnableAPIGatewayTracing`

Descripción

El `AWSConfigRemediation-EnableAPIGatewayTracing`grunbook permite el rastreo en una etapa de Amazon API Gateway (API Gateway). AWS Configdebe estar habilitado en el Región de AWSlugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- Stagearn

  Tipo: String

  Descripción: (obligatorio) El nombre de recurso de Amazon (ARN) de la etapa de API Gateway en la que desea habilitar el seguimiento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Habilita el rastreo en la etapa API Gateway especificada en el `StageArn`parámetro.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descripción

El `AWSConfigRemediation-UpdateAPIGatewayMethodCaching`grunbook actualiza la configuración del método de caché para un recurso de etapa de Amazon API Gateway.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: String

Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.

- Almacenamiento en caché de métodos autorizados

  Tipo: StringList

  Descripción: (Obligatorio) Los métodos autorizados para habilitar el almacenamiento en caché. La lista debe ser una combinación de `DELETEGET`,`HEAD`,`OPTIONS`, `PATCHPOST`, y`PUT`. El almacenamiento en caché está habilitado para los métodos seleccionados y deshabilitado para los métodos no seleccionados. El almacenamiento en caché está habilitado para todos los métodos si `ANY`está seleccionado y está deshabilitado para todos los métodos si `NONE`está seleccionado.

- StageArn

  Tipo: String

  Descripción: (Obligatorio) El ARN de la etapa API Gateway para la `RESTAPI`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Acepta el ID de recurso de la etapa como entrada, actualiza la configuración del método de caché para una etapa de API Gateway mediante la acción de la `UpdateStage`API y verifica la actualización.

AWS Batch

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Batch Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

Descripción

El `AWSSupport-TroubleshootAWSBatchJob` manual le ayuda a solucionar los problemas que impiden que un AWS Batch trabajo pase de un estado a `RUNNABLE` otro. `STARTING`

¿Cómo funciona?

Este manual realiza las siguientes comprobaciones:

- Si el entorno informático está en `DISABLED` estado `INVALID` o.
- Si el `Max vCPU` parámetro del entorno de cómputo es lo suficientemente grande como para acomodar el volumen de trabajos de la cola de trabajos.
- Si los trabajos requieren más vCPU o recursos de memoria de los que pueden proporcionar los tipos de instancias del entorno de procesamiento.
- Si los trabajos deben ejecutarse en instancias basadas en GPU, pero el entorno de procesamiento no está configurado para usar instancias basadas en GPU.
- Si el grupo de Auto Scaling del entorno de cómputo no pudo lanzar las instancias.
- Si las instancias lanzadas pueden unirse al clúster subyacente de Amazon Elastic Container Service (Amazon ECS); de lo contrario, ejecuta AWSSupport el runbook -TroubleShootecs. ContainerInstance
- Si algún problema con los permisos bloquea acciones específicas necesarias para ejecutar el trabajo.

Important

- Este manual debe iniciarse en la misma AWS región en la que se encuentra el trabajo cuyo `RUNNABLE` estado está estancado.
- Este manual se puede iniciar para los AWS Batch trabajos programados en instancias de Amazon ECS AWS Fargate o Amazon Elastic Compute Cloud (Amazon EC2). Si se inicia la automatización para un AWS Batch trabajo en Amazon Elastic Kubernetes Service (Amazon EKS), la iniciación se detiene.
- Si hay instancias disponibles para ejecutar el trabajo pero no registran el clúster de Amazon ECS, este manual de ejecución inicia el manual de `AWSSupport-TroubleshootECSContainerInstance` automatización para intentar determinar el motivo. Para obtener más información, consulte el manual de ejecución de - TroubleShootecsAWSSupport. ContainerInstance

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- JobId

  Tipo: cadena

  Descripción: (Obligatorio) El ID del AWS Batch Job cuyo RUNNABLE estado está atascado.

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

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

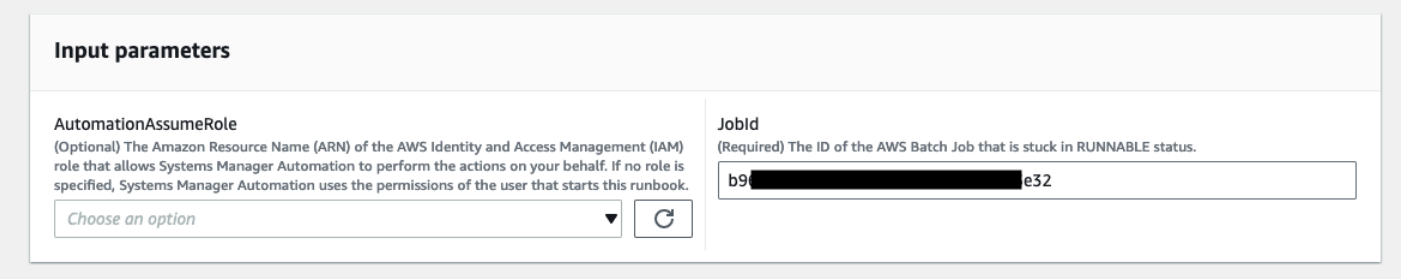
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ecs:DescribeClusters
- ecs:DescribeContainerInstances
- ecs:ListContainerInstances
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions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

Instrucciones

1. Navegue hasta la sección AWSSupportSolución de problemas AWSBatchJob en la AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización)
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
   - JobId (Obligatorio):

     El ID del AWS Batch Job que está atascado en el RUNNABLE estado.



4. Seleccione Ejecutar.
5. Observe que se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - PreflightPermissionChecks:

     Realiza comprobaciones previas a la verificación de los permisos de IAM con el usuario o rol iniciador. Si falta algún permiso, en este paso se indican las acciones de la API que faltan en la sección de resultados globales.
   - ProceedOnlyIfUserHasPermission:

     Se ramifica en función de si tiene permisos para realizar todas las acciones necesarias para el manual.
   - AWSBatchJobEvaluation:

     Realiza comprobaciones con respecto al AWS Batch Job para comprobar que existe y se encuentra en ese `RUNNABLE` estado.
   - ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

     Se ramifica en función de si los trabajos existen y se encuentran en ese `RUNNABLE` estado.
   - BatchComputeEnvironmentEvaluation:

     Realiza comprobaciones con respecto al entorno AWS Batch informático.
   - ProceedOnlyIfComputeEnvironmentChecksAreDe acuerdo:

     Las ramas se basan en si las comprobaciones del entorno de cómputo se realizaron correctamente.
   - UnderlyingInfraEvaluation:

     Realiza comprobaciones con respecto a la solicitud subyacente de Auto Scaling Group o Spot Fleet.

- ProceedOnlyIfInstancesNotJoiningEcsClúster:

  Las sucursales se basan en si hay instancias que no se unen al clúster de Amazon ECS.

- EcsAutomationRunner:

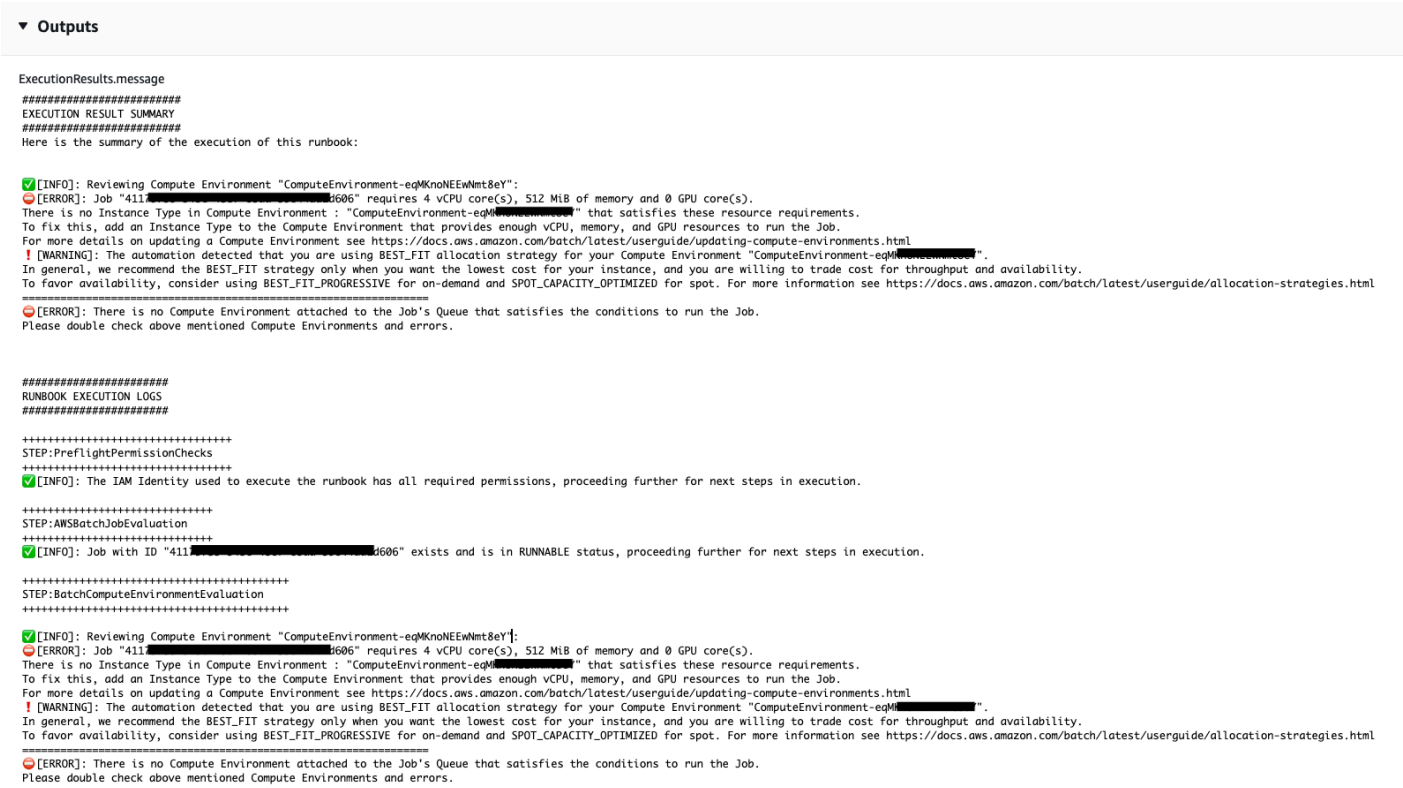
  Ejecuta la automatización de Amazon ECS para las instancias que no se unen al clúster.

- ExecutionResults:

  Genera resultados en función de los pasos anteriores.

7. Una vez completados, se proporciona el URI del archivo HTML del informe de evaluación:

   Enlace a la consola S3 y URI de Amazon S3 para el informe sobre la ejecución correcta del manual de procedimientos



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización

- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS CloudFormation

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CloudFormation Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

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

`AWS-DeleteCloudFormationStack`

Descripción

Elimine una pila de AWS CloudFormation.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- StackNameOrId

  Tipo: String

  Descripción: (Obligatorio) nombre o ID único de la pila de CloudFormation que se va a eliminar

AWS-EnableCloudFormationSNSNotification

Descripción

El `AWS-EnableCloudFormationSNSNotification` runbook habilita las notificaciones del Amazon Simple Notification Service (Amazon SNS) para la pila AWS CloudFormation (AWS CloudFormation) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- StackArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN o el nombre de la AWS CloudFormation pila para la que desea habilitar las notificaciones de Amazon SNS.

- NotificationArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del tema de Amazon SNS que desea asociar a la pila. AWS CloudFormation

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- formación de nubes: DescribeStacks
- formación de nubes: UpdateStack
- kms:Decrypt
- kms: GenerateDataKey
- sns:Publish
- sqs: GetQueueAttributes

Pasos de documentos

- CheckCfnSnsLimits (AWS:ExecuteScript): verifica el número máximo de temas de Amazon SNS que aún no se han asociado a la pila que especifique. AWS CloudFormation

- EnableCfnSnsNotification (aws:executeAwsApi) - Activa las notificaciones de Amazon SNS para la AWS CloudFormation pila.
- VerificationCfnSnsNotification (AWS:Executescript): verifica que las notificaciones de Amazon SNS estén habilitadas para la pila. AWS CloudFormation

Salidas

CheckCfnSnsLimits. NotificationArnList - Una lista de los ARN que reciben notificaciones de Amazon SNS para AWS CloudFormation la pila.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Respuesta de la operación de API que confirma que las notificaciones de Amazon SNS están habilitadas para la AWS CloudFormation pila.

AWS-RunCfnLint

Descripción

Este manual de procedimientos utiliza un Linter de AWS CloudFormation(`cfn-python-lint`) para validar plantillas YAML y JSON respecto a la especificación de recurso de AWS CloudFormation. El manual de procedimientos `AWS-RunCfnLint`realiza comprobaciones adicionales, como asegurarse de que se han introducido valores válidos para las propiedades de los recursos. Si la validación no se realiza correctamente, el paso `RunCfnLintAgainstTemplate`produce un error y la salida de la herramienta de linter se proporciona en un mensaje de error. Este manual de procedimientos utiliza cfn-lint v0.24.4.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: String

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- ConfigureRuleFlag

  Tipo: String

  Descripción: (Opcional) opciones de configuración que una regla pasará al parámetro `--configure-rule`.

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

- FormatFlag

  Tipo: String

  Descripción: (Opcional) valor que se pasa al parámetro `--format`para especificar el formato de salida.

  Valores válidos: Predeterminado | inactividad | analizable | json

  Valor predeterminado: Default

- IgnoreChecksFlag

  Tipo: String

  Descripción: (Opcional) el ID de reglas que se pasan al parámetro --ignore-checks. Estas reglas no se comprueban.

  Ejemplo: E1001, E1003, W7001

- IncludeChecksFlag

  Tipo: String

  Descripción: (Opcional) el ID de reglas que se pasan al parámetro `--include-checks`. Estas reglas se comprueban.

  Ejemplo: E1001, E1003, W7001

- InfoFlag

  Tipo: String

  Descripción: (Opcional) opción para el parámetro `--info`. Incluya la opción para habilitar información adicional de registro sobre el procesamiento de la plantilla.

  Valor predeterminado: falso

- TemplateFileName

  Tipo: String

  Descripción: el nombre, o clave, del archivo de plantilla en el bucket de S3.

- TemplateS3BucketName

  Tipo: String

  Descripción: el nombre del bucket de S3 que contiene la plantilla de empaquetador.

- RegionsFlag

  Tipo: String

  Descripción: (Opcional) valores que se pasan al parámetro `--regions`para probar la plantilla en las regiones Regiones de AWSespecificadas.

  Ejemplo: us-east-1,us-west-1

Pasos de documentos

RunCfnLintAgainstTemplate - Ejecuta la herramienta `cfn-python-lint`con respecto a la plantilla de AWS CloudFormationespecificada.

Salidas

RunCfnLintAgainstTemplate.output - El stdout de la herramienta `cfn-python-lint`.

AWSSupport-TroubleshootCFNCustomResource

Descripción

El `AWSSupport-TroubleshootCFNCustomResource`manual ayuda a diagnosticar por qué una AWS CloudFormationpila no pudo crear, actualizar o eliminar un recurso personalizado. El manual comprueba el token de servicio utilizado para el recurso personalizado y el mensaje de error devuelto. Tras revisar los detalles del recurso personalizado, el resultado del runbook proporciona una explicación del comportamiento de la pila y los pasos para solucionar el problema del recurso personalizado.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- StackName

  Tipo: String

  Descripción: (obligatorio) El nombre de la AWS CloudFormationpila en la que se produjo un error en el recurso personalizado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `validateCloudFormationStack`- Comprueba que la AWS CloudFormationpila existe en la misma Cuenta de AWSbanda. Región de AWS
- `checkCustomResource`- Analiza la AWS CloudFormationpila, comprueba el recurso personalizado que ha fallado y genera información sobre cómo solucionar el problema del recurso personalizado que ha fallado.

AWS-UpdateCloudFormationStack

Descripción

Actualice una AWS CloudFormation pila mediante una AWS CloudFormation plantilla almacenada en un bucket de Amazon S3.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LambdaAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el ARN del rol asumido por Lambda.
- StackNameOrId

  Tipo: cadena

  Descripción: (obligatorio) Nombre o identificador único de la AWS CloudFormation pila que se va a actualizar
- TemplateUrl

  Tipo: cadena

  Descripción: (Obligatoria) ubicación del depósito de S3 que contiene la CloudFormation plantilla actualizada (p. ej. `https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/updated.template`)

CloudFront

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon CloudFront. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCloudFrontDefaultRootObject`configura el objeto raíz predeterminado para la distribución de Amazon CloudFront (CloudFront) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- CloudFrontDistributionId

  Tipo: String

Descripción: (Obligatorio) El ID de la distribución de CloudFront para la que desea configurar el objeto raíz predeterminado.

- DefaultRootObject

  Tipo: String

  Descripción: (Obligatorio) El objeto que desea que regrese CloudFront cuando una solicitud de un espectador apunte a su raíz URL.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Configura el objeto raíz predeterminado para la distribución de CloudFront que especifique en el parámetro `CloudFrontDistributionId`.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descripción

El `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook permite el registro de acceso para la distribución de Amazon CloudFront (CloudFront) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- BucketName

  Tipo: cadena

  Descripción: (Obligatorio) El nombre del bucket de Amazon Simple Storage Service (Amazon S3) en el que desea almacenar los registros de acceso. No se admiten los buckets de la Región de AWSaf-south-1, ap-east-1, eu-south-1 y me-south-1.
- CloudFrontId

  Tipo: cadena

  Descripción: (obligatorio) El ID de la CloudFront distribución a la que quieres permitir el acceso al iniciar sesión.
- IncludeCookies

  Tipo: Booleano

  Valores válidos: true | false

  Descripción: (Obligatorio) Defina este parámetro en`true`, si desea que las cookies se incluyan en los registros de acceso.
- Prefix

  Tipo: cadena

  Descripción: (opcional) Una cadena opcional que desee CloudFront añadir como prefijo al registro `filenames` de acceso de su distribución, por ejemplo. `myprefix/`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

> **Note**
>
> La `s3:GetBucketLocation` API solo se puede usar para los buckets de S3 de la misma cuenta. No puedes usarla para buckets de S3 entre cuentas.

Pasos de documentos

- `aws:executeScript`- Habilita el registro de acceso para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro.

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity`habilita la identidad de acceso de origen para la distribución de Amazon CloudFront (CloudFront) que especifique. Esta automatización asigna la misma identidad de acceso de origen de CloudFront a todos los orígenes del tipo de origen de Amazon Simple Storage Service (Amazon S3) sin identidad de acceso de origen para la distribución de CloudFront que especifique. Esta automatización no concede permiso de lectura a la identidad de

acceso de origen para que CloudFront pueda obtener acceso a objetos en su bucket de Amazon S3. Debe actualizar los permisos de su bucket de Amazon S3 para permitir el acceso.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- CloudFrontDistributionId

  Tipo: String

  Descripción: (Obligatorio) El ID de la distribución de CloudFront en la que desea habilitar la conmutación por error de origen.
- OriginAccessIdentityId

  Tipo: String

  Descripción: (oblgatoria) La identidad de acceso de origen de CloudFront a asociar con el origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Habilita la identidad de acceso de origen para la distribución de CloudFront que especifique en el parámetro `CloudFrontDistributionId`y verifica que se haya asignado la identidad de acceso de origen.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCloudFrontOriginFailover`permite la conmutación por error de origen para la distribución de Amazon CloudFront (CloudFront) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.

- CloudFrontDistributionId

  Tipo: String

  Descripción: (Obligatorio) El ID de la distribución de CloudFront en la que desea habilitar la conmutación por error de origen.

- OriginGroupId

  Tipo: String

  Descripción: (Obligatorio) ID del grupo original.

- PrimaryOriginId

  Tipo: String

  Descripción: (Obligatorio) El ID del origen principal en el grupo de origen.

- SecondaryOriginId

  Tipo: String

  Descripción: (Obligatorio) El ID del origen secundario en el grupo de origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Habilita la conmutación por error de origen para la distribución de CloudFront que especifique en el parámetro `CloudFrontDistributionId`y verifica que la conmutación por error esté habilitada.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS`habilita la política de protocolo de visualización para la distribución de Amazon CloudFront (CloudFront) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- CloudFrontDistributionId

  Tipo: String

  Descripción: (Obligatorio) El ID de la distribución de CloudFront en la que desea habilitar la política de protocolo de visualización.
- ViewerProtocolPolicy

  Tipo: String

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

Descripción: (Obligatorio) El protocolo que los lectores pueden utilizar para acceder a los archivos en el origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Habilita la política de protocolo de visualización para la distribución de CloudFront que especifique en el parámetro `CloudFrontDistributionId`y verifica que la política se haya asignado.

CloudTrail

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CloudTrail Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-CreateCloudTrailMultiRegionTrail
- AWS-EnableCloudTrail
- AWS-EnableCloudTrailCloudWatchLogs
- AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS
- AWS-EnableCloudTrailKmsEncryption

- AWSConfigRemediation-EnableCloudTrailLogFileValidation
- AWS-EnableCloudTrailLogFileValidation
- AWS-QueryCloudTrailLogs

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

Descripción

El `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`runbook crea un registro de seguimiento AWS CloudTrail(CloudTrail) que distribuye archivos de registro de Regiones de AWSvarios archivos de registro al bucket de Amazon Simple Storage Service (Amazon S3) de su elección.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- BucketName

  Tipo: String

  Descripción: (obligatorio) Nombre del bucket de Amazon S3 en el que desea cargar registros.

- KeyPrefix

  Tipo: String

  Descripción: (Opcional) El prefijo de clave de Amazon S3 que viene después el nombre del bucket que ha designado para la entrega del archivo de registros.

- TrailName

  Tipo: String

  Descripción: (Obligatorio) El nombre de la ruta de CloudTrail que se va a crear.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Acepta el nombre de la ruta y el nombre del bucket de Amazon S3 como entrada y crea una ruta de CloudTrail.
- `aws:executeAwsApi`- Permite iniciar sesión en la ruta creada e inicia la entrega de registros en el depósito de Amazon S3 que especificó.
- `aws:assertAwsResourceProperty`- Verifica que se haya creado el rastro de CloudTrail.

AWS-EnableCloudTrail

Descripción

Cree un registro de seguimiento de AWS CloudTraily configure el registro en un bucket de S3.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- S3BucketName

  Tipo: String

  Descripción: (Obligatorio) el nombre del bucket de S3 designado para la publicación de archivos de registro.

  > **Note**
  >
  > El bucket de S3 debe existir y la política de bucket debe conceder a CloudTrail permiso para escribir en él. Para obtener más información, consulte Política de bucket de Amazon S3 para CloudTrail.

- TrailName

  Tipo: String

  Descripción: (Obligatorio) el nombre del nuevo registro de seguimiento.

AWS-EnableCloudTrailCloudWatchLogs

Descripción

Este runbook actualiza la configuración de una o más AWS CloudTrail rutas para enviar eventos a un grupo de CloudWatch registros de Amazon Logs.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- CloudWatchLogsLogGroupArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del grupo de CloudWatch registros al que se entregarán los CloudTrail registros.

- CloudWatchLogsRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del rol de IAM Logs Logs asume que escribe en el grupo de CloudWatch registros especificado.
- TrailNames

  Tipo: StringList

  Descripción: (Obligatorio) Una lista separada por comas con los nombres de las CloudTrail rutas cuyos eventos quieres enviar a CloudWatch Logs.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Actualiza las CloudTrail rutas especificadas para enviar los eventos al grupo de CloudWatch registros especificado.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Descripción

El `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS`runbook cifra un rastro (AWS CloudTrailCloudTrail) mediante la clave gestionada por el cliente AWS Key Management Service(AWS KMS) que especifique. Este manual solo debe usarse como referencia para garantizar que sus rutas de CloudTrail estén cifradas de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varias rutas con diferentes claves de KMS. Los archivos de resumen de CloudTrail no están cifrados. Si anteriormente configuró el `EnableLogFileValidation`parámetro como `true`para la ruta, consulte la sección «Uso del cifrado del lado del servidor con claves AWS KMSadministradas» del tema Prácticas recomendadas

de seguridad preventiva de CloudTrail en la Guía del AWS CloudTrailusuario para obtener más información.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- KMSKeyId

  Tipo: String

  Descripción: (obligatorio) El ARN, el ID de clave o el alias de la clave gestionada por el cliente que desea utilizar para cifrar la ruta que especifique en el parámetro. `TrailName`
- TrailName

  Tipo: String

  Descripción: (Obligatorio) El ARN o el nombre de la ruta que quieres actualizar para cifrarla.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Habilita el cifrado en la ruta que especifique en el `TrailName`parámetro.
- `aws:executeAwsApi`- Recopila el ARN de la clave gestionada por el cliente que especifique en `KMSKeyId`el parámetro.
- `aws:assertAwsResourceProperty`- Verifica que el cifrado esté habilitado en la ruta de CloudTrail.

AWS-EnableCloudTrailKmsEncryption

Descripción

Este manual actualiza la configuración de una o más AWS CloudTrail rutas para utilizar el cifrado AWS Key Management Service (AWS KMS).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- KMS KeyId

  Tipo: cadena

  Descripción: (obligatorio) El identificador de la clave gestionada por el cliente que desea utilizar para cifrar la ruta especificada en el `TrailName` parámetro. El valor puede ser un nombre de alias con el prefijo «alias/», un ARN completamente especificado para un alias o un ARN completamente especificado para una clave.

- TrailNames

  Tipo: StringList

  Descripción: (Obligatorio) Una lista separada por comas de las rutas que deseas actualizar para cifrarlas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Permite el AWS KMS cifrado de las rutas que especifique en el `TrailName` parámetro.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Descripción

El `AWSConfigRemediation-EnableCloudTrailLogFileValidation`libro de rutas permite la validación del archivo de registro de su AWS CloudTrailsendero.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- TrailName

  Tipo: cadena

  Descripción: (Obligatorio) el nombre o nombre de recurso de Amazon (ARN) de la ruta para la que desea habilitar la validación de registros.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Permite la validación del registro de la AWS CloudTrailruta que especifique en el `TrailName`parámetro.
- `aws:assertAwsResourceProperty`- Verifica que la validación del registro esté habilitada para su ruta.

`AWS-EnableCloudTrailLogFileValidation`

Descripción

El `AWS-EnableCloudTrailLogFileValidation` libro de rutas permite la validación del archivo de registro de los AWS CloudTrail senderos que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- TrailNames

  Tipo: StringList

Descripción: (Obligatorio) Una lista separada por comas con los nombres de las CloudTrail rutas para las que desea habilitar la validación de registros.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Permite la validación del registro de las AWS CloudTrail rutas que especifique en el `TrailNames` parámetro.

AWS-QueryCloudTrailLogs

Descripción

El manual de procedimientos `AWS-QueryCloudTrailLogs`crea una tabla de Amazon Athena a partir del bucket de Amazon Simple Storage Service (Amazon S3) de su elección que contenga registros AWS CloudTrail(CloudTrail). Tras crear la tabla, la automatización ejecuta las consultas SQL que especifique y, a continuación, elimina la tabla.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- Consulta

  Tipo: String

  Descripción: (Obligatoria) La consulta SQL que desea ejecutar.

- SourceBucketPath

  Tipo: String

  Descripción: (Obligatorio) El nombre del bucket de Amazon S3 que contiene los archivos de registro de CloudTrail que desea consultar.

- TableName

  Tipo: String

  Descripción: (Opcional) El nombre de la tabla Athena creada por la automatización.

  Predeterminado: cloudtrail_logs

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeAwsApi - Crear una tabla de Athena.
- aws:executeAwsApi - Ejecuta la cadena de consulta que especifique en el parámetro Query.
- aws:executeScript - Sondea y espera a que se complete la consulta.
- aws:executeAwsApi - Obtiene los resultados de la consulta.
- aws:executeAwsApi - Elimina la tabla creada por la automatización.

CloudWatch

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon CloudWatch. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

AWS-ConfigureCloudWatchOnEC2Instance

Descripción

Habilite o deshabilite la supervisión en instancias administradas de Amazon CloudWatch.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) el ID de la instancia Amazon EC2 en la que desea habilitar la supervisión de CloudWatch.
- propiedades

  Tipo: String

  Descripción: (Opcional) no se admite este parámetro. Se enumera aquí por motivos de compatibilidad con versiones anteriores.
- status

  Valores válidos: ENABLED | DISABLED

  Descripción: (Opcional) especifica si desea habilitar o deshabilitar CloudWatch.

Valor predeterminado: Enabled

Pasos de documentos

configureCloudWatch: configura CloudWatch en la instancia Amazon EC2 con el estado dado.

Salidas

Esta automatización no tiene salidas.

AWS-EnableCWAlarm

Descripción

El `AWS-EnableCWAlarm` runbook crea alarmas de Amazon CloudWatch (CloudWatch) para AWS los recursos suyos Cuenta de AWS que aún no tienen una. CloudWatch las alarmas se crean para los siguientes AWS recursos:

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2)
- Volúmenes de Amazon Elastic Block Store (Amazon EBS)
- Buckets de Amazon Simple Storage Service (Amazon S3)
- Clústeres de Amazon Relational Database Service (Amazon RDS)

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- ComparisonOperator

  Tipo: cadena

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

  Descripción: (Obligatoria) La operación aritmética que se utilizará al comparar la estadística y el umbral especificados.

- MetricName

  Tipo: cadena

  Descripción: (Obligatorio) Nombre de la métrica asociada a la alarma.

- Período

  Tipo: entero

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

  Descripción: (Obligatorio) El período, en segundos, durante el que se aplica la estadística.

- El recurso gana

  Tipo: StringList

  Descripción: (Obligatorio) Una lista separada por comas de los ARN de los recursos para los que se va a crear una alarma CloudWatch

- Estadística

  Tipo: cadena

  Valores válidos: Promedio | Máximo | Mínimo | | Suma SampleCount

Descripción: (Obligatorio) La estadística de la métrica asociada a la alarma.

- Threshold

  Tipo: entero

  Descripción: (Obligatorio) El valor que se va a comparar con la estadística especificada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudwatch:PutMetricAlarm`

Pasos de documentos

- `aws:executeScript`- Crea una CloudWatch alarma según los valores especificados en los parámetros del manual para los recursos que especifique en el `ResourceARNs` parámetro.

Salidas

Habilite la alarma. FailedResources: una lista cartográfica de los ARN de recursos para los que no se creó una CloudWatch alarma y el motivo del error.

Habilite la alarma. SuccessfulResources: una lista de los ARN de recursos para los que se creó correctamente una CloudWatch alarma.

Amazon DocumentDB

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon DocumentDB (con compatibilidad con MongoDB). Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableDocDbClusterBackupRetentionPeriod

AWS-EnableDocDbClusterBackupRetentionPeriod

Descripción

El AWS-EnableDocDbClusterBackupRetentionPeriod runbook habilita un período de retención de copias de seguridad para el clúster de Amazon DocumentDB que especifique. Esta función establece el número total de días durante los que se conserva una copia de seguridad automática. Para modificar un clúster, el clúster debe estar en el estado disponible con un tipo de motor dedocdb.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- BASE DE DATOS ClusterResourceId

  Tipo: cadena

  Descripción: (obligatorio) El ID de recurso del clúster de Amazon DocumentDB para el que desea habilitar el período de retención de copias de seguridad.

- BackupRetentionPeriod

  Tipo: entero

  Descripción: (obligatorio) El número de días durante los que se conservan las copias de seguridad automatizadas. Debe tener un valor de 7 a 35 días.

- PreferredBackupWindow

  Tipo: cadena

  Descripción: (opcional) Un intervalo de tiempo diario en hora universal coordinada (UTC) con el formato hh24:mm-hh24:mm, por ejemplo, 07:14-07:44. El valor debe ser de al menos 30 minutos y no puede entrar en conflicto con el período de mantenimiento preferido.

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

Pasos de documentos

- GetDocDbClusterIdentifier (aws:executeAwsApi) - Devuelve el identificador del clúster de Amazon DocumentDB utilizando el ID de recurso proporcionado.
- VerifyDocDbEngine (aws: assertAwsResource Property): verifica que el tipo de motor de Amazon DocumentDB `docdb` sea para evitar cambios inadvertidos en otros tipos de motores de Amazon RDS.
- VerifyDocDbStatus (aws: waitAwsResource Property): verifica que el estado del clúster de Amazon DocumentDB sea. `available`
- ModifyDocDbRetentionPeriod (aws:executeAwsApi) - Establece el período de retención mediante los valores proporcionados para el clúster de Amazon DocumentDB especificado.
- VerifyDocDbBackupsEnabled (AWS:ExecuteScript): verifica que el período de retención del clúster de Amazon DocumentDB y la ventana de respaldo preferida, si se especificó, se hayan establecido correctamente.

Salidas

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - Respuesta de la operación de la `ModifyDBCluster` API.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse - Resultado del `VerifyDocDbBackupsEnabled` paso que confirma la modificación correcta del clúster de Amazon DocumentDB.

CodeBuild

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CodeBuild Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK`

Descripción

El `AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` manual cifra los artefactos de construcción de un proyecto AWS CodeBuild (CodeBuild) con la clave administrada por el cliente AWS Key Management Service (AWS KMS) que especifiques. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre.
- KMS KeyId

  Tipo: cadena

  Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la clave gestionada por el AWS KMS cliente que desea utilizar para cifrar el CodeBuild proyecto que especifique en el parámetro. `ProjectId`
- ProjectId

  Tipo: cadena

  Descripción: (obligatorio) El ID del CodeBuild proyecto cuyos artefactos de construcción desea cifrar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Recopila el nombre del CodeBuild proyecto a partir del ID del proyecto.
- `aws:executeAwsApi`- Habilita el cifrado en el CodeBuild proyecto que especifique en el `ProjectId` parámetro.
- `aws:assertAwsResourceProperty`- Verifica que el cifrado esté habilitado en el CodeBuild proyecto.

Salidas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Respuesta de la llamada a la `UpdateFunctionConfiguration` API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject`elimina las variables de entorno `AWS_ACCESS_KEY_ID`y `AWS_SECRET_ACCESS_KEY`del proyecto AWS CodeBuild(CodeBuild) que especifique. AWS Configdebe estar habilitado en la Región de AWSdonde ejecute esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.

- ResourceId

  Tipo: String

  Descripción: (Obligatorio) El ID del proyecto CodeBuild cuyas variables de entorno de clave de acceso desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Elimina las variables de entorno de clave de acceso del proyecto CodeBuild especificado en el parámetro `ResourceId`.

AWS CodeDeploy

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CodeDeploy Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-TroubleshootCodeDeploy

AWSSupport-TroubleshootCodeDeploy

Descripción

El manual de procedimientos `AWSSupport-TroubleshootCodeDeploy`ayuda a diagnosticar por qué se produjo un error AWS CodeDeployen una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El manual de procedimientos proporciona pasos para ayudarle a resolver el problema o a resolver problemas adicionales. También proporciona prácticas recomendadas para CodeDeploy para ayudarle a evitar problemas similares en el futuro.

Este manual de procedimientos puede ayudarle a resolver los siguientes problemas:

- El agente CodeDeploy no está instalado o no se está ejecutando en la instancia de Amazon EC2
- La instancia de Amazon EC2 no tiene un perfil de instancia AWS Identity and Access Management(de IAM) adjunto
- El perfil de instancia de IAM adjunto a la instancia de Amazon EC2 no cuenta con los permisos de Amazon Simple Storage Service (Amazon S3) necesarios
- Falta una revisión almacenada en Amazon S3 o el bucket de Amazon S3 utilizado está en una Región de AWSque es diferente a la instancia de Amazon EC2
- Problemas con el archivo de especificación de la aplicación (AppSpec)
- Errores de tipo “El archivo ya existe en la ubicación”
- Enlaces de eventos fallidos del ciclo de vida gestionados por CodeDeploy
- Enlaces de eventos fallidos del ciclo de vida gestionados por el cliente
- Eventos de escalado durante una implementación

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- DeploymentId

  Tipo: String

  Descripción: (Obligatorio) El ID de la implementación que falló.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia Amazon EC2 en que la implementación ha fallado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi` - Verifica los valores proporcionados para los parámetros `DeploymentId`y `InstanceId`.
- `aws:executeScript` - Recopila información de la instancia de Amazon EC2, como el estado de la instancia y los detalles del perfil de instancia de IAM.
- `aws:executeScript` - Revisa la implementación especificada y regresa un análisis sobre los motivos por los que se ha producido un error en la implementación.

AWS Config

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Config Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

AWSSupport-SetupConfig

Descripción

El manual de procedimientos `AWSSupport-SetupConfig`crea un rol vinculado a un servicio AWS Identity and Access Management(de IAM), un registrador de configuración con tecnología AWS Configy un canal de entrega con un bucket de Amazon Simple Storage Service (Amazon S3) desde el que AWS Configenvía las instantáneas de la configuración y los archivos del historial de la configuración. Si especifica valores para los parámetros `AggregatorAccountId`y `AggregatorAccountRegion`, el manual de procedimientos también crea autorizaciones para la agregación de datos a fin de recopilar datos de configuración y conformidad AWS Configde varias Cuentas de AWSy varias Regiones de AWS. Para obtener más información sobre la agregación de datos de varias cuentas y regiones, consulte la sección Agregación de datos multicuenta y multirregionales en la AWS ConfigGuía para desarrolladores .

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- AggregatorAccountId

  Tipo: String

  Descripción: (Opcional) El ID de la Cuenta de AWSdonde se añadirá un agregador para agregar los datos AWS Configde configuración y cumplimiento de varias cuentas y Regiones de AWS. El agregador también utiliza esta cuenta para autorizar las cuentas de origen.
- AggregatorAccountRegion

  Tipo: String

  Descripción: (Opcional) La región en la que se añadirá un agregador para agregar los datos AWS Configde configuración y cumplimiento de varias cuentas y regiones.
- IncludeGlobalResourcesRegion

  Tipo: String

  Predeterminado: us-east-1

  Descripción: (Obligatorio) Para evitar registrar los datos de los recursos globales en cada región, especifique una región desde la que registrar los datos de los recursos globales.
- Partition

  Tipo: String

  Valor predeterminado: `aws`

  Descripción: (Obligatoria) La partición de la que desea recopilar datos AWS Configde configuración y conformidad.
- S3BucketName

Tipo: String

Valor predeterminado: `aws-config-delivery-channel`

Descripción: (Opcional) El nombre que desea aplicar al bucket de Amazon S3 creado para el canal de entrega. El ID de la cuenta se adjunta al final del nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript` - Crea una función de IAM vinculada a un servicio para AWS Configsi aún no existe ninguna.
- `aws:executeScript` - Crea un grabador de configuración si aún no existe ninguno.
- `aws:executeScript` - Crea un bucket de Amazon S3 para que lo utilice el canal de entrega si aún no existe ninguno.

- `aws:executeScript` - Crea un canal de entrega con los recursos creados por el manual de procedimientos.
- `aws:executeAwsApi` - Para detener o iniciar el registro de configuración:
- `aws:executeScript` - Si ha especificado valores para los parámetros `AggregatorAccountId`y `AggregatorAccountRegion`, se configuran las autorizaciones para la agregación de datos de varias cuentas y regiones.

Amazon Connect

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Connect. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`

Descripción

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`Esto le ayuda a asociar números de teléfono a los flujos de contactos de su instancia de Amazon Connect. Al proporcionar las asignaciones de números de teléfono y flujos de contactos en un archivo de entrada de valores separados por comas (CSV), el manual asocia tantos números de teléfono a los flujos de contactos como sea posible en 14,5 minutos. El manual genera un archivo CSV con todos los pares de números de teléfono y flujos de contactos que no ha podido asociar dentro del límite de tiempo para que puedas introducirlos en la siguiente ejecución.

¿Cómo funciona?

El manual le `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` ayuda a asociar números de teléfono a los flujos de contactos de su instancia de Amazon Connect mediante un archivo CSV de datos de mapeo que se almacena en un depósito de Amazon Simple Storage Service (Amazon S3). El archivo CSV de entrada debe alinearse con el siguiente formato, con `PhoneNumber` los valores en formato E.164.

Ejemplo del archivo CSV de entrada

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

El manual de automatización también crea los siguientes archivos en la ubicación de destino especificada en `DestinationFileBucket` y`DestinationFilePath`.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: un archivo temporal que contiene los `ContactFlowId` pares `PhoneNumberId` y necesarios para la `AssociatePhoneNumberContactFlow` API.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: un archivo que contiene los pares de números de teléfono y flujo de contactos que no se pudieron procesar debido a un error, por ejemplo, `ResourceNotFoundException` en el formato de`PhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: un archivo que contiene los pares de número de teléfono y flujo de contactos que no se procesaron. El manual intenta procesar tantos números de teléfono y flujos de contactos como sea posible en 14,5 minutos (15 minutos después del tiempo de espera de la AWS Lambda función, 30 segundos de búfer). Si hay algunos números de teléfono o flujos de contactos que no se han podido procesar por falta de tiempo, el runbook los incluye en un archivo CSV para usarlos como entrada en la siguiente ejecución del runbook.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta AWSSupport-AssociatePhoneNumbersToConnectContactFlowsSystems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional)

  El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- ConnectInstanceId (Obligatorio)

  El ID de tu instancia de Amazon Connect.

- SourceFileBucket (Obligatorio)

  El depósito de Amazon S3 que almacena el archivo CSV que contiene los pares de número de teléfono y flujo de contacto.

- SourceFilePath (Obligatorio)

  La clave de objeto de Amazon S3 del archivo CSV que contiene los pares de número de teléfono y flujo de contacto. Por ejemplo, `path/to/input.csv`.

- DestinationFileBucket (Obligatorio)

  El depósito de Amazon S3 en el que la automatización colocará un archivo intermedio y un informe de resultados.

- DestinationFilePath (Opcional)

  La ruta del objeto de Amazon S3 en `DestinationFileBucket` la que se deben almacenar un archivo intermedio y un informe de resultados. Por ejemplo, si lo especifica`path/to/files/`, los archivos se almacenan en`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

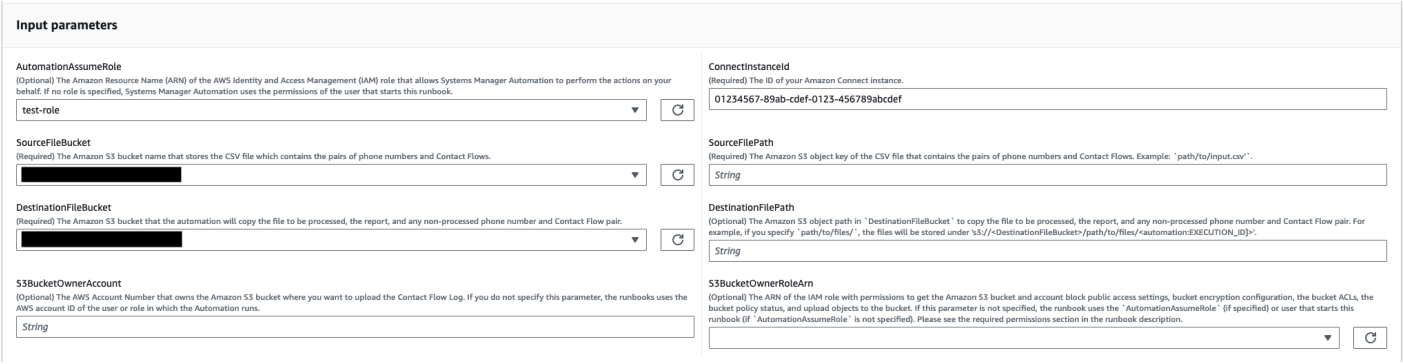
- S3 BucketOwnerAccount (opcional)

  El número de AWS cuenta propietario del bucket de Amazon S3 en el que desea cargar el registro de flujo de contactos. Si no especificas este parámetro, los manuales utilizan el ID de AWS cuenta del usuario o rol en el que se ejecuta la automatización.

- S3 BucketOwnerRoleArn (opcional)

  El ARN de la función de IAM con permisos para obtener la configuración de acceso público del bucket y el bloqueo de cuentas de Amazon S3, la configuración de cifrado del bucket, las ACL del bucket, el estado de la política del bucket y cargar objetos al bucket. Si no se especifica este

parámetro, el runbook utiliza el runbook `AutomationAssumeRole` (si se ha especificado) o el usuario que inicia este runbook (si `AutomationAssumeRole` no se ha especificado). Por favor consulte la sección de permisos necesarios en la descripción del manual de procedimientos.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - CheckConnectInstanceExistance

     Comprueba si la instancia de Amazon Connect proporcionada `ConnectInstanceId` existe.
   - Comprueba [S3] BucketPublicStatus

     Comprueba si los buckets de Amazon S3 especificados en `SourceFileBucket` y `DestinationFileBucket` permiten permisos de acceso de lectura o escritura públicos o anónimos.
   - CheckSourceFileExistenceAndSize

     Comprueba si el archivo CSV de origen especificado en el `SourceFilePath` existe y si el tamaño del archivo supera el límite de 25 MiB.
   - GenerateResourceIdMap

     Descarga el archivo CSV de origen especificado en el `SourceFilePath` identificador `PhoneNumberId` y `ContactFlowId` para cada recurso. Una vez hecho esto, carga un archivo CSV que contiene`PhoneNumber`, `PhoneNumberId``ContactFlowName`, y `ContactFlowId` al bucket Amazon S3 de destino especificado en`DestinationFileBucket`. Si `PhoneNumberId` no se puede identificar con un número determinado, el archivo estará vacío en el archivo CSV.
   - AssociatePhoneNumbersToContactFlows

Crea una AWS Lambda función en tu cuenta mediante una AWS CloudFormation pila. La AWS Lambda función asocia cada número a un flujo de contactos que aparece en el archivo CSV de origen especificado en `SourceFileBucket` `SourceFilePath` y, a continuación, la AWS CloudFormation pila invoca la función. La AWS Lambda función asigna tantos números de teléfono a los flujos de contactos como sea posible antes de que se agote el tiempo de espera (15 minutos). Se carga la lista de números de teléfono y flujos de contactos que no se pudieron procesar debido a un error`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Se cargan los que no se han podido procesar debido a que se ha superado el número máximo de números de teléfono que se pueden procesar en una sola ejecución`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Si se produce un error en este paso, se pasa al `DescribeCloudFormationErrorFromStackEvents` paso siguiente para mostrar el motivo del error debido a los eventos de la AWS CloudFormation pila.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Espera hasta que se cree la AWS Lambda función que asigna los números de teléfono a los flujos de contactos y la AWS CloudFormation pila complete su invocación.

- GenerateReport

  Genera el informe que contiene el número de números de teléfono asignados a los flujos de contactos, los que no se pudieron procesar debido a un error y los que no se pudieron procesar debido a un exceso del número máximo de números de teléfono que se pueden procesar en una sola ejecución. El informe también muestra la ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) de `[automation:EXECUTION_ID]/ErrorResourceList.csv` o`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`, si corresponde.

- **`DeleteCloudFormationStack`**

  Elimina la AWS CloudFormation pila, incluida la función Lambda para el mapeo.

- **`DescribeCloudFormationErrorFromStackEvent`**

  Describe los errores de la AWS CloudFormation pila del `AssociatePhoneNumbersToContactFlows` paso.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

   - GenerateReport.OutputPayload

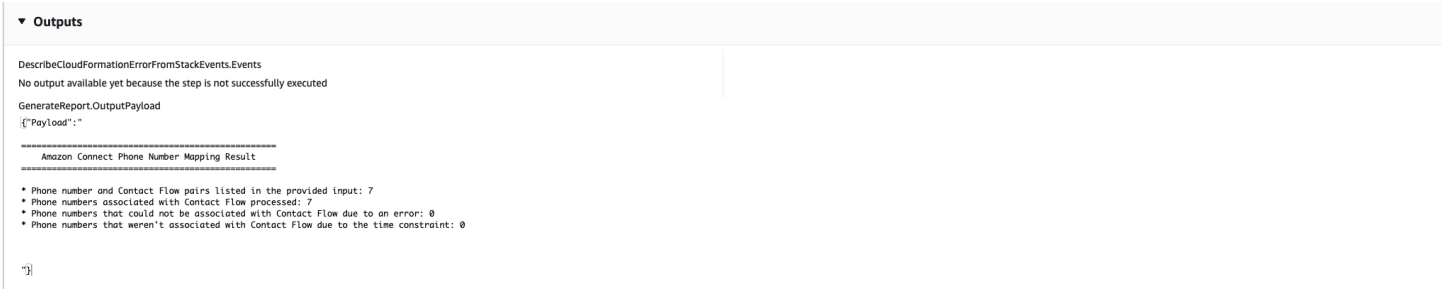
Resultado de las asociaciones de números de teléfono y flujo de contactos. Este informe contiene la siguiente información:

- El número de pares de números de teléfono y flujo de contactos que aparecen en el archivo CSV de entrada
- El número de números de teléfono asociados a los flujos de contactos, tal como se especifica en el archivo CSV de entrada
- El número de números de teléfono que no se pudieron asociar a los flujos de contactos debido a un error
- El número de números de teléfono que no estaban asociados a los flujos de contactos por falta de tiempo
- La ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) del archivo CSV que contiene los pares de número de teléfono y flujo de contactos que no se pudieron asociar debido a un error
- La ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) del archivo CSV que contiene los pares de números de teléfono y flujo de contactos que no estaban asociados por falta de tiempo

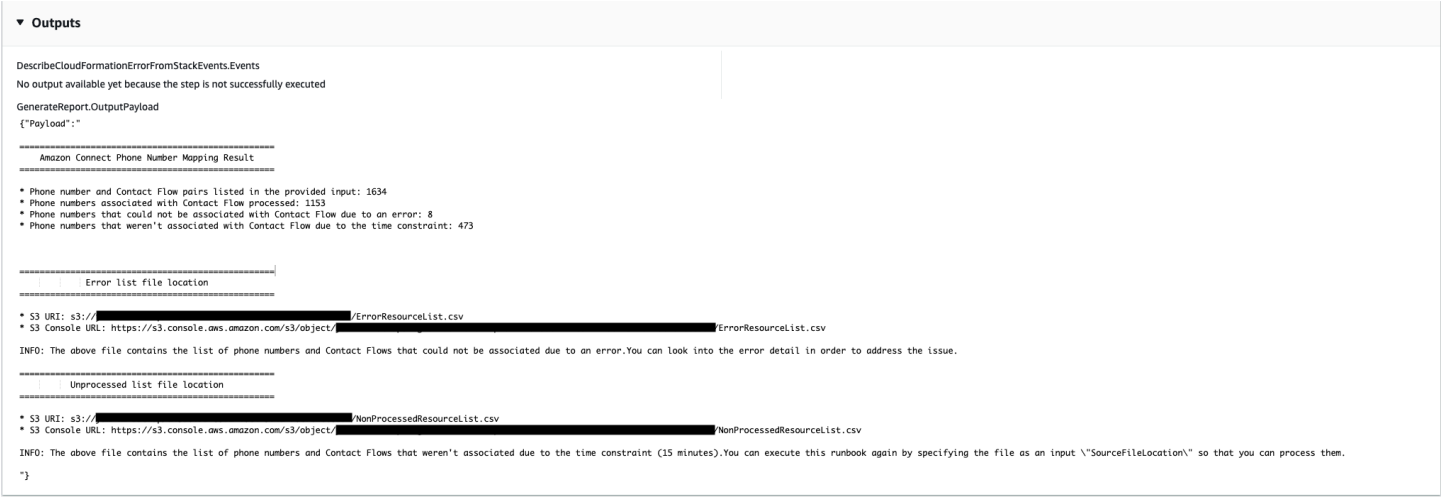
- DescribeCloudFormationErrorFromStackEvents.Eventos

  Resultado que muestra los eventos de la AWS CloudFormation pila si el `AssociatePhoneNumbersToContactFlows` paso falla.

Resultado de la ejecución con un número reducido de números de teléfono y flujos de contactos



Resultado de la ejecución con una gran cantidad de números de teléfono y flujos de contactos y números de teléfono que no estaban asociados debido a un error o a una limitación de tiempo



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS Directory Service

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Directory Service Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

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

AWS-CreateDSManagementInstance

Descripción

El manual de procedimientos `AWS-CreateDSManagementInstance`crea una instancia de Windows de Amazon Elastic Compute Cloud (Amazon EC2) que puede utilizar para administrar su directorio AWS Directory Service. La instancia de administración no se puede usar para administrar los directorios del conector de AD.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- AmiID

  Tipo: String

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

  Descripción: (Obligatorio) El ID de la Amazon Machine Image(AMI) que desea utilizar para lanzar la instancia de administración.
- DirectoryId

  Tipo: String

Descripción: (Obligatorio) El ID del directorio AWS Directory Serviceque desea administrar. La instancia se une al directorio que especifique.

- IamInstanceProfileName

  Tipo: String

  Descripción: (Obligatorio) El nombre que especifique se aplica al perfil de instancia de IAM creado por la automatización y adjunto a la instancia de administración.

- InstanceType

  Tipo: String

  Valor predeterminado: 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

  Descripción: (Obligatorio) tipo de instancia que se va a lanzar.

- KeyPairName

  Tipo: String

Descripción: (Opcional) el par de claves que se utilizará al crear la nueva instancia. Si no especifica un valor, no se asociará ningún par de claves a la instancia.

- RemoteAccessCidr

  Tipo: String

  Descripción: (Obligatorio) El bloque CIDR desde el que desea permitir el tráfico RDP (puerto 3389). El bloque CIDR que especifique se aplica a una regla de entrada que se agrega al grupo de seguridad creado por la automatización.

- SecurityGroupName

  Tipo: String

  Descripción: (Obligatorio) El nombre que especifique se aplica al grupo de seguridad creado por la automatización y asociado a la instancia de administración.

- Etiquetas

  Tipo: MapList

  Descripción: (Opcional) Un par clave-valor que desee aplicar a los recursos creados por la automatización.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- `aws:executeAwsApi` - Recopila detalles sobre el directorio que especifique en el parámetro `DirectoryId`.
- `aws:executeAwsApi` - Obtiene el bloque CIDR de la nube privada virtual (VPC) en la que se lanzó el directorio.
- `aws:executeAwsApi` - Crea un grupo de seguridad con el valor que especifique en el parámetro `SecurityGroupName`.
- `aws:executeAwsApi` - Crea una regla de entrada para el grupo de seguridad recién creado que permite el tráfico RDP desde el CIDR que especifique en el parámetro `RemoteAccessCidr`.
- `aws:executeAwsApi` - Crea un un rol de IAM y un perfil de instancia con el valor que especifique en el parámetro `IamInstanceProfileName`.
- `aws:executeAwsApi` - Lanza una instancia de Amazon EC2 en función de los valores que especifique en los parámetros del manual de procedimientos.
- `aws:executeAwsApi` - Crea un documento AWS Systems Managerpara unir la instancia recién lanzada a su directorio.
- `aws:runCommand` - Une la nueva instancia a su directorio.
- `aws:runCommand` - Instala herramientas de administración remota del servidor en la nueva instancia.

AWSSupport-TroubleshootADConnectorConnectivity

Descripción

El manual de procedimientos `AWSSupport-TroubleshootADConnectorConnectivity`verifica los siguientes requisitos previos para el conector de AD.

- Comprueba si el grupo de seguridad y las reglas de la lista de control de acceso (ACL) de la red asociados a su conector de AD permiten el tráfico necesario.
- Comprueba si AWS Systems Manager, AWS Security Token Servicey los puntos de conexión de VPC de la interfaz de Amazon CloudWatch se encuentran en la misma nube privada virtual (VPC) que el conector de AD.

Cuando las comprobaciones de los requisitos previos se completen correctamente, el manual de procedimientos lanza dos instancias Linux t2.micro de Amazon Elastic Compute Cloud (Amazon

EC2) Linux en las mismas subredes que el conector de AD. Después se realizan las pruebas de conectividad de red con las utilidades `netcaty` `nslookup`.

Ejecuta esta automatización (consola)

> **Important**
>
> El uso de este manual de procedimientos puede implicar cargos adicionales a su Cuenta de AWSpara las instancias de Amazon EC2, los volúmenes de Amazon Elastic Block Store y las Amazon Machine Imagey (AMI) creadas durante la automatización. Para obtener más información, consulte Precios de Amazon Elastic Compute Cloud y Precios de Amazon Elastic Block Store.
>
> Si el paso `aws:deletestackno` funciona, vaya a la consola AWS CloudFormationpara eliminar la pila manualmente. El nombre de la pila creado por este manual de procedimientos comienza por `AWSSupport-TroubleshootADConnectorConnectivity`. Para obtener información sobre la eliminación de pilas AWS CloudFormation, consulte Eliminar una pila en la AWS CloudFormationGuía del usuario.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- DirectoryId

  Tipo: String

  Descripción: (Obligatorio) El ID del directorio del conector de AD con el que desea solucionar los problemas de conectividad.

- Ec2InstanceProfile

  Tipo: String

  Máximo de caracteres: 128

  Descripción: (Obligatorio) El nombre del perfil de instancia que desea asignar a las instancias que se lanzan para realizar pruebas de conectividad. El perfil de instancia que especifique debe tener la política `AmazonSSMManagedInstanceCore` o los permisos equivalentes adjuntos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:assertAwsResourceProperty - Confirma que el directorio especificado en el parámetro DirectoryIdes un conector de AD.
- aws:executeAwsApi - Recopila información sobre el conector de AD.
- aws:executeAwsApi - Recopila información sobre los grupos de seguridad asociados al conector de AD.
- aws:executeAwsApi - Recopila información sobre las reglas de ACL de la red asociadas a las subredes del conector de AD.
- aws:executeScript - Evalúa las reglas del grupo de seguridad del conector de AD para verificar que se permite el tráfico saliente necesario.
- aws:executeScript - Evalúa las reglas de ACL de la red del conector de AD para verificar que se permite el tráfico de red saliente y entrante requerido.
- aws:executeScript - Comprueba si los puntos de conexión de AWS Systems Manager, AWS Security Token Servicey la interfaz de Amazon CloudWatch se encuentran en la misma VPC que el conector de AD.
- aws:executeScript - Compila los resultados de las comprobaciones realizadas en los pasos anteriores.
- aws:branch - Ramifica la automatización en función del resultado de los pasos anteriores. La automatización se detiene aquí si faltan las reglas de salida y entrada requeridas para los grupos de seguridad y las ACL de la red.
- aws:createStack - Crea una pila AWS CloudFormationpara lanzar instancias de Amazon EC2 para realizar pruebas de conectividad.
- aws:executeAwsApi - Recopila los ID de las instancias de Amazon EC2 recién lanzadas.

- `aws:waitForAwsResourceProperty` - Espera a que la primera instancia de Amazon EC2 recién lanzada muestre que está gestionada por AWS Systems Manager.
- `aws:waitForAwsResourceProperty` - Espera a que la segunda instancia de Amazon EC2 recién lanzada muestre que está gestionada por AWS Systems Manager.
- `aws:runCommand` - Realiza pruebas de conectividad de red con las direcciones IP del servidor DNS en las instalaciones desde la primera instancia de Amazon EC2.
- `aws:runCommand` - Realiza pruebas de conectividad de red con las direcciones IP del servidor DNS en las instalaciones desde la segunda instancia de Amazon EC2.
- `aws:changeInstanceState` - Detiene las instancias de Amazon EC2 utilizadas para las pruebas de conectividad.
- `aws:deleteStack` - Elimina la AWS CloudFormationpila.
- `aws:executeScript` - Muestra instrucciones sobre cómo eliminar manualmente la pila AWS CloudFormationsi la automatización no logra eliminar la pila.

`AWSSupport-TroubleshootDirectoryTrust`

Descripción

El manual de procedimientos `AWSSupport-TroubleshootDirectoryTrust`diagnostica los problemas de creación de confianza entre un AWS Managed Microsoft ADy un directorio activo de Microsoft. La automatización garantiza que el tipo de directorio admita confianzas y, a continuación, comprueba las reglas de grupo de seguridad asociadas, las listas de control de acceso a la red (ACL de red) y las tablas de ruteo para detectar posibles problemas de conectividad.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- DirectoryId

  Tipo: String

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

  Descripción: (Obligatorio) el ID de AWS Managed Microsoft ADpara solucionar problemas.

- RemoteDomainCidrs

  Tipo: StringList

  Valores 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]))$

  Descripción: (Obligatorio) el CIDR (s) del dominio remoto con el que intenta establecer una relación de confianza. Puede agregar varios CIDR utilizando valores separados por comas. Por ejemplo, 172.31.48.0/20, 192.168.1.10/32.

- RemotedomainName

  Tipo: String

  Descripción: (Obligatorio) nombre completo del dominio remoto con el que está estableciendo una relación de confianza.

- RequiredTrafficACL

  Tipo: String

  Descripción: (Obligatorio) los requisitos de puerto por defecto para AWS Managed Microsoft AD. En la mayoría de los casos, no debe modificar el valor predeterminado.

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

- RequiredTrafficSG

  Tipo: String

  Descripción: (Obligatorio) los requisitos de puerto por defecto para AWS Managed Microsoft AD. En la mayoría de los casos, no debe modificar el valor predeterminado.

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

- TrustId

  Tipo: String

  Descripción: (Opcional) ID de la relación de confianza para solucionar el problema.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:assertAwsResourceProperty` - Confirma que el tipo de directorio sea AWS Managed Microsoft AD.

- `aws:executeAwsApi` - Obtiene información acerca de AWS Managed Microsoft AD.
- `aws:branch` - Ramifica la automatización si se proporciona un valor para el parámetro `TrustId`de entrada.
- `aws:executeAwsApi` - Obtiene información sobre la relación de confianza.
- `aws:executeAwsApi` - Obtiene las direcciones IP DNS del reenviador condicional para el .
- `aws:executeAwsApi` - Obtiene información acerca de las rutas IP que se han agregado a .
- `aws:executeAwsApi` - Obtiene los CIDR de las subredes AWS Managed Microsoft AD.
- `aws:executeAwsApi` - Obtiene información acerca de los grupos de seguridad asociados con AWS Managed Microsoft AD.
- `aws:executeAwsApi` - Obtiene información acerca de las ACL de red asociadas con AWS Managed Microsoft AD.
- `aws:executeScript` - Confirma que `RemoteDomainCidrs`son valores válidos. Confirma que AWS Managed Microsoft ADtiene reenviadores condicionales para los `RemoteDomainCidrs`, y que las rutas IP requeridas se han agregado a AWS Managed Microsoft ADsi los `RemoteDomainCidrs`son direcciones IP no RFC 1918.
- `aws:executeScript` - Evalúa las reglas de los grupos de seguridad.
- `aws:executeScript` - Evalúa las ACL de la red.

Salidas

evalDirectorySecurityGroup.output: resultados de la evaluación de si las reglas de grupo de seguridad asociadas a AWS Managed Microsoft ADpermiten el tráfico necesario para la creación de confianza.

evalAclEntries.output: resultados de la evaluación de si las ACL de red asociadas a AWS Managed Microsoft ADpermiten el tráfico necesario para la creación de confianza.

evaluateRemoteDomaincidr.output: resultados de la evaluación si los `RemoteDomainCidrs`son valores válidos. Confirma que AWS Managed Microsoft ADtiene reenviadores condicionales para los `RemoteDomainCidrs`, y que las rutas IP requeridas se han agregado a AWS Managed Microsoft ADsi los `RemoteDomainCidrs`son direcciones IP no RFC 1918.

AWS AppSync

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS AppSync Para obtener información acerca de los manuales de procedimientos,

consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

Descripción

El `AWS-EnableAppSyncGraphQLApiLogging` runbook permite el registro a nivel de campo y el registro a nivel de solicitud para la API AWS AppSync GraphQL que especifique. El runbook aplicará los cambios a la API GraphQL especificada incluso si el registro ya está habilitado.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- ApiId

Tipo: cadena

Descripción: (obligatorio) El ID de la API para la que quieres habilitar el registro.

- FieldLogLevel

  Tipo: cadena

  Valores válidos: ERROR | TODOS

  Descripción: (obligatorio) El nivel de registro del campo.

- CloudWatchLogsRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del rol de servicio que AWS AppSync asume publicar en Amazon CloudWatch Logs.

- ExcludeVerboseContent

  Tipo: Booleano

  Valor predeterminado: False

  Descripción: (opcional) Se configura `True` para excluir información como los encabezados, el contexto y las plantillas de mapeo evaluadas, independientemente del nivel de registro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws: executeAwsApi - Recopila el tipo de autenticación y la información de configuración relevante para el tipo de autenticación principal.
- aws:branch: se ramifica según el tipo de autenticación.
- aws: executeAwsApi - Actualiza la configuración de registro de la API AWS AppSync GraphQL en función de los valores especificados para los parámetros de entrada del runbook.

Salidas

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphqlApi` llamada.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphqlApi` llamada.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphqlApi` llamada.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphqlApi` llamada.

Amazon Athena

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Athena. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableAthenaWorkGroupEncryptionAtRest

`AWS-EnableAthenaWorkGroupEncryptionAtRest`

Descripción

El `AWS-EnableAthenaWorkGroupEncryptionAtRest` runbook permite el cifrado en reposo para el grupo de trabajo de Amazon Athena que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- WorkGroup

  Tipo: cadena

  Descripción: (Obligatorio) El grupo de trabajo para el que desea habilitar el cifrado en reposo.
- EncryptionOption

  Tipo: cadena

  Valores válidos: SSE_S3 | SSE_KMS | CSE_KMS

  Descripción: (obligatorio) Especifica qué opción de cifrado se utiliza. Puede elegir el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE_S3), el cifrado del lado del servidor con claves administradas (SSE_KMS) o el cifrado del lado del cliente con claves AWS KMS administradas (CSE_KMS). AWS KMS
- KmsKeyId

  Tipo: cadena

Descripción: (opcional) Si utiliza una opción de AWS KMS cifrado, especifique el ARN de la clave, el ID de la clave o el alias de la clave que desee utilizar.

- EnableMinimumEncryptionConfiguration

  Tipo: Booleano

  Valor predeterminado: True

  Descripción: (opcional) Aplica un nivel mínimo de cifrado al grupo de trabajo para los resultados de consultas y cálculos que se escriben en Amazon S3. Cuando está habilitada, los usuarios del grupo de trabajo solo pueden establecer el cifrado en el nivel mínimo establecido por el administrador o en un nivel superior al enviar consultas. Esta configuración no se aplica a los grupos de trabajo habilitados para Spark.
- EnforceWorkGroupConfiguration

  Tipo: Booleano

  Valor predeterminado: True

  Descripción: (Opcional) Si se establece en`True`, la configuración del grupo de trabajo anulará la configuración del lado del cliente. Si se establece en`False`, se utiliza la configuración del lado del cliente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:branch: se ramifica según la opción de cifrado especificada en el parámetro. `EncryptionOption`

- aws: executeAwsApi - Este paso actualiza el Grupo de Trabajo de Athena con la configuración de cifrado especificada.
- aws: executeAwsApi - Actualiza el Grupo de Trabajo de Athena con la configuración de cifrado especificada.
- aws: assertAwsResource Property: verifica que se haya habilitado el cifrado para el grupo de trabajo.

DynamoDB

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para Amazon DynamoDB. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

AWS-ChangeDDBRWCapacityMode

Descripción

El `AWS-ChangeDDBRWCapacityMode` runbook cambia el modo de capacidad de lectura/escritura de una o más tablas de Amazon DynamoDB (DynamoDB) al modo bajo demanda o al modo aprovisionado.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- CapacityMode

  Tipo: cadena

  Valores válidos: PROVISIONED | PAY_PER_REQUEST

  Descripción: (Obligatorio) El modo de capacidad de lectura/escritura deseado. Al cambiar de la capacidad bajo demanda (pay-per-request) a la aprovisionada, se deben establecer los valores iniciales de la capacidad aprovisionada. Los valores de la capacidad aprovisionada inicial se estiman en función de la capacidad de lectura y escritura consumida por la tabla y los índices secundarios globales durante los últimos 30 minutos.
- ReadCapacityUnits

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) El número máximo de lecturas muy consistentes que se consumen por segundo antes de que DynamoDB devuelva una excepción de limitación.
- TableNames

Tipo: cadena

Descripción: (Obligatoria) Lista de nombres de tablas de DynamoDB separados por comas para cambiar el modo de capacidad de lectura/escritura de...

- WriteCapacityUnits

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) El número máximo de escrituras consumidas por segundo antes de que DynamoDB devuelva una excepción de limitación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Cambia el modo de capacidad de lectura/escritura de las tablas de DynamoDB especificadas en el parámetro. `TableNames`

Salidas

CapacityModeSe ha cambiado el DBRW. SuccessesTables - Lista de nombres de tablas de DynamoDB en las que se ha cambiado correctamente el modo de capacidad

Se ha cambiado el DBRW. CapacityMode FailedTables - Lista cartográfica de los nombres de las tablas de DynamoDB en las que se ha producido un error al cambiar el modo de capacidad y el motivo del error.

AWS-CreateDynamoDBBackup

Descripción

Creación de una tabla de Amazon DynamoDB

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- BackupName

  Tipo: String

  Descripción: (Obligatorio) nombre de la copia de seguridad que se va a crear.
- LambdaAssumeRole

  Tipo: String

  Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.
- TableName

  Tipo: String

Descripción: (Obligatorio) nombre de la tabla de DynamoDB.

AWS-DeleteDynamoDbBackup

Descripción

Elimina la copia de seguridad de una tabla de Amazon DynamoDB.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BackupArn

  Tipo: String

  Descripción: (Obligatorio) ARN de la copia de seguridad de la tabla de DynamoDB que eliminar.

AWSConfigRemediation-DeleteDynamoDbTable

Descripción

El `AWSConfigRemediation-DeleteDynamoDbTable`runbook elimina la tabla de Amazon DynamoDB (DynamoDB) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- TableName

  Tipo: String

  Descripción: (Obligatorio) nombre de la tabla de DynamoDB que quiere eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Elimina la tabla de DynamoDB especificada en el parámetro. `TableName`
- `aws:executeScript`- Comprueba que se ha eliminado la tabla de DynamoDB.

`AWS-DeleteDynamoDbTableBackups`

Descripción

Elimine las copias de seguridad de tabla de DynamoDB basadas en días de retención o al recuento.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LambdaAssumeRole

  Tipo: String

  Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- RetentionCount

  Tipo: String

  Valor predeterminado: 10

  Descripción: (Opcional) el número de copias de seguridad que conservar para la tabla. Si existen más copias de seguridad que el número especificado de copias de seguridad, se eliminarán las copias de seguridad más antiguas. Se puede usar RetentionCount o RetentionDays, pero no ambos.
- RetentionDays

  Tipo: String

  Descripción: (Opcional) el número de días que conservar las copias de seguridad para la tabla. Las copias de seguridad más antiguas que el número de días especificado se eliminarán. Se puede usar RetentionCount o RetentionDays, pero no ambos.
- TableName

  Tipo: String

  Descripción: (Obligatorio) nombre de la tabla de DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descripción

El `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` runbook cifra una tabla de Amazon DynamoDB (DynamoDB) mediante la clave gestionada por el cliente AWS KMS() que especifique para AWS Key Management Service el parámetro. `KMSKeyId`

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre.
- KMS KeyId

  Tipo: cadena

  Descripción: (Obligatorio) El ARN de la clave administrada por el cliente que desea utilizar para cifrar la tabla de DynamoDB que especifica en el parámetro. `TableName`
- TableName

  Tipo: cadena

  Descripción: (Obligatorio) El nombre de la tabla de DynamoDB que quiere encriptar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Cifra la tabla de DynamoDB que especifique en el parámetro. `TableName`
- `aws:waitForAwsResourceProperty`- Comprueba que la `Enabled`propiedad de la tabla `SSESpecification`de DynamoDB esté establecida en. `true`

- `aws:assertAwsResourceProperty`- Comprueba que la tabla de DynamoDB esté cifrada con la clave gestionada por el cliente especificada en el parámetro. `KMSKeyId`

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descripción

El `AWSConfigRemediation-EnablePITRForDynamoDbTable`runbook habilita la recuperación a un momento dado (PITR) en la tabla de Amazon DynamoDB que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.

- TableName

  Tipo: String

  Descripción: (Obligatorio) El nombre de la tabla de DynamoDB para habilitar la recuperación a un momento dado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Permite la recuperación puntual en la tabla de DynamoDB que especifique en el parámetro. `TableName`
- `aws:assertAwsResourceProperty`- Confirma que la recuperación a un momento dado está habilitada en la tabla DynamoDB.

AWS-EnableDynamoDbAutoscaling

Descripción

El `AWS-EnableDynamoDbAutoscaling` runbook habilita Application Auto Scaling para la tabla de Amazon DynamoDB de capacidad aprovisionada que especifique. Application Auto Scaling ajusta dinámicamente la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico. Para obtener más información, consulte Administrar la capacidad de rendimiento automáticamente con el escalado automático de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- TableName

  Tipo: cadena

  Descripción: (Obligatorio) El nombre de la tabla de DynamoDB en la que desea activar Application Auto Scaling.

- MinReadCapacity

  Tipo: entero

  Descripción: (Obligatorio) El número mínimo de unidades de capacidad de lectura de rendimiento aprovisionadas para la tabla de DynamoDB.

- MaxReadCapacity

  Tipo: entero

  Descripción: (obligatorio) El número máximo de unidades de capacidad de lectura de rendimiento aprovisionadas para la tabla de DynamoDB.

- TargetReadCapacityUtilization

  Tipo: entero

  Descripción: (Obligatorio) El objetivo de utilización de la capacidad de lectura deseado. La utilización objetivo es el porcentaje del rendimiento aprovisionado consumido en un momento dado. Puede establecer los valores de utilización objetivo del escalado automático entre el 20 y el 90 por ciento.

- ReadScaleOutCooldown

  Tipo: entero

  Descripción: (Obligatorio) Cantidad de tiempo en segundos que se tarda en esperar a que surta efecto una actividad anterior de ampliación de la capacidad de lectura.

- ReadScaleInCooldown

  Tipo: entero

  Descripción: (Obligatorio) El tiempo en segundos transcurrido desde que se completa una actividad de ampliación de la capacidad de lectura antes de que se pueda iniciar otra actividad de ampliación horizontal.

- MinWriteCapacity

  Tipo: entero

  Descripción: (Obligatorio) El número mínimo de unidades de escritura de rendimiento aprovisionadas para la tabla de DynamoDB.

- MaxWriteCapacity

  Tipo: entero

  Descripción: (obligatorio) El número máximo de unidades de escritura de rendimiento aprovisionadas para la tabla de DynamoDB.

- TargetWriteCapacityUtilization

  Tipo: entero

  Descripción: (Obligatorio) El uso deseado de la capacidad de escritura objetivo. La utilización objetivo es el porcentaje del rendimiento aprovisionado consumido en un momento dado. Puede establecer los valores de utilización objetivo del escalado automático entre el 20 y el 90 por ciento.

- WriteScaleOutCooldown

  Tipo: entero

  Descripción: (Obligatorio) Cantidad de tiempo en segundos que se tarda en esperar a que surta efecto una actividad anterior de ampliación de la capacidad de escritura.

- WriteScaleInCooldown

  Tipo: entero

  Descripción: (Obligatorio) El tiempo en segundos transcurrido desde que se completa una actividad de ampliación de la capacidad de escritura antes de que se pueda iniciar otra actividad de ampliación horizontal.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi) - Configura Application Auto Scaling en la tabla de DynamoDB que especifique.
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep): duerme para evitar la limitación de la API.
- PutScalingPolicyWrite (aws:executeAwsApi) - Configura la utilización de la capacidad de escritura objetivo para la tabla de DynamoDB.
- PutScalingPolicyWriteDelay (aws:sleep): duerme para evitar la limitación de la API.
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi) - Configura las unidades de capacidad de lectura mínima y máxima para la tabla de DynamoDB.
- RegisterAppAutoscalingTargetReadDelay (aws:sleep): duerme para evitar la limitación de la API.
- PutScalingPolicyRead (aws:executeAwsApi) - Configura la utilización de la capacidad de lectura objetivo para la tabla de DynamoDB.
- VerifyDynamoDbAutoscalingEnabled (AWS:ExecuteScript) - Comprueba que Application Auto Scaling esté habilitado para la tabla de DynamoDB según los valores que especifique.

Salidas

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

AWS-RestoreDynamoDBTable

Descripción

El AWS-RestoreDynamoDBTablerunbook restaura la tabla de Amazon DynamoDB que haya especificado mediante la recuperación a un momento dado (PITR).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Habilite la recuperación puntual según sea necesario

  Tipo: booleano

  Valor predeterminado: true

  Descripción: (opcional) Determina si la automatización activa la recuperación puntual según sea necesario para restaurar la tabla.
- Anulación del índice secundario global

  Tipo: String

Descripción: (opcional) Los nuevos índices secundarios globales sustituirán a los índices secundarios existentes en la nueva tabla.

- Anulación del índice secundario local

  Tipo: String

  Descripción: (opcional) Los nuevos índices secundarios locales sustituirán a los índices secundarios existentes de la nueva tabla.

- RestoreDateTime

  Tipo: String

  Descripción: (Obligatorio) La recuperación a un momento dado a la que desea restaurar la tabla en los últimos 35 días. Especifique la fecha y hora en el siguiente formato: `DD/MM/YYYY HH:MM:SS`.

- Fuente: TabLearn

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia de ARN que desea reiniciar.

- Anulación de la especificación SSE

  Tipo: String

  Descripción: (opcional) La configuración de cifrado del lado del servidor que se utilizará en la nueva tabla.

- Nombre de la tabla de destino

  Tipo: String

  Descripción: (obligatorio) El nombre de la tabla que se va a restaurar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `dynamodb:BatchWriteItem`
- `dynamodb:DeleteItem`

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

Pasos de documentos

- `aws:executeScript`- Restaura la tabla de DynamoDB que especifique en `TargetTableName`el parámetro mediante la recuperación puntual.

Amazon EBS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Block Store. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

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

- AWS-ExtendEbsVolume
- AWSSupport-ModifyEBSSnapshotPermission
- AWSConfigRemediation-ModifyEBSVolumeType

AWSSupport-AnalyzeEBSResourceUsage

Descripción

El manual de `AWSSupport-AnalyzeEBSResourceUsage` automatización se utiliza para analizar el uso de los recursos en Amazon Elastic Block Store (Amazon Block Store). Analiza el uso del volumen e identifica los volúmenes, imágenes e instantáneas abandonados en una región determinada. AWS

¿Cómo funciona?

El manual realiza las cuatro tareas siguientes:

1. Comprueba que existe un bucket de Amazon Simple Storage Service (Amazon S3) o crea uno nuevo.
2. Reúne todos los volúmenes de Amazon EBS en el estado disponible.
3. Reúne todas las instantáneas de Amazon EBS para las que se ha eliminado el volumen de origen.
4. Reúne todas las imágenes de máquina de Amazon (AMI) que no estén siendo utilizadas por ninguna instancia no terminada de Amazon Elastic Compute Cloud (Amazon EC2).

El runbook genera informes CSV y los almacena en un bucket de Amazon S3 proporcionado por el usuario. El depósito proporcionado debe estar protegido siguiendo las mejores prácticas AWS de seguridad, tal como se describe al final. Si el bucket de Amazon S3 proporcionado por el usuario no existe en la cuenta, el runbook crea un nuevo bucket de Amazon S3 con el formato de nombre`<User-provided-name>-awssupport-YYYY-MM-DD`, cifrado con una clave personalizada AWS Key Management Service (AWS KMS), con el control de versiones de objetos habilitado, bloquea el acceso público y requiere solicitudes para usar SSL/TLS.

Si desea especificar su propio bucket de Amazon S3, asegúrese de que esté configurado siguiendo estas prácticas recomendadas:

- Bloquee el acceso público al bucket (establecido `IsPublic` en`False`).
- Active el registro de acceso a Amazon S3.

- Permita solo las solicitudes de SSL en su bucket.
- Activa el control de versiones de objetos.
- Usa una clave AWS Key Management Service (AWS KMS) para cifrar tu bucket.

> **Important**
>
> El uso de este manual puede implicar cargos adicionales en su cuenta por la creación de buckets y objetos de Amazon S3. Consulte los precios de Amazon S3 para obtener más información sobre los cargos en los que se puede incurrir.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- S3 BucketName

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

  Descripción: (obligatorio) El bucket de Amazon S3 de su cuenta en el que cargar el informe. Asegúrese de que la política de compartimentos no conceda permisos de lectura/escritura

innecesarios a las partes que no necesiten acceder a los registros recopilados. Si el depósito especificado no existe en la cuenta, la automatización crea un nuevo depósito en la región en la que se inicia la automatización con el formato de nombre<User-provided-name>-awssupport-YYYY-MM-DD, cifrado con una clave personalizada AWS KMS .

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

- CustomerManagedKmsKeyArn

  Tipo: cadena

  Descripción: (opcional) La AWS KMS clave personalizada Amazon Resource Name (ARN) para cifrar el nuevo bucket de Amazon S3 que se creará si el bucket especificado no existe en la cuenta. La automatización falla si se intenta crear el depósito sin especificar un ARN de AWS KMS clave personalizada.

  Valor permitido: (^$|^arn:aws:kms:[-a-z0-9]:[0-9]:key/[-a-z0-9]*$)

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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

Ejemplo de política con los permisos de IAM mínimos necesarios para ejecutar este manual:

```
       {
           "Version": "2012-10-17",
           "Statement": [{
               "Sid": "Read_Only_Permissions",
               "Effect": "Allow",
               "Action": [
                   "ec2:DescribeImages",
                   "ec2:DescribeInstances",
                   "ec2:DescribeSnapshots",
                   "ec2:DescribeVolumes",
                   "ssm:DescribeAutomationExecutions"
               ],
               "Resource": ""
           }, {
               "Sid": "KMS_Generate_Permissions",
               "Effect": "Allow",
               "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
               "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
           }, {
               "Sid": "S3_Read_Only_Permissions",
               "Effect": "Allow",
               "Action": [
                   "s3:GetBucketAcl",
                   "s3:GetBucketPolicyStatus",
                   "s3:GetBucketPublicAccessBlock",
                   "s3:ListBucket"
               ],
```

```
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/"
            ]
        }, {
            "Sid": "S3_Create_Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:PutBucketLogging",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }]
    }
```

Instrucciones

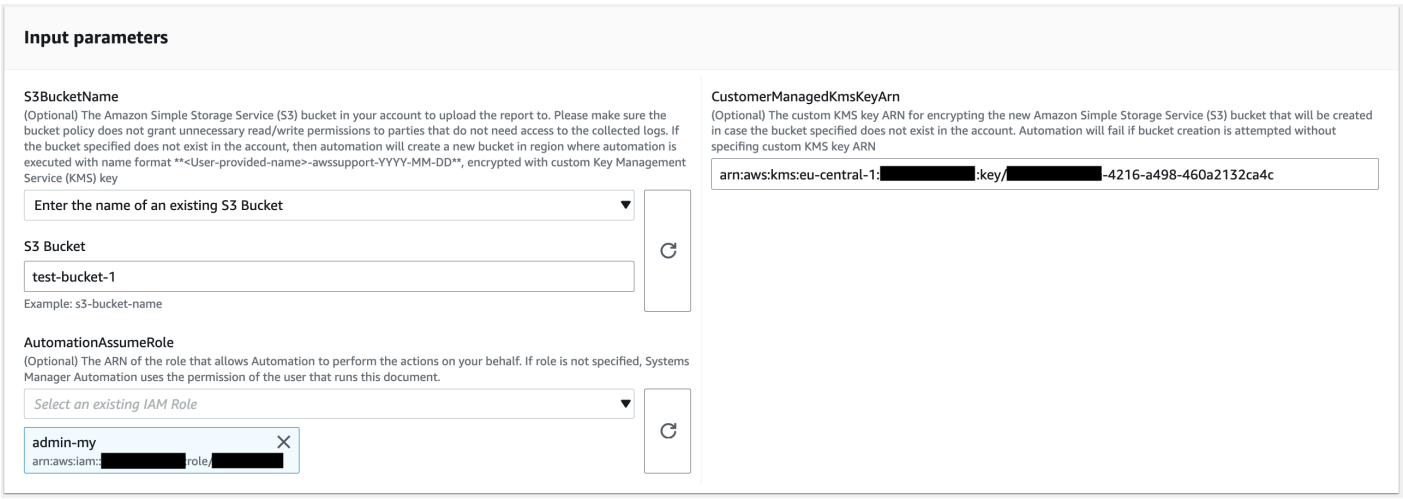
Siga estos pasos para configurar la automatización:

1. Navegue hasta AWSSupportResourceUsage-AnalyzeEBS en la consola. AWS Systems Manager
2. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
   - S3 BucketName (obligatorio):

     El bucket de Amazon S3 de su cuenta en el que cargar el informe.
   - CustomerManagedKmsKeyArn (Opcional):

     La AWS KMS clave personalizada Amazon Resource Name (ARN) para cifrar el nuevo bucket de Amazon S3 que se creará si el bucket especificado no existe en la cuenta.



3. Seleccione Ejecutar.
4. Se inicia la automatización.
5. El manual de procedimientos de automatización realiza los siguientes pasos:
   - Compruebe la simultaneidad:

     Garantiza que solo haya una iniciación de este manual en la región. Si el runbook encuentra otra ejecución en curso, devuelve un error y finaliza.
   - verifica OrCreate S3bucket:

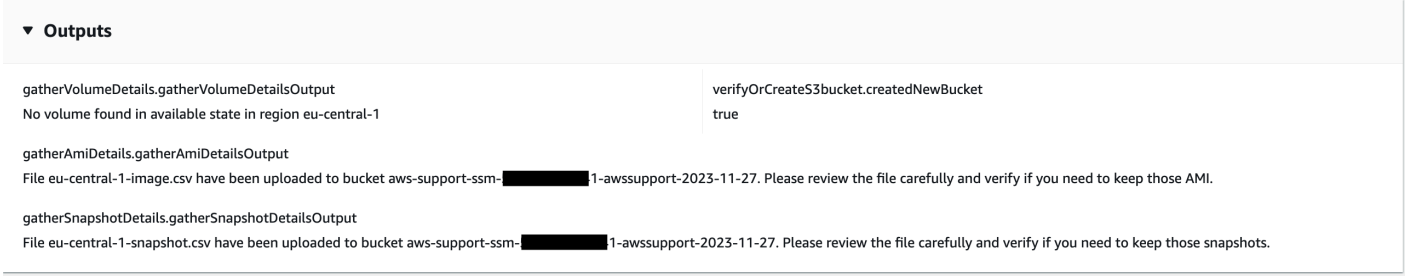
     Comprueba si existe el bucket de Amazon S3. De lo contrario, crea un nuevo bucket de Amazon S3 en la región en la que se inicia la automatización con el formato de nombre`<User-provided-name>-awssupport-YYYY-MM-DD`, cifrado con una AWS KMS clave personalizada.
   - recopilarAmiDetails:

     Busca AMI que no estén siendo utilizadas por ninguna instancia de Amazon EC2, genera el informe con el formato `<region>-images.csv` de nombre y lo carga en el bucket de Amazon S3.
   - recopila: VolumeDetails

     Verifica los volúmenes de Amazon EBS en el estado disponible, genera el informe con el formato `<region>-volume.csv` de nombre y lo carga en un bucket de Amazon S3.
   - recopila: SnapshotDetails

Busca las instantáneas de Amazon EBS de los volúmenes de Amazon EBS que ya se han eliminado, genera el informe con el formato `<region>-snapshot.csv` del nombre y lo carga en el bucket de Amazon S3.

6. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automatización
- Página de inicio de Support Automation Workflows

AWS-ArchiveEBSSnapshots

Descripción

El manual de procedimientos `AWS-ArchiveEBSSnapshots` le ayuda a archivar las instantáneas de los volúmenes de Amazon Elastic Block Store (Amazon EBS) especificando la etiqueta que ha aplicado a sus instantáneas. Como alternativa, puede proporcionar el ID de un volumen si sus instantáneas no están etiquetadas.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Descripción

  Tipo: cadena

  Descripción: (opcional) una descripción para la instantánea de Amazon EBS.
- DryRun

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (obligatorio) comprueba si tiene los permisos necesarios para la acción, sin realizar realmente la solicitud, y proporciona una respuesta de error.
- RetentionCount

  Tipo: cadena

  Descripción: (opcional) el número de instantáneas que desea archivar. No especifique un valor para este parámetro si especifica un valor para `RetentionDays`.
- RetentionDays

  Tipo: cadena

  Descripción: (opcional) el número de días anteriores de instantáneas que desea archivar. No especifique un valor para este parámetro si especifica un valor para `RetentionCount`.

- SnapshotWithEtiqueta

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (obligatorio) especifica si las instantáneas que desea archivar están etiquetadas.
- TagKey

  Tipo: cadena

  Descripción: (opcional) la clave de la etiqueta asignada a las instantáneas que desea archivar.
- TagValue

  Tipo: cadena

  Descripción: (opcional) el valor de la etiqueta asignada a las instantáneas que desea archivar.
- VolumeId

  Tipo: cadena

  Descripción: (opcional) el ID del volumen cuyas instantáneas desea archivar. Utilice este parámetro si sus instantáneas no están etiquetadas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

`aws:executeScript`: archiva las instantáneas usando la etiqueta que especifique mediante los parámetros `TagKey` y `TagValue` o el parámetro `VolumeId`.

AWS-AttachEBSVolume

Descripción

Adjunte una Amazon Elastic Block Store (Amazon EBS) a una instancia Amazon Elastic Compute Cloud (Amazon EC2).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Dispositivo

  Tipo: cadena

  Descripción: (obligatorio) el nombre del dispositivo (por ejemplo, /dev/sdh o xvdh).
- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia en la que desea asociar el volumen.
- VolumeId

  Tipo: cadena

  Descripción: (obligatorio) ID del volumen de Amazon EBS. El volumen y la instancia deben estar dentro de la misma zona de disponibilidad.

AWSSupport-CalculateEBSPerformanceMetrics

Descripción

El `AWSSupport-CalculateEBSPerformanceMetrics` manual ayuda a diagnosticar los problemas de rendimiento de Amazon EBS mediante el cálculo y la publicación de las métricas de rendimiento en un CloudWatch panel de control. El panel muestra las IOPS y el rendimiento medios estimados para un volumen de Amazon EBS objetivo o todos los volúmenes adjuntos a la instancia de Amazon Elastic Compute Cloud (Amazon EC2) de destino. En el caso de las instancias Amazon EC2, también muestra el rendimiento y las IOPS promedio de la instancia. El manual muestra el enlace al CloudWatch panel recién creado, que muestra las métricas calculadas relevantes. CloudWatch El CloudWatch panel se crea en su cuenta con el nombre:`AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

¿Cómo funciona?

El manual realiza los siguientes pasos:

- Garantiza que las marcas de tiempo especificadas sean válidas.
- Valida si el ID de recurso (volumen de Amazon EBS o instancia de Amazon EC2) es válido.
- Cuando proporciona un Amazon EC2 como ResourceID, se crea un CloudWatch panel con las IOPs/rendimiento totales reales de esa instancia de Amazon EC2 y un gráfico de IOPs/rendimiento promedio estimado para todos los volúmenes de Amazon EBS adjuntos a una instancia de Amazon EC2.
- Cuando proporcionas un volumen de Amazon EBS como ResourceID, se crea un panel con CloudWatch un gráfico de IOPs/rendimiento promedio estimado para ese volumen.
- Una vez generado el CloudWatch panel, si las IOPS promedio estimadas o el rendimiento promedio estimado son superiores a las IOPS máximas o al rendimiento máximo, respectivamente, es posible realizar microráfagas para el volumen o los volúmenes adjuntos a una instancia de Amazon EC2.

> **Note**
>
> En el caso de los volúmenes con capacidad de ráfaga (gp2, sc2 y st1), se debe tener en cuenta el rendimiento y las IOPs máximos hasta lograr un equilibrio de ráfaga. Una vez que

el equilibrio de ráfaga se haya utilizado por completo, es decir, cuando pase a cero, tenga en cuenta las métricas de rendimiento y IOPS de referencia.

Important

La creación del CloudWatch panel de control puede conllevar cargos adicionales a su cuenta. Para obtener más información, consulta la guía de CloudWatch precios de Amazon.

Ejecuta esta automatización (consola)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Ejemplo de política

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

Instrucciones

Siga estos pasos para configurar la automatización:

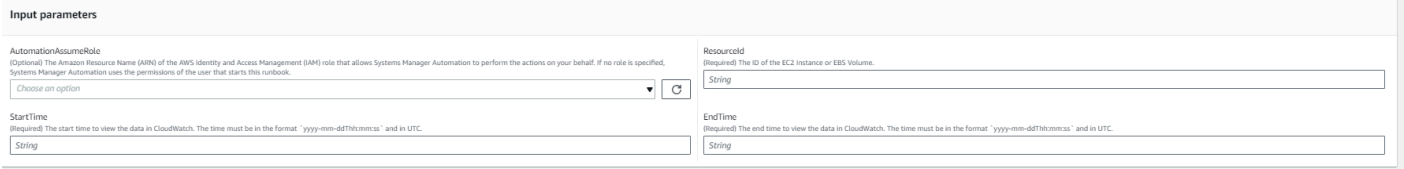
1. Navegue hasta AWSSupport-CalculateEBSPerformanceMetricsSystems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
   - ResourceID (obligatorio):

     El ID de la instancia de Amazon EC2 o del volumen de Amazon EBS.
   - Hora de inicio (obligatorio):

     Hora de inicio para ver los datos CloudWatch. La hora debe estar en el formato `yyyy-mm-ddThh:mm:ss` y en UTC.
   - Hora de finalización (obligatoria):

     Hora de finalización para ver los datos CloudWatch. La hora debe estar en el formato `yyyy-mm-ddThh:mm:ss` y en UTC.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - CheckResourceIdAndTimeStamps:

     Comprueba si la hora de finalización es superior a la hora de inicio en al menos un minuto y si el recurso proporcionado existe.
   - CreateCloudWatchDashboard:

     Calcula el rendimiento de Amazon EBS y muestra un gráfico basado en su ID de recurso. Si proporciona un ID de volumen de Amazon EBS para el parámetro ID de recurso, este manual crea un panel con el promedio estimado de IOPS y el rendimiento promedio estimado para el volumen de Amazon EBS. Si proporciona un ID de instancia de Amazon EC2 para el parámetro ID de recurso, este manual crea un CloudWatch panel con el promedio de IOPS totales y el rendimiento total promedio de la instancia de Amazon EC2 y con el promedio estimado de IOPS y el rendimiento promedio estimado para todos los volúmenes de Amazon EBS adjuntos a la instancia de Amazon EC2.
7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

Ejemplo de CloudWatch panel para el ID de recurso como instancia de 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

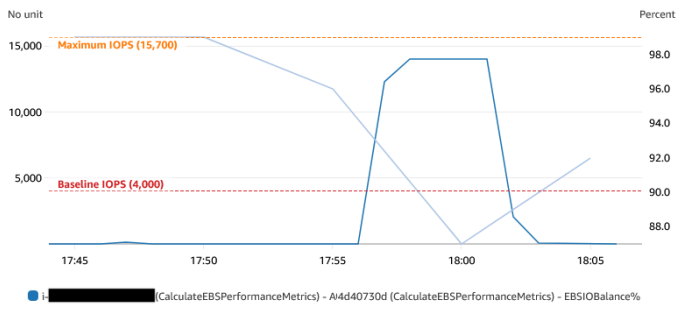
More details on EBS Optimized instances | More details on EBS Volume Types

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

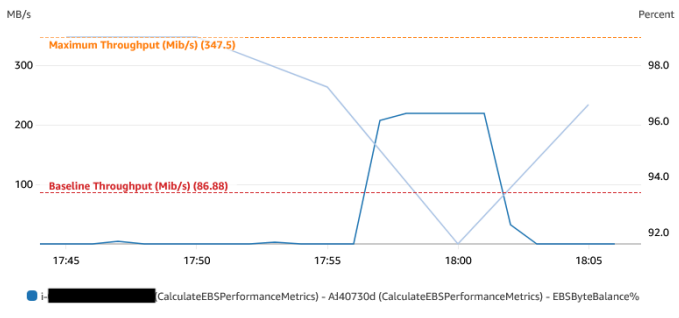
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

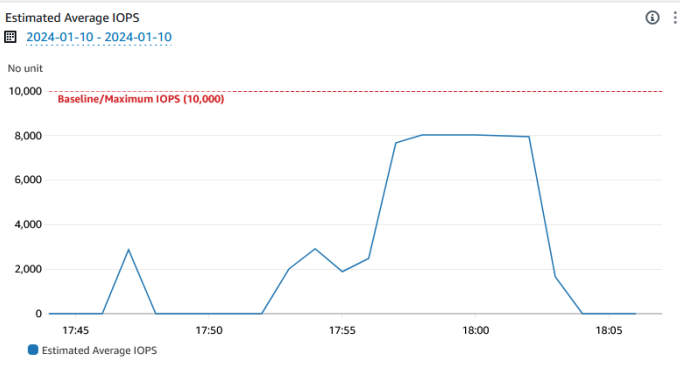
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

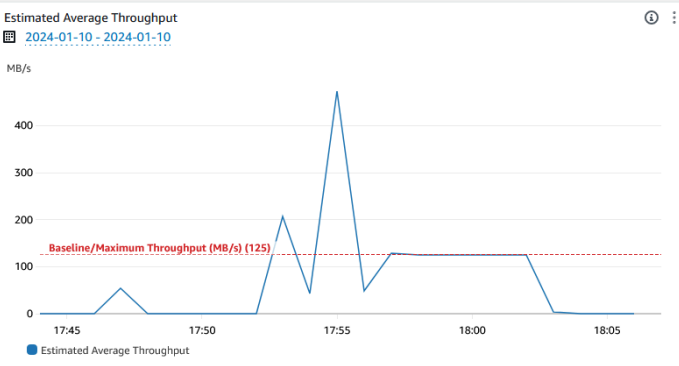
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

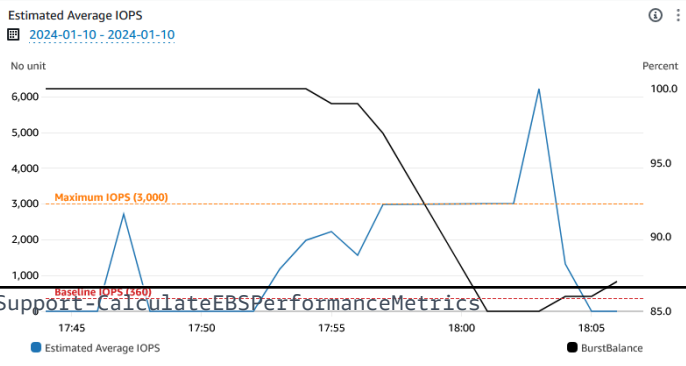


Estimated Average Throughput
2024-01-10 - 2024-01-10

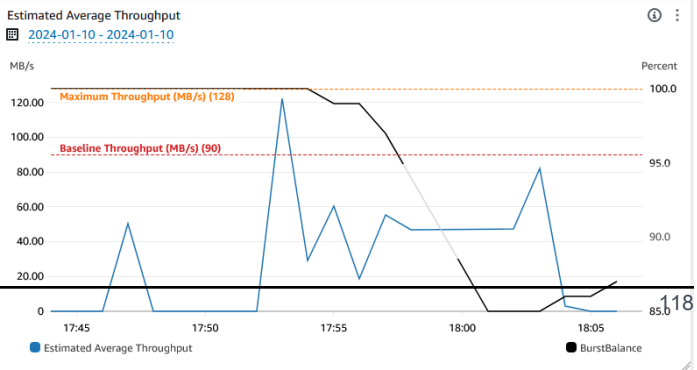


Volume: vol[redacted] | Type: gp2

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



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

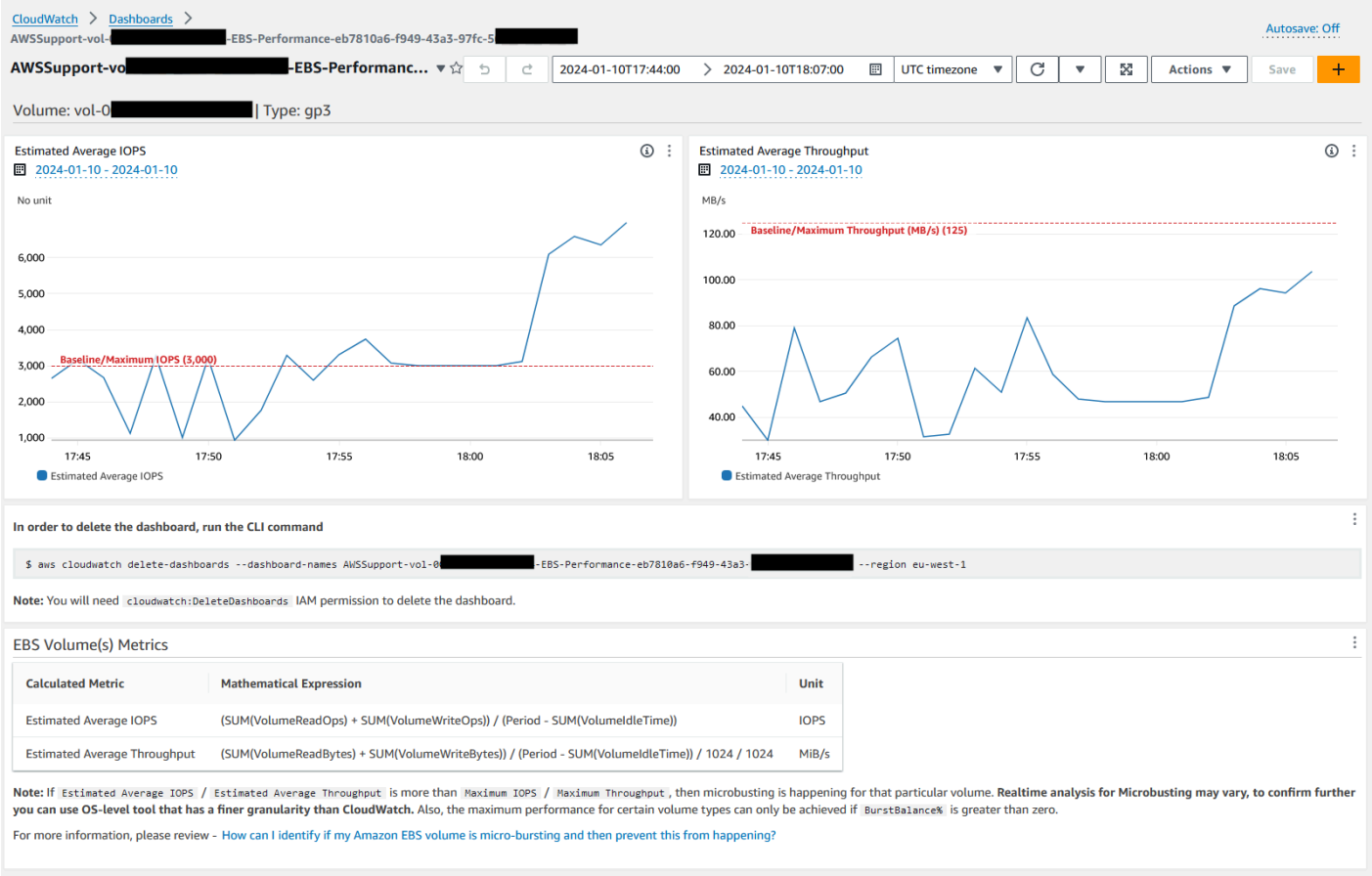


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

Ejemplo de CloudWatch panel para el identificador de recurso como identificador de volumen de Amazon EBS



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- ¿Cómo puedo identificar si mi volumen de Amazon EBS tiene una microráfaga y evitar que esto suceda?

- ¿Cómo puedo CloudWatch ver las métricas de rendimiento agregadas de Amazon EBS para una instancia EC2?

AWS-CopySnapshot

Descripción

Copia una point-in-time instantánea de un volumen de Amazon Elastic Block Store (Amazon EBS). Puede copiar la instantánea dentro de la misma región Región de AWS o de una región a otra. Las copias de instantáneas de EBS cifradas permanecen cifradas. Las copias de instantáneas sin cifrar permanecen sin cifrar. Para copiar una instantánea cifrada que se compartió desde otra cuenta, debe tener permisos para la clave maestra del cliente (CMK) de KMS utilizada para cifrar la instantánea. Las instantáneas creadas mediante la copia de otra instantánea tienen un ID de volumen arbitrario que no debe utilizarse para ningún fin.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Descripción

Tipo: cadena

Descripción: (opcional) una descripción para la instantánea de Amazon EBS.

- SnapshotId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instantánea de Amazon EBS que copiar.

- SourceRegion

  Tipo: cadena

  Descripción: (obligatorio) la región en la que se encuentra actualmente la instantánea de origen.

Pasos de documentos

copySnapshot: copia una instantánea de un volumen de Amazon EBS.

Salidas

CopySnapshot. SnapshotId - El ID de la nueva instantánea.

AWS-CreateSnapshot

Descripción

Cree una instantánea de un volumen de Amazon EBS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Descripción

  Tipo: cadena

  Descripción: (opcional) una descripción de la instantánea.
- VolumeId

  Tipo: cadena

  Descripción: (obligatorio) ID del volumen.

AWS-DeleteSnapshot

Descripción

Elimina una instantánea de volumen de Amazon EBS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- SnapshotId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instantánea de EBS.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedEBSVolume` elimina un volumen de Amazon Elastic Block Store (Amazon EBS) no utilizado.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- CreateSnapshot

  Tipo: Booleano

  Descripción: (opcional) si se establece en `true`, la automatización crea una instantánea del volumen de Amazon EBS antes de eliminarlo.
- VolumeId

  Tipo: cadena

  Descripción: (obligatorio) el ID del volumen de Amazon EBS que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: verifica que el volumen de Amazon EBS que especifique en el parámetro `VolumeId` no esté en uso y crea una instantánea en función del valor que elija para el parámetro `CreateSnapshot`.
- `aws:branch`: se ramifica en función del valor que haya elegido para el parámetro `CreateSnapshot`.
- `aws:waitForAwsResourceProperty`: espera a que se complete la instantánea.
- `aws:executeAwsApi`: elimina la instantánea si la creación de la instantánea ha fallado.
- `aws:executeAwsApi`: elimina el volumen de Amazon EBS que especifique en el parámetro `VolumeId`.
- `aws:executeScript`: verifica que se haya eliminado el volumen de Amazon EBS.

AWS-DeregisterAMIs

Descripción

El manual de procedimientos `AWS-DeregisterAMIs` le ayuda a anular el registro Amazon Machine Images (AMIs) especificando la etiqueta que ha aplicado a su AMIs.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- DryRun

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (obligatorio) comprueba si tiene los permisos necesarios para la acción, sin realizar realmente la solicitud, y proporciona una respuesta de error.
- RetainNumber

  Tipo: cadena

Descripción: (opcional) el número de AMIs que desea retener. No especifique un valor para este parámetro si especifica un valor para `Age`.

- Antigüedad

  Tipo: cadena

  Descripción: (opcional) El número de días anteriores de AMIs que desea retener. No especifique un valor para este parámetro si especifica un valor para `RetainNumber`.

- TagKey

  Tipo: cadena

  Descripción: (obligatorio) la clave de la etiqueta asignada a la AMIs cuyo registro desea anular.

- TagValue

  Tipo: cadena

  Descripción: (obligatorio) el valor de la etiqueta asignada a la AMIs cuyo registro desea anular.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: valida los valores que especifique para los parámetros de entrada del manual de procedimientos.
- `aws:executeAwsApi`: anula el registro AMIs con la etiqueta que especifique con los parámetros `TagKey` y `TagValue`.

AWS-DetachEBSVolume

Descripción

Separa un volumen de Amazon EBS de una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LambdaAssumeRol

  Tipo: cadena

  Descripción: (opcional) el ARN del rol asumido por Lambda.
- VolumeId

  Tipo: cadena

  Descripción: (obligatorio) ID del volumen de EBS. El volumen y la instancia deben estar dentro de la misma zona de disponibilidad.

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descripción

El `AWSConfigRemediation-EnableEbsEncryptionByDefault` manual permite el cifrado de todos los volúmenes nuevos de Amazon Elastic Block Store (Amazon EBS) que se encuentren en el Región de AWS lugar donde se ejecute la Cuenta de AWS automatización. Los volúmenes que se crearon antes de ejecutar la automatización no están cifrados.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: habilita la configuración de cifrado predeterminada de Amazon EBS en la cuenta y la región actual.
- `aws:assertAwsResourceProperty`: verifica que la configuración de cifrado predeterminada de Amazon EBS esté habilitada.

AWS-ExtendEbsVolume

Descripción

El manual de procedimientos `AWS-ExtendEbsVolume` aumenta el tamaño de un volumen de Amazon EBS y amplía el sistema de archivos. Esta automatización es compatible con los sistemas de archivos `xfs` y `ext4`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- DriveLetter

  Tipo: cadena

Descripción: (opcional) la letra de la unidad cuyo sistema de archivos desea ampliar. Este parámetro es obligatorio para las instancias de Windows.

- InstanceId

  Tipo: cadena

  Descripción: (opcional) el ID de la instancia de Amazon EC2 a la que se adjunta el volumen de Amazon EBS que desea ampliar.

- KeepSnapshot

  Tipo: Booleano

  Predeterminado: true

  Descripción: (opcional) determina si se debe conservar la instantánea creada antes de aumentar el tamaño del volumen de su Amazon EBS.

- MountPoint

  Tipo: cadena

  Descripción: (opcional) el punto de montaje de la unidad cuyo sistema de archivos desea ampliar. Este parámetro es obligatorio para las instancias de Linux.

- SizeGib

  Tipo: cadena

  Descripción: (obligatorio) el tamaño en GiB al que desea modificar su volumen de Amazon EBS.

- VolumeId

  Tipo: cadena

  Descripción: (obligatorio) el ID del volumen de EBS que desea ampliar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:CreateSnapshot`

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

Pasos de documentos

- aws:executeScript: aumenta el tamaño del volumen hasta el valor que especifique en el parámetro VolumeId y amplía el sistema de archivos.

AWSSupport-ModifyEBSSnapshotPermission

Descripción

El manual de procedimientos AWSSupport-ModifyEBSSnapshotPermission le ayuda a modificar los permisos de varias instantáneas de Amazon Elastic Block Store (Amazon EBS). Con este manual de procedimientos, puede crear instantáneas Public o Private y compartirlas con otras Cuentas de AWS. Las instantáneas cifradas con una clave de KMS predeterminada no se pueden compartir con otras cuentas que utilicen este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AccountIds

  Tipo: StringList

  Predeterminado: none

  Descripción: (opcional) los ID de las cuentas con las que desea compartir instantáneas. Este parámetro es obligatorio si especifica un valor No para el parámetro `Private`.

- AccountPermissionOperación

  Tipo: cadena

  Valores válidos: add | remove

  Predeterminado: none

  Descripción: (opcional) el tipo de operación que se va a realizar.

- Private

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (obligatorio) introduzca No para el valor si desea compartir instantáneas con cuentas específicas.

- SnapshotIds

  Tipo: StringList

  Descripción: (obligatorio) los ID de las instantáneas de Amazon EBS cuyo permiso desea modificar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

1. `aws:executeScript`: verifica los ID de las instantáneas proporcionadas en el parámetro `SnapshotIds`. Tras comprobar los ID, el script comprueba si hay instantáneas cifradas y genera una lista si encuentra alguna.
2. `aws:branch`: ramifica la automatización en función del valor que introduzca para el parámetro `Private`.
3. `aws:executeScript`: modifica los permisos de las instantáneas especificadas para compartirlas con las cuentas especificadas.
4. `aws:executeScript`: modifica los permisos de las instantáneas para cambiarlos de `Public` a `Private`.

Salidas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherCuentas. Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSConfigRemediation-ModifyEBSVolumeType

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyEBSVolumeType` modifica el tipo de volumen de un volumen de Amazon Elastic Block Store (Amazon EBS). Una vez modificado el

tipo de volumen, el volumen entra en un estado `optimizing`. Para obtener información sobre la supervisión del progreso de las modificaciones de volumen, consulte Supervisar el progreso de las modificaciones de volumen en la Guía del usuario de Amazon EC2.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- EbsVolumeID

  Tipo: cadena

  Descripción: (obligatorio) el ID del volumen de Amazon EBS que desea modificar.
- EbsVolumeTipo

  Tipo: cadena

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

  Descripción: El tipo de volumen al que desea cambiar el volumen de Amazon EBS. Para obtener información sobre los tipos de volúmenes de Amazon EBS, consulte los tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EC2.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:waitForAwsResourceProperty`: verifica que el estado del volumen es `available` o `in-use`.
- `aws:executeAwsApi`: modifica el volumen de Amazon EBS que especifique en el parámetro `EbsVolumeId`.
- `aws:waitForAwsResourceProperty`: verifica que el tipo de volumen se ha cambiado al valor que especificó en el parámetro `EbsVolumeType`.

Amazon EC2

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Compute Cloud. Los manuales de procedimientos de Amazon Elastic Block Store se encuentran en la sección Amazon EBS de referencia del manual de procedimientos. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- 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

Descripción

Cambie el estado de espera de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de Auto Scaling.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de una instancia Amazon EC2 para la que desea cambiar el estado de espera dentro de un grupo de Auto Scaling.
- LambdaRoleArn

  Tipo: String

  Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

AWS-ASGExitStandby

Descripción

Cambie el estado de espera de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de Auto Scaling.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de una instancia EC2 para la que desea cambiar el estado de espera dentro de un grupo de Auto Scaling.
- LambdaRoleArn

  Tipo: String

  Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

AWS-CreateImage

Descripción

Lanza una Amazon Machine Image(AMI) nueva de una instancia Amazon Elastic Compute Cloud (Amazon EC2).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia EC2.
- NoReboot

  Tipo: booleano

  Descripción: (Opcional) no reinicie la instancia antes de crear la imagen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage",
```

```
                "ec2:DescribeImages"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS-DeleteImage

Descripción

Elimine una Amazon Machine Image(AMI) y todas las instantáneas asociadas.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- ImageId

  Tipo: String

Descripción: (Obligatorio) ID de la AMI.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

```
{
    "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

Descripción

Parchee instancias de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de escalado automático.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia que parchear. No especifique un ID de instancia que esté configurado para ejecutarse durante un período de mantenimiento.
- LambdaRoleArn

  Tipo: String

  Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función de Lambda.
- WaitForInstance

  Tipo: String

  Valor predeterminado: PT2M

  Descripción: (Opcional) la duración de la Automation debería suspenderse para permitir a la instancia regresar al servicio.
- WaitForReboot

Tipo: String

Valor predeterminado: PT5M

Descripción: (Opcional) la duración de la Automation debería suspenderse para permitir el reinicio de una instancia parcheada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Descripción

Hace que una instancia de EC2 cumpla con la línea de base de revisiones aplicable. Revierte el volumen raíz en caso de fallo.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) InstanceId de EC2 al que aplicamos la base de referencia de parches.
- LambdaAssumeRole

  Tipo: String

Descripción: (Opcional) ARN del rol que permite a la Lambda creada por la Automation para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- ReportS3Bucket

  Tipo: String

  Descripción: (Opcional) destino del bucket de Amazon S3 Bucket para el informe de conformidad generado durante el proceso.

Pasos de documentos

Número de paso	Nombre de paso	Acción de Automation
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`

Número de paso	Nombre de paso	Acción de Automation
10	DeleteSnapshot	`aws:invokeLambdaFunction`
11	deleteCloudFormationTemplate	`aws:deleteStack`

Salidas

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

`AWS-QuarantineEC2Instance`

Descripción

Con el manual de procedimientos `AWS-QuarantineEC2Instance`, puede asignar un grupo de seguridad a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que no permita tráfico entrante o saliente.

> **Important**
>
> Los cambios en la configuración de RDP deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia administrada para administrar la configuración de RDP.
- IsolationSecurityGroup

  Tipo: String

  Descripción: (Obligatorio) El nombre del grupo de seguridad que desea asignar a la instancia para evitar el tráfico entrante o saliente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:ModifyInstanceAttribute
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

Pasos de documentos

- aws:executeAwsApi - Recopila detalles sobre la instancia.
- aws:executeScript - Verifica que la instancia no forma parte de un grupo de escalado automático.
- aws:executeAwsApi - Crea una instantánea del volumen raíz adjunta a la instancia.
- aws:waitForAwsResourceProperty - Espera a que el estado de la instantánea sea completed.
- aws:executeAwsApi - Asigna el grupo de seguridad especificado en el parámetro IsolationSecurityGroupa su instancia.

Salidas

GetEC2InstanceResources.RevokedSecurityGroupsIds

GetEC2InstanceResources.RevokedSecurityGroupsNames

createSnapshot.SnapId

AWS-ResizeInstance

Descripción

Cambie la instancia de replicación de una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia.
- InstanceType

  Tipo: String

  Descripción: (Obligatorio) tipo de instancia.
- LambdaAssumeRole

  Tipo: String

  Descripción: (Opcional) el ARN del rol asumido por Lambda.

AWS-RestartEC2Instance

Descripción

Renicar una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2)

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: StringList

  Descripción: (Obligatorio) ID de la instancia Amazon EC2 que reiniciar.

AWS-SetupJupyter

Descripción

El manual de procedimientos `AWS-SetupJupyter`le ayuda a configurar el cuaderno de Jupyter en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Puede especificar una instancia existente o proporcionar un ID Amazon Machine Image(AMI) para que la automatización lance y configure una nueva instancia. Antes de comenzar, debe crear un parámetro `SecureString`en Parameter Store para usarlo como contraseña del cuaderno de Jupyter. Parameter Store es una función de AWS Systems Manager. Para obtener más información acerca de la creación de parámetros, consulte Cración de parámetros en el Guía del usuario de AWS Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- AmiId

  Tipo: String

  Descripción: (Opcional) El ID de AMIque desea usar para lanzar una nueva instancia y configurar el cuaderno de Jupyter.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia en la que desea confgurar el cuaderno de Jupyter.
- InstanceType

  Tipo: String

  Valor predeterminado: t3.medium

  Descripción: (Opcional) Si va a lanzar una nueva instancia para configurar el cuaderno de Jupyter, especifique el tipo de instancia que desea usar.

- JupyterPasswordSSMKey

  Tipo: String

  Descripción: (Obligatorio) El nombre del parámetro `SecureString`en Parameter Store que desea utilizar como contraseña para el cuaderno de Jupyter.
- KeyPairName

  Tipo: String

  Descripción: (Opcional) El par de claves que desea asociar con la instancia recién lanzada.
- RemoteAccessCidr

  Tipo: String

  Valor predeterminado: 0.0.0.0/0

  Descripción: (Opcional) El rango de CIDR desde el que desea permitir el tráfico SSH.
- RoleName

  Tipo: String

  Valor predeterminado: SSMManagedInstanceProfileRole

  Descripción: (Opcional) El nombre del perfil de instancia de la instancia recién lanzada.
- StackName

  Tipo: String

  Valor predeterminado: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  Descripción: (Opcional) El nombre de la pila AWS CloudFormationque desea que utilice la automatización.
- SubnetId

  Tipo: String

  Valor predeterminado: Default

  Descripción: (Opcional) La subred en la que desea lanzar la instancia nueva para usarla.
- VpcId

Tipo: String

Valor predeterminado: Default

Descripción: (Opcional) El ID de la nube privada virtual (VPC) en la que desea lanzar la instancia nueva.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript` - Configura el cuaderno de Jupyter en la instancia que especifique, o en una instancia recién lanzada, utilizando los valores que especifique para los parámetros de entrada del manual de procedimientos.

`AWS-StartEC2Instance`

Descripción

Empieza una o más Instancias de Amazon Elastic Compute Cloud (Amazon EC2)

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- InstanceId

  Tipo: StringList

  Descripción: (Requerido) instancias EC2 para iniciar.

AWS-StopEC2Instance

Descripción

Detiene una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2)

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: StringList

  Descripción: (Requerido) instancias EC2 para detener.

AWS-TerminateEC2Instance

Descripción

Termine una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: StringList

  Descripción: (Obligatorio) ID de una o varias instancias EC2 que se van a terminar.

AWS-UpdateLinuxAmi

Descripción

Actualice un Amazon Machine Image (AMI) con los paquetes de distribución de Linux y el software de Amazon.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ExcludePackages

  Tipo: cadena

  Predeterminado: none

  Descripción: (opcional) nombres de los paquetes a los que no se aplicarán las actualizaciones, en todas las condiciones. De forma predeterminada (“none”), no se excluye ningún paquete.
- IamInstanceProfileName

  Tipo: cadena

  Predeterminado: ManagedInstanceProfile

  Descripción: (obligatorio) perfil de instancia que permite a Systems Manager administrar la instancia.
- IncludePackages

Tipo: cadena

Valor predeterminado: all

Descripción: (opcional) actualizar solo estos paquetes designados. De forma predeterminada (“all”), se aplican todas las actualizaciones disponibles.

- InstanceType

  Tipo: cadena

  Valor predeterminado: t2.micro

  Descripción: (opcional) tipo de instancia que se lanzará como el host de espacio de trabajo. Los tipos de instancia varían según la región.

- MetadataOptions

  Tipo: StringMap

  Predeterminado: {» HttpEndpoint «: «habilitado», "HttpTokens«: «opcional"}

  Descripción: (opcional) las opciones de metadatos de la instancia. Para obtener más información, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

  Tipo: cadena

  Predeterminado: none

  Descripción: (opcional) URL de un script que se ejecutará después de que se apliquen las actualizaciones de paquete. El valor predeterminado (“none”) es no ejecutar un script.

- PreUpdateScript

  Tipo: cadena

  Predeterminado: none

  Descripción: (opcional) URL de un script que se ejecutará antes de que se apliquen las actualizaciones. El valor predeterminado (“none”) es no ejecutar un script.

- SecurityGroupIds

Tipo: cadena

Descripción: (Obligatorio) Lista separada por comas de los identificadores de los grupos de seguridad que desea aplicar a losAMI.

- SourceAmiId

  Tipo: cadena

  Descripción: (obligatorio) ID de la imagen de máquina de Amazon de origen.

- SubnetId

  Tipo: cadena

  Descripción: (opcional) el ID de la subred en la que quiere lanzar la instancia. Si ha eliminado la VPC predeterminada, se necesita este parámetro.

- TargetAmiName

  Tipo: cadena

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

  Descripción: (opcional) nombre de la nueva AMI que se va a crear. El valor predeterminado es una cadena generada por el sistema que incluye el ID de la AMI de origen, así como la hora y la fecha de creación.

AWS-UpdateWindowsAmi

Descripción

Actualice una Amazon Machine Image (AMI) de Microsoft Windows. De forma predeterminada, este manual de procedimientos instala todas las actualizaciones de Windows, el software de Amazon y los controladores de Amazon. A continuación, ejecuta Sysprep para crear una nueva AMI. Admite Windows Server 2008 R2 o posterior.

> **Important**
>
> Si tus instancias se conectan AWS Systems Manager mediante puntos de enlace de VPC, este manual fallará a menos que se utilice en la región us-east-1. Las instancias deben tener habilitado TLS 1.2 para usar este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Categorías

  Tipo: cadena

  Descripción: (opcional) especificar una o más categorías de actualización. Puede filtrar las categorías usando valores separados por comas. Opciones: Aplicación, conectores, CriticalUpdates, DefinitionUpdates DeveloperKits, ControladoresFeaturePacks, Guía, Microsoft SecurityUpdates, ServicePacks, HerramientasUpdateRollups, Actualizaciones. Los formatos válidos incluyen una sola entrada, por ejemplo:CriticalUpdates. O puede especificar una lista

separada por comas:CriticalUpdates,SecurityUpdates. NOTA: No puede haber ningún espacio ni antes ni después de las comas.

- ExcludeKbs

  Tipo: cadena

  Descripción: (opcional) especificar uno o varios ID de artículo de la Base de conocimientos de Microsoft (KB) para excluirlos. Puede excluir varios ID utilizando valores separados por comas. Formatos válidos: KB9876543 o 9876543.

- IamInstanceProfileName

  Tipo: cadena

  Predeterminado: ManagedInstanceProfile

  Descripción: (obligatorio) nombre del rol que permite a Systems Manager administrar la instancia.

- IncludeKbs

  Tipo: cadena

  Descripción: (opcional) especificar uno o varios ID de artículo de la Base de conocimientos de Microsoft (KB) para incluirlos. Puede instalar varios ID utilizando valores separados por comas. Formatos válidos: KB9876543 o 9876543.

- InstanceType

  Tipo: cadena

  Valor predeterminado: t2.medium

  Descripción: (opcional) tipo de instancia que se lanzará como el host de espacio de trabajo. Los tipos de instancia varían según la región. El valor predeterminado es t2.medium.

- MetadataOptions

  Tipo: StringMap

  Predeterminado: {» HttpEndpoint «: «habilitado», "HttpTokens«: «opcional"}

  Descripción: (opcional) las opciones de metadatos de la instancia. Para obtener más información, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

Tipo: cadena

Descripción: (opcional) script proporcionado como una cadena. Se ejecutará después de instalar las actualizaciones del SO.

- PreUpdateScript

  Tipo: cadena

  Descripción: (opcional) script proporcionado como una cadena. Se ejecutará antes de instalar las actualizaciones del SO.

- PublishedDateAfter

  Tipo: cadena

  Descripción: (opcional) especificar la fecha después de la cual deben haberse publicado las actualizaciones. Por ejemplo, si se especifica 01/01/2017, devolverá las actualizaciones que se encontraron durante la búsqueda de Windows Update y que se publicaron a partir del 01/01/2017.

- PublishedDateBefore

  Tipo: cadena

  Descripción: (opcional) especificar la fecha antes de la cual deben haberse publicado las actualizaciones. Por ejemplo, si se especifica 01/01/2017, devolverá las actualizaciones que se encontraron durante la búsqueda de Windows Update y que se publicaron antes del 01/01/2017.

- PublishedDaysOld

  Tipo: cadena

  Descripción: (opcional) especificar el número de días de antigüedad que tienen que tener las actualizaciones desde la fecha de publicación. Por ejemplo, si se especifica 10, devolverá todas las actualizaciones que se encuentren durante la búsqueda de Windows Update y que se hayan publicado hace 10 o más días.

- SecurityGroupIds

  Tipo: cadena

  Descripción: (Obligatorio) Lista separada por comas de los identificadores de los grupos de seguridad que desea aplicar a losAMI.

- SeverityLevels

  Tipo: cadena

  Descripción: (opcional) especificar uno o varios niveles de gravedad de MSRC asociados con una actualización. Puede filtrar los niveles de gravedad usando valores separados por comas. De forma predeterminada, se seleccionan parches para todos los niveles de seguridad. Si se suministra un valor, la lista de actualizaciones se filtrará por dichos valores. Opciones: Critical, Important, Low, Moderate o Unspecified. Los formatos válidos incluyen una sola entrada, por ejemplo: Critical. O bien, puede especificar una lista separada por comas: Critical,Important,Low.
- SourceAmiId

  Tipo: cadena

  Descripción: (obligatorio) El AMI ID de origen.
- SubnetId

  Tipo: cadena

  Descripción: (opcional) el ID de la subred en la que quiere lanzar la instancia. Si ha eliminado la VPC predeterminada, se necesita este parámetro.
- TargetAmiName

  Tipo: cadena

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

  Descripción: (opcional) nombre de la nueva AMI que se va a crear. El valor predeterminado es una cadena generada por el sistema que incluye el ID de la AMI de origen, así como la hora y la fecha de creación.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck`permite realizar comprobaciones de estado para el grupo de escalado automático de Amazon EC2 (Auto Scaling) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- AutoScalingGroupARN

  Tipo: String

  Descripción: (Obligatorio) El nombre de recurso de Amazon (ARN) del grupo de escalado automático en el que desea habilitar las comprobaciones de estado.
- HealthCheckGracePeriod

  Tipo: entero

  Predeterminado: 300

  Descripción: (Opcional) La cantidad de tiempo, en segundos, que Auto Scaling espera antes de comprobar el estado de una instancia Amazon Elastic Compute Cloud (Amazon EC2) que haya entrado en servicio.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:executeScript - Activa las comprobaciones de estado en el grupo de escalado automático que especifique en el parámetro AutoScalingGroupARN.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descripción

El manual de procedimientos AWSConfigRemediation-EnforceEC2InstanceIMDSv2requiere la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique para usar Instance Metadata Service Version 2 (IMDSv2).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- InstanceId

  Tipo: cadena

  Descripción: (Obligatorio) ID de la instancia de Amazon EC2 que desea pedir para usar IMDSv2.

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre.
- HttpPutResponseHopLimit

  Tipo: entero

  Descripción: (opcional) El límite de respuesta de Hop desde el servicio IMDS hasta el solicitante. Establézcalo en 2 o más para las instancias EC2 que alojan contenedores. Establézcalo en 0 para no cambiarlo (predeterminado).

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

  Predeterminado: 0

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript` - Establece la opción `HttpTokens`como `required`en la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.
- `aws:assertAwsResourceProperty` - Comprueba que IMDSv2 es necesario en la instancia de Amazon EC2.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descripción

Cree una AMIa partir de una instancia EC2 para que Windows Serverejecute SQL Server 2008 (o posterior) y actualice la AMI para una version posterior de SQL Server.

Las rutas de actualización admitidas son las siguientes:

- SQL Server 2008 a SQL Server 2017, 2016 o 2014
- SQL Server 2008 R2 a SQL Server 2017, 2016 o 2014
- SQL Server 2012 a SQL Server 2019, 2017, 2016 o 2014
- SQL Server 2014 a SQL Server 2019, 2017 o 2016
- SQL Server 2016 a SQL Server 2019 o 2017
- SQL Server 2017 a SQL Server 2019

Si utiliza una versión anterior de Windows Server que no es compatible con SQL Server 2019, el documento de automatización debe actualizar su versión de Windows Server a 2016.

La actualización es un proceso de múltiples pasos que puede tardar 2 horas en completarse. La automatización crea una AMI a partir de la instancia y, a continuación, inicia una instancia temporal desde la nueva AMIen la `SubnetID`especificada. Los grupos de seguridad asociados a la instancia original se aplican a la instancia temporal. A continuación, la automatización realiza una actualización in situ a la `TargetSQLVersion` en la instancia temporal. Después de la actualización, el automatización crea una nueva AMIa partir de la instancia temporal y, después, termina la instancia temporal.

Puede probar la funcionalidad de aplicaciones ejecutando la nueva AMIen la VPC. Una vez que haya terminado las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

> **Note**
>
> Si desea modificar el nombre de equipo de la instancia EC2 iniciada desde la nueva AMI, consulte Cambiar el nombre de un equipo que aloja una instancia independiente de SQL Server.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

Requisitos previos

- TLS versión 1.2.
- La instancia EC2 debe utilizar una versión de Windows Serverque sea Windows Server2008 R2 (o posterior) y SQL Server 2008 (o posterior).
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte Instalación y configuración de SSM Agent en instancias de EC2 para Windows Server.
- Configure la instancia para usar un rol de perfil de instancia de AWS Identity and Access Management(IAM). Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager.
- Verifique que la instancia tiene 20 GB de espacio libre en el disco de arranque de la instancia.
- Para las instancias que utilizan una versión Bring Your Own License (BYOL) de SQL Server, se aplican los siguientes requisitos previos adicionales:
  - Proporcione un ID de instantánea de EBS que incluya medios de instalación de destino de SQL Server. Para ello:

    1. Compruebe que la instancia EC2 ejecute Windows Server 2008 EC2 o una versión posterior.
    2. Cree un volumen de EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
    3. Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
    4. Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
    5. Cree una instantánea de EBS del volumen de 6 GB creado en el paso 2.

Limitaciones

- La actualización solo se puede realizar en un SQL Server mediante la autenticación de Windows.
- Verifique que no exista ninguna actualización de parches de seguridad pendiente en las instancias. Abra Control Panel (Panel de control) y elija Check for updates (Buscar actualizaciones).
- No se admiten las implementaciones de SQL Server en HA y el modo de duplicación.

Parámetros

- IamInstanceProfile

  Tipo: String

  Descripción: (Obligatorio) el perfil de instancia de IAM.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) la instancia que ejecuta Windows ServerServer 2008 R2 (o posterior) y SQL Server 2008 (o posterior).
- KeepPreUpgradeImageBackUp

  Tipo: String

  Descripción: (Opcional) si se establece en `true`, la Automation no elimina la AMI creada a partir de la instancia antes de la actualización. Si se establece en `true`, debe eliminar la AMI. De forma predeterminada, se elimina la AMI.
- SubnetId

  Tipo: String

  Descripción: (Obligatorio) proporcionar una subred para el proceso de actualización. Compruebe que la subred tiene conectividad saliente a los servicios de AWS, Amazon S3 y Microsoft (para descargar parches).
- SQLServerSnapshotId

  Tipo: String

  Descripción: (Condicional) ID de instantánea para los medios de instalación de SQL Server. Este parámetro es necesario para las instancias que utilizan una versión BYOL de SQL Server. Este parámetro es opcional para las instancias con licencia incluida de SQL Server (instancias lanzadas

mediante una imagen de Amazon Machine provista por AWSpara Windows Server con Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

  Tipo: String

  Descripción: (Opcional) si se establece en `true`, la Automation reinicia la instancia antes de crear una AMI previa a la actualización. De forma predeterminada, la Automation no se reinicia antes de la actualización.

- TargetSQLVersion

  Tipo: String

  Descripción: (Opcional) Seleccione la versión de SQL Server de destino.

  Posibles objetivos:

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

  Destino predeterminado: SQL Server 2016

Salidas

AMIId: El ID de la AMI creada a partir de la instancia que se actualizó a la úultima versión de SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descripción

Cree una Amazon Machine Image (AMI) a partir de una instancia de Windows Server 2008 R2, 2012 R2, 2016 o 2019 y, a continuación, Windows Server actualícela AMI a 2016, 2019 o 2022. Las rutas de actualización admitidas son las siguientes.

- Windows Server2008 R2 a Windows Server 2016.
- Windows Server 2012 R2 a Windows Server2016.

- Windows Server 2012 R2 a Windows Server2019.
- Windows Server 2012 R2 a Windows Server2022.
- Windows Server 2016 a Windows Server2019.
- Windows Server 2016 a Windows Server2022.
- Windows Server2019 a Windows Server2022.

La operación de actualización es un proceso de múltiples pasos que puede tardar 2 horas en completarse. Recomendamos realizar una actualización del sistema operativo en instancias con al menos dos vCPU y 4 GB de RAM. Automation crea una AMI a partir de la instancia y, a continuación, inicia una instancia temporal desde la AMI recién creada en la `SubnetId`especificada. Los grupos de seguridad asociados a la instancia original se aplican a la instancia temporal. A continuación, la automatización realiza una actualización in situ a la `TargetWindowsVersion` en la instancia temporal. Para actualizar la instancia de Windows Server2008 R2 a Windows Server2016, 2019 o 2022 es necesario realizar una actualización in situ dos veces, ya que no se puede actualizar directamente de Windows Server2008 R2 a Windows Server2016, 2019 o 2022. Automation también actualiza o instala los controladores de AWS que necesita la instancia actualizada. Después de la actualización, Automation crea una nueva AMI a partir de la instancia temporal y, después, termina la instancia temporal.

Puede probar la funcionalidad de la aplicación iniciando una instancia de prueba desde la AMI actualizada en la Amazon Virtual Private Cloud (Amazon VPC). Una vez que haya terminado las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Ediciones Standard y Datacenter de Windows Server2008 R2, 2012 R2, 2016 0 2019.

Requisitos previos

- TLS versión 1.2.
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte Instalación y configuración de SSM Agent en instancias de EC2 para Windows Server.
- Debe estar instalado Windows PowerShell 3.0 o una versión posterior en la instancia.
- Para las instancias que están unidas a un dominio de Microsoft Active Directory, se recomienda especificar un `SubnetId`que no tenga conectividad con los controladores de dominio para evitar conflictos con nombres de host.
- La subred de la instancia debe tener conectividad saliente a Internet, lo que proporciona acceso a Servicios de AWS Amazon S3 y acceso a la descarga de parches de Microsoft. Este requisito se cumple si la subred es pública y la instancia tiene una dirección IP pública, o si la subred es una subred privada con una ruta que envía el tráfico de Internet a un dispositivo de NAT público.
- Esta automatización solo funciona con instancias de Windows Server2008 R2, 2012 R2, 2016 y 2019.
- Configure la Windows Server instancia con un perfil de instancia AWS Identity and Access Management (IAM) que proporcione los permisos necesarios para Systems Manager. Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager.
- Verifique que la instancia tiene 20 GB de espacio libre en el disco de arranque.
- Si la instancia no usa una licencia AWS de Windows proporcionada, especifique un ID de instantánea de Amazon EBS que incluya los medios de instalación de Windows Server 2012 R2. Para ello:
  - Compruebe que la instancia EC2 ejecuta Windows Server2012 o una versión posterior.
  - Cree un volumen de EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
  - Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
  - Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
  - Cree una instantánea de EBS del volumen de 6 GB creado en el paso 2 anterior.

Limitaciones

Esta Automation no admite la actualización de controladores de dominio de Windows, clústeres o sistemas operativos de escritorio de Windows. Esta Automation tampoco admite instancias EC2 para Windows Servercon los siguientes roles instalados.

- Host de sesión de Escritorio remoto (RDSH)
- Agente de conexión a Escritorio remoto (RDCB)
- Host de virtualización de Escritorio remoto (RDVH)
- Acceso web de Escritorio remoto (RDWA)

Parámetros

- AlternativeKeyPairName

  Tipo: cadena

  Descripción: (opcional) El nombre de un par de claves alternativo que se utilizará durante el proceso de actualización. Esto resulta útil en situaciones en las que el key pair asignado a la instancia original no está disponible. Si a la instancia original no se le asignó un key pair, debe especificar un valor para este parámetro.
- BYOL WindowsMediaSnapshotId

  Tipo: cadena

  Descripción: (Opcional) el ID de la instantánea de Amazon EBS para copiar lo que incluyen los medios de instalación de Windows Server 2012 2012R2. Solo es necesario si se está actualizando una instancia BYOL.
- IamInstanceProfile

  Tipo: cadena

  Descripción: (obligatorio) el nombre del perfil de instancia de IAM que permite que Systems Manager administre la instancia.
- InstanceId

  Tipo: cadena

  Descripción: (Obligatorio) la instancia que ejecuta Windows Server2008 R2, 2012 R2, 2016 o 2019.
- KeepPreUpgradeImageBackUp

  Tipo: cadena

Descripción: (Opcional) si se establece en True, la Automation no elimina la AMI creada a partir de la instancia EC2 antes de la actualización. Si se establece en True, debe eliminar la AMI. De forma predeterminada, se elimina la AMI.

- SubnetId

  Tipo: cadena

  Descripción: (Requerido) Esta es la subred para el proceso de actualización y donde reside su instancia EC2 de origen. Compruebe que la subred tenga conectividad saliente con los AWS servicios, Amazon S3 y Microsoft (para descargar los parches).

- TargetWindowsVersion

  Tipo: cadena

  Descripción: (Obligatorio) seleccionar la versión de Windows de destino.

  Predeterminado: 2022

- RebootInstanceBeforeTakingImage

  Tipo: cadena

  Descripción: (Opcional) si se establece en True, la Automation reinicia la instancia antes de crear una AMI previa a la actualización. De forma predeterminada, la Automation no se reinicia antes de la actualización.

AWSEC2-ConfigureSTIG

Las Guías de implementación técnica de seguridad (STIG) son los estándares de optimización de configuración creados por la Agencia de sistemas de información de defensa (DISA) para asegurar los sistemas de información y el software Para hacer nuestros sistemas de conformidad con los estándares de STIG, debe instalar, configurar y probar varias configuraciones de seguridad.

Amazon EC2 proporciona un manual de instrucciones de Systems ManagerAWSEC2-ConfigureSTIG, que puede utilizar para aplicar la configuración de STIG a una instancia. Este documento le ayuda a crear rápidamente imágenes compatibles con los estándares STIG. El documento STIG Systems Manager escanea en busca de configuraciones incorrectas y ejecuta un script de corrección. También se instala InstallRoot desde el Departamento de Defensa (DoD) en las AMI de Windows para instalar y actualizar los certificados del DoD y eliminar los certificados

innecesarios a fin de mantener la conformidad con el STIG. El uso del documento de STIG no tiene costos adicionales.

> **Important**
>
> Con pocas excepciones, los componentes de refuerzo de STIG que descarga el documento de Systems Manager no instalan paquetes de terceros. Si los paquetes de terceros ya están instalados en la instancia y si hay STIG relacionados que Amazon EC2 admite para ese paquete, se aplican esos STIG.

En esta página se enumeran todos los STIG compatibles con Amazon EC2 y que los componentes de refuerzo de STIG aplican a su instancia de EC2.

Puede elegir qué categoría de conformidad con el STIG desea aplicar.

Niveles de conformidad

- Alto (Categoría I)

  El riesgo más grave. Incluye cualquier vulnerabilidad que pueda resultar en la pérdida de confidencialidad, disponibilidad o integridad.
- Medio (Categoría II)

  Incluye cualquier vulnerabilidad que pueda resultar en la pérdida de confidencialidad, disponibilidad o integridad, pero el riesgo puede mitigarse.
- Bajo (Categoría III)

  Incluye cualquier vulnerabilidad que degrade las medidas de protección contra la pérdida de confidencialidad, disponibilidad o integridad.

Temas

Descargas de componentes de endurecimiento STIG

Amazon agrupa los componentes de refuerzo de STIG en paquetes relacionados con el sistema operativo para cada versión. Los paquetes son archivos de almacenamiento adecuados para el sistema operativo de destino en el que se descargan y se ejecutan. Los paquetes de componentes de Linux se almacenan como archivos TAR (extensión de archivo.tgz). Los paquetes de componentes de Windows se almacenan como archivos ZIP (extensión de archivo.zip).

Amazon almacena los paquetes de componentes en el `STIG`depósito S3 de Image Builder de cada uno de ellos Región de AWS. Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.

Los patrones y ejemplos de las rutas de almacenamiento de los componentes y los nombres de los archivos de paquetes son los siguientes:

Ruta de almacenamiento de componentes

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

Variables de ruta de componentes

region

Región de AWS (Cada región tiene su propio grupo de componentes).

bundle file name

El formato es <os bundle name>_ <YYYY>_Q <quarter>[_<release>]. <file extension>. Tenga en cuenta que el nombre tiene guiones bajos entre los nodos, no puntos.

os bundle name

El prefijo de nombre estándar del paquete del sistema operativo es o`LinuxAWSConfigureSTIG`. `AWSConfigureSTIG` Para mantener la compatibilidad con versiones anteriores, la descarga para Windows no incluye un prefijo de plataforma.

YYYY

El año de cuatro dígitos de la publicación.

quarter

Identifica el trimestre del año: 1, 2, 3 o 4.

release

Número incremental que comienza en uno y se incrementa en uno por cada nueva versión. La versión no se incluye en la primera versión del trimestre y solo se añade en las versiones posteriores.

file extension

Formato de archivo comprimido `tgz`(Linux) o `zip`(Windows).

Ejemplos de nombres de archivos de paquete

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

Configuración de Windows STIG

Las AMI y los componentes de refuerzo STIG de Amazon EC2 Windows están diseñados para servidores independientes y aplican una política de grupo local. Los componentes compatibles con STIG se instalan InstallRoot desde el Departamento de Defensa (DoD) en las AMI de Windows para descargar, instalar y actualizar los certificados del DoD. También eliminan los certificados innecesarios para mantener el cumplimiento del STIG. Actualmente, Amazon EC2 admite las líneas base de STIG para las siguientes versiones de Windows Server: 2012 R2, 2016, 2019 y 2022.

En esta sección se enumeran las configuraciones de STIG actuales que Amazon EC2 admite para su infraestructura de Windows, seguidas de un registro del historial de versiones.

Puede aplicar una configuración de STIG baja, media o alta.

STIG de Windows Windows versión bajo (Categoría III)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa de las STIG de Windows, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

- Windows Server 2022 STIG Version 1 Release 1

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 y V-254481

- Windows Server 2019 STIG Version 2 Release 5

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 y V-205923.

- Windows Server 2016 STIG Version 2 Release 5

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 y V-225060.

- Windows Server 2012 R2 MS STIG Version 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 y V-225250.

- Microsoft .NET Framework 4.0 STIG Version 2 Release 2

  No se aplica ninguna configuración de STIG a Microsoft .NET Framework para vulnerabilidades de categoría III.

- Windows Firewall STIG Version 2 Release 1

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 y V-242008

- Internet Explorer 11 STIG Version 2 Release 3

  V-46477, V-46629 y V-97527

- Microsoft Edge STIG versión 1, versión 6 (solo Windows Server 2022)

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

STIG de Windows Windows versión II (Categoría II)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también

pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa de las STIG de Windows, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

> **Note**
>
> La categoría STIG Medium de Windows incluye todas las configuraciones de refuerzo STIG enumeradas que se aplican a Windows STIG low (categoría III), además de las configuraciones de endurecimiento STIG que Amazon EC2 admite para las vulnerabilidades de categoría II.

- Windows Server 2022 STIG Version 1 Release 1

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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 y V-254512
- Windows Server 2019 STIG Version 2 Release 5

Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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 y V-236001

- Windows Server 2016 STIG Version 2 Release 5

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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 y V-236000

- Windows Server 2012 R2 MS STIG Version 3 Release 5

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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 y V-225239

- Microsoft .NET Framework STIG 4.0 Version 2 Release 2

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además de:

V-225238

- Windows Firewall STIG Version 2 Release 1

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además de:

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

- Internet Explorer 11 STIG Version 2 Release 3

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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 y V-75171

- STIG de Microsoft Edge versión 6 (solo 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 y V-246736

- STIG de Defender versión 4 (solo 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 y V-213466

STIG de Windows versión I (Categoría I)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa de las STIG de Windows, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

> **Note**
>
> La categoría STIG High de Windows incluye todas las configuraciones de refuerzo STIG enumeradas que se aplican a las categorías STIG Media y Baja de Windows, además de las configuraciones de endurecimiento STIG que Amazon EC2 admite para las vulnerabilidades de categoría I.

- Windows Server 2022 STIG Version 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 y V-254500
- Windows Server 2019 STIG Version 2 Release 5

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además 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 y V-205919
- Windows Server 2016 STIG Version 2 Release 5

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además 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 y V-225079

- Windows Server 2012 R2 MS STIG Version 3 Release 5

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además 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 y V-225274
- Microsoft .NET Framework STIG 4.0 Version 2 Release 2

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja) de Microsoft.NET Framework. No se aplica ninguna configuración de STIG adicional para vulnerabilidades de categoría I.
- Windows Firewall STIG Version 2 Release 1

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además de:

  V-241992, V-241997 y V-242002
- Internet Explorer 11 STIG Version 2 Release 3

  Incluye todos los ajustes de refuerzo STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja) de Internet Explorer 11. No se aplica ninguna configuración de STIG adicional para vulnerabilidades de categoría I.
- STIG de Microsoft Edge versión 6 (solo Windows Server 2022)

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además de:

  V-235758 y V-235759
- STIG de Defender versión 4 (solo Windows Server 2022)

  Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además de:

  V-213426, V-213452 y V-213453

Historial de versiones de STIG de Windows

Esta sección registra el historial de versiones de los componentes de Windows para las actualizaciones trimestrales de STIG. Para ver los cambios y las versiones publicadas durante un trimestre, elija el título para ampliar la información.

Cambios en el primer trimestre de 2024:23 de febrero de 2024 (sin cambios):

No hubo cambios en el STIGS, componente de Windows, en la versión del primer trimestre de 2024.

Cambios en el cuarto trimestre de 2023:12 de julio de 2023 (sin cambios):

No hubo cambios en el STIGS, componente de Windows, para la versión del cuarto trimestre de 2023.

Cambios en el tercer trimestre de 2023:4 de octubre de 2023 (sin cambios):

No hubo cambios en el componente STIGS de Windows para la versión del tercer trimestre de 2023.

Cambios en el segundo trimestre de 2023:5 de marzo de 2023 (sin cambios):

No hubo cambios en el componente STIGS de Windows para la versión del segundo trimestre de 2023.

Cambios en el primer trimestre de 2023:27/03/2023 (sin cambios):

No hubo cambios en el componente STIGS de Windows para la versión del primer trimestre de 2023.

Cambios en el cuarto trimestre de 2022:1 de febrero de 2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del cuarto trimestre de 2022 de la siguiente manera:

STIG-Build-Windows-Low, versión 2022.4.0

- Windows Server 2022 STIG versión 1, versión 1
- Windows Server 2019 STIG versión 2, versión 5
- Windows Server 2016 STIG versión 2, versión 5
- Windows Server 2012 R2 MS STIG versión 3, versión 5
- Microsoft .NET Framework 4.0 STIG versión 2, versión 2
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG versión 2, versión 3

- STIG de Microsoft Edge versión 6 (solo Windows Server 2022)

STIG-Build-Windows-Medium versión 2022.4.0

- Windows Server 2022 STIG versión 1, versión 1
- Windows Server 2019 STIG versión 2, versión 5
- Windows Server 2016 STIG versión 2, versión 5
- Windows Server 2012 R2 MS STIG versión 3, versión 5
- Microsoft .NET Framework 4.0 STIG versión 2, versión 2
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG versión 2, versión 3
- Microsoft Edge STIG versión 1, versión 6 (solo Windows Server 2022)
- STIG de Defender versión 4 (solo Windows Server 2022)

STIG-Build-Windows-High versión 2022.4.0

- Windows Server 2022 STIG versión 1, versión 1
- Windows Server 2019 STIG versión 2, versión 5
- Windows Server 2016 STIG versión 2, versión 5
- Windows Server 2012 R2 MS STIG versión 3, versión 5
- Microsoft .NET Framework 4.0 STIG versión 2, versión 2
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG versión 2, versión 3
- Microsoft Edge STIG versión 1, versión 6 (solo Windows Server 2022)
- STIG de Defender versión 4 (solo Windows Server 2022)

Cambios en el tercer trimestre de 2022:30 de septiembre de 2022 (sin cambios):

No hubo cambios en el componente STIGS de Windows para la versión del tercer trimestre de 2022.

Cambios en el segundo trimestre de 2022:8 de febrero de 2022:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del segundo trimestre de 2022.

STIG-Build-Windows-Low versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

STIG-Build-Windows-Medium versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

STIG-Build-Windows-High versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

Cambios en el primer trimestre de 2022:8 de febrero de 2022 (sin cambios):

No se produjeron cambios en el STIGS, componente de Windows, en la versión del primer trimestre de 2022.

Cambios en el cuarto trimestre de 2021:20 de diciembre de 2021:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del cuarto trimestre de 2021.

STIG-Build-Windows-Low versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

STIG-Build-Windows-Medium versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

STIG-Build-Windows-High versión 1.5.0

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Firewall de Windows STIG versión 2, versión 1
- Internet Explorer 11 STIG Version 1 Release 19

Cambios en el tercer trimestre de 2021:30 de septiembre de 2021:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del tercer trimestre de 2021.

STIG-Build-Windows-Low versión 1.4.0

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

STIG-Build-Windows-Medium versión 1.4.0

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

versión 1.4.0 de STIG

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

Configuración de Linux STIG

Esta sección contiene información sobre la configuración de endurecimiento de STIG de Linux que admite Amazon EC2, seguida de un registro del historial de versiones. Si la distribución de Linux no tiene una configuración de refuerzo STIG propia, Amazon EC2 utiliza la configuración de RHEL. La configuración de endurecimiento STIG admitida se aplica a las AMI Linux Amazon EC2 y a los componentes basados en la distribución de Linux, de la siguiente manera:

- Red Hat Enterprise Linux (RHEL) 7 STIG settings
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Configuración de STIG de RHEL 8
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)

STIG de Linux versión III (Categoría III)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

RHEL 7 STIG, versión 3, versión 14

- RHEL 7/CentOS 7

  V-204452, V-204576 y V-204605
- AL2

  V-204452, V-204576 y V-204605

RHEL 8 STIG, versión 1, versión 13

- RHEL 8/CentOS 8/AL 2023

  V-230241, V-244527, V-230269, V-230270, V-230285, V-230253, V-230346, V-230381, V-230395, V-230468, V-230469, V-230491, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 y V-230281

Ubuntu 18.04 STIG versión 2, versión 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 y V-219333

Ubuntu 20.04 STIG versión 1, versión 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 y V-238308

STIG de Linux versión II (Categoría II)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

> **Note**
>
> La categoría Linux STIG Medium incluye todas las configuraciones de refuerzo STIG enumeradas que se aplican a Linux STIG Low (categoría III), además de las configuraciones de endurecimiento STIG que Amazon EC2 admite para las vulnerabilidades de categoría II.

RHEL 7 STIG versión 3, versión 14

Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204551, 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-20204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204579, V-204631, V-204633 y V-256970

- AL2:

  V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204551, 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-20204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204579, V-204631, V-204633 y V-256970

RHEL 8 STIG, versión 1, versión 13

Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para vulnerabilidades de categoría III (baja), además 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-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244553, V-244553 4, 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-244524 33, V-251713, V-251717, V-251714, 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-23034, V-23034 345, V-230240, V-230282, V-250315, V-250316, V-230255, V-230277, V-230278, V-230348, V-230353, V-230386, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230403 404, 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-2302930 1, 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-230-230488 489, V-230559, V-230560, V-230561, V-237640 y V-256974

Ubuntu 18.04 STIG versión 2, versión 13

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219303, V-219326, V-219328, V-219330, V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-21922, V-219223, V-219224, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, V-219298,

V-219299, V-219300, V-219309, V-219310, V-219311, V-219312, V-233779, V-233780, V-255906, V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219155, V-219156, V-219160, V-219306, V-219149, V-219166, V-219176, V-219339, V-219331, V-219337 y V-219335

Ubuntu 20.04 STIG versión 1, versión 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-238333, V-238333 369, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-251505, V-238360, V-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238358, V-238356, V-238359, V-238370 y V-238334

STIG de Linux versión I (Categoría I)

La siguiente lista contiene las configuraciones de STIG que Amazon EC2 admite en su infraestructura. Si una configuración compatible no es aplicable a su infraestructura, Amazon EC2 omite esa configuración y continúa. Por ejemplo, es posible que algunas configuraciones de STIG no se apliquen a los servidores independientes. Las políticas específicas de la organización también pueden afectar la configuración aplicada como, por ejemplo, pedir requisitos a los administradores para revisar la configuración de los documentos.

Para obtener una lista completa, consulte la Biblioteca de documentos de STIG. Para obtener información acerca de cómo ver la lista completa, consulte Herramientas de visualización de STIG.

> **Note**
>
> La categoría STIG High de Linux incluye todas las configuraciones de refuerzo STIG enumeradas que se aplican a las categorías STIG Media y Baja de Linux, además de las configuraciones de endurecimiento STIG que Amazon EC2 admite para las vulnerabilidades de categoría I.

RHEL 7 STIG versión 3, versión 14

Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además 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 y V-204621
- AL2:

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

RHEL 8 STIG versión 1, versión 13

Incluye todos los ajustes de refuerzo de STIG que Amazon EC2 admite para las vulnerabilidades de las categorías II y III (media y baja), además de:

- RHEL 8/CentOS 8/AL 2023

  V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533 y V-230558

Ubuntu 18.04 STIG versión 2, versión 13

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316 y V-251507

Ubuntu 20.04 STIG versión 1, versión 11

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

Historial de versiones de Linux STIG

Esta sección registra el historial de versiones de los componentes de Linux para las actualizaciones trimestrales de STIG. Para ver los cambios y las versiones publicadas durante un trimestre, elija el título para ampliar la información.

Cambios en el primer trimestre de 2024:2 de junio de 2024:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del primer trimestre de 2024 de la siguiente manera:

STIG-Build-Linux-Low, versión 2024.1.x

- RHEL 7 STIG versión 3, versión 14
- RHEL 8 STIG, versión 1, versión 13
- Ubuntu 18.04 STIG versión 2, versión 13
- Ubuntu 20.04 STIG versión 1, versión 11

STIG-Build-Linux-Medium versión 2024.1.x

- RHEL 7 STIG versión 3, versión 14
- RHEL 8 STIG, versión 1, versión 13
- Ubuntu 18.04 STIG versión 2, versión 13
- Ubuntu 20.04 STIG versión 1, versión 11

STIG-Build-Linux-High versión 2024.1.x

- RHEL 7 STIG versión 3, versión 14
- RHEL 8 STIG, versión 1, versión 13
- Ubuntu 18.04 STIG versión 2, versión 13
- Ubuntu 20.04 STIG versión 1, versión 11

Cambios en el cuarto trimestre de 2023:7 de diciembre de 2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del cuarto trimestre de 2023 de la siguiente manera:

STIG-Build-Linux-Low versión 2023.4.x

- RHEL 7 STIG versión 3, versión 13
- RHEL 8 STIG versión 1 versión 12
- Ubuntu 18.04 STIG versión 2, versión 12
- Ubuntu 20.04 STIG versión 1, versión 10

STIG-Build-Linux-Medium versión 2023.4.x

- RHEL 7 STIG versión 3, versión 13
- RHEL 8 STIG versión 1 versión 12
- Ubuntu 18.04 STIG versión 2, versión 12
- Ubuntu 20.04 STIG versión 1, versión 10

STIG-Build-Linux-High versión 2023.4.x

- RHEL 7 STIG versión 3, versión 13
- RHEL 8 STIG versión 1 versión 12
- Ubuntu 18.04 STIG versión 2, versión 12
- Ubuntu 20.04 STIG versión 1, versión 10

Cambios en el tercer trimestre de 2023:4 de octubre de 2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del tercer trimestre de 2023 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 12
- RHEL 8 STIG versión 1, lanzamiento 11
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 9

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 12
- RHEL 8 STIG versión 1, lanzamiento 11
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 9

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 12
- RHEL 8 STIG versión 1, lanzamiento 11
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 9

Cambios en el segundo trimestre de 2023:5 de marzo de 2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del segundo trimestre de 2023 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 11
- RHEL 8 STIG versión 1, lanzamiento 10
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- versión 1, lanzamiento 8

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 11
- RHEL 8 STIG versión 1, lanzamiento 10
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- versión 1, lanzamiento 8

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 11
- RHEL 8 STIG versión 1, lanzamiento 10
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 11
- Ubuntu 20.04 STIG versión 1, versión 8

Cambios en el primer trimestre de 2023:27/03/2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del primer trimestre de 2023 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 10
- RHEL 8 STIG versión 1, lanzamiento 9
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 10
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 7

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 10
- RHEL 8 STIG versión 1, lanzamiento 9
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 10
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 7

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 10
- RHEL 8 STIG versión 1, lanzamiento 9
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 10
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 7

Cambios en el cuarto trimestre de 2022:01/02/2023:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del cuarto trimestre de 2022 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 9
- RHEL 8 STIG versión 1, lanzamiento 8
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 9

- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 6

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 9
- RHEL 8 STIG versión 1, lanzamiento 8
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 9
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 6

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 9
- RHEL 8 STIG versión 1, lanzamiento 8
- versión 2 de Ubuntu 18.04 versión 2, lanzamiento 9
- versión 1 de Ubuntu 20.04 versión 1, lanzamiento 6

Cambios en el tercer trimestre de 2022:30 de septiembre de 2022 (sin cambios):

No hubo cambios en el componente de Linux STIGS para la versión del tercer trimestre de 2022.

Cambios en el segundo trimestre de 2022:8 de febrero de 2022:

Introdujimos el soporte para Ubuntu, actualizamos las versiones de STIG y aplicamos el STIGS para la versión del segundo trimestre de 2022 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 7
- RHEL 8 STIG versión 1, lanzamiento 6
- Ubuntu 18.04 STIG versión 2, versión 6 (nueva)
- Ubuntu 20.04 STIG versión 1, versión 4 (nueva)

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 7

- RHEL 8 STIG versión 1, lanzamiento 6
- Ubuntu 18.04 STIG versión 2, versión 6 (nueva)
- Ubuntu 20.04 STIG versión 1, versión 4 (nueva)

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 7
- RHEL 8 STIG versión 1, lanzamiento 6
- Ubuntu 18.04 STIG versión 2, versión 6 (nueva)
- Ubuntu 20.04 STIG versión 1, versión 4 (nueva)

Cambios en el primer trimestre de 2022:26 de abril de 2022:

Refactorizado para incluir un mejor soporte para los contenedores. Combinó el script AL2 anterior con RHEL 7. Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del primer trimestre de 2022 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 6
- RHEL 8 STIG versión 1, lanzamiento 5

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 6
- RHEL 8 STIG versión 1, lanzamiento 5

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 6
- RHEL 8 STIG versión 1, lanzamiento 5

Cambios en el cuarto trimestre de 2021:20 de diciembre de 2021:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del cuarto trimestre de 2021 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 5
- RHEL 8 STIG versión 1, lanzamiento 4

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 5
- RHEL 8 STIG versión 1, lanzamiento 4

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 5
- RHEL 8 STIG versión 1, lanzamiento 4

Cambios en el tercer trimestre de 2021:30 de septiembre de 2021:

Se actualizaron las versiones de STIG y se aplicó el STIGS para la versión del tercer trimestre de 2021 de la siguiente manera:

STIG de Linux versión III (Categoría III)

- RHEL 7 STIG versión 3, lanzamiento 4
- RHEL 8 STIG versión 1, lanzamiento 3

STIG de Linux versión II (Categoría II)

- RHEL 7 STIG versión 3, lanzamiento 4
- RHEL 8 STIG versión 1, lanzamiento 3

STIG de Linux versión I (Categoría I)

- RHEL 7 STIG versión 3, lanzamiento 4
- RHEL 8 STIG versión 1, lanzamiento 3

AWSEC2-PatchLoadBalancerInstance

Descripción

Actualice y aplique parches a la versión secundaria de una instancia de Amazon EC2 (Windows o Linux) conectada a cualquier balanceador de carga (clásico, ALB o NLB). El tiempo de carga de conexión predeterminado se aplica antes de parchear la instancia. Puede anular el tiempo de espera introduciendo el tiempo de descarga personalizado en minutos (**1**-**59**) para el parámetro ConnectionDrainTime.

La Automation es la siguiente:

1. Se determina el balanceador de carga o el grupo objetivo al que se adjunta la instancia y se verifica que la instancia esté en buen estado.
2. La instancia se elimina del balanceador de cargas o del grupo objetivo.
3. La automatización espera el período de tiempo especificado para el tiempo de agotamiento de la conexión.
4. Se llama a la automatización AWS-RunPatchBaseline para parchear la instancia.
5. La instancia se vuelve a conectar al balanceador de carga o al grupo objetivo.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Requisitos previos

- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte Uso de SSM Agent en instancias de EC2 para Windows Server.

Parámetros

- InstanceId

  Tipo: String

Descripción: ID (obligatorio) de la instancia a la que se va a aplicar el parche y que está asociada a un balanceador de cargas (clásico, ALB o NLB).

- Tiempo de drenaje de la conexión

  Tipo: String

  Descripción: (Opcional) El tiempo de agotamiento de la conexión del balanceador de cargas, en minutos (-). 159

AWSEC2-SQLServerDBRestore

Descripción

El manual de procedimientos `AWSEC2-SQLServerDBRestore`restaura las copias de seguridad de bases de datos de Amazon S3 a Server 2017 en ejecución en una instancia Amazon Elastic Compute Cloud (EC2) de Linux. Puede proporcionar su propia instancia EC2 con SQL Server 2017 para Linux. Si no se proporciona ninguna instancia EC2, Automation inicia y configura una nueva instancia EC2 de Ubuntu 16.04 con SQL Server 2017. Automation admite la restauración de copias de seguridad completas, diferenciales y de registros de transacciones. Automation acepta varios archivos de copia de seguridad de bases de datos y restaura automáticamente la copia de seguridad válida más reciente de cada base de datos de los archivos proporcionados.

Para automatizar tanto la creación de copias de seguridad como la restauración de una base de datos de SQL Server local en una instancia EC2 que ejecuta SQL Server 2017 para Linux, puede usar el script de PowerShell firmado por AWS`MigrateSQLServerToEC2Linux`.

> **Important**
>
> Este manual de procedimientos restablece la contraseña de usuario de administrador del servidor (SA) de SQL Server cada vez que se ejecuta Automation. Una vez que finalice Automation, debe establecer su propia contraseña de usuario de SA de nuevo antes de conectarse a la instancia de SQL Server.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Requisitos previos

Para ejecutar esta automatización, debe cumplir los siguientes requisitos previos:

- El usuario o rol de IAM que ejecute esta automatización debe tener una política integrada asociada con los permisos que se describen en. Permisos de IAM necesarios
- Si proporciona su propia instancia EC2, haga lo siguiente:
  - La instancia EC2 que proporcione debe ser una instancia de Linux que ejecute Microsoft SQL Server 2017.
  - La instancia EC2 debe ser configurada con un perfil de instancia de AWS Identity and Access Management(IAM) que tenga asociado la política administrada `AmazonSSMManagedInstanceCore`adjunta. Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager.
  - El agente de SSM debe estar instalado en su instancia EC2. Para obtener más información, consulte Installing and Configuring SSM Agent on EC2 Instances para Linux.
  - La instancia EC2 debe tener suficiente espacio libre en disco para descargar y restaurar las copias de seguridad de SQL Server.

Limitaciones

Automation no admite la restauración de SQL Server en ejecución en instancias EC2 para Windows Server. Automation solo restaura las copias de seguridad de bases de datos que sean compatibles con SQL Server 2017 para Linux. Para obtener más información, consulte la sección Ediciones y características admitidas de SQL Server 2017 para Linux.

Parámetros

Esta Automation tiene los siguientes parámetros:

- DatabaseNames

  Tipo: String

  Descripción: (Opcional) la lista separada por comas de los nombres de las bases de datos que se restaurarán.

- DataDirectorySize

  Tipo: String

  Descripción: (Opcional) el tamaño del volumen (GiB) deseado del directorio Data de SQL Server para la nueva instancia EC2.

  Valor predeterminado: 100

- KeyPair

  Tipo: String

  Descripción: (Opcional) el par de claves que se utilizará al crear la nueva instancia EC2.

- IamInstanceProfileName

  Tipo: String

  Descripción: (Opcional) el perfil de instancia de IAM que se asociará a la nueva instancia EC2. El perfil de instancia de IAM debe tener la política administrada asociada de `AmazonSSMManagedInstanceCore`.

- InstanceId

  Tipo: String

  Descripción: (Opcional) la instancia que ejecuta SQL Server 2017 en Linux. Si no se proporciona el valor de InstanceId, Automation inicia una nueva instancia EC2 utilizando los valores de InstanceType y SQLServerEdition proporcionados.

- InstanceType

  Tipo: String

  Descripción: (Opcional) el tipo de instancia EC2 que se va iniciar.

- IsS3PresignedUrl

Tipo: String

Descripción: (Opcional) si S3Input es una URL de S3 prefirmada, indique `yes`.

Valor predeterminado: no

Valores válidos: yes | no

- LogDirectorySize

  Tipo: String

  Descripción: (Opcional) el tamaño del volumen (GiB) deseado del directorio Log de SQL Server para la nueva instancia EC2.

  Valor predeterminado: 100

- S3Input

  Tipo: String

  Descripción: (Obligatorio) el nombre de bucket de S3, la lista separada por comas de claves de objetos de S3 o la lista separada por comas de URL de S3 prefirmadas con los archivos de copias de seguridad de SQL que se restaurarán.

- SQLServerEdition

  Tipo: String

  Descripción: (Opcional) la edición de SQL Server 2017 que se instalará en la instancia EC2 recién creada.

  Valores permitidos: Standard | Enterprise | Web | Express

- SubnetId

  Tipo: String

  Descripción: (Opcional) la subred en la que se iniciará la nueva instancia EC2. La subred debe tener conectividad saliente a los servicios de AWS. Si no se proporciona ningún valor para SubnetId, Automation utiliza la subred predeterminada.

- TempDbDirectorySize

Tipo: String

Descripción: (Opcional) el tamaño del volumen (GiB) deseado del directorio TempDB de SQL Server para la nueva instancia EC2.

Valor predeterminado: 100

Permisos de IAM necesarios

El `AutomationAssumeRole`parámetro requiere las siguientes acciones para utilizar correctamente el runbook.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands",
                "ssm:SendCommand",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::ACCOUNTID:role/ROLENAME"
        }
    ]
}
```

Pasos de documentos

Para usar esta automatización, sigue los pasos que se aplican a tu tipo de instancia:

Para las nuevas instancias EC2:

1. `aws:executeAwsApi`- Recupere el ID de AMI para SQL Server 2017 en Ubuntu 16.04.
2. `aws:runInstances` - Lance una nueva instancia EC2 para Linux.
3. `aws:waitForAwsResourceProperty`- Espere a que la instancia EC2 recién creada esté lista.
4. `aws:executeAwsApi`- Reinicie la instancia si no está lista.
5. `aws:assertAwsResourceProperty`- Compruebe que el agente de SSM esté instalado.
6. `aws:runCommand`- Ejecute el script de restauración de SQL Server en PowerShell.

Para las instancias EC2 existentes:

1. `aws:waitForAwsResourceProperty`- Verifique que la instancia está lista
2. `aws:executeAwsApi`- Reinicie la instancia si no está lista.
3. `aws:assertAwsResourceProperty`- Compruebe que el agente de SSM esté instalado.
4. `aws:runCommand`- Ejecute el script de restauración de SQL Server en PowerShell.

Salidas

getInstance.InstanceId

restoreToNewInstance.Output

restoreToExistingInstance.Output

AWSSupport-ActivateWindowsWithAmazonLicense

Descripción

El `AWSSupport-ActivateWindowsWithAmazonLicense`manual de procesos activa una instancia de Amazon Elastic Compute Cloud (Amazon EC2) Windows Servercon una licencia proporcionada por Amazon. La automatización verifica y configura los ajustes necesarios del sistema operativo del servicio de administración de claves e intenta realizar la activación. Esto

incluye las rutas del sistema operativo a los servidores de administración de claves de Amazon y la configuración del sistema operativo del servicio de administración de claves. Cuando el parámetro `AllowOfflinese` establece en `true`, la automatización se dirige correctamente a instancias que no están administradas por AWS Systems Manager, pero que requieren que se detenga e inicie la instancia.

> **Note**
>
> Este manual de procedimientos no se puede utilizar en las instancias del modelo Windows ServerBring Your Own License (BYOL). Para obtener más información acerca del uso de su propia licencia, consulte Licencias de Microsoft en AWS.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

- AllowOffline

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (opcional) Establézcalo en `true`si permite una corrección de activación de Windows sin conexión en caso de que la solución de problemas en línea produzca un error o que la instancia proporcionada no sea una instancia administrada.

> **Important**
>
> El método sin conexión requiere detener y volver a iniciar la instancia EC2 proporcionada. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ForceActivation

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) establecerlo en `true`si desea continuar incluso si Windows ya está activado.

- InstanceId

  Tipo: String

  Descripción: (Necesario) ID de su instancia EC2 administrada para Windows Server.

- SubnetId

  Tipo: String

  Valor predeterminado: CreateNewVPC

  Descripción: (Opcional) solo sin conexión: el ID de subred para la instancia EC2Rescue utilizada para realizar la solución de problemas sin conexión. Utilice `SelectedInstanceSubnet`para utilizar la misma subred que la instancia, o utilice `CreateNewVPC`para crear una nueva VPC.

IMPORTANTE: La subred debe estar en la misma zona de disponibilidad que InstanceId y debe permitir el acceso a puntos de enlace de SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Recomendamos que la instancia EC2 que recibe el comando tenga un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. Debe tener al menos ssm:StartAutomationExecution y ssm:SendCommand para ejecutar Automation y enviar el comando a la instancia, así como ssm:GetAutomationExecution para poder leer la salida de Automation. Para obtener información sobre la corrección sin conexión, consulte los permisos que necesita. `AWSSupport-StartEC2RescueWorkflow`

Pasos de documentos

1. `aws:assertAwsResourceProperty`- Compruebe que la plataforma de la instancia proporcionada sea Windows.
2. `aws:assertAwsResourceProperty`- Confirma que la instancia proporcionada es una instancia gestionada:
   a. (Solución de la activación online) Si la instancia de entrada es una instancia administrada, utilice `aws:runCommand` para ejecutar el script de PowerShell con el fin de corregir la activación de Windows.
   b. (Solución de activación sin conexión) Si la instancia de entrada no es una instancia administrada:
      i. `aws:assertAwsResourceProperty`- Verifica que el `AllowOfflineindicador` esté establecido en. `true` En caso afirmativo, comienza la corrección sin conexión; de lo contrario, la auutomatización de trabajo finaliza.
      ii. `aws:executeAutomation`- Invoque `AWSSupport-StartEC2RescueWorkflowcon` el script de corrección fuera de línea para la activación de Windows. El script utiliza EC2Config o EC2Launch en función de la versión del sistema operativo.
      iii. `aws:executeAwsApi`- Lee el resultado de`AWSSupport-StartEC2RescueWorkflow`.

Salidas

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descripción

El manual de procedimientos `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`analiza la conectividad desde una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o desde una interfaz de red elástica a un punto de conexión Servicio de AWS . No se admite IPv6. El manual de procedimientos utiliza el valor que especifique para el parámetro `ServiceEndpoint`a fin de analizar la conectividad con un punto de conexión. Si no se encuentra un punto de conexión AWS PrivateLink en su VPC, el manual de procedimientos utiliza una dirección IP pública para el servicio en la Región de AWS actual. Esta automatización utiliza el Reachability Analyzer de la nube privada virtual de Amazon. Para obtener más información, consulte What is Reachability Analyzer? en el Reachability Analyzer.

Esta automatización comprueba lo siguiente:

- Compruebe si su nube privada virtual (VPC) está configurada para usar el servidor DNS proporcionado por Amazon.
- Comprueba si existe un AWS PrivateLink punto final en la VPC para el Servicio de AWS que especifique. Si se encuentra un punto de conexión, la automatización verifica que el atributo `privateDnsesté` activado.
- Comprueba si el AWS PrivateLink punto final utiliza la política de puntos finales predeterminada.

Consideraciones

- Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte Precios de Amazon VPC.
- Durante la automatización, se crea una ruta de información de la red y un análisis de la información de la red. Si la automatización se completa correctamente, el manual de procedimientos elimina estos recursos. Si se produce un error en el paso de limpieza, el manual de procedimientos no eliminará la ruta de información de la red y tendrá que eliminarla manualmente. Si no elimina la ruta de información de la red de forma manual, se seguirá teniendo en cuenta para la cuota de su Cuenta de AWS. Para obtener más información sobre las cuotas del Reachability Analyzer, consulte Quotas for Reachability Analyzer en Reachability Analyzer.

- Las configuraciones a nivel del sistema operativo, como el uso de un proxy, una resolución de DNS local o un archivo de hosts, pueden afectar a la conectividad incluso si el Reachability Analyzer muestra `PASS`.
- Revise la evaluación de todas las comprobaciones realizadas por el Reachability Analyzer. Si alguna de las comprobaciones regresa un estado de `FAIL`, esto podría afectar a la conectividad, incluso si la comprobación de accesibilidad general regresa un estado de `PASS`.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- Origen

  Tipo: cadena

  Descripción: (Obligatorio) El ID de la instancia de Amazon EC2 o la interfaz de red desde la que desea analizar la accesibilidad.
- ServiceEndpoint

  Tipo: cadena

Descripción: (Obligatorio) El nombre de host del punto de conexión del servicio en el que desea analizar la accesibilidad.

- RetainVpcReachabilityAnalysis

  Tipo: cadena

  Predeterminado: false

  Descripción: (Opcional) Determina si se retienen la ruta de conocimiento de la red y los análisis relacionados creados. De forma predeterminada, los recursos utilizados para analizar la accesibilidad se eliminan cuando el análisis se realiza correctamente. Si decide retener el análisis, el manual de procedimientos no lo elimina y puede visualizarlo en la consola de Amazon VPC. Hay un enlace a la consola disponible en el resultado de la automatización.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:executeScript`: Valida el punto de conexión del servicio intentando resolver el nombre de host.
2. `aws:executeScript`: Recopila detalles sobre la VPC y la subred.
3. `aws:executeScript`: Evalúa la configuración de DNS de la VPC.
4. `aws:executeScript`: Evalúa las comprobaciones de punto de conexión de VPC.
5. `aws:executeScript`: Localiza una puerta de enlace de Internet para conectarse al punto de conexión del servicio público.
6. `aws:executeScript`: Determina el destino que se utilizará para el análisis de accesibilidad.
7. `aws:executeScript`: Analiza la accesibilidad desde el origen hasta el punto de conexión mediante el Reachability Analyzer y limpia los recursos si el análisis se realiza correctamente.
8. `aws:executeScript`: Genera un informe de evaluación de la accesibilidad.
9. `aws:executeScript`: Genera el resultado en JSON.

Salidas

- `generateReport.EvalReport` - Los resultados de las comprobaciones realizadas por la automatización en formato de texto.
- `generateJsonOutput.Output` - Una versión mínima de los resultados en formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descripción

El manual de procedimientos `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD`automatiza las migraciones desde instancias de Amazon Elastic Compute Cloud (Amazon EC2) con tecnología Intel a tipos de instancias equivalentes con tecnología AMD. Este manual de procedimientos admite instancias de uso general (M), de desempeño con ráfagas (T), optimizadas para cómputo (C) y optimizadas para memoria (R) creadas

en el sistema Nitro. Este manual de procedimientos se puede usar en instancias que no estén administradas por Systems Manager.

Para reducir el posible riesgo de pérdida de datos y tiempo de inactividad, el manual de procedimientos comprueba el comportamiento de parada de la instancia, si la instancia está en un grupo de Amazon EC2 Auto Scaling, el estado de la instancia y si el tipo de instancia equivalente con tecnología AMD está disponible en la misma zona de disponibilidad. De forma predeterminada, este manual de procedimientos no cambiará el tipo de instancia si hay volúmenes de almacén de instancias adjuntos o si la instancia forma parte de una pila AWS CloudFormation. Si desea cambiar este comportamiento, especifique `yes`para cualquiera de los parámetros `AllowInstanceStoreInstances`y `AllowCloudFormationInstances`.

> **Important**
>
> El acceso a los manuales de procedimientos de `AWSPremiumSupport-*` requiere una suscripción Enterprise o Business Support. Para obtener más información, consulte Comparar AWS Supportplanes.

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos.
- Para cambiar el tipo de instancia, es necesario que el manual de procedimientos detenga su instancia. Cuando se detiene una instancia, se pierden todos los datos almacenados en la RAM o en los volúmenes del almacén de instancias y se libera la dirección IPv4 pública automática. Para obtener más información, consulte Detenimiento e inicio de la instancia.
- Si no especifica un valor para el parámetro `TargetInstanceType`, el manual de procedimientos intenta identificar la instancia AMD equivalente en términos de CPU virtuales y memoria dentro de la misma familia de instancias. El manual de procedimientos finaliza si no es capaz de identificar un tipo de instancia AMD equivalente.
- Al usar la opción `DryRun`, puede capturar el tipo de instancia AMD equivalente y validar los requisitos sin cambiar realmente el tipo de instancia.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- Acknowledge

  Tipo: String

  Descripción: (Obligatorio) Introduzca `yes`para confirmar que la instancia de destino se detendrá si se está ejecutando.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) El ID de la instancia de Amazon EC2 cuyo tipo desea cambiar.
- TargetInstanceType

  Tipo: String

  Predeterminado: automatic

  Descripción: (Opcional) El tipo de instancia AMD al que desea cambiar su instancia. El valor predeterminado `automatic`usa el tipo de instancia equivalente en términos de CPU virtuales y memoria. Por ejemplo, un m5.large se cambiaría a m5a.large.
- AllowInstanceStoreInstances

Tipo: String

Valores válidos: no | yes

Valor predeterminado: no

Descripción: (Opcional) Si especifica `yes`, el manual de procedimientos se ejecuta en instancias que tienen volúmenes de almacén de instancias adjuntos.

- AllowCloudFormationInstances

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si se establece en `yes`, el manual de procedimientos se ejecuta en las instancias que forman parte de una pila AWS CloudFormation.

- AllowCrossGeneration

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si se establece en `yes`, el manual de procedimientos intenta encontrar el tipo de instancia AMD equivalente más reciente dentro de la misma familia de instancias.

- DryRun

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si se establece en `yes`, el manual de procedimientos regresa el tipo de instancia AMD equivalente y valida los requisitos de migración sin realizar cambios en el tipo de instancia.

- SleepWait

Tipo: String

Predeterminado: PT3S

Descripción: (Opcional) El tiempo que debe esperar el manual de procedimientos antes de iniciar una nueva automatización. El valor que proporcione para este parámetro debe coincidir con la norma ISO 8601. Para obtener más información sobre la creación de cadenas ISO 8601, consulte Formatear cadenas de fecha y hora para Systems Manager.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: Confirma que el estado de la instancia de Amazon EC2 de destino es `running`, `pending`, `stopped` o `stopping`. De lo contrario, la automatización finaliza.
2. `aws:executeAwsApi`: Reúne las propiedades de la instancia de Amazon EC2 de destino.

3. `aws:branch`: Ramifica la automatización en función del estado de la instancia de Amazon EC2.
   a. En caso de `stopped`o `stopping`, la automatización se ejecuta `aws:waitForAwsResourceProperty`hasta que la instancia de Amazon EC2 se detenga por completo.
   b. En caso de `running`o `pending`, la automatización se ejecuta `aws:waitForAwsResourceProperty`hasta que la instancia de Amazon EC2 supere las comprobaciones de estado.
4. `aws:assertAwsResourceProperty`: Confirma que la instancia de Amazon EC2 no forma parte de un grupo de escalado automático comprobando si la etiqueta `aws:autoscaling:groupName`está aplicada.
5. `aws:executeAwsApi`: Reúne las propiedades del tipo de instancia actual para buscar el tipo de instancia AMD equivalente.
6. `aws:assertAwsResourceProperty`: Confirma que el código de producto AWS Marketplaceno está asociado a la instancia de Amazon EC2. Algunos productos no están disponibles en todos los tipos de instancias.
7. `aws:branch`: Ramifica la automatización en función de si desea que la automatización compruebe si la instancia de Amazon EC2 forma parte de una pila AWS CloudFormation
   a. Si la etiqueta `aws:cloudformation:stack-name`se aplica a la instancia, la automatización se ejecuta `aws:assertAwsResourceProperty`para confirmar que la instancia no forma parte de una pila AWS CloudFormation.
8. `aws:branch`: Ramifica la automatización en función de si el tipo de volumen raíz de la instancia es Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: Confirma que el comportamiento de cierre de la instancia sea `stop`y no `terminate`.
10. `aws:executeScript`: Confirma que solo hay una automatización de este manual de procedimientos dirigida a la instancia actual. Si ya hay otra automatización en curso dirigida a la misma instancia, regresa un error y finaliza.
11. `aws:executeAwsApi`: Regresa una lista de los tipos de instancia AMD con la misma cantidad de memoria y vCPU.
12. `aws:executeScript`: Comprueba si el tipo de instancia actual es compatible y regresa su tipo de instancia AMD equivalente. Si no hay un equivalente, la automatización finaliza.
13. `aws:executeScript`: Confirma que el tipo de instancia AMD está disponible en la misma zona de disponibilidad y verifica los permisos de IAM proporcionados.
14. `aws:branch`: Ramifica la automatización en función de si el valor del parámetro `DryRun`es `yes`.

15. `aws:branch`: Comprueba si el tipo de instancia original y el de destino son iguales. Si son iguales, la automatización finaliza.
16. `aws:executeAwsApi`: Obtiene el estado actual de la instancia.
17. `aws:changeInstanceState`: Crea la instancia de Amazon EC2.
18. `aws:changeInstanceState`: Obliga a la instancia a detenerse si está atascada en el estado de parada.
19. `aws:executeAwsApi`: Cambia el tipo de instancia por el tipo de instancia AMD de destino.
20. `aws:sleep`: Espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
21. `aws:branch`: Ramifica la automatización en función del estado de la instancia anterior. Si se estaba `running`, se inicia la instancia.
    a. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
    b. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado. Si la instancia no supera las comprobaciones de estado, la instancia cambia de regreso a su tipo de instancia original.
        i. `aws:changeInstanceState`: Detiene la instancia de Amazon EC2 antes de cambiarla a su tipo de instancia original.
        ii. `aws:changeInstanceState`: Obliga a la instancia de Amazon EC2 a detenerse antes de cambiarla a su tipo de instancia original en caso de que se quede atascada en un estado de parada.
        iii. `aws:executeAwsApi`: Cambia la instancia de Amazon EC2 a su tipo original.
        iv. `aws:sleep`: Espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
        v. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
        vi. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado.
22. `aws:sleep`: Espera antes de finalizar el manual de procedimientos.

AWSSupport-CheckXenToNitroMigrationRequirements

Descripción

El manual de procedimientos `AWSSupport-CheckXenToNitroMigrationRequirements`verifica que una instancia de Amazon Elastic Compute Cloud (Amazon EC2) cumpla con los requisitos previos para cambiar correctamente el tipo de instancia de una instancia de tipo Xen a una instancia basada en Nitro. Esta automatización comprueba lo siguiente:

- El dispositivo raíz es un volumen Amazon Elastic Block Store (Amazon EBS).
- El atributo `enaSupport`está activado.
- El módulo ENA está instalado en la instancia.
- El módulo NVMe está instalado en la instancia. En caso afirmativo, el módulo está instalado y un script verifica que el módulo esté cargado en la imagen `initramfs`.
- Analiza `/etc/fstab`y busca los dispositivos de bloques que se están montando utilizando los nombres de los dispositivos.
- Determina si el sistema operativo (SO) utiliza de manera predeterminada nombres de interfaz de red predecibles.

Este manual de procedimientos admite los siguientes sistemas operativos:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Servidor Debian
- Servidor Ubuntu
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Valor predeterminado: falso

  Descripción: (Obligatorio) El ID de la instancia de Amazon EC2 cuyos requisitos previos desea comprobar antes de migrar a un tipo de instancia basado en Nitro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeAwsApi - Recopila detalles sobre la instancia.
- aws:executeAwsApi - Recopila información sobre el hipervisor de la instancia.
- aws:branch - Se ramifica en función de si la instancia de destino ya ejecuta un tipo de instancia basado en Nitro.
- aws:branch - Comprueba si el sistema operativo de la instancia es compatible con las instancias basadas en Nitro.
- aws:assertAwsResourceProperty - Verifica que la instancia que especificó esté gestionada por Systems Manager y que su estado sea Online.
- aws:branch - Se ramifica en función de si el dispositivo raíz de la instancia es un volumen de Amazon EBS.
- aws:branch - Se ramifica en función de si el atributo ENA está o no habilitado para la instancia.
- aws:runCommand - Comprueba si hay controladores ENA en la instancia.
- aws:runCommand - Comprueba los controladores NVMe en la instancia.
- aws:runCommand - Comprueba si hay formatos no reconocidos en el archivo fstab.
- aws:runCommand - Comprueba si hay una configuración predecible del nombre de la interfaz en la instancia.
- aws:executeScript - Genera resultados en función de los pasos anteriores.

Salidas

finalOutput.output - Los resultados de las comprobaciones realizadas por la automatización.

AWSSupport-ConfigureEC2Metadata

Descripción

Este manual de procedimientos le ayuda a configurar las opciones del servicio de metadatos de instancias (IMDS) para instancias de Amazon Elastic Compute Cloud (Amazon EC2). Mediante este manual de procedimientos, puede realizar la configuración de:

- Requerir el uso de IMDSv2 para metadatos de la instancia.
- Configurar el valor `HttpPutResponseHopLimit`.
- Permitir o denegar el acceso a los metadatos de la instancia.

Para obtener más información sobre los metadatos de la instancia, consulte Configuración del servicio de metadatos de la instancia en la Guía del usuario de Amazon EC2.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EnforceIMDSv2

  Tipo: cadena

  Valores válidos: obligatorio | opcional

Predeterminado: opcional

Descripción: (opcional) Requerir IMDSv2. Si elije `required`, la instancia de Amazon EC2 solo usará IMDSv2. Si elije `optional`, puede elegir entre IMDSv1 e IMDSv2 para el acceso a los metadatos.

> **Important**
>
> Si aplica IMDSv2, es posible que las aplicaciones que utilizan IMDSv1 no funcionen correctamente. Antes de aplicar IMDSv2, asegúrese de que las aplicaciones que utilizan IMDS estén actualizadas a una versión compatible con IMDSv2. Para obtener información sobre la versión 2 del servicio de metadatos de instancias (IMDSv2), consulte Configuración del servicio de metadatos de instancias en la Guía del usuario de Amazon EC2.

- HttpPutResponseHopLímite

  Tipo: entero

  Valores válidos: 0 - 64

  Predeterminado: 0

  Descripción: (opcional) el valor del límite de saltos de respuesta HTTP PUT deseado (1 - 64) para las solicitudes de metadatos de instancia. Este valor controla el número de saltos que puede recorrer la respuesta PUT. Para evitar que la respuesta viaje fuera de la instancia, especifique 1 para el valor del parámetro.

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la instancia de Amazon EC2 cuya configuración de metadatos desea configurar.

- MetadataAccess

  Tipo: cadena

  Valores válidos: enabled | disabled

Valor predeterminado: habilitado

Descripción: (opcional) permite o deniega el acceso a los metadatos de la instancia de Amazon EC2. Si especifica `disabled`, se ignorarán todos los demás parámetros y se denegará el acceso a los metadatos de la instancia.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

1. sucursalOnMetadataAccess : automatización de sucursales basada en el valor del `MetadataAccess` parámetro.
2. disableMetadataAccess - Solicita a la ModifyInstanceMetadataOptions API una acción para deshabilitar el acceso al punto final de los metadatos.
3. branchOnHttpPutResponseHopLimit : automatización de sucursales en función del valor del `HttpPutResponseHopLimit` parámetro.
4. mantenerHopLimitAndConfigureImdsVersion : si `HttpPutResponseHopLimit` es 0, mantiene el límite de saltos actual y cambia otras opciones de metadatos.
5. wait BeforeAsserting IMDSv2State: espera 30 segundos antes de confirmar el estado de IMDSv2.
6. setHopLimitAndConfigureImdsVersion : si `HttpPutResponseHopLimit` es mayor que 0, configura las opciones de metadatos utilizando los parámetros de entrada indicados.
7. esperarBeforeAssertingHopLimit : espera 30 segundos antes de activar las opciones de metadatos.
8. assertHopLimit - Afirma que la `HttpPutResponseHopLimit` propiedad está establecida en el valor que especificó.

9. branch VerificationOn IMDSv2Option: verificación de ramificaciones en función del valor del parámetro. `EnforceIMDSv2`
10. IsOptional assertImdsV2: afirma el valor establecido en. `HttpTokens optional`
11. IsEnforced assertImdsV2: afirma el valor establecido en. `HttpTokens required`
12. esperarBeforeAssertingMetadataState : espera 30 segundos antes de confirmar que el estado de los metadatos está deshabilitado.
13. afirmarMetadataIsDisabled : afirma que los metadatos son. `disabled`
14. describeMetadataOptions - Obtiene las opciones de metadatos una vez aplicados los cambios que ha especificado.

Salidas

describa MetadataOptions .State

describirMetadataOptions. MetadataAccess

describe MetadataOptions .IMDSv2

MetadataOptionsdescribir. HttpPutResponseHopLímite

AWSSupport-CopyEC2Instance

Descripción

El manual de procedimientos `AWSSupport-CopyEC2Instance`proporciona una solución automatizada para el procedimiento descrito en el artículo del Centro de Conocimiento ¿Cómo muevo mi instancia EC2 a otra subred, zona de disponibilidad o VPC? La automatización se ramifica en función de los valores que especifique para los parámetros `Region`y `SubnetId`.

Si especifica un valor para el parámetro `SubnetId`pero no un valor para el parámetro `Region`, la automatización crea una Amazon Machine Image(AMI) de la instancia de destino y lanza una nueva instancia desde la AMIen la subred que especificó.

Si especifica un valor para el parámetro `SubnetId`y el parámetro `Region`, la automatización crea una instancia AMIde destino, copia la AMIen la Región de AWSque especificó y lanza una nueva instancia desde la AMIen la subred que especificó.

Si especifica un valor para el parámetro `Region`pero no un valor para el parámetro `SubnetId`, la automatización crea una AMIde las instancias de destino, copia la AMIen la región que especificó

y lanza una nueva instancia desde la AMIen la subred predeterminada de su nube privada virtual (VPC) en la región de destino.

Si no se especifica ningún valor para los parámetros `Region`o `SubnetId`, la automatización crea una AMIde las instancias de destino y lanza una nueva instancia desde la AMIen la subred predeterminada de su VPC.

Para copiar una AMIa una región diferente, debe proporcionar un valor para el parámetro `AutomationAssumeRole`. Si se agota el tiempo de espera de la automatización durante el paso `waitForAvailableDestinationAmi`, es posible que la AMIaún esté copiando. En este caso puede esperar a que se complete la copia y lanzar la instancia manualmente.

Antes de ejecutar esta automatización, tenga en cuenta lo siguiente:

- Las AMIse basan en instantáneas de Amazon Elastic Block Store (Amazon EBS). En el caso de sistemas de archivos de gran tamaño sin una instantánea previa, la creación de AMIpuede tardar varias horas. Para reducir el tiempo de creación de AMI, cree una instantánea de Amazon EBS antes de crear laAMI.
- Al crear una AMIno se crea una instantánea para el almacén de instancias en la instancia. Para obtener información sobre cómo realizar copias de seguridad de los volúmenes del almacén de instancias en Amazon EBS, consulte ¿Cómo puedo hacer una copia de seguridad de un volumen de almacén de instancias de mi instancia de Amazon EC2 en Amazon EBS?
- La nueva instancia de Amazon EC2 tiene una dirección IP IPv4 privada o IPv6 pública diferente. Debe actualizar todas las referencias a las direcciones IP antiguas (por ejemplo, en las entradas de DNS) con las nuevas direcciones IP asignadas a la nueva instancia. Si utiliza una dirección IP elástica en la instancia de origen, asegúrese de adjuntarla a la nueva instancia.
- Se pueden producir problemas con el identificador de seguridad de dominio (SID) cuando la copia se lanza e intenta contactar con el dominio. Antes de capturar la AMI, utilice Sysprep o elimine la instancia unida al dominio del dominio para evitar problemas de conflicto. Para obtener más información, consulte ¿Cómo puedo usar Sysprep para crear e instalar AMI de Windows personalizadas y reutilizables?

Ejecuta esta automatización (consola)

> **Important**
>
> No recomendamos usar este manual de procedimientos para copiar instancias del controlador de dominio de Microsoft Active Directory.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia de que desea reiniciar.

- KeyPair

  Tipo: String

  Descripción: (Opcional) El par de claves que desea asociar con la nueva instancia copiada. Si va a copiar la instancia a una región diferente, asegúrese de que el par de claves existe en la región especificada.

- Región

  Tipo: String

  Descripción: (Opcional) La región a la que quiere copiar la instancia. Si especifica un valor para este parámetro, pero no especifica valores para los parámetros `SubnetId`y `SecurityGroupIds`, la automatización intentará lanzar la instancia en la VPC predeterminada con el grupo de seguridad predeterminado. Si EC2-Classic está activado en la región de destino, se producirá un error en el lanzamiento.

- SubnetId

  Tipo: String

  Descripción: (Opcional) El ID de la subred en la que desea copiar la instancia. Si EC2-Classic está activado en la región de destino, debe proporcionar un valor para este parámetro.

- InstanceType

  Tipo: String

  Descripción: (Opcional) el tipo de instancia EC2 que se va iniciar. Si no especifica un valor para este parámetro, se utiliza el tipo de instancia de origen. Si el tipo de instancia de origen no es compatible con la región en la que se está copiando la instancia, se produce un error en la automatización.

- SecurityGroupIds

  Tipo: String

  Descripción: (Opcional) Una lista separada por comas de los identificadores de grupo de seguridad que desea asociar con la instancia copiada. Si no especifica un valor para este parámetro y la instancia no se copia en una región diferente, se utilizan los grupos de seguridad asociados a la instancia de origen. Si va a copiar la instancia a una región diferente, se utiliza el grupo de seguridad predeterminado para la VPC predeterminada de la región de destino.

- KeepImageSourceRegion

  Tipo: booleano

  Valores válidos: true | false

  Valor predeterminado: true

Descripción: (Opcional) Si especifica `true`para este parámetro, la automatización no elimina la AMIde la instancia de origen. Si especifica `false` para este parámetro, la automatización anula el registro de AMI y elimina las instantáneas asociadas.

- KeepImageDestinationRegion

  Tipo: booleano

  Valores válidos: true | false

  Valor predeterminado: true

  Descripción: (Opcional) Si especifica `true`para este parámetro, la automatización no elimina la AMIque se haya copiado en la región que especificó. Si especifica `false` para este parámetro, la automatización anula el registro de AMI y elimina las instantáneas asociadas.

- NoRebootInstanceBeforeTakingImage

  Tipo: booleano

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) Si especifica `true`para este parámetro, la instancia de origen no se reiniciará antes de crear la AMI. Cuando se utiliza esta opción, no se puede garantizar la integridad del sistema de archivos en la imagen creada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Si está copiando la instancia en una región diferente, también necesitará los siguientes permisos.

- `ec2:CopyImage`

Pasos de documentos

- describeOriginalInstanceDetails - Recopila los detalles de la instancia que se va a copiar.
- assertRootVolumeIsEbs - Comprueba si el tipo de dispositivo de volumen raíz es `ebs`y, de no ser así, finaliza la automatización.
- evalInputParameters - Evalúa los valores proporcionados para los parámetros de entrada.
- createLocalAmi - Crea una AMIde la instancia de origen.
- tagLocalAmi - Etiqueta la AMIcreada en el paso anterior.
- branchAssertRegionIsSame - Se ramifica en función de si la instancia se está copiando en la misma región o en una región diferente.
- branchAssertSameRegionWithKeyPair - Se ramifica en función de si se ha proporcionado un valor para el parámetro `KeyPair`de una instancia que se está copiando en la misma región.
- sameRegionLaunchInstanceWithKeyPair - Lanza una instancia de Amazon EC2 desde la AMIde la instancia de origen de la misma subred o de la subred que especifique mediante el par de claves que especificó.
- sameRegionLaunchInstanceWithoutKeyPair - Lanza una instancia de Amazon EC2 desde la AMIde la instancia de origen de la misma subred o de la subred que especifique sin un par de claves.
- copyAmiToRegion - Copia la AMIpara la región de destino.
- waitForAvailableDestinationAmi - Espera a que el estado copiado de AMIpase a ser `available`.
- destinationRegionLaunchInstance - Lanza una instancia de Amazon EC2 utilizando la AMIcopiada.
- branchAssertDestinationAmiToDelete - Se ramifica en función del valor que haya proporcionado para el parámetro `KeepImageDestinationRegion`.
- deregisterDestinationAmiAndDeleteSnapshots - Anula el registro de la AMIcopiada y elimina las instantáneas asociadas.
- branchAssertSourceAmiTodelete - Se ramifica en función del valor que haya proporcionado para el parámetro `KeepImageSourceRegion`.
- deregisterSourceAmiAndDeleteSnapshots - Anula el registro de la AMIcreada en la instancia de origen y elimina las instantáneas asociadas.
- sleep - Suspende la automatización durante 2 segundos. Se trata de un estado terminal.

Salidas

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstance.DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

Descripción

El manual le `AWSSupport-EnableWindowsEC2SerialConsole` ayuda a habilitar la consola serie Amazon EC2, la consola de administración especial (SAC) y el menú de arranque en su instancia Amazon EC2 de Windows. Con la función Amazon Elastic Compute Cloud (Amazon EC2) Serial Console, tiene acceso al puerto serie de su instancia Amazon EC2 para solucionar problemas de arranque, configuración de red y otros problemas. El manual automatiza los pasos necesarios para habilitar la función en las instancias en estado de ejecución y administradas por AWS Systems Manager, así como en las que están detenidas o no están administradas por. AWS Systems Manager

¿Cómo funciona?

El manual de `AWSSupport-EnableWindowsEC2SerialConsole` automatización ayuda a habilitar el SAC y el menú de arranque en las instancias de Amazon EC2 que ejecutan Microsoft Windows Server. En el caso de las instancias en estado de ejecución y administradas por AWS Systems Manager, el runbook AWS Systems Manager ejecuta un PowerShell script Run Command para activar el SAC y el menú de arranque. En el caso de las instancias detenidas o no gestionadas por AWS Systems Manager, el runbook utiliza AWSSupport-Startec2 RescueWorkflow para crear una instancia temporal de Amazon EC2 a fin de realizar los cambios necesarios sin conexión a Internet.

Para obtener más información, consulte Amazon EC2 Serial Console para instancias de Windows.

> **Important**
>
> - Si habilita SAC en una instancia, los servicios de Amazon EC2 que se basan en la recuperación de contraseñas no funcionarán desde la consola de Amazon EC2. Para obtener más información, consulte Usar SAC para solucionar problemas de su instancia de Windows.

- Para configurar el acceso a la consola en serie, debe conceder el acceso a la consola en serie a nivel de cuenta y, a continuación, configurar las políticas AWS Identity and Access Management (IAM) para conceder el acceso a sus usuarios. También debe configurar un usuario basado en contraseña en cada instancia para que los usuarios puedan utilizar la consola serie para solucionar problemas. Para obtener más información, consulte Configurar el acceso a la consola en serie Amazon EC2.
- Para comprobar si la consola serie está habilitada en su cuenta, consulte Ver el estado de acceso de la cuenta a la consola serie.
- El acceso a la consola en serie solo se admite en las instancias virtualizadas integradas en el sistema Nitro.

Para obtener más información, consulte los requisitos previos de la consola serie Amazon EC2.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-EnableWindowsEC2SerialConsole` la AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - InstanceId: (Obligatorio)

     El ID de la instancia de Amazon EC2 en la que desea habilitar la consola serie (SAC) y el menú de arranque de Amazon EC2.
   - AutomationAssumeRole: (Opcional)

El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- HelperInstanceType: (Condicional)

  El tipo de instancia de Amazon EC2 que el runbook proporciona para configurar la consola serie Amazon EC2 para una instancia fuera de línea.

- HelperInstanceProfileName: (Condicional)

  El nombre de un perfil de instancia de IAM existente para la instancia auxiliar. Si habilitas el SAC y el menú de arranque en una instancia que está detenida o no está gestionada por ella AWS Systems Manager, es obligatorio. Si no se especifica un perfil de instancia de IAM, la automatización crea uno en tu nombre.

- SubnetId: (Condicional)

  El ID de subred de una instancia auxiliar. De forma predeterminada, usa la misma subred en la que reside la instancia proporcionada.

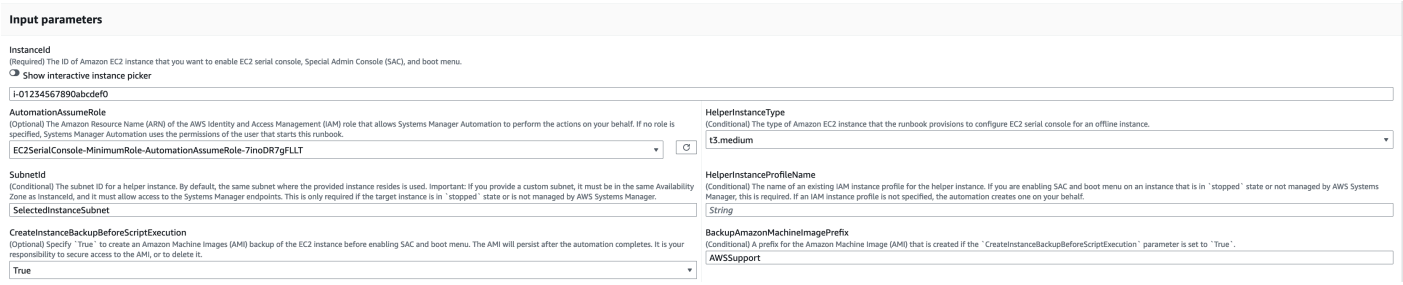
  > **Important**
  >
  > Si proporciona una subred personalizada, debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales de Systems Manager. Esto solo es necesario si la instancia de destino está detenida o no está gestionada por ella. AWS Systems Manager

- CreateInstanceBackupBeforeScriptExecution: (Opcional)

  Especifique True para crear una copia de seguridad de Amazon Machine Images (AMI) de la instancia Amazon EC2 antes de activar SAC y el menú de arranque. La AMI se conservará una vez terminada la Automation. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- BackupAmazonMachineImagePrefix: (Condicional)

  Un prefijo para la Amazon Machine Image (AMI) que se crea si el `CreateInstanceBackupBeforeScriptExecution` parámetro está establecido en. `True`



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - CheckIfEc2: SerialConsoleAccessEnabled

     Comprueba si el acceso a la consola serie Amazon EC2 está habilitado a nivel de cuenta. Nota: El acceso a la consola serie no está disponible de forma predeterminada. Para obtener más información, consulte Configurar el acceso a la consola en serie Amazon EC2.
   - CheckIfEc2: InstanceIsWindows

     Afirma si la plataforma de la instancia de destino es Windows.
   - GetInstanceType:

     Recupera el tipo de instancia de la instancia de destino.
   - CheckIfInstanceTypeIsNitro:

     Comprueba si el hipervisor del tipo de instancia está basado en Nitro. El acceso a la consola en serie solo se admite en instancias virtualizadas creadas en el sistema Nitro.
   - CheckIfInstanceIsInAutoScalingGrupo:

     Comprueba si la instancia de Amazon EC2 forma parte de un grupo de Auto Scaling de Amazon EC2 mediante `DescribeAutoScalingInstances` una llamada a la API. Si la instancia forma parte de un grupo de Auto Scaling de Amazon EC2, se asegura de que la instancia de Porting Assistant para.NET esté en estado de ciclo de vida en espera.
   - WaitForEc2: InstanceStateStablized

     Espera a que la instancia esté en estado de ejecución o parada.
   - GetEc2: InstanceState

     Obtiene el estado actual de la instancia.

- BranchOnEc2InstanceState:

  Se ramifica en función del estado de la instancia recuperado en el paso anterior. Si ese estado de instancia se está ejecutando, pasa al `CheckIfEc2InstanceIsManagedBySSM` paso y, si no, va al `CheckIfHelperInstanceProfileIsProvided` paso.

- CheckIfEc2 InstanceIsManagedBy SSM:

  Comprueba si la instancia está gestionada por AWS Systems Manager. Si se administra, el runbook habilita el SAC y el menú de arranque mediante un comando de PowerShell ejecución.

- BranchOnPreEC2RescueBackup:

  Se ramifica en función del parámetro `CreateInstanceBackupBeforeScriptExecution` de entrada.

- CreateAmazonMachineImageBackup:

  Crea una copia de seguridad AMI de la instancia.

- Habilita SACAndBootMenu:

  Activa el SAC y el menú de arranque mediante la ejecución de un script de PowerShell ejecución de comandos.

- RebootInstance:

  Reinicia la instancia Amazon EC2 para aplicar la configuración. Este es el último paso si la instancia está en línea y la administra. AWS Systems Manager

- CheckIfHelperInstanceProfileIsProvided:

  Comprueba si lo `HelperInstanceProfileName` especificado existe antes de habilitar el SAC y el menú de arranque sin conexión mediante una instancia temporal de Amazon EC2.

- RunAutomationToInjectOfflineScriptForHabilitar el SACAndBootMenu:

  Ejecuta el menú `AWSSupport-StartEC2RescueWorkflow` para habilitar el SAC y el menú de arranque cuando la instancia está detenida o no está gestionada por ella. AWS Systems Manager

- GetExecutionDetails:

  Recupera el identificador de imagen de la copia de seguridad y la salida del script sin conexión.

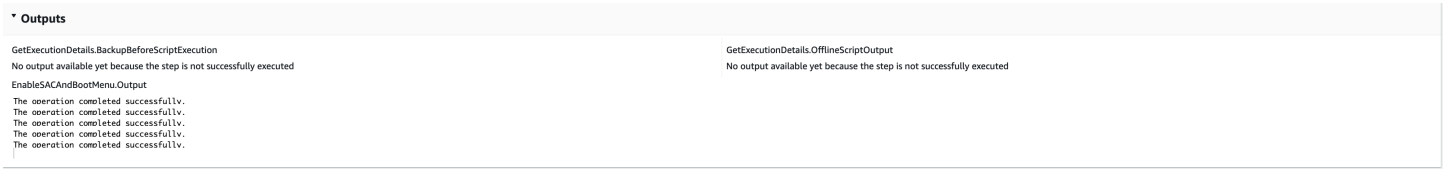
7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:
   - Habilite AC. SalidaAndBootMenu:

     Resultado de la ejecución del comando en el paso. `EnableSACAndBootMenu`
   - GetExecutionDetails.OfflineScriptOutput:

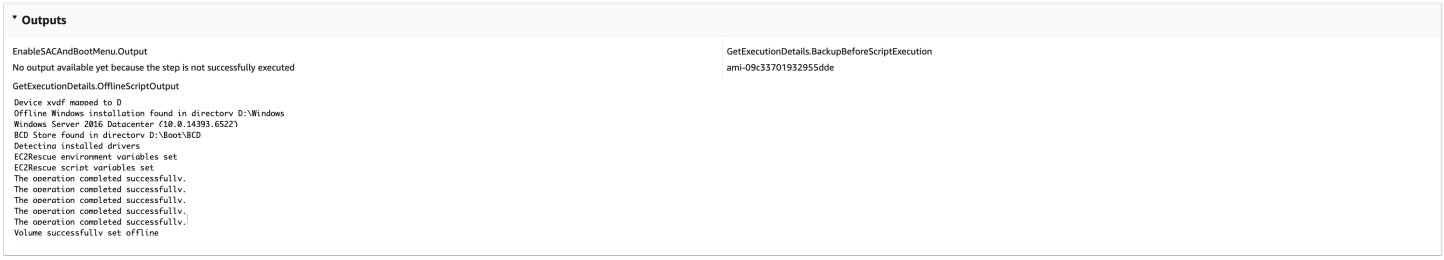
     Resultado del script fuera de línea ejecutado en el `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` paso.
   - GetExecutionDetails.BackupBeforeScriptExecution:

     ID de imagen de la copia de seguridad de la AMI tomada si el parámetro `CreateInstanceBackupBeforeScriptExecution` de entrada es True.

Resultado de la ejecución en una instancia que está en ejecución y gestionada por AWS Systems Manager



Resultado de la ejecución en una instancia que está detenida o no gestionada por AWS Systems Manager



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWSSupport-ExecuteEC2Rescue

Descripción

En este runbook, se utiliza la EC2Rescueherramienta para solucionar problemas y, en la medida de lo posible, reparar problemas de conectividad comunes con la instancia de Amazon Elastic Compute Cloud (Amazon EC2) especificada para Linux o. Windows Server No se admiten instancias con volúmenes raíz cifrados.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EC2RescueInstanceType

  Tipo: String

  Valores permitidos: t2.small | t2.medium | t2.large

  Valor predeterminado: t2.small

  Descripción: (Obligatorio): el tipo de instancia EC2 para la instancia EC2Rescue. Tamaño recomendado: `t2.small`

- LogDestination

  Tipo: String

  Descripción: (Opcional) nombre del bucket de Amazon S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- SubnetId

  Tipo: String

  Valor predeterminado: CreateNewVPC

  Descripción: (Opcional) el ID de subred para la instancia EC2Rescue. De forma predeterminada, AWS Systems ManagerAutomation crea una nueva VPC. De forma alternativa, utilice `SelectedInstanceSubnet`para usar la misma subred que la instancia o especifique un ID de subred personalizado.

  > **Important**
  >
  > La subred debe estar en la misma zona de disponibilidad que `UnreachableInstanceId`y debe permitir el acceso a puntos de enlace de SSM.

- UnreachableInstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia EC2 inaccesible.

  > **Important**
  >
  > Systems Manager Automation detiene esta instancia y crea una AMI antes de intentar realizar cualquier operación. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Debe tener al menos `ssm:StartAutomationExecution`y `ssm:GetAutomationExecution`para poder leer el resultado de la automatización. Para obtener más información sobre los permisos necesarios, consulte `AWSSupport-StartEC2RescueWorkflow`.

Pasos de documentos

1. `aws:assertAwsResourceProperty` - Confirma si la instancia proporcionada esWindows Server:
   a. (EC2Rescue para Windows Server) Si la instancia proporcionada es de Windows Server:
      i. `aws:executeAutomation`- Se invoca `AWSSupport-StartEC2RescueWorkflow`con el script EC2Rescue para fuera de línea. Windows Server
      ii. `aws:executeAwsApi` - Recuperar el ID de AMI de copia de seguridad de la Automation anidada.
      iii. `aws:executeAwsApi` - Recuperar el resumen de EC2Rescue de la Automation anidada.
   b. (EC2Rescue para Linux) Si la instancia proporcionada es de Linux:
      i. `aws:executeAutomation` - Se invoca `AWSSupport-StartEC2RescueWorkflow`con EC2Rescue para Linux con scripts offline
      ii. `aws:executeAwsApi` - Recuperar el ID de AMI de copia de seguridad de la Automation anidada.
      iii. `aws:executeAwsApi` - Recuperar el resumen de EC2Rescue de la Automation anidada.

Salidas

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descripción

El `AWSSupport-ListEC2Resources`runbook devuelve información sobre las instancias de Amazon EC2 y los recursos relacionados, como los volúmenes de Amazon Elastic Block Store (Amazon EBS), las direcciones IP elásticas y los grupos de Amazon EC2 Auto Scaling de las Regiones de AWSespecificadas. De forma predeterminada, la información se recopila de todas las regiones y se muestra en el resultado de la automatización. Si lo desea, puede especificar un bucket de Amazon Simple Storage Service (Amazon S3) donde se cargue la información como un archivo de valores separados por comas (.csv).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Bucket

  Tipo: String

  Descripción: (opcional) El nombre del bucket de S3 donde se carga la información recopilada.
- Mostrar la documentación sobre la eliminación de recursos

  Tipo: String

  Valor predeterminado: true

Descripción: (Opcional) Si se establece en`true`, la automatización crea enlaces en el resultado a la documentación relacionada con la eliminación de los recursos.

- Regiones para consultar

  Tipo: String

  Valor predeterminado: All

  Descripción: (opcional) Las regiones de las que desea recopilar información relacionada con Amazon EC2.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Además, para cargar correctamente la información recopilada en el depósito de S3 que especifique, es `AutomationAssumeRole`necesario realizar las siguientes acciones:

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

Pasos de documentos

- `aws:executeAwsApi`- Recopila las regiones habilitadas para la cuenta.
- `aws:executeScript`- Confirma que las regiones habilitadas para la cuenta admiten las regiones especificadas en el `RegionsToQuery`parámetro.
- `aws:branch`- Si no hay ninguna región habilitada para la cuenta, la automatización finaliza.
- `aws:executeScript`- Muestra todas las instancias de EC2 de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todas las imágenes de máquinas de Amazon (AMI) de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todos los volúmenes de EBS de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todas las direcciones IP elásticas de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todas las interfaces de red elásticas de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todos los grupos de Auto Scaling de la cuenta y las regiones que especifique.
- `aws:executeScript`- Muestra todos los balanceadores de carga de la cuenta y las regiones que especifique.
- `aws:executeScript`- Carga la información recopilada en el depósito de S3 especificado si se proporciona un valor para el `Bucket`parámetro.

`AWSSupport-ManageRDPSettings`

Descripción

El manual de procedimientos de `AWSSupport-ManageRDPSettings`permite al usuario administrar la configuración común del protocolo de escritorio remoto (RDP), como, por ejemplo, la configuración del puerto RDP y la autenticación en el nivel de red (NLA). De forma predeterminada, el manual de procedimientos lee los valores de estos ajustes y los incluye en la salida.

> **Important**
>
> Los cambios en la configuración de RDP deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia administrada para administrar la configuración de RDP.
- NLASettingAction

  Tipo: String

  Valores válidos: Check | Enable | Disable

  Valor predeterminado: Check

  Descripción: (Obligatorio) una acción para realizar en la configuración de NLA: comprobar, habilitar, deshabilitar.
- RDPPort

Tipo: String

Valor predeterminado: 3389

Descripción: (Opcional) especifique el nuevo puerto RDP. Solo se utiliza cuando la acción se establece en Modify. El número de puerto debe estar comprendido entre 1025 y 65535. Nota: Después de que se cambia el puerto, se reinicia el servicio de RDP.

- RDPPortAction

  Tipo: String

  Valores válidos: Check | Modify

  Valor predeterminado: Check

  Descripción: (Obligatorio) una acción que aplicar al puerto RDP.

- RemoteConnections

  Tipo: String

  Valores válidos: Check | Enable | Disable

  Valor predeterminado: Check

  Descripción: (Obligatorio) una acción para realizar en la configuración de fDenyTSConnections.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

La instancia EC2 que recibe el comando debe tener un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. El usuario debe tener al menos ssm:SendCommand para enviar el comando a la instancia, además de ssm:GetCommandInvocation para poder leer la salida del comando.

Pasos de documentos

`aws:runCommand` - Ejecute el script de PowerShell para cambiar o comprobar la configuración de RDP en la instancia de destino.

Salidas

manageRDPSettings.Output

AWSSupport-ManageWindowsService

Descripción

El AWSSupport-ManageWindowsServicerunbook permite detener, iniciar, reiniciar, pausar o deshabilitar cualquier servicio de Windows en la instancia de destino.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia administrada para administrar los servicios de.
- ServiceAction

  Tipo: String

Valores permitidos: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

Valor predeterminado: Check

Descripción: (Obligatoria) Una acción para aplicarla al servicio de Windows. Tenga en cuenta que `Force-Restarty` `Force-Stop` se pueden utilizar para reiniciar y detener un servicio que tiene servicios dependientes.

- StartupType

  Tipo: String

  Valores permitidos: Check | Auto | Demand | Disabled | DelayedAutoStart

  Valor predeterminado: Check

  Descripción: (Obligatorio) Un tipo de inicio para aplicarlo al servicio de Windows.

- WindowsServiceName

  Tipo: String

  Descripción: (Obligatorio) un nombre de servicio de Windows válido.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la instancia EC2 que recibe el comando tenga un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. El usuario debe tener al menos ssm:StartAutomationExecution y ssm:SendCommand para ejecutar Automation y enviar el comando a la instancia, así como ssm:GetAutomationExecution para poder leer la salida de Automation.

Pasos de documentos

`aws:runCommand` - Ejecute el script de PowerShell para aplicar la configuración deseada al servicio de Windows en la instancia de destino.

Salidas

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

Descripción

El `AWSSupport-MigrateEC2ClassicToVPC`manual de procedimientos migra una instancia de Amazon Elastic Compute Cloud (Amazon EC2) de EC2-Classic a una nube privada virtual (VPC). Este manual de procedimientos admite la migración de instancias de Amazon EC2 del tipo de virtualización de máquina virtual de hardware (HVM) con volúmenes raíz de Amazon Elastic Block Store (Amazon EBS).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Obligatorio) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre.
- Apruebe la IAM

  Tipo: StringList

  Descripción: (opcional) Los nombres de los recursos de Amazon (ARN) de los usuarios de IAM que pueden aprobar o denegar la acción. Este parámetro es obligatorio si especifica un valor `CutOver`para el parámetro `MigrationType`.
- DestinationSecurityGroupId

Tipo: StringList

Descripción: (opcional) El ID del grupo de seguridad que desea asociar a la instancia de Amazon EC2 que se lanza en la VPC. Si no especifica un valor para este parámetro, la automatización crea un grupo de seguridad en la VPC y copia las reglas del grupo de seguridad en EC2-Classic. Si las reglas no se copian en el nuevo grupo de seguridad, el grupo de seguridad predeterminado de la VPC se asocia con la instancia de Amazon EC2.

- ID de subred de destino

  Tipo: String

  Descripción: (Opcional) El ID de la subred a la que quiere migrar la instancia de Amazon EC2. Si no especifica un valor para este parámetro, la automatización elige de forma aleatoria una subred de la VPC.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia de Amazon EC2 que desea reiniciar.

- MigrationType

  Tipo: String

  Valores válidos: CutOver

  Descripción: (Obligatorio) El tipo de migración que desea realizar.

  La `CutOver`opción requiere aprobación para detener la instancia de Amazon EC2 que se ejecuta en EC2-Classic. Una vez aprobada esta acción, la instancia de Amazon EC2 se detiene y la automatización crea un Amazon Machine Image()AMI. Cuando el AMIestado es`available`, se lanza una nueva instancia de Amazon EC2 desde allí AMIen la `DestinationSubnetId`que especifique en su VPC. Si la instancia de Amazon EC2 que se ejecuta en EC2-Classic tiene una dirección IP elástica adjunta, la instancia se moverá a la instancia de Amazon EC2 recién creada en su VPC. Si la instancia de Amazon EC2 que se está lanzando en su VPC no se crea por algún motivo, se cancela y se solicita la aprobación para iniciar la instancia de Amazon EC2 en EC2-Classic.

  La `Test`opción crea una instancia AMIde Amazon EC2 que se ejecuta en EC2-Classic sin necesidad de reiniciarse. Como la instancia de Amazon EC2 no se reinicia, no podemos garantizar

la integridad del sistema de archivos de la imagen creada. Cuando el AMIestado es`available`, se lanza una nueva instancia de Amazon EC2 desde allí, AMIen la `DestinationSubnetId`que especifique en su VPC. Si la instancia de Amazon EC2 que se ejecuta en EC2-Classic tiene una dirección IP elástica adjunta, la automatización verifica que la `DestinationSubnetId`que especifique sea pública. Si la instancia de Amazon EC2 que se está lanzando en su VPC no se crea por algún motivo, se termina y la automatización finaliza.

- Se envía una notificación de DNS para su aprobación

  Tipo: String

  Descripción: (Opcional) Se establece el ARN del tema de Amazon Simple Notification Service (Amazon SNS) al que desea enviar las solicitudes de aprobación. Este parámetro es obligatorio si especifica un valor `CutOver`para el parámetro `MigrationType`.

- TargetInstanceType

  Tipo: String

  Predeterminado: t2.2xlarge

  Descripción: (opcional) El tipo de instancia de Amazon EC2 que desea lanzar en la VPC. Solo se admiten los tipos de instancias basados en Xen, como T2, M4 o C4.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeAwsApi- Recopila detalles sobre la instancia de Amazon EC2 que especifique en InstanceIdel parámetro.
- aws:assertAwsResourceProperty- Confirma que el tipo de instancia que especifica en el TargetInstanceTypeparámetro está basado en Xen.
- aws:assertAwsResourceProperty- Confirma que la instancia de Amazon EC2 que especificó en el InstanceIdparámetro es del tipo de virtualización HVM.
- aws:assertAwsResourceProperty- Confirma que la instancia de Amazon EC2 que especificó en el InstanceIdparámetro tiene un volumen raíz de Amazon EBS.

- `aws:executeScript`- Crea un grupo de seguridad según sea necesario en función del valor que especifique para el `DestinationSecurityGroupId`parámetro.
- `aws:branch`- Se ramifica en función del valor que especifique en el `DestinationSubnetId`parámetro.
- `aws:executeAwsApi`- Identifica la VPC predeterminada en la que Región de AWSse ejecuta esta automatización.
- `aws:executeAwsApi`- Elige aleatoriamente el ID de una subred ubicada en la VPC predeterminada.
- `aws:createImage`- Crea una AMIinstancia de Amazon EC2 sin reiniciar.
- `aws:branch`- Se ramifica en función del valor que especifique para el parámetro. `MigrationType`
- `aws:branch`- Se ramifica en función del valor que especifique para el `DestinationSubnetId`parámetro.
- `aws:runInstances`- Lanza una nueva instancia a partir de la AMIcreada sin reiniciar la instancia de Amazon EC2 en EC2-Classic.
- `aws:changeInstanceState`- Termina la instancia de Amazon EC2 recién lanzada si el paso anterior falla por algún motivo.
- `aws:runInstances`- Lanza una nueva instancia a partir de la AMIcreada sin reiniciar la instancia de Amazon EC2 en EC2-Classic si se proporciona. `DestinationSubnetId`
- `aws:changeInstanceState`- Termina la instancia de Amazon EC2 recién lanzada si el paso anterior falla por algún motivo.
- `aws:assertAwsResourceProperty`- Confirma el comportamiento de parada de la instancia de Amazon EC2 que se ejecuta en EC2-Classic.
- `aws:approve`- Espera la aprobación para detener la instancia de Amazon EC2.
- `aws:changeInstanceState`- Detiene la instancia de Amazon EC2 que se ejecuta en EC2-Classic.
- `aws:changeInstanceState`- La fuerza detiene la instancia de Amazon EC2 que se ejecuta en EC2-Classic si es necesario.
- `aws:createImage`- Crea una instancia AMIde Amazon EC2 una vez detenida.
- `aws:branch` - Se ramifica en función del valor especificado para el parámetro `DestinationSubnetId`.
- `aws:runInstances`- Lanza una nueva instancia a partir de AMIla instancia de Amazon EC2 detenida en EC2-Classic.

- `aws:approve`- Espera la aprobación para finalizar la instancia recién lanzada e inicia la instancia de Amazon EC2 en EC2-Classic si el paso anterior falla por algún motivo.
- `aws:changeInstanceState`- Termina la instancia de Amazon EC2 recién lanzada.
- `aws:runInstances`- Lanza una nueva instancia a partir de AMIla instancia de Amazon EC2 detenida en EC2-Classic a partir del parámetro. `DestinationSubnetId`
- `aws:approve`- Espera la aprobación para finalizar la instancia recién lanzada e inicia la instancia de Amazon EC2 en EC2-Classic si el paso anterior falla por algún motivo.
- `aws:changeInstanceState`- Termina la instancia de Amazon EC2 recién lanzada.
- `aws:changeInstanceState`- Inicia la instancia de Amazon EC2 que se detuvo en EC2-Classic.
- `aws:branch`- Se ramifica en función de si la instancia de Amazon EC2 tiene una dirección IP pública.
- `aws:executeAwsApi`- Verifica si la dirección IP pública es una dirección IP elástica.
- `aws:branch`- Se ramifica en función del valor que especifique en el `MigrationType`parámetro.
- `aws:executeAwsApi`- Mueve la dirección IP elástica a la VPC.
- `aws:executeAwsApi`- Recopila el ID de asignación de la dirección IP elástica que se trasladó a la VPC.
- `aws:branch`- Las sucursales se basan en la subred en la que se lanzó la instancia de Amazon EC2 que se ejecuta en la VPC.
- `aws:executeAwsApi`- Adjunta la dirección IP elástica a la instancia recién lanzada en la VPC.
- `aws:executeScript`- Confirma que la subred que acaba de lanzar la instancia de Amazon EC2 que se ejecuta en la VPC es pública.

Salidas

`getInstanceProperties.virtualizationType`: el tipo de virtualización de la instancia de Amazon EC2 que se ejecuta en EC2-Classic.

`getInstanceProperties.rootDeviceType`- El tipo de dispositivo raíz de la instancia de Amazon EC2 que se ejecuta en EC2-Classic.

`createAMIWithoutReboot.ImageId`- El ID de la instancia AMIcreada sin reiniciar la instancia de Amazon EC2 que se ejecuta en EC2-Classic.

`getDefaultVPC.VpcId`- El ID de la VPC predeterminada en la que se lanza la nueva instancia de Amazon EC2 si no se proporciona un valor para `DestinationSubnetId`del parámetro.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- El ID de la subred de la VPC predeterminada en la que se lanza la nueva instancia de Amazon EC2 si no se proporciona un valor para `DestinationSubnetId`el parámetro.

`launchTestInstanceDefaultVPC.InstanceIds`- El ID de la instancia de Amazon EC2 recién lanzada en la VPC predeterminada durante el tipo de migración. `Test`

`launchTestInstanceProvidedSubnet.InstanceIds`- El ID de la instancia de Amazon EC2 recién lanzada `DestinationSubnetId`que especificó durante el tipo de `Test`migración.

`createAMIAfterStoppingInstance.ImageId`- El ID de la instancia AMIcreada tras detener la ejecución de la instancia de Amazon EC2 en EC2-Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- El ID de la instancia de Amazon EC2 recién lanzada `DestinationSubnetId`que especificó durante el tipo de `CutOver`migración.

`launchCutOverInstanceDefaultVPC.InstanceIds`- El ID de la instancia de Amazon EC2 recién lanzada en la VPC predeterminada durante el tipo de migración. `CutOver`

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Si la subred elegida por la automatización en tu VPC predeterminada es pública.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Si la subred que especificó en la `DestinationSubnetId`es pública.

AWSSupport-MigrateXenToNitroLinux

Descripción

El `AWSSupport-MigrateXenToNitroLinux`manual de procedimientos clona, prepara y migra una instancia de Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen de Amazon EC2 a un tipo de instancia. Nitro Este manual de ejecución ofrece dos opciones para los tipos de operaciones:

- `Clone&Migrate`— El flujo de trabajo de esta opción consiste en las comprobaciones preliminares, las pruebas y Clone&Migratelas fases. El flujo de trabajo se ejecuta mediante el `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro`manual de ejecución.
- `FullMigration`— Esta opción ejecuta el `Clone&Migrate`flujo de trabajo y, a continuación, realiza el paso adicional de reemplazar los volúmenes raíz de Amazon EBS.

> **Important**
>
> El uso de este manual de procedimientos implica costes en la cuenta por el tiempo de funcionamiento de las instancias de Amazon EC2, la creación de volúmenes de Amazon Elastic Block Store (Amazon EBS) y. AMIs Para obtener más detalles, consulte Precios de Amazon EC2 y Precios de Amazon EBS.

Controles preliminares

La automatización realiza las siguientes comprobaciones preliminares antes de continuar con la migración. Si alguna de las comprobaciones falla, la automatización finaliza. Esta fase es solo una parte del `Clone&Migrate`flujo de trabajo.

- Comprueba si la instancia de destino ya es de un tipo de Nitroinstancia.
- Comprueba si se utilizó la opción de compra de instancias puntuales para la instancia de destino.
- Comprueba si los volúmenes del almacén de instancias están adjuntos a la instancia de destino.
- Comprueba si el sistema operativo (SO) de la instancia de destino es Linux.
- Comprueba si la instancia de destino forma parte de un grupo de Amazon EC2 Auto Scaling. Si forma parte de un grupo de Auto Scaling, la automatización verifica si la instancia se encuentra en ese `standby`estado.
- Verifica que la instancia esté gestionada por. AWS Systems Manager

Pruebas

La automatización crea un Amazon Machine Image(AMI) a partir de la instancia de destino y lanza una instancia de prueba a partir de la recién creadaAMI. Esta fase solo forma parte del `Clone&Migrate`flujo de trabajo.

Si la instancia de prueba supera todas las comprobaciones de estado, la automatización se detiene y se solicita la aprobación de los directores designados mediante una notificación del Servicio de Notificación Simple de Amazon (Amazon SNS). Si se aprueba, la automatización finaliza la instancia de prueba, detiene la instancia de destino y continúa con la migración, mientras que la recién creada AMIse anula del registro al final del flujo de trabajo. `Clone&Migrate`

> **Note**
>
> Antes de conceder la aprobación, recomendamos comprobar que todas las aplicaciones que se ejecutan en la instancia de destino se hayan cerrado correctamente.

Clonar y migrar

La automatización crea otra AMIa partir de la instancia de destino y lanza una nueva instancia para cambiarla a un tipo de Nitroinstancia. La automatización cumple los siguientes requisitos previos antes de continuar con la migración. Si alguna de las comprobaciones falla, la automatización finaliza. Esta fase también es solo una parte del `Clone&Migrate`flujo de trabajo.

- Activa el atributo de red mejorada (ENA).
- Instala la versión más reciente de los controladores ENA si aún no están instalados, o actualiza la versión de los controladores ENA a la versión más reciente. Para garantizar el máximo rendimiento de la red, es necesario actualizar a la última versión del controlador ENA si el tipo de Nitroinstancia es de sexta generación.
- Verifica que el módulo NVMe esté instalado. Si el módulo está instalado, la automatización verifica si el módulo está cargado. `initramfs`
- Analiza `/etc/fstab`y reemplaza las entradas con nombres de dispositivos de bloques (`/dev/sd*o/dev/xvd*`) con sus respectivos UUID. Antes de modificar la configuración, la automatización crea una copia de seguridad del archivo en la ruta`/etc/fstab*`.
- Desactiva la nomenclatura predecible de la interfaz añadiendo la `net.ifnames=0`opción a la `GRUB_CMDLINE_LINUX`línea del `/etc/default/grub`archivo, si existe, o al núcleo en el que se encuentra`/boot/grub/menu.lst`.
- Elimina el `/etc/udev/rules.d/70-persistent-net.rules`archivo si existe. Antes de eliminar el archivo, la automatización crea una copia de seguridad del archivo en la ruta`/etc/udev/rules.d/`.

Tras comprobar todos los requisitos, el tipo de instancia se cambia Nitropor el tipo de instancia que especifique. La automatización espera a que la instancia recién creada pase todas las comprobaciones de estado después de empezar como un tipo de Nitroinstancia. A continuación, la automatización espera la aprobación de los responsables designados para crear una AMIde las instancias lanzadas correctamente. Nitro Si se deniega la aprobación, la automatización finaliza, dejando la instancia recién creada en ejecución y la instancia de destino permanece detenida.

Reemplazar un volumen de Amazon EBS

Si elige `FullMigration`como`OperationType`, la automatización migra la instancia Amazon EC2 de destino Nitroal tipo de instancia que especifique. La automatización solicita la aprobación de los responsables designados para reemplazar el volumen raíz de Amazon EBS de la instancia Amazon EC2 de destino por el volumen raíz de la instancia Amazon EC2 clonada. Una vez que la migración se haya realizado correctamente, la instancia clonada de Amazon EC2 finaliza. Si se produce un error en la automatización, el volumen raíz original de Amazon EBS se adjunta a la instancia Amazon EC2 de destino. Si el volumen raíz de Amazon EBS adjunto a la instancia Amazon EC2 de destino tiene etiquetas con `aws:`el prefijo aplicado, no se admite `FullMigration`la operación.

Antes de empezar

La instancia de destino debe tener acceso saliente a Internet. Esto es para acceder a los repositorios de controladores y dependencias comokernel-devel,gcc,,patch,rpm-build, wgetdracutmake, linux-headersy. unzip Si es necesario, se usa el administrador de paquetes.

Se requiere un tema de Amazon SNS para enviar notificaciones de aprobaciones y actualizaciones. Para obtener más información acerca de la creación de un tema Amazon SNS, consulte Creating an Amazon SNS topic (Creación de un tema de Amazon SNS) en la Guía para desarrolladores de Amazon Simple Notification Service.

Este manual de procedimientos admite los siguientes sistemas operativos:

- RHEL7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Servidor Debian
- Ubuntu Server 18.04 LTS, 20.04 LTS, and 20.10 STR
- SUSE Linux Enterprise Server(SUSE 12 SP5, SUSE 15 SP2)

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Reconocimiento

  Tipo: String

  Descripción: (Obligatorio) Lea los detalles completos de las acciones realizadas por este manual de automatización e introdúzcalo **`Yes, I understand and acknowledge`**para continuar con el uso del manual.

- Apruebe la IAM

  Tipo: String

  Descripción: (obligatorio) Los ARN de las funciones, los usuarios o los nombres de usuario de IAM que pueden aprobar la automatización. Puede especificar un máximo de 10 aprobadores.

- Elimine los recursos en caso de error

  Tipo: booleano

  Descripción: (opcional) Determina si la instancia recién creada y AMIpara la migración se eliminan si se produce un error en la automatización.

  Valores válidos: True | False

  Valor predeterminado: True

- Aprobaciones mínimas requeridas

  Tipo: String

Descripción: (opcional) El número mínimo de aprobaciones necesario para seguir ejecutando la automatización cuando se solicitan aprobaciones.

Valores válidos: 1-10

Predeterminado: 1

- Tipo de instancia de Nitro

  Tipo: String

  Descripción: (Obligatorio) El tipo de Nitroinstancia al que quieres cambiarla. Los tipos de instancias compatibles incluyen M5, M6, C5, C6, R5, R6 y T3.

  Predeterminado: m5.xlarge

- OperationType

  Tipo: String

  Descripción: (Obligatorio) La operación que desea realizar. La `FullMigration`opción realiza las mismas tareas que el volumen raíz de la instancia de destino `Clone&Migrate`y, además, lo reemplaza. Tras el proceso de migración, el volumen raíz de la instancia de destino se sustituye por el volumen raíz de la instancia recién creada. La `FullMigration`operación no admite los volúmenes raíz definidos por Logical Volume Manager (LVM).

  Valores válidos: Clone&Migrate | FullMigration

- SNSTopicArn

  Tipo: String

  Descripción: (Obligatorio) el ARN del tema de SNS para que se notifique la aprobación. El tema Amazon SNS se utiliza para enviar las notificaciones de aprobación obligatorias durante la automatización.

- ID de instancia de destino

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia Amazon EC2 a mitigar.

Flujo de trabajo de Clone&Migrate

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- startOfPreliminaryChecksBranch- Se ramifica al flujo de trabajo de las comprobaciones preliminares.
- getTargetInstanceProperties- Recopila detalles de la instancia de destino.
- checkIfNitroInstanceTypeIsSupportedInAZ- Determina si el tipo de instancia de Amazon EC2 de destino se admite en la misma zona de disponibilidad que la instancia de destino.
- getXenInstanceTypeDetails- Recopila detalles sobre el tipo de instancia de origen.
- checkIfInstanceHypervisorIsNitroAlready- Comprueba si la instancia de destino ya se está ejecutando como un tipo de Nitroinstancia.
- checkIfTargetInstanceLifecycleIsSpot- Comprueba si la opción de compra de la instancia de destino es Spot.
- checkIfOperatingSystemIsLinux- Comprueba si el sistema operativo de la instancia de destino es Linux.
- verifySSMConnectivityForTargetInstance- Verifica que la instancia de destino esté gestionada por Systems Manager.
- checkIfEphemeralVolumeAreSupported- Comprueba si el tipo de instancia actual de la instancia de destino admite los volúmenes de almacén de instancias.
- verifyIfTargetInstanceHasEphemeralVolumesAttached- Comprueba si la instancia de destino tiene volúmenes de almacenamiento de instancias adjuntos.
- checkIfRootVolumeIsEBS- Comprueba si el tipo de volumen raíz de la instancia de destino es EBS.
- checkIfTargetInstanceIsInASG- Comprueba si la instancia de destino forma parte de un grupo de Auto Scaling.
- endOfPreliminaryChecksBranch- Fin de la rama de comprobaciones preliminares.
- startOfTestBranch- Se ramifica en el flujo de trabajo de las pruebas.
- createTestImage- Crea una prueba AMIde la instancia de destino.
- launchTestInstanceInSameSubnet- Lanza una instancia de prueba a partir de la prueba AMIcon la misma configuración que la instancia de destino.
- cleanupTestInstance- Termina la instancia EC2.

- `endOfTestBranch`- Fin de la rama de pruebas.
- `checkIfTestingBranchSucceeded`- Comprueba el estado de la rama de pruebas.
- `approvalToStopTargetInstance`- Espera la aprobación de los directores designados para detener la instancia de destino.
- `stopTargetEC2Instance`- Detiene la instancia de destino.
- `forceStopTargetEC2Instance`- La fuerza detiene la instancia de destino solo si el paso anterior no logra detenerla.
- `startOfCloneAndMigrateBranch`- Se ramifica en el Clone&Migrateflujo de trabajo.
- `createBackupImage`- Crea una AMIde las instancias de destino para que sirva de respaldo.
- `launchInstanceInSameSubnet`- Lanza una nueva instancia desde la copia de seguridad AMIcon la misma configuración que la instancia de origen.
- `waitForClonedInstanceToPassStatusChecks`- Espera a que la instancia recién creada pase todas las comprobaciones de estado.
- `verifySSMConnectivityForClonedInstance`- Verifica que la instancia recién creada esté gestionada por Systems Manager.
- `checkAndInstallENADrivers`- Comprueba si los controladores ENA están instalados en la instancia recién creada e instala los controladores si es necesario.
- `checkAndAddNVMEDrivers`- Comprueba si los controladores NVMe están instalados en la instancia recién creada e instala los controladores si es necesario.
- `checkAndModifyFSTABEntries`- Comprueba si se utilizan nombres de dispositivos `/etc/fstab`y los sustituye por UUID si es necesario.
- `stopClonedInstance`- Detiene la instancia recién creada.
- `forceStopClonedInstance`- Force detiene la instancia recién creada solo si el paso anterior no logra detenerla.
- `checkENAAttributeForClonedInstance`- Comprueba si el atributo de red mejorado está activado en la instancia recién creada.
- `setNitroInstanceTypeForClonedInstance`- Cambia el tipo de instancia de la instancia recién creada por el tipo de Nitroinstancia que especifique.
- `startClonedInstance`- Inicia la instancia recién creada cuyo tipo de instancia ha cambiado.
- `approvalForCreatingImageAfterDriversInstallation`- Si la instancia se inicia correctamente como un tipo de Nitroinstancia, la automatización espera la aprobación de los directores necesarios. Si se proporciona la aprobación, AMIse crea una para usarla como Golden. AMI

- `createImageAfterDriversInstallation`- Crea un AMIhombre para usarlo como doradoAMI.
- `endOfCloneAndMigrateBranch`- Final de la Clone&Migraterama.
- `cleanupTestImage`- Anula el registro de lo AMIcreado para probarlo.
- `failureHandling`- Comprueba si ha optado por cancelar los recursos en caso de fallo.
- `onFailureTerminateClonedInstance`- Termina la instancia recién creada si se produce un error en la automatización.
- `onFailurecleanupTestImage`- Anula el registro de lo AMIcreado para probarlo.
- `onFailureApprovalToStartTargetInstance`- Si la automatización falla, espera la aprobación de los directores designados para iniciar la instancia de destino.
- `onFailureStartTargetInstance`- Si la automatización falla, inicia la instancia de destino.

Flujo de trabajo de FullMigration

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

El FullMigrationflujo de trabajo ejecuta los mismos pasos que el Clone&Migrateflujo de trabajo y, además, realiza los siguientes pasos:

- checkConcurrency- Verifica que solo haya una automatización de este runbook dirigida a la instancia de Amazon EC2 que especifique. Si el runbook encuentra otra automatización en curso dirigida a la misma instancia, la automatización finaliza.
- getTargetInstanceProperties- Recopila detalles de la instancia de destino.
- checkRootVolumeTags- Determina si el volumen raíz de la instancia Amazon EC2 de destino contiene etiquetas AWSreservadas.
- cloneTargetInstanceAndMigrateToNitro- Inicia una automatización secundaria utilizando el manual de instruccionesAWS-CloneXenInstanceToNitro.
- branchOnTheOperationType- Se ramifica según el valor que especifique para el OperationTypeparámetro.

- `getClonedInstanceId`- Recupera el ID de la instancia recién lanzada de la automatización secundaria.
- `checkIfRootVolumeIsBasedOnLVM`- Determina si la partición raíz está gestionada por LVM.
- `branchOnTheRootVolumeLVMStatus`- Si se reciben las aprobaciones mínimas requeridas por parte de los directores, la automatización continúa con la sustitución del volumen raíz.
- `manualInstructionsInCaseOfLVM`- Si LVM administra el volumen raíz, la automatización envía un resultado que contiene instrucciones sobre cómo reemplazar manualmente los volúmenes raíz.
- `startOfReplaceRootEBSVolumeBranch`- Inicia el flujo de trabajo de la rama Reemplazar el volumen raíz de EBS.
- `checkIfTargetInstanceIsManagedByCFN`- Determina si la instancia de destino está gestionada por una AWS CloudFormationpila.
- `branchOnCFNStackStatus`- Ramas basadas en el estado de la pila de CloudFormation.
- `approvalForRootVolumesReplacement(WithCFN)`- Si CloudFormation lanzó la instancia de destino, la automatización espera su aprobación después de que la instancia recién lanzada se inicie correctamente como un Nitrotipo de instancia. Cuando se proporcionan las aprobaciones, los volúmenes de Amazon EBS de la instancia de destino se sustituyen por los volúmenes raíz de la instancia recién lanzada.
- `approvalForRootVolumesReplacement`- Espera la aprobación después de que la instancia recién lanzada se inicie correctamente como tipo de instancia. Nitro Cuando se proporcionan las aprobaciones, los volúmenes de Amazon EBS de la instancia de destino se sustituyen por los volúmenes raíz de la instancia recién lanzada.
- `assertIfTargetEC2InstanceIsStillStopped`- Verifica que la instancia de destino esté en un `stopped`estado antes de reemplazar el volumen raíz.
- `stopTargetInstanceForRootVolumeReplacement`- Si la instancia de destino está en ejecución, la automatización detiene la instancia antes de reemplazar el volumen raíz.
- `forceStopTargetInstanceForRootVolumeReplacement`- La instancia de destino se detiene por la fuerza si se produce un error en el paso anterior.
- `stopClonedInstanceForRootVolumeReplacement`- Detiene la instancia recién creada antes de sustituir los volúmenes de Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- Fuerza detiene la instancia recién creada si se produce un error en el paso anterior.
- `getBlockDeviceMappings`- Recupera las asignaciones de dispositivos de bloques tanto para las instancias de destino como para las recién creadas.

- `replaceRootEbsVolumes`- Sustituye el volumen raíz de la instancia de destino por el volumen raíz de la instancia recién creada.
- `EndOfReplaceRootEBSVolumeBranch`- Finalización del flujo de trabajo de la rama Replace Root EBS Volume.
- `checkENAAttributeForTargetInstance`- Comprueba si el atributo de red mejorada (ENA) está activado para la instancia Amazon EC2 de destino.
- `enableENAAttributeForTargetInstance`- Activa el atributo ENA para la instancia Amazon EC2 de destino si es necesario.
- `setNitroInstanceTypeForTargetInstance`- Cambia la instancia de destino al tipo de Nitroinstancia que especifique.
- `replicateRootVolumeTags`- Replica las etiquetas del volumen raíz de Amazon EBS de la instancia Amazon EC2 de destino.
- `startTargetInstance`- Inicia la instancia Amazon EC2 de destino tras cambiar el tipo de instancia.
- `onFailureStopTargetEC2Instance`- Detiene la instancia Amazon EC2 de destino si no se inicia como un tipo de Nitroinstancia.
- `onFailureForceStopTargetEC2Instance`- Fuerza detiene la instancia Amazon EC2 de destino si se produce un error en el paso anterior.
- `OnFailureRevertOriginalInstanceType`- Revierte la instancia Amazon EC2 de destino al tipo de instancia original si la instancia de destino no se inicia como Nitroun tipo de instancia.
- `onFailureRollbackRootVolumeReplacement`- Si es necesario, revierte todos los cambios realizados por el `replaceRootEbsVolumes`paso.
- `onFailureApprovalToStartTargetInstance`- Espera la aprobación del director designado para iniciar la instancia Amazon EC2 de destino tras anular los cambios anteriores.
- `onFailureStartTargetInstance`- Inicia la instancia Amazon EC2 de destino.
- `terminateClonedEC2Instance`- Finaliza la instancia de Amazon EC2 clonada tras sustituir el volumen raíz de Amazon EBS.

AWSSupport-ResetAccess

Descripción

Este manual de procedimientos utilizará la herramienta EC2Rescue en la instancia EC2 especificada para volver a habilitar el descifrado de contraseñas a través de la consola de EC2 (Windows) o

para generar y añadir un nuevo par de claves SSH (Linux). Si ha perdido el par de claves, esta Automation creará una AMI habilitada por contraseña que puede utilizar para lanzar una nueva instancia EC2 con un par de claves de su propiedad (Windows).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EC2RescueInstanceType

  Tipo: String

  Valores permitidos: t2.small | t2.medium | t2.large

  Valor predeterminado: t2.small

  Descripción: (Obligatorio): el tipo de instancia EC2 para la instancia EC2Rescue. Tamaño recomendado: t2.small.
- InstanceId

  Tipo: String

Descripción: (Obligatorio) ID de la instancia EC2 cuyo acceso desea restablecer.

> **Important**
>
> Systems Manager Automation detiene esta instancia y crea una AMI antes de intentar realizar cualquier operación. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- SubnetId

  Tipo: String

  Valor predeterminado: CreateNewVPC

  Descripción: (Opcional) el ID de subred para la instancia EC2Rescue. De forma predeterminada, Systems Manager Automation crea una nueva VPC. De forma alternativa, utilice SelectedInstanceSubnet para usar la misma subred que la instancia o especifique un ID de subred personalizado.

  > **Important**
  >
  > La subred debe estar en la misma zona de disponibilidad que InstanceId y debe permitir el acceso a puntos de enlace de SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Debe tener al menos ssm:StartAutomationExecution, ssm:GetParameter (para recuperar el nombre del parámetro de claves SSH) y ssm:GetAutomationExecution para poder leer la salida de la Automation. Para obtener más información sobre los permisos necesarios, consulte `AWSSupport-StartEC2RescueWorkflow`.

Pasos de documentos

1. `aws:assertAwsResourceProperty`- Afirme si la instancia proporcionada es Windows.

a. (EC2Rescue para Windows) Si la instancia proporcionada es Windows:
   i. `aws:executeAutomation`- Invoque `AWSSupport-StartEC2RescueWorkflow`con el script de restablecimiento de contraseñas sin conexión EC2Rescue para Windows
   ii. `aws:executeAwsApi` - Recuperar el ID de AMI de copia de seguridad de la Automation anidada.
   iii. `aws:executeAwsApi` - Recuperar el ID de AMI habilitada para contraseña de la Automation anidada.
   iv. `aws:executeAwsApi` - Recuperar el resumen de EC2Rescue de la Automation anidada.
b. (EC2Rescue para Linux) Si la instancia proporcionada es Linux:
   i. `aws:executeAutomation`- Invoque `AWSSupport-StartEC2RescueWorkflow`con el script de inyección de claves SSH fuera de línea de EC2Rescue para Linux
   ii. `aws:executeAwsApi` - Recuperar el ID de AMI de copia de seguridad de la Automation anidada.
   iii. `aws:executeAwsApi` - Recuperar el nombre de parámetro de SSM para la clave SSH inyectada.
   iv. `aws:executeAwsApi` - Recuperar el resumen de EC2Rescue de la Automation anidada.

Salidas

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getWindowsPasswordEnabledAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

getLinuxSSHKeyParameter.Name

AWSSupport-ResetLinuxUserPassword

Descripción

El manual de procedimientos `AWSSupport-ResetLinuxUserPassword` le ayuda a restablecer la contraseña de un usuario del sistema operativo (SO) local. Este manual de procedimientos es

especialmente útil para los usuarios que necesitan acceder a sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) mediante la consola de serie. El runbook crea una instancia temporal de Amazon EC2 en Cuenta de AWS usted y AWS Identity and Access Management un rol (IAM) con permisos para recuperar AWS Secrets Manager un valor secreto que contiene la contraseña.

El manual de procedimientos detiene la instancia de Amazon EC2 de destino, separa el volumen raíz de Amazon Elastic Block Store (Amazon EBS) y lo conecta a la instancia de Amazon EC2 temporal. Con Run Command, se ejecuta un script en la instancia temporal para establecer la contraseña del usuario del sistema operativo que especifique. A continuación, el volumen raíz de Amazon EBS se vuelve a adjuntar a la instancia de destino. El manual de procedimientos también ofrece una opción para crear una instantánea del volumen raíz al comienzo de la automatización.

Antes de empezar

Cree un secreto de Secrets Manager con el valor de la contraseña que desee asignar al usuario de su sistema operativo. El valor debe estar en texto sin formato. Para obtener más información, consulte Crear un secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager .

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos. Considere la posibilidad de establecer el valor del parámetro `CreateSnapshot` como **`Yes`**.
- Para cambiar la contraseña del usuario local, es necesario que el manual de procedimientos detenga la instancia. Los datos guardados en la memoria o en el almacén de instancias se perderán cuando se detenga una instancia. Además, se libera cualquier dirección IPv4 pública asignada automáticamente. Para obtener más información sobre lo que ocurre cuando detiene una instancia, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon EC2.
- Si los volúmenes de Amazon EBS adjuntos a su instancia Amazon EC2 de destino están cifrados con una clave AWS Key Management Service gestionada por el cliente AWS KMS(), asegúrese de que AWS KMS la clave `deleted` no lo esté `disabled` o la instancia no podrá iniciarse.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la instancia Linux Amazon EC2 que contiene la contraseña de usuario del sistema operativo que desea restablecer.
- LinuxUserNombre

  Tipo: cadena

  Predeterminado: ec2-user

  Descripción: (opcional) la cuenta de usuario del sistema operativo cuya contraseña desea restablecer.
- SecretArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN del secreto de Secrets Manager que contiene la nueva contraseña.
- SecurityGroupID

  Tipo: cadena

Descripción: (opcional) el ID del grupo de seguridad que se va a asociar a la instancia de Amazon EC2 temporal. Si no proporciona un valor para este parámetro, se usa el grupo de seguridad Amazon Virtual Private Cloud (Amazon VPC) predeterminado.

- SubnetId

  Tipo: cadena

  Descripción: (opcional) el ID de la subred en la que desea lanzar la instancia temporal de Amazon EC2. De forma predeterminada, la automatización elige la misma subred que la instancia de destino. Si elige proporcionar una subred diferente, debe estar en la misma zona de disponibilidad que la instancia de destino y tener acceso a los puntos de enlace de Systems Manager.

- CreateSnapshot

  Tipo: cadena

  Valores válidos: Yes | No

  Valor predeterminado: Yes

  Descripción: (opcional) determina si se crea una instantánea del volumen raíz de la instancia Amazon EC2 de destino antes de que se ejecute la automatización.

- StopConsent

  Tipo: cadena

  Valores válidos: Yes | No

  Valor predeterminado: No

  Descripción: introduzca **`Yes`** para confirmar que su instancia Amazon EC2 de destino se detendrá durante esta automatización. Cuando se detiene la instancia Amazon EC2, se pierden todos los datos almacenados en la memoria o en los volúmenes del almacén de instancias y se libera la dirección IPv4 pública automática. Para obtener más información, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon EC2.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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

Pasos de documentos

1. aws:branch: se ramifica en función de si ha dado su consentimiento para detener la instancia Amazon EC2 de destino.
2. aws:assertAwsResourceProperty garantiza que el estado de la instancia Amazon EC2 esté en estado running o stopped. De lo contrario, la automatización finaliza.
3. aws:executeAwsApi obtiene las propiedades de la instancia de Amazon EC2.
4. aws:executeAwsApi obtiene las propiedades del volumen raíz.
5. aws:branch ramifica la automatización en función de si se proporcionó un ID de subred para la instancia temporal de Amazon EC2.
6. aws:assertAwsResourceProperty garantiza que la subred que especifique en el parámetro SubnetId esté en la misma zona de disponibilidad que la instancia de Amazon EC2 de destino.
7. aws:assertAwsResourceProperty garantiza que el volumen raíz de la instancia de Amazon EC2 de destino es un volumen de Amazon EBS.
8. aws:assertAwsResourceProperty garantiza que la arquitectura de la instancia Amazon EC2 sea arm64 o x86_64.
9. aws:assertAwsResourceProperty garantiza que el comportamiento de cierre de la instancia de Amazon EC2 sea stop y no terminate.
10. aws:branch garantiza que la instancia de Amazon EC2 no sea una instancia de spot. De lo contrario, la automatización finaliza.
11. aws:executeScript garantiza que la instancia de Amazon EC2 no forme parte de un grupo de escalado automático. Si la instancia forma parte de un grupo de escalado automático, la automatización confirma que la instancia de Amazon EC2 se encuentra en un estado Standby de ciclo de vida.
12. aws:createStack crea una instancia Amazon EC2 temporal que se utiliza para restablecer la contraseña del usuario del sistema operativo que especifique.
13. aws:waitForAwsResourceProperty espera hasta que se ejecute la instancia temporal de Amazon EC2 recién lanzada.
14. aws:executeAwsApi obtiene el ID de la instancia de Amazon EC2 temporal.

15 `aws:waitForAwsResourceProperty` espera a que la instancia de Amazon EC2 muestre que la administra Systems Manager.

16 `aws:changeInstanceState` detiene la instancia de Amazon EC2 de destino.

17 `aws:changeInstanceState` obliga a la instancia Amazon EC2 de destino a detenerse en caso de que se quede atascada en un estado de parada.

18 `aws:branch` ramifica la automatización en función de si se solicitó una instantánea del volumen raíz de la instancia Amazon EC2 de destino.

19 `aws:executeAwsApi` crea una instantánea del volumen de Amazon EBS raíz de la instancia de Amazon EC2.

20 `aws:waitForAwsResourceProperty` espera a que la instantánea esté en un estado. `completed`

21 `aws:executeAwsApi` desconecta el volumen raíz de Amazon EBS antiguo de la instancia de Amazon EC2.

22 `aws:waitForAwsResourceProperty` espera a que el volumen raíz de Amazon EBS se separe de la instancia Amazon EC2 de destino.

23 `aws:executeAwsApi` adjunta el volumen raíz de Amazon EBS a la instancia temporal de Amazon EC2.

24 `aws:waitForAwsResourceProperty` espera a que el volumen raíz de Amazon EBS se adjunte a la instancia temporal de Amazon EC2.

25 `aws:runCommand` restablece la contraseña del usuario de destino mediante la ejecución de un script del intérprete de comandos mediante Run Command en la instancia temporal de Amazon EC2.

26 `aws:executeAwsApi` desconecta el volumen raíz de Amazon EBS antiguo de la instancia temporal de Amazon EC2.

27 `aws:waitForAwsResourceProperty` espera a que el volumen raíz de Amazon EBS se separe de la instancia temporal de Amazon EC2.

28 `aws:executeAwsApi` separa el volumen raíz de Amazon EBS de la instancia temporal de Amazon EC2 tras un error.

29 `aws:waitForAwsResourceProperty` espera a que el volumen raíz de Amazon EBS se separe de la instancia temporal de Amazon EC2 tras un error.

30 `aws:branch` ramifica la automatización en función de si se solicitó una instantánea del volumen raíz para determinar la ruta de recuperación en caso de error.

31. `aws:executeAwsApi` vuelve a conectar el volumen raíz de Amazon EBS a la instancia Amazon EC2 de destino.
32. `aws:waitForAwsResourceProperty` espera a que el volumen raíz de Amazon EBS se adjunte a la instancia de Amazon EC2.
33. `aws:executeAwsApi` crea un nuevo volumen de Amazon EBS a partir de la instantánea del volumen raíz de la instancia Amazon EC2 de destino.
34. `aws:waitForAwsResourceProperty` espera hasta que el nuevo volumen de Amazon EBS esté en estado `available`.
35. `aws:executeAwsApi` adjunta el nuevo volumen de Amazon EBS a la instancia de destino como volumen raíz.
36. `aws:waitForAwsResourceProperty` espera a que el volumen de Amazon EBS esté en estado `attached`.
37. `aws:executeAwsApi`Describe los eventos de la AWS CloudFormation pila si los runbooks no pueden crear o actualizar la AWS CloudFormation pila.
38. `aws:branch` ramifica la automatización en función del estado anterior de la instancia de Amazon EC2. Si el estado era `running`, se inicia la instancia. Si estaba en un estado `stopped`, la automatización continúa.
39. `aws:changeInstanceState` inicia la instancia de Amazon EC2 si es necesario.
40. `aws:waitForAwsResourceProperty`Espera a que la AWS CloudFormation pila esté en estado terminal antes de eliminarla.
41. `aws:executeAwsApi`Elimina la AWS CloudFormation pila, incluida la instancia temporal de Amazon EC2.

AWSPremiumSupport-ResizeNitroInstance

Descripción

El manual de procedimientos `AWSPremiumSupport-ResizeNitroInstance`proporciona una solución automatizada para cambiar el tamaño de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) creadas en el sistema Nitro.

Para reducir el riesgo potencial de pérdida de datos y tiempo de inactividad, el manual de procedimientos verifica lo siguiente:

- El comportamiento de detención de instancias.

- Si la instancia forma parte de un grupo de Amazon EC2 Auto Scaling y está en modo `standby`.
- El estado y tenencia de la instancia.
- El tipo de instancia al que quiere cambiar es compatible con la cantidad de interfaces de red actualmente conectadas a su instancia.
- La arquitectura del procesador y el tipo de virtualización tanto para el tipo de instancia actual como para el de destino son los mismos.
- Si la instancia está en ejecución, supera todas las comprobaciones de estado.
- El tipo de instancia que ha seleccionado está disponible en la msma zona de disponibilidad elegida.

Si Amazon EC2 no supera las comprobaciones de estado después de cambiar el tipo de instancia, el manual de procedimientos regresa automáticamente al tipo de instancia anterior.

De forma predeterminada, este manual de procedimientos no cambiará el tipo de instancia si está en ejecución y hay volúmenes de almacén de instancias adjuntos. El manual de procedimientos tampoco cambiará el tipo de instancia si la instancia forma parte de una pila AWS CloudFormation. Si quiere cambiar alguno de estos comportamientos, especifique `yes`para los parámetros `AllowInstanceStoreInstances`y `AllowCloudFormationInstances`.

El manual de procedimientos proporciona dos formas diferentes de especificar el tipo de instancia al que quiere cambiar:

- Para las automatizaciones simples dirigidas a una sola instancia, especifique el tipo de instancia al que quiere cambiar mediante el parámetro `TargetInstanceTypeFromParameter`.
- Para ejecutar automatizaciones a escala y cambiar el tipo de instancia de varias instancias, especifique el tipo de instancia mediante el parámetro `TargetInstanceTypeFromTagValue`. Para obtener información sobre la ejecución de automatizaciones a escala, consulte Ejecutar automatizaciones a escala.

Si no especifica un valor para ninguno de los parámetros, la automatización falla.

> **Important**
>
> El acceso a los manuales de procedimientos de `AWSPremiumSupport-*` requiere una suscripción Enterprise o Business Support. Para obtener más información, consulte Comparar AWS Supportplanes.

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos.
- Para obtener información sobre la compatibilidad para cambiar los tipos de instancia, consulte Compatibilidad para cambiar el tipo de instancia.
- Si la automatización falla y regresa al tipo de instancia original, consulte Cómo solucionar problemas al cambiar el tipo de instancia.
- Para cambiar el tipo de instancia, es necesario que el manual de procedimientos detenga su instancia. Los datos guardados en la memoria o en el almacén de instancias se perderán cuando se detenga una instancia. Además, se libera cualquier dirección IPv4 pública asignada automáticamente. Para obtener información sobre lo que ocurre cuando detiene una instancia, consulte Detener y terminar una instancia.
- Con el parámetro `SkipInstancesWithTagKey`, puede omitir las instancias a las que se haya aplicado una clave de etiqueta específica de Amazon EC2.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- Acknowledge

  Tipo: String

  Descripción: (Obligatorio) Introduzca **`yes`**para confirmar que su instancia se detendrá si se está ejecutando actualmente.

- AllowInstanceStoreInstances

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si especifica `yes`, permite que el manual de procedimientos se ejecute en instancias que tengan volúmenes de almacén de instancias adjuntos.

- AllowCloudFormationInstances

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si especifica `yes`, el manual de procedimientos se ejecuta en instancias que forman parte de una pila AWS CloudFormation.

- DryRun

  Tipo: String

  Valores válidos: no | yes

  Valor predeterminado: no

  Descripción: (Opcional) Si especifica `yes`, el manual de procedimientos valida los requisitos de cambio de tamaño sin realizar cambios en el tipo de instancia.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia Amazon EC2 de la que quiera cambiar el tipo.

- SkipInstancesWithTagKey

  Tipo: String

  Descripción: (Opcional) La automatización omite una instancia de destino si la clave de etiqueta que especifique se aplica a la instancia.

- SleepTime

  Tipo: String

  Predeterminado: 3

  Descripción: (Opcional) El número de segundos que debe permanecer inactivo este manual de procedimientos una vez finalizado.

- TagInstance

  Tipo: String

  Descripción: (Opcional) Etiquete las instancias con la clave y el valor que prefiera con el siguiente formato: *`Key=ChangingType,Value=True`*. Esta opción le permite realizar un seguimiento de las instancias a las que se ha dirigido este manual de procedimientos. Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.

- TargetInstanceTypeFromParameter

  Tipo: String

  Descripción: (Opcional) El tipo de instancia al que quiere cambiar su instancia. Deje este parámetro en blanco si quiere usar el valor de la clave de etiqueta proporcionada en el parámetro `TargetInstanceTypeFromTagValue`.

- TargetInstanceTypeFromTagValue

  Tipo: String

  Descripción: (Opcional) La clave de etiqueta que se aplica a las instancias de destino cuyo valor contiene el tipo de instancia al que desea cambiar. Si no especifica un valor para el `TargetInstanceTypeFromParameter`parámetro, anula cualquier valor que especifique para el parámetro .

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: Garantiza que la instancia de Amazon EC2 no esté etiquetada con la clave de etiqueta de recurso especificada en el parámetro `SkipInstancesWithTagKey`. Si se encuentra la clave de etiqueta aplicada a la instancia, se produce un error en el paso y finaliza la automatización.
2. `aws:assertAwsResourceProperty`: Confirma que el estado de la instancia de Amazon EC2 de destino es `running`, `pending`, `stopped` o `stopping`. De lo contrario, la automatización finaliza.
3. `aws:executeAwsApi`: Recopila las propiedades de la instancia de Amazon EC2.
4. `aws:executeAwsApi`: Recopila detalles sobre el tipo de instancia de Amazon EC2 actual.
5. `aws:branch`: Comprueba si el tipo de instancia actual y el tipo de instancia especificado en el parámetro `TargetInstanceTypeFromParameter`son iguales. Si lo son, la automatización finaliza.
6. `aws:assertAwsResourceProperty`: Garantiza que la instancia se ejecute en el sistema Nitro.

7. `aws:branch`: Garantiza que el tipo de volumen raíz de la instancia de Amazon EC2 sea un volumen de Amazon Elastic Block Store (Amazon EBS).
8. `aws:assertAwsResourceProperty`: Confirma que el comportamiento de cierre de la instancia sea `stop`y no `terminate`.
9. `aws:branch`: Garantiza que la instancia de Amazon EC2 no sea una instancia de spot.
10. `aws:branch`: Garantiza que la tenencia de la instancia de Amazon EC2 sea la predeterminada y no el host dedicado o la instancia dedicada.
11. `aws:executeScript`: Confirma que solo hay una automatización de este manual de procedimientos dirigida al ID de la instancia actual. Si ya hay otra automatización en curso dirigida a la misma instancia, la automatización regresa un error y finaliza.
12. `aws:branch`: Ramifica la automatización en función del estado de la instancia de Amazon EC2.
    a. En caso de `stopped`o `stopping`, la automatización se ejecuta `aws:waitForAwsResourceProperty`hasta que la instancia de Amazon EC2 se detenga por completo.
    b. En caso de `running`o `pending`, la automatización se ejecuta `aws:waitForAwsResourceProperty`hasta que la instancia de Amazon EC2 supere las comprobaciones de estado.
13. `aws:assertAwsResourceProperty`: Confirma que la instancia de Amazon EC2 no forma parte de un grupo de escalado automático mediante una llamada a la operación de `DescribeAutoScalingInstances`API. Si la instancia forma parte de un grupo de escalado automático, asegúrese de que la instancia de Amazon EC2 esté en modo `standby`.
14. `aws:branch`: Ramifica la automatización en función de si desea que la automatización compruebe si la instancia de Amazon EC2 forma parte de una pila AWS CloudFormation:
    a. `aws:executeScript` Garantiza que la instancia de Amazon EC2 no forme parte de una pila AWS CloudFormationmediante una llamada a la operación de `DescribeStackResources`API.
15. `aws:executeAwsApi`: Regresa una lista de tipos de instancias con el mismo tipo de arquitectura de procesador y tipo de virtualización y que admite el número de interfaces de red actualmente conectadas a la instancia de destino.
16. `aws:executeAwsApi`: Obtiene el valor del tipo de instancia de destino a partir de la clave de etiqueta especificada en el parámetro `TargetInstanceTypeFromTagValue`.
17. `aws:executeScript`: Confirma que los tipos de instancia actual y de destino son compatibles. Garantiza que el tipo de instancia de destino esté disponible en la misma subred. Comprueba que

la entidad principal que inició el manual de procedimientos tiene permisos para cambiar el tipo de instancia y detener e iniciar la instancia si se estaba ejecutando.

18. `aws:branch`: Ramifica la automatización en función de si el valor del parámetro `DryRun`está establecido en `yes`. Si `yes`, la automatización finaliza.
19. `aws:branch`: Comprueba si el tipo de instancia original y el de destino son iguales. Si son iguales, la automatización finaliza.
20. `aws:executeAwsApi`: Obtiene el estado actual de la instancia.
21. `aws:changeInstanceState`: Crea la instancia de Amazon EC2.
22. `aws:changeInstanceState`: Obliga a la instancia a detenerse si está atascada en el estado `stopping`.
23. `aws:executeAwsApi`: Cambia el tipo de instancia por el tipo de instancia de destino.
24. `aws:sleep`: Espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
25. `aws:branch`: Ramifica la automatización en función del estado de la instancia anterior. Si se estaba `running`, se inicia la instancia.
    a. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
    b. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado. Si la instancia no supera las comprobaciones de estado, la instancia cambia de regreso a su tipo de instancia original.
        i. `aws:changeInstanceState`: Detiene la instancia de Amazon EC2 antes de cambiarla a su tipo de instancia original.
        ii. `aws:changeInstanceState`: Obliga a la instancia de Amazon EC2 a detenerse antes de cambiarla a su tipo de instancia original en caso de que se quede atascada en un estado de parada.
        iii. `aws:executeAwsApi`: Cambia la instancia de Amazon EC2 a su tipo original.
        iv. `aws:sleep`: Espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
        v. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
        vi. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado.
26. `aws:sleep`: Espera antes de finalizar el manual de procedimientos.

AWSSupport-RestoreEC2InstanceFromSnapshot

Descripción

El manual de procedimientos `AWSSupport-RestoreEC2InstanceFromSnapshot`le ayuda a identificar y restaurar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a partir de una instantánea en funcionamiento de Amazon Elastic Block Store (Amazon EBS) del volumen raíz.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- EndDate

  Tipo: String

  Descripción: (Opcional) La última fecha en la que quiere que la automatización busque una instantánea.
- InplaceSwap

  Tipo: booleano

  Valores válidos: true | false

Descripción: (Opcional) Si el valor de este parámetro se establece en `true`, el volumen recién creado a partir de la instantánea sustituirá al volumen raíz existente adjunto a su instancia.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) el ID de la instancia de base de datos de que desea restaurar de una instantánea.

- LookForInstanceStatusCheck

  Tipo: booleano

  Valores válidos: true | false

  Valor predeterminado: true

  Descripción: (Opcional) Si el valor de este parámetro se establece en `true`, la automatización comprueba si las comprobaciones de estado de las instancias fallan en las instancias de prueba lanzadas desde las instantáneas.

- SkipSnapshotsBy

  Tipo: String

  Descripción: (Opcional) El intervalo en el que se omiten las instantáneas al buscar instantáneas para restaurar su instancia. Por ejemplo, si hay 100 instantáneas disponibles y especifica un valor de 2 para este parámetro, se revisará una de cada tres instantáneas.

  Predeterminado: 0

- SnapshotId

  Tipo: String

  Descripción: (Opcional) El ID de la instantánea desde la que quiere restaurar la instancia.

- StartDate

  Tipo: String

  Descripción: (Opcional) La primera fecha en la que quiere que la automatización busque una instantánea.

- TotalSnapshotsToLook

  Tipo: String

  Descripción: (Opcional) El número de instantáneas que revisa la automatización.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:executeAwsApi` - Recopila detalles sobre la instancia de destino.
2. `aws:assertAwsResourceProperty` - Verifica la existencia de la instancia de destino.
3. `aws:assertAwsResourceProperty` - Verifica que el volumen raíz sea un volumen de Amazon EBS.
4. `aws:assertAwsResourceProperty` - Verifica que no se esté ejecutando otra automatización dirigida a esta instancia.
5. `aws:executeAwsApi` - Etiqueta la instancia de destino.
6. `aws:executeAwsApi` - Crea una AMIde la instancia de la clase.
7. `aws:executeAwsApi` - Recopila detalles sobre la AMIcreada en el paso anterior.
8. `aws:waitForAwsResourceProperty` - Espera a que el estado AMIse convierta en `available`antes de continuar.
9. `aws:executeScript` - Lanza una nueva instancia a partir de la AMIrecién creada.
10. `aws:assertAwsResourceProperty` - Comprueba que el estado de la instancia sea `available`.
11. `aws:executeAwsApi` - Recopila detalles sobre la instancia recién lanzada.
12. `aws:branch` - Se ramifica en función de si ha proporcionado un valor para el parámetro `SnapshotId`.
13. `aws:executeScript` - Regresa una lista de instantáneas dentro del período de tiempo especificado.
14. `aws:executeAwsApi` - Detiene la instancia.
15. `aws:waitForAwsResourceProperty` - Espera a que el estado del volumen sea `available`.
16. `aws:waitForAwsResourceProperty` - Espera a que el estado de la instancia sea `stopped`.
17. `aws:executeAwsApi` - Separe el volumen raíz.
18. `aws:waitForAwsResourceProperty` - Espera a que se separe el volumen raíz.
19. `aws:executeAwsApi` - Fija el nuevo volumen raíz.
20. `aws:waitForAwsResourceProperty` - Espera a que se adjunte el nuevo volumen.
21. `aws:executeAwsApi` - Inicie la instancia.
22. `aws:waitForAwsResourceProperty` - Espera a que el estado de la instancia sea `available`.
23. `aws:waitForAwsResourceProperty` - Espera a que las comprobaciones de estado del sistema y de la instancia sean superadas por la instancia.
24. `aws:executeScript` - Ejecuta un script para encontrar una instantánea que pueda usarse para crear correctamente un volumen.

25. `aws:executeScript` - Ejecuta un script para recuperar la instancia utilizando el volumen recién creado a partir de la instantánea identificada por la automatización, o utilizando el volumen creado a partir de la instantánea que especificó en el parámetro `SnapshotId`.
26. `aws:executeScript` - Elimina los recursos creados por la automatización.

Salidas

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

Descripción

El manual de procedimientos `AWSSupport-SendLogBundleToS3Bucket`carga un paquete de registro generado por la herramienta EC2Rescue desde la instancia de destino al bucket de S3 especificado. El manual de procedimientos instala la versión específica de la plataforma de EC2Rescue en función de la plataforma de la instancia de destino. EC2Rescue se utiliza para recopilar todos los registros disponibles del sistema operativo (SO).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia administrada de Windows o Linux de la que desea recopilar los registros.

- S3BucketName

  Tipo: String

  Descripción: (Obligatorio) bucket de S3 en el que cargar los registros.

- S3Path

  Tipo: String

  Valor predeterminado: `AWSSupport-SendLogBundleToS3Bucket/`

  Descripción: (Opcional) ruta de S3 para los registros recopilados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la instancia EC2 que recibe el comando tenga un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. El usuario debe tener al menos ssm:StartAutomationExecution y ssm:SendCommand para ejecutar Automation y enviar el comando a la instancia, así como ssm:GetAutomationExecution para poder leer la salida de Automation.

Pasos de documentos

1. `aws:runCommand` - Instalar EC2Rescue mediante `AWS-ConfigureAWSPackage`.
2. `aws:runCommand` - Ejecute el script de PowerShell para recopilar los registros de solución de problemas de Windows con EC2Rescue.
3. `aws:runCommand` - Ejecute el script bash para recopilar los registros de solución de problemas de Linux con EC2Rescue.

Salidas

collectAndUploadWindowsLogBundle.Output

collectAndUploadLinuxLogBundle.Output

`AWSSupport-StartEC2RescueWorkflow`

Descripción

El manual de procedimientos `AWSSupport-StartEC2RescueWorkflow`ejecuta el script codificado en base64 (Bash o PowerShell) en una instancia auxiliar creada para rescatar la instancia. El volumen raíz de la instancia se asocia a la instancia auxiliar y se monta, también conocida como instancia EC2Rescue. Si la instancia es Windows, proporcione un script de PowerShell. De lo contrario, utilice Bash. El flujo de trabajo establece algunas variables de entorno que se puede utilizar en su script. Las variables de entorno contienen información sobre la entrada que ha facilitado, así como información sobre el volumen raíz sin conexión. El volumen sin conexión ya está montado y listo para su uso. Por ejemplo, puede guardar un archivo de configuración de estado deseado en un volumen raíz de Windows sin conexión o usar chroot en un volumen raíz de Linux sin conexión y realizar una corrección sin conexión.

Ejecuta esta automatización (consola)

> **Important**
>
> Las instancias Amazon EC2 creadas a partir de imágenes de Amazon Machine (AMI) no son compatibles con esta automatización.

Información adicional

Para codificar un script en base64, puede utilizar PowerShell o Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::Rea
```

Bash:

```
base64 PATH_TO_FILE
```

A continuación se muestra una lista de variables de entorno puede utilizar en sus scripts sin conexión, en función del sistema operativo de destino.

Windows:

Variable	Descripción	Ejemplo de valor
$env:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
$env:EC2RESCUE_DATE	{{ global:DATE }}	07/09/2018
$env:EC2RESCUE_DATE_TIME	*{{ global:DATE_TIME }}	2018-09-07_18.09.59
$env:EC2RESCUE_EC2RW_DIR	Ruta de instalación de EC2Rescue para Windows	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EC2RW_DIR	Ruta de instalación de EC2Rescue para Windows	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	Ruta del conjunto de control actual de Windows sin conexión	`HKLM:\AWSTempSystem\ControlSet001`
$env:EC2RESCUE_OFFLINE_DRIVE	Letra de unidad de Windows sin conexión	D:\
$env:EC2RESCUE_OFFLINE_EBS_DEVICE	Dispositivo de EBS de volumen raíz sin conexión	xvdf

Variable	Descripción	Ejemplo de valor
$env:EC2RESCUE_OFFLINE_KERNEL_VER	Versión del kernel de Windows sin conexión	6.1.7601.24214
$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	Arquitectura de Windows sin conexión	AMD64
$env:EC2RESCUE_OFFLINE_OS_CAPTION	Título de Windows sin conexión	Windows Server 2008 R2 Datacenter
$env:EC2RESCUE_OFFLINE_OS_TYPE	Tipo del sistema operativo Windows sin conexión	Servidor
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	Ruta del directorio Program Files de Windows sin conexión	D:\Program Files
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	Ruta del directorio Program Files x86 de Windows sin conexión	D:\Program Files (x86)
$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	Ruta del directorio del Registro de Windows sin conexión	D:\Windows\System32\config
$ env: EC2RESCUE_OFFLINE_SYSTEM_ROOT	Ruta del directorio raíz del sistema de Windows sin conexión	D:\Windows
$ env: EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket
$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Variable	Descripción	Ejemplo de valor
$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	Metadatos de la instalación de Windows sin conexión	Objeto de Powershell del cliente

Linux:

Variable	Descripción	Ejemplo de valor
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	07/09/2018
EC2RESCUE_DATE_TIME	*{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	Ruta de instalación de EC2Rescue para Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	Nombre del dispositivo sin conexión	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	Dispositivo de EBS de volumen raíz sin conexión	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Punto de montaje del volumen raíz sin conexión	/mnt/mount
EC2RESCUE_PYTHON	Versión de Python	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/

Variable	Descripción	Ejemplo de valor
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AMIPrefix

  Tipo: String

  Valor predeterminado: `AWSSupport-EC2Rescue`

  Descripción: (Opcional) prefijo para el nombre de la AMI de copia de seguridad.
- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- CreatePostEC2RescueBackup

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

Descripción: (Opcional) establezca el valor en `true`para crear una AMI de InstanceId después de ejecutar el script (antes de iniciarlo). La AMI se conservará una vez terminada la Automation. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- CreatePreEC2RescueBackup

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) establezca el valor en `true`para crear una AMI de InstanceId antes de ejecutar el script. La AMI se conservará una vez terminada la Automation. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- EC2RescueInstanceType

  Tipo: String

  Valores permitidos: t2.small | t2.medium | t2.large

  Valor predeterminado: t2.small

  Descripción: (Opcional) tipo de instancia EC2 para la instancia EC2Rescue.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia EC2. IMPORTANTE: AWS Systems ManagerAutomation detiene esta instancia. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- OfflineScript

  Tipo: String

  Descripción: (Obligatorio) el script con codificación base64 que se ejecuta en la instancia auxiliar. Utilice Bash si la instancia de origen es Linux y PowerShell si se trata de Windows.

- S3BucketName

Tipo: String

Descripción: (Opcional) nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- S3Prefix

  Tipo: String

  Valor predeterminado: `AWSSupport-EC2Rescue`

  Descripción: (Opcional) prefijo para los registros de S3.

- SubnetId

  Tipo: String

  Valor predeterminado: SelectedInstanceSubnet

  Descripción: (Opcional) el ID de subred para la instancia EC2Rescue. De forma predeterminada, se utiliza la misma subred en la que reside instancia proporcionada. IMPORTANTE: Si proporciona una subred personalizada, debe estar en la misma zona de disponibilidad que InstanceId y debe permitir el acceso a puntos de enlace de SSM.

- UniqueId

  Tipo: String

  Valor predeterminado: {{ automation:EXECUTION_ID }}

  Descripción: (Opcional) un identificador único para la automatización.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Es recomendable que el usuario que ejecuta Automation tenga asociada la política administrada de IAM AmazonSSMAutomationRole. Además de dicha política, el usuario debe tener:

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

Pasos de documentos

1. `aws:executeAwsApi` - Describir la instancia proporcionada
2. `aws:executeAwsApi` - Describir el volumen raíz de la instancia proporcionada.
3. `aws:assertAwsResourceProperty` - Comprobar que el tipo de dispositivo del volumen raíz sea EBS
4. `aws:assertAwsResourceProperty` - Comprobar que el volumen raíz no esté cifrado
5. `aws:assertAwsResourceProperty` - Comprobar el ID de subred proporcionado
   a. (Utilice subred de instancia actual): si *SubnetId = SelectedInstanceSubnet*, entonces ejecute `aws:createStack`para implementar la pila CloudFormation de EC2Rescue.

b. (Crear nueva VPC): Si *SubnetId = CreateNewVPC*, entonces ejecute `aws:createStack`para implementar la pila CloudFormation de EC2Rescue.

c. (Usar subred personalizada): en el resto de casos:

`aws:assertAwsResourceProperty` - Comprobar que la subred proporcionada está en la misma zona de disponibilidad que la instancia proporcionada.

`aws:createStack` - Implementar la pila CloudFormation de EC2Rescue.

6. `aws:invokeLambdaFunction` - Realizar una validación de entrada adicional
7. `aws:executeAwsApi` - Actualizar la pila CloudFormation de EC2Rescue para crear la instancia auxiliar de EC2Rescue.
8. `aws:waitForAwsResourceProperty` - Esperar a que se complete la actualización de la pila CloudFormation de EC2Rescue.
9. `aws:executeAwsApi` - Describir la salida de la pila CloudFormation de EC2Rescue para obtener el ID de la instancia auxiliar de EC2Rescue.
10. `aws:waitForAwsResourceProperty` - Esperar a que la instancia auxiliar de EC2Rescue se convierta en una instancia administrada.
11. `aws:changeInstanceState` - Detener la instancia proporcionada
12. `aws:changeInstanceState` - Detener la instancia proporcionada
13. `aws:changeInstanceState` - Forzar la detención de la instancia proporcionada
14. `aws:assertAwsResourceProperty` - Comprobar el valor de entrada CreatePreEC2RescueBackup
    a. (Crear una copia de seguridad previa a EC2Rescue): si *CreatePreEC2RescueBackup = true*
    b. `aws:executeAwsApi` - Crear una copia de seguridad de AMI de la instancia proporcionada.
    c. `aws:createTags` - Etiquetar la copia de seguridad de la AMI
15. `aws:runCommand` - Instalar EC2Rescue en la instancia auxiliar de EC2Rescue.
16. `aws:executeAwsApi` - Desconectar el volumen raíz de la instancia
17. `aws:assertAwsResourceProperty` - Comprobar la plataforma de instancia proporcionada
    a. (La instancia es Windows):

    `aws:executeAwsApi` - Asociar el volumen raíz a la instancia auxiliar EC2Rescue como *xvdf*.

    `aws:sleep` - En espera 10 segundos

`aws:runCommand` - Ejecutar el script sin conexión proporcionado en PowerShell.

b. (Instancia es Linux):

`aws:executeAwsApi` - Asociar el volumen raíz a la instancia auxiliar EC2Rescue como */dev/sdf*.

`aws:sleep` - En espera 10 segundos

`aws:runCommand` - Ejecutar el script sin conexión proporcionado en Bash.

18. `aws:changeInstanceState` - Detener la instancia auxiliar de EC2Rescue
19. `aws:changeInstanceState` - Forzar la detención de la instancia auxiliar de EC2Rescue
20. `aws:executeAwsApi` - Desconectar el volumen raíz de la instancia auxiliar EC2Rescue.
21. `aws:executeAwsApi` - Volver a asociar el volumen raíz a la instancia proporcionada.
22. `aws:assertAwsResourceProperty` - Comprobar el valor de entrada CreatePostEC2RescueBackup
    a. (Crear una copia de seguridad después de EC2Rescue): si *CreatePostEC2RescueBackup = true*
    b. `aws:executeAwsApi` - Crear una copia de seguridad de AMI de la instancia proporcionada.
    c. `aws:createTags` - Etiquetar la copia de seguridad de la AMI
23. `aws:executeAwsApi` - Restaurar la eliminación inicial en estado de terminación para el volumen raíz de la instancia proporcionada.
24. `aws:changeInstanceState` - Restaurar el estado inicial de la instancia proporcionada (en ejecución/detenida).
25. `aws:deleteStack` - Eliminar la pila CloudFormation de EC2Rescue.

Salidas

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descripción

El manual de procedimientos AWSPremiumSupport-TroubleshootEC2DiskUsagele ayuda a investigar y, si es posible, solucionar problemas relacionados con el uso de discos raíz y no raíz de instancias de Amazon Elastic Compute Cloud (Amazon EC2). Si es posible, el manual de procedimientos intenta solucionar los problemas ampliando el volumen y su sistema de archivos. Para realizar estas tareas, este manual de procedimientos orquesta la ejecución de varios manuales de procedimientos en función del sistema operativo de la instancia afectada.

El primer manual de procedimientos, AWSPremiumSupport-DiagnoseDiskUsageOnWindowso AWSPremiumSupport-DiagnoseDiskUsageOnLinux, determina si los problemas del disco se pueden mitigar expandiendo el volumen.

El segundo manual de procedimientos, AWSPremiumSupport-ExtendVolumesOnWindowsoAWSPremiumSupport-ExtendVolumesOnLinux, utiliza la salida del primer manual de procedimientos para ejecutar el código de Python que modifica el volumen. Una vez modificado el volumen, el manual de procedimientos amplía la partición y el sistema de archivos de los volúmenes afectados.

> **Important**
>
> El acceso a los manuales de procedimientos de AWSPremiumSupport-* requiere una suscripción a Enterprise o Business Support. Para obtener más información, consulte Comparar AWS Supportplanes.

Este documento se creó en colaboración con AWS Managed Services(AMS). AMS le ayuda a gestionar su infraestructura AWSde forma más eficiente y segura. AMS también proporciona flexibilidad operativa, seguridad y cumplimiento mejorados, optimización de la capacidad e identificación del ahorro de costos. Para obtener más información, consulte AWS Managed Services.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- InstanceId

  Tipo: String

  Valores permitidos: ^i-[a-z0-9]{8,17}$

  Descripción: (Obligatorio) ID de la instancia Amazon EC2.
- VolumeExpansionEnabled

  Tipo: booleano

  Descripción: (Opcional) Indicador para controlar si el documento ampliará los volúmenes y las particiones afectados.

  Valor predeterminado: true
- VolumeExpansionUsageTrigger

  Tipo: String

  Descripción: (Opcional) Uso mínimo del espacio de partición necesario para activar la extensión (en porcentaje).

  Valores permitidos: ^[0-9]{1,2}$

  Predeterminado: 85
- VolumeExpansionCapSize

  Tipo: String

  Descripción: (Opcional) El volumen máximo de Amazon Elastic Block Store (Amazon EBS) se incrementará a (en GiB).

  Valores permitidos: ^[0-9]{1,4}$

Predeterminado: 2048

- VolumeExpansionGibIncrease

  Tipo: String

  Descripción: (Opcional) Aumento en GiB del volumen. Se utilizará el mayor aumento neto entre VolumeExpansionGibIncrease y VolumeExpansionPercentageIncrease.

  Valores permitidos: ^[0-9]{1,4}$

  Valor predeterminado: 20
- VolumeExpansionPercentageIncrease

  Tipo: String

  Descripción: (Opcional) Aumento en el porcentaje del volumen. Se utilizará el mayor aumento neto entre VolumeExpansionGibIncrease y VolumeExpansionPercentageIncrease.

  Valores permitidos: ^[0-9]{1,2}$

  Valor predeterminado: 20
- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

1. aws:assertAwsResourceProperty - Comprueba si la instancia está gestionada por Systems Manager
2. aws:executeAwsApi - Describe la instancia para obtener la plataforma.
3. aws:branch - Ramifica la automatización en función de la plataforma de la instancia.
   a. Si la instancia es Windows:
      i. aws:executeAutomation - Ejecuta el manual de procedimientos AWSPremiumSupport-DiagnoseDiskUsageOnWindowspara diagnosticar los problemas de uso del disco en la instancia.
      ii. aws:executeAwsApi - Obtiene el resultado de la automatización anterior.
      iii. aws:branch - Se ramifica en función del resultado de los diagnósticos y de si hay volúmenes que se puedan ampliar para mitigar la alerta.

      A. No hay volúmenes que deban ampliarse: Finalizar la automatización.

      B. Hay volúmenes que deben ampliarse:

         I. aws:executeAwsApi - Crea una Amazon Machine Image(AMI) de la instancia.

II. `aws:waitForAwsResourceProperty` - Espera a que el estado de AMIsea `available`.

III. `aws:executeAutomation` - Ejecuta el manual de procedimientos `AWSPremiumSupport-ExtendVolumesOnWindows`para realizar la modificación del volumen y también los pasos necesarios en el sistema operativo (SO) para disponer del nuevo espacio.

b. (La plataforma no es Windows) Si la instancia de entrada no es Windows:

i. `aws:executeAutomation` - Ejecuta el manual de procedimientos `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`para diagnosticar los problemas de uso del disco en la instancia.

ii. `aws:executeAwsApi` - Obtiene el resultado de la automatización anterior.

iii. `aws:branch` - Se ramifica en función del resultado de los diagnósticos y de si hay volúmenes que se puedan ampliar para mitigar la alerta.

A. No hay volúmenes que deban ampliarse: Finalizar la automatización.

B. Hay volúmenes que deben ampliarse:

I. `aws:executeAwsApi` - Cree una AMIde la instancia.

II. `aws:waitForAwsResourceProperty` - Espera a que el estado de AMIsea `available`.

III. `aws:executeAutomation` - Ejecuta el manual de procedimientos `AWSPremiumSupport-ExtendVolumesOnLinux`para realizar la modificación del volumen y también los pasos necesarios en el sistema operativo para disponer del nuevo espacio.

Salidas

diagnoseDiskUsageAlertOnWindows.Output

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Output

extendVolumesOnLinux.Output

BackupAMILinux.ImageId

BackupAMIWindows.ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Descripción

`AWSSupport-TroubleshootEC2InstanceConnect`la automatización ayuda a analizar y detectar los errores que impiden la conexión a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante Amazon EC2 Instance Connect. Identifica los problemas causados por una imagen de máquina de Amazon (AMI) no compatible, la falta de instalación o configuración del paquete a nivel del sistema operativo, la falta de permisos AWS Identity and Access Management (IAM) o problemas de configuración de la red.

¿Cómo funciona?

El runbook incluye el ID de instancia de Amazon EC2, el nombre de usuario, el modo de conexión, el CIDR de IP de origen, el puerto SSH y el nombre de recurso de Amazon (ARN) del rol o usuario de IAM que tenga problemas con Amazon EC2 Instance Connect. A continuación, comprueba los requisitos previos para conectarse a una instancia de Amazon EC2 mediante Amazon EC2 Instance Connect:

- La instancia está en ejecución y en buen estado.
- La instancia está ubicada en una AWS región compatible con Amazon EC2 Instance Connect.
- Amazon EC2 Instance Connect admite la AMI de la instancia.
- La instancia puede acceder al servicio de metadatos de instancias (IMDSv2).
- El paquete Amazon EC2 Instance Connect está correctamente instalado y configurado a nivel del sistema operativo.
- La configuración de red (grupos de seguridad, ACL de red y reglas de tabla de enrutamiento) permite la conexión a la instancia a través de Amazon EC2 Instance Connect.
- El rol o usuario de IAM que se utiliza para aprovechar Amazon EC2 Instance Connect tiene acceso a las teclas push de la instancia de Amazon EC2.

> **Important**
>
> - Para comprobar la AMI de la instancia, la accesibilidad de IMDSv2 y la instalación del paquete Instance Connect de Amazon EC2, la instancia debe estar gestionada por SSM. De lo contrario, omite esos pasos. Para obtener más información, consulte ¿Por qué mi instancia de Amazon EC2 no se muestra como un nodo gestionado?

- La comprobación de red solo detectará si el grupo de seguridad y las reglas de ACL de la red bloquean el tráfico cuando se proporciona el SourceIp CIDR como parámetro de entrada. De lo contrario, solo mostrará las reglas relacionadas con SSH.
- Las conexiones que utilizan Amazon EC2 Instance Connect Endpoint no se validan en este manual de ejecución.
- En el caso de las conexiones privadas, la automatización no comprueba si el cliente SSH está instalado en la máquina de origen ni si puede acceder a la dirección IP privada de la instancia.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`

- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-TroubleshootEC2InstanceConnect` la AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - InstanceId (Obligatorio):

     El ID de la instancia de Amazon EC2 de destino a la que no se pudo conectar mediante Amazon EC2 Instance Connect.
   - AutomationAssumeRole (Opcional):

     El ARN de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
   - Nombre de usuario (obligatorio):

     El nombre de usuario utilizado para conectarse a la instancia de Amazon EC2 mediante Amazon EC2 Instance Connect. Se utiliza para evaluar si se concede el acceso de IAM a este usuario en particular.
   - EC2 InstanceConnectRoleOrUser (obligatorio):

     El ARN del rol o usuario de IAM que utiliza Amazon EC2 Instance Connect para introducir las teclas de la instancia.
   - SSHport (opcional):

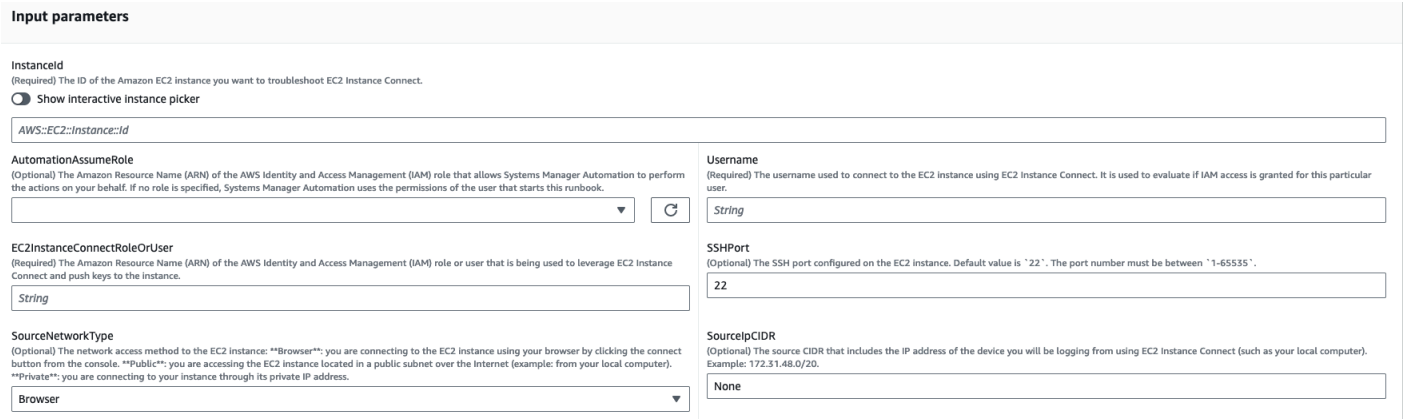
     El puerto SSH configurado en la instancia de Amazon EC2. El valor predeterminado es 22. El número de puerto debe estar intermedio. `1-65535`
   - SourceNetworkType (Opcional):

     El método de acceso de red a la instancia de Amazon EC2:
     - Navegador: se conecta desde la consola AWS de administración.

- Pública: se conecta a la instancia ubicada en una subred pública a través de Internet (por ejemplo, su ordenador local).
- Privado: te conectas a través de la dirección IP privada de la instancia.

- SourceIpCIDR (opcional):

  El CIDR de origen que incluye la dirección IP del dispositivo (por ejemplo, su ordenador local) desde el que iniciará sesión mediante Amazon EC2 Instance Connect. Ejemplo: 172.31.48.6/32. Si no se proporciona ningún valor con el modo de acceso público o privado, el runbook no evaluará si el grupo de seguridad de la instancia Amazon EC2 y las reglas de ACL de la red permiten el tráfico SSH. En su lugar, mostrará las reglas relacionadas con SSH.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:

   - AssertInitialState:

     Garantiza que el estado de la instancia de Amazon EC2 se esté ejecutando. De lo contrario, la automatización finaliza.

   - GetInstanceProperties:

     Obtiene las propiedades actuales de la instancia Amazon EC2 (PlatformDetails, PublicIpAddress VpcId, SubnetId y MetadataHttpEndpoint).

   - GatherInstanceInformationFromSSM:

     Obtiene el estado de ping de la instancia de Systems Manager y los detalles del sistema operativo si la instancia está gestionada por SSM.

   - CheckIfAWSRegionSupported:

Comprueba si la instancia de Amazon EC2 se encuentra en una región compatible con Amazon EC2 Instance ConnectAWS.

- BranchOnIfAWSRegionSupported:

  Continúa la ejecución si Amazon EC2 Instance Connect admite la AWS región. De lo contrario, crea la salida y sale de la automatización.

- CheckIfInstanceAMIIsSupported:

  Comprueba si la AMI asociada a la instancia es compatible con Amazon EC2 Instance Connect.

- BranchOnIfInstanceAMIIsSupported:

  Si la AMI de la instancia es compatible, realiza las comprobaciones a nivel del sistema operativo, como la accesibilidad de los metadatos y la instalación y configuración del paquete Amazon EC2 Instance Connect. De lo contrario, comprueba si los metadatos HTTP están habilitados mediante la AWS API y, a continuación, pasa al paso de comprobación de la red.

- Compruebe IMDSReachabilityFromOs:

  Ejecuta un script Bash en la instancia Linux Amazon EC2 de destino para comprobar si es capaz de acceder al IMDSv2.

- Compruebe IC: PackageInstallation

  Ejecuta un script Bash en la instancia de Amazon EC2 Linux de destino para comprobar si el paquete Amazon EC2 Instance Connect está correctamente instalado y configurado.

- Compruebe SSH: ConfigFromOs

  Ejecuta un script Bash en la instancia Linux Amazon EC2 de destino para comprobar si el puerto SSH configurado coincide con el parámetro de entrada `SSHport. `

- CheckMetadataHTTPEndpointIsEnabled:

  Comprueba si el punto final HTTP del servicio de metadatos de la instancia está habilitado.

- Compruebe la ID: NetworkAccess

  Comprueba si la configuración de la red (grupos de seguridad, ACL de red y reglas de la tabla de enrutamiento) permite la conexión a la instancia a través de Amazon EC2 Instance Connect.

- Compruebe IAMRoleOrUserPermissions:

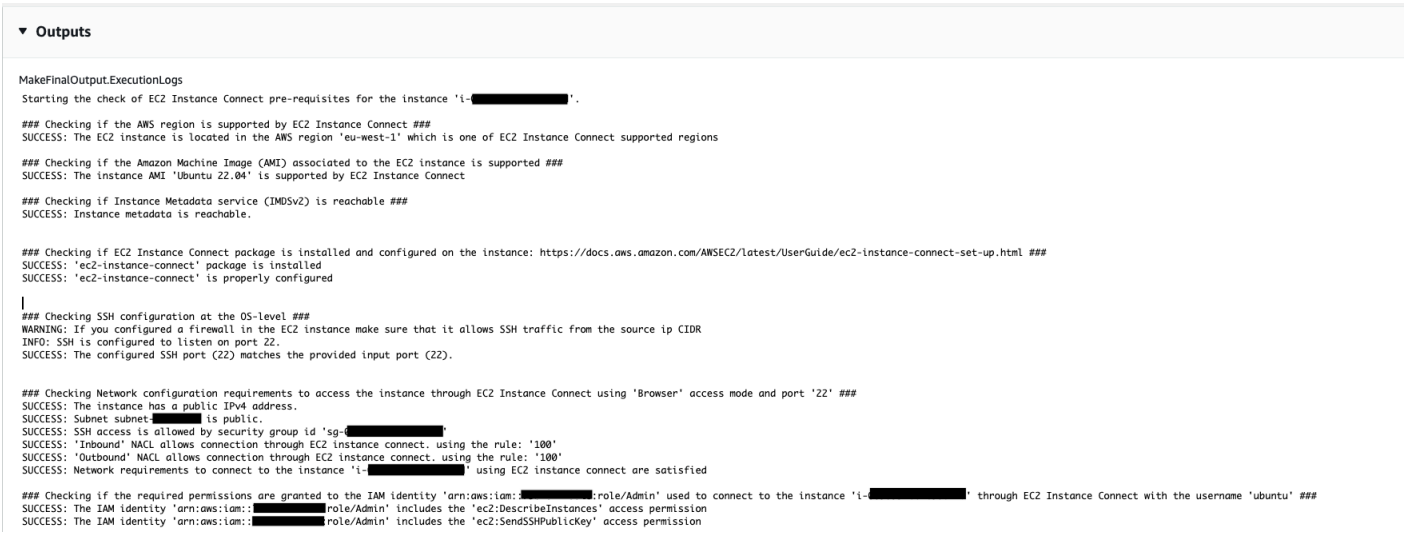
Comprueba si el rol o usuario de IAM utilizado para aprovechar Amazon EC2 Instance Connect tiene acceso a las teclas push de la instancia de Amazon EC2 mediante el nombre de usuario proporcionado.

- MakeFinalOutput:

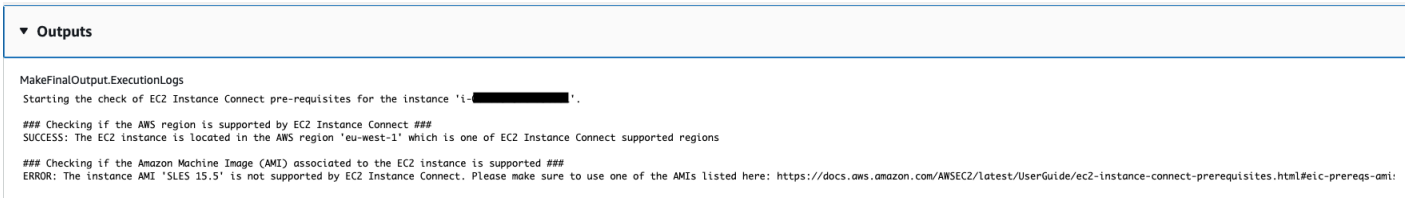
  Consolida el resultado de todos los pasos anteriores.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

   Ejecución en la que la instancia de destino cumple todos los requisitos previos necesarios:



   Ejecución en la que no se admite la AMI de la instancia de destino:



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- ¿Cómo soluciono los problemas de conexión a mi instancia de Amazon EC2 mediante Amazon EC2 Instance Connect?

AWSSupport-TroubleshootRDP

Descripción

El `AWSSupport-TroubleshootRDP`manual de procedimientos de Automation AWSSupport-TroubleshootRDP permite al usuario comprobar o modificar los ajustes comunes de la instancia de destino que podrían afectar a las conexiones del Protocolo de escritorio remoto (RDP), tales como los perfiles de puerto RDP, Autenticación en el nivel de red (NLA) y Firewall de Windows. Opcionalmente, los cambios se pueden aplicar sin conexión parando e iniciando la instancia, si el usuario permite explícitamente la corrección sin conexión. De forma predeterminada, el manual de procedimientos lee los valores de estos ajustes y los incluye en la salida.

> **Important**
>
> Los cambios realizados a los perfiles de configuración de RDP, el servicio RDP y el Firewall de Windows deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

- Acción

  Tipo: String

  Valores válidos: CheckAll | FixAll | Custom

  Valor predeterminado: Custom

  Descripción: (Opcional) [Personalizado] Utilice los valores de Firewall, RDPServiceStartupType, RDPServiceAction, RDPPortAction, NLASettingAction y RemoteConnections para administrar la configuración. [CheckAll] Lee los valores de los ajustes sin cambiarlos. [FixAll] Restaurar la configuración predeterminada de RDP y deshabilitar todos los perfiles de Firewall de Windows
- AllowOffline

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) Solo corregir: establecer en True si permite una corrección de RDP sin conexión en caso de que falle la solución de problemas online o que la instancia proporcionada no sea una instancia administrada. Nota: Para la corrección sin conexión, SSM Automation detiene la instancia y crea una AMI antes de intentar realizar ninguna operación.
- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- Firewall

  Tipo: String

  Valores válidos: Check | Disable

  Valor predeterminado: Check

  Descripción: (Opcional) comprobar o deshabilitar el Firewall de Windows (todos los perfiles).

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia para solucionar problemas de la configuración de RDP.

- NLASettingAction

  Tipo: String

  Valores válidos: Check | Disable

  Valor predeterminado: Check

  Descripción: (Opcional) comprobar o deshabilitar la Autenticación en el nivel de red (NLA).

- RDPPortAction

  Tipo: String

  Valores válidos: Check | Modify

  Valor predeterminado: Check

  Descripción: (Opcional) comprobar el puerto utilizado actualmente para las conexiones RDP o modificar el puerto RDP y volver a establecerlo en 3389 y reiniciar el servicio.

- RDPServiceAction

  Tipo: String

  Valores permitidos: Check | Start | Restart | Force-Restart

  Valor predeterminado: Check

  Descripción: (Opcional) comprobar, comenzar, reiniciar o forzar el reinicio del servicio RDP (TermService).

- RDPServiceStartupType

  Tipo: String

  Valores válidos: Check | Auto

  Valor predeterminado: Check

Descripción: (Opcional) comprobar o establecer el servicio RDP para que se comience automáticamente cuando se inicia Windows.

- RemoteConnections

  Tipo: String

  Valores válidos: Check | Enable

  Valor predeterminado: Check

  Descripción: (Opcional) una acción para realizar en la configuración de fDenyTSConnections: comprobar, habilitar.

- S3BucketName

  Tipo: String

  Descripción: (Opcional) Solo sin conexión: nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- SubnetId

  Tipo: String

  Valor predeterminado: SelectedInstanceSubnet

  Descripción: (Opcional) solo sin conexión: el ID de subred para la instancia EC2Rescue utilizada para realizar la solución de problemas sin conexión. Si no se especifica ningún ID de subred, AWS Systems ManagerAutomation creará una nueva VPC. IMPORTANTE: La subred debe estar en la misma zona de disponibilidad que InstanceId y debe permitir el acceso a puntos de enlace de SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la instancia EC2 que recibe el comando tenga un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. Para la corrección online,

el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution y ssm:SendCommand para ejecutar Automation y enviar el comando a la instancia, así como ssm:GetAutomationExecution para poder leer la salida de Automation. Para la corrección sin conexión, el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances, además de ssm:GetAutomationExecution para poder leer el resultado de la automatización. `AWSSupport-TroubleshootRDP` llama a `AWSSupport-ExecuteEC2Rescue` para realizar la corrección sin conexión. Por favor revise los permisos `AWSSupport-ExecuteEC2Rescue` para asegurarse de que puede ejecutar la automatización correctamente.

Pasos de documentos

1. `aws:assertAwsResourceProperty` - Compruebe si la instancia es una instancia Windows Server
2. `aws:assertAwsResourceProperty` - Compruebe si la instancia es una instancia gestionada
3. (Solución de problemas online) Si la instancia es una instancia administrada, entonces:
   a. `aws:assertAwsResourceProperty` - Compruebe el valor de acción proporcionado
   b. (Comprobación online) Si Action = CheckAll, entonces:

      `aws:runPowerShellScript` - Ejecuta el script de PowerShell para obtener el estado de los perfiles del Firewall de Windows.

      `aws:executeAutomation` - Llama a `AWSSupport-ManageWindowsService`para obtener el estado del servicio RDP.

      `aws:executeAutomation` - Llama a `AWSSupport-ManageRDPSettings`para obtener la configuración del RDP.
   c. (Corrección online) Si Action = FixAll, entonces:

      `aws:runPowerShellScript` - Ejecuta el script de PowerShell para deshabilitar todos los perfiles del Firewall de Windows.

      `aws:executeAutomation` - Llama a `AWSSupport-ManageWindowsService`para iniciar el servicio RDP.

      `aws:executeAutomation` - Llama a `AWSSupport-ManageRDPSettings`para habilitar las conexiones remotas y deshabilitar el NLA.
   d. (Administración online) Si Action = Custom, entonces:

`aws:runPowerShellScript` - Ejecuta el script de PowerShell para administrar los perfiles del Firewall de Windows.

`aws:executeAutomation` - Llama a `AWSSupport-ManageWindowsService`para gestionar el servicio RDP.

`aws:executeAutomation` - Llama a `AWSSupport-ManageRDPSettings`para gestionar la configuración del RDP.

4. (Corrección sin conexión) Si la instancia de entrada no es una instancia administrada, entonces:
   a. `aws:assertAwsResourceProperty` - Confirma AllowOffline = true
   b. `aws:assertAwsResourceProperty` - Confirma Action = FixAll
   c. `aws:assertAwsResourceProperty` - Confirma el valor de SubnetId

      (Usar la subred de la instancia proporcionada) Si SubnetId es SELECTED_INSTANCE_SUBNET.

      `aws:executeAwsApi` - Recupera la subred de la instancia actual.

      `aws:executeAutomation` - Ejecuta `AWSSupport-ExecuteEC2Rescue`con la subred de la instancia proporcionada.
   d. (Usar la subred personalizada proporcionada) Si SubnetId no es SELECTED_INSTANCE_SUBNET.

      `aws:executeAutomation` - Ejecuta `AWSSupport-ExecuteEC2Rescue`con el valor de SubnetID proporcionado.

Salidas

manageFirewallProfiles.Output

manageRDPServiceSettings.Output

manageRDPSettings.Output

checkFirewallProfiles.Output

checkRDPServiceSettings.Output

checkRDPSettings.Output

disableFirewallProfiles.Output

restoreDefaultRDPServiceSettings.Output

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

Descripción

El manual de procedimientos de AWSSupport-TroubleshootSSH instala Amazon EC2Rescue para Linux y luego usa la herramienta EC2Rescue para comprobar o intentar solucionar problemas comunes que impiden una conexión remota al equipo Linux a través de SSH. Opcionalmente, los cambios se pueden aplicar sin conexión parando e iniciando la instancia, si el usuario permite explícitamente la corrección sin conexión. De forma predeterminada, el manual de procedimientos opera en modo de solo lectura.

Ejecuta esta automatización (consola)

Para obtener información sobre cómo trabajar con el manual de procedimientos AWSSupport-TroubleshootSSH, consulte este AWSSupport-TroubleshootSSHtema de solución de problemas de AWSPremium Support.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- Acción

  Tipo: String

Valores válidos: CheckAll | FixAll

Valor predeterminado: CheckAll

Descripción: (Obligatorio) especificar si buscar errores sin corregirlos o buscar y corregir automáticamente cualquier problema descubierto.

- AllowOffline

  Tipo: String

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) Solo corregir: establecer en True si permite una corrección de SSH sin conexión en caso de que falle la solución de problemas online o que la instancia proporcionada no sea una instancia administrada. Nota: Para la corrección sin conexión, SSM Automation detiene la instancia y crea una AMI antes de intentar realizar ninguna operación.

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia EC2 para Linux.

- S3BucketName

  Tipo: String

  Descripción: (Opcional) Solo sin conexión: nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- SubnetId

  Tipo: String

  Valor predeterminado: SelectedInstanceSubnet

  Descripción: (Opcional) solo sin conexión: el ID de subred para la instancia EC2Rescue utilizada para realizar la solución de problemas sin conexión. Si no se especifica ningún ID de subred, AWS Systems ManagerAutomation creará una nueva VPC.

  > **Important**
  >
  > La subred debe estar en la misma zona de disponibilidad que InstanceId y debe permitir el acceso a puntos de enlace de SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la instancia EC2 que recibe el comando tenga un rol de IAM con la política administrada AmazonSSMManagedInstanceCore de Amazon asociada. Para la corrección online, el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution y ssm:SendCommand para ejecutar Automation y enviar el comando a la instancia, así como ssm:GetAutomationExecution para poder leer la salida de Automation. Para la corrección sin conexión, el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances, además de ssm:GetAutomationExecution para poder leer el resultado de la automatización. `AWSSupport-TroubleshootSSH`llama a `AWSSupport-ExecuteEC2Rescue`para realizar la corrección sin conexión. Por favor revise los permisos `AWSSupport-ExecuteEC2Rescue` para asegurarse de que puede ejecutar la automatización correctamente.

Pasos de documentos

1. `aws:assertAwsResourceProperty` - Compruebe si la instancia es una instancia gestionada
   a. (Corrección online) Si la instancia de entrada no es una instancia administrada, entonces:
      i. `aws:configurePackage` - Instalar EC2Rescue para Linux a través de `AWS-ConfigureAWSPackage`.

ii. `aws:runCommand` - Ejecutar el script bash para ejecutar EC2Rescue para Linux.

b. (Corrección sin conexión) Si la instancia de entrada no es una instancia administrada, entonces:

i. `aws:assertAwsResourceProperty` - Confirma AllowOffline = true

ii. `aws:assertAwsResourceProperty` - Confirma Action = FixAll

iii. `aws:assertAwsResourceProperty` - Confirma el valor de SubnetId

iv. (Utilice la subred de la instancia proporcionada) Si el valor de SubnetId es SelectedInstanceSubnet, utilice `aws:executeAutomation`para ejecutar `AWSSupport-ExecuteEC2Rescue`con la subred de la instancia proporcionada.

v. (Utilice la subred personalizada proporcionada) Si el valor de SubnetId no es SelectedInstanceSubnet, use `aws:executeAutomation`para ejecutar `AWSSupport-ExecuteEC2Rescue`con el valor SubnetId proporcionado.

Salidas

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSSupport-TroubleshootSUSERegistration

Descripción

El manual de procedimientos `AWSSupport-TroubleshootSUSERegistration`le ayuda a identificar por qué se produjo un error al registrar una instancia SUSE Linux Enterprise Serverde Amazon Elastic Compute Cloud (Amazon EC2) con SUSE Update Infrastructure. El resultado de la automatización proporciona los pasos para resolver el problema o le ayuda a solucionar el problema. Si la instancia supera todas las comprobaciones durante la automatización, la instancia se registra en SUSE Update Infrastructure.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: String

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: String

  Descripción: (Obligatorio) ID de la instancia Amazon EC2 que quiere resolver.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Pasos de documentos

- `aws:assertAwsResourceProperty` - Comprueba si la instancia de Amazon EC2 está gestionada por AWS Systems Manager.
- `aws:runCommand` - Comprueba si la plataforma de instancias de Amazon EC2 es SLES.

- `aws:runCommand` - Comprueba si la versión del paquete `cloud-regionsrv-clientes` superior o igual a la versión 9.0.10 requerida.
- `aws:runCommand` - Comprueba si el enlace simbólico del producto base está roto y corrige el enlace si está roto.
- `aws:runCommand` - Comprueba si el archivo de hosts (`/etc/hosts`) contiene registros para `smt-ec2-suscloud.net`. La automatización elimina cualquier entrada duplicada.
- `aws:runCommand` - Comprueba si el comando `curl`está instalado.
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 puede acceder a la dirección 169.254.169.254 del servicio de metadatos de instancias (IMDS).
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 tiene un código de facturación o un código de producto AWS Marketplace.
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 puede llegar al menos a 1 servidor regional a través de HTTPS.
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 puede acceder a los servidores de la herramienta de gestión de suscripciones (SMT) a través de HTTP.
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 puede acceder a los servidores de la herramienta de gestión de suscripciones (SMT) a través de HTTPS.
- `aws:runCommand` - Comprueba si la instancia de Amazon EC2 puede acceder a la dirección `smt-ec2.susecloud.net`a través de HTTPS.
- `aws:runCommand` - Registra la instancia de Amazon EC2 en SUSE Update Infrastructure.
- `aws:executeScript` - Recopila y genera el resultado de todos los pasos anteriores.

AWSSupport-TroubleshootWindowsPerformance

Descripción

El manual `AWSSupport-TroubleshootWindowsPerformance` ayuda a solucionar problemas de rendimiento continuos en la instancia de Windows de Amazon Elastic Compute Cloud (Amazon EC2). El manual captura los registros de la instancia de destino y analiza las métricas de rendimiento de la CPU, la memoria, el disco y la red. Opcionalmente, la automatización puede capturar un volcado de procesos para ayudarte a determinar la posible causa de la degradación del rendimiento. La automatización también captura los registros de eventos y del sistema con la `EC2Rescue`herramienta más reciente, si permite que este manual la instale.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba los requisitos previos de la instancia Amazon EC2.
- Genera registros de rendimiento en el disco raíz de la instancia Amazon EC2 de Windows
- Almacena los registros capturados en una carpeta `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Si se proporciona un bucket de Amazon Simple Storage Service (Amazon S3) y el rol de responsable de automatización tiene los permisos necesarios, los registros capturados se cargan en el bucket de Amazon S3.
- Instala la `EC2Rescue` herramienta más reciente en la instancia Amazon EC2 de Windows para capturar eventos y registros del sistema si decide instalarla, pero no analiza el volcado de procesos ni los registros capturados por ella. `EC2Rescue`

Important

- Para ejecutar este runbook, la instancia de Windows de Amazon EC2 debe estar gestionada por. AWS Systems Manager Para obtener más información, consulte ¿Por qué mi instancia de Amazon EC2 no se muestra como un nodo gestionado?
- Para ejecutar este runbook, la instancia de Windows de Amazon EC2 debe ejecutarse en las versiones Windows 8.1/Windows Server 2012 R2 (6.3) o posterior PowerShell con 4.0 o superior. Para obtener más información, consulte la versión del sistema operativo Windows.
- Para generar los registros de rendimiento, se requieren al menos 10 GB de espacio libre en el dispositivo raíz. Si el disco raíz tiene más de 100 GB, el espacio libre debe ser superior al 10% del tamaño del disco. Si descarga un proceso durante la ejecución, el espacio libre debe ser superior a 10 GB más el tamaño total de memoria consumido por el proceso cuando el proceso consume más de 10 GB de memoria.
- Los registros generados en el dispositivo raíz no se eliminan automáticamente.
- El runbook no desinstala la `EC2Rescue` herramienta. Para obtener más información, consulte Uso `EC2Rescue` para Windows Server.
- Se recomienda ejecutar esta automatización durante un período en el que el rendimiento se vea afectado. También puede ejecutarla periódicamente mediante una asociación de AWS Systems Manager administradores estatales o programando Windows AWS Systems Manager de mantenimiento.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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) La función de IAM asociada al perfil de la instancia o al usuario de IAM configurado en la instancia requiere las siguientes acciones para cargar los registros en el bucket de Amazon S3 especificado para el parámetro: *LogUploadBucketName*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-TroubleshootWindowsPerformance`Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
   - InstanceId (Obligatorio):

     El ID de la instancia Amazon EC2 de Windows de destino en la que desea ejecutar la automatización. La instancia debe estar gestionada por Systems Manager para ejecutar la automatización.
   - CaptureProcessDump (Opcional):

     El tipo de volcado del proceso que se va a capturar. La automatización puede capturar un volcado de proceso para el proceso que podría estar causando un impacto en el rendimiento al principio de la automatización. El volumen raíz de la instancia requiere al menos 10 GB de espacio libre (más del 10% del tamaño del disco cuando el tamaño del volumen raíz es superior a 100 GB y 10 GB más el tamaño total de memoria que consume el proceso cuando el proceso consume más de 10 GB de memoria).
   - LogCaptureDuration (Opcional):

El número de minutos transcurridos entre 1 y 15 durante los que esta automatización capturará los registros mientras el problema esté presente. El valor predeterminado es 5.

- LogUploadBucketName (Opcional):

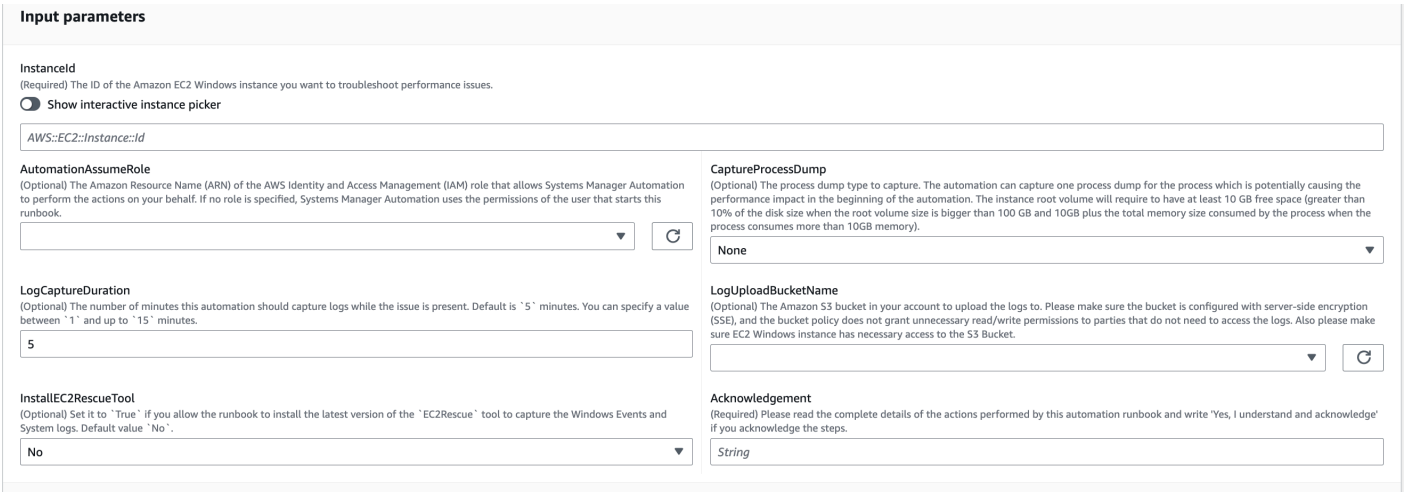
  El depósito de Amazon S3 de su cuenta en el que desea cargar los registros. El depósito debe configurarse con el cifrado del lado del servidor (SSE) y la política del depósito no debe conceder permisos de lectura y escritura innecesarios a las partes que no necesiten acceder a los registros capturados. La instancia Amazon EC2 para Windows debe tener acceso al bucket de Amazon S3.

- Instale EC2 RescueTool (opcional):

  `Yes`Configúrelo para permitir que el runbook instale la última versión de la `EC2Rescue` herramienta para capturar los eventos de Windows y los registros del sistema. El valor predeterminado es `No`.

- Reconocimiento (obligatorio):

  Lea los detalles completos de las acciones realizadas por este manual de automatización y, si está de acuerdo, escriba. `Yes, I understand and acknowledge`



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:

   - **`CheckConcurrency:`**

     Garantiza que solo haya una ejecución de este manual dirigida a la instancia. Si el runbook encuentra otra ejecución dirigida a la misma instancia, devuelve un error y finaliza.

- **AssertInstanceIsWindows:**

  Afirma que la instancia de Amazon EC2 se ejecuta en el sistema operativo Windows. De lo contrario, la automatización finaliza.

- **AssertInstanceIsManagedInstance:**

  Afirma que la instancia de Amazon EC2 está gestionada por. AWS Systems Manager De lo contrario, la automatización finaliza.

- **VerifyPrerequisites:**

  Verifica la PowerShell versión en el sistema operativo de la instancia y se asegura de que la instancia se pueda conectar a través de Systems Manager para ejecutar PowerShell comandos. Esta automatización es compatible con la versión PowerShell 4.0 y superior que se ejecuta en las versiones Windows 8.1/Server 2012 R2 (6.3) o posteriores. Si la versión es anterior, se produce un error en la automatización. Cuando decide cargar los registros al bucket de Amazon S3, esta automatización comprueba que el PowerShell módulo AWS Tools for esté disponible. Si no, la automatización finaliza.

- **BranchOnProcessDump:**

  Se ramifica en función de si lo configuró para capturar el cúmulo de procesos que afectaron al rendimiento.

- **CaptureProcessDump:**

  Comprueba si la instancia tiene suficiente espacio para ejecutar esta automatización (si eliges la CPU o memoria más altas).

- **CapturePerformanceLogs:**

  Comprueba de nuevo el espacio en disco y ejecuta el PowerShell script en la instancia para crear contadores perfectos e iniciar el registro de Performance Monitor y Windows Performance Recorder. El script se detiene cuando `LogCaptureDuration` se cumple lo definido.

- **SummarizePerformanceLogs:**

  Resume el informe XML generado en el paso anterior para encontrar el proceso responsable que consume más el WorkingSet 64 (memoria) y el% de tiempo de procesador (CPU) mostrado como resultado de la automatización. `CapturePerformanceLogs` Genera información similar sobre el uso de la interfaz de red LogicalDisk, la memoria, el TCPv4, el IPv4 y el UDPv4 y la guarda en la carpeta de resultados. `analysis_output.log`

- **BranchOnInstallEC2Rescue:**

  Se ramifica si lo configuró para instalar la EC2Rescue herramienta más reciente en la instancia de Amazon EC2.

- **InstallEC2RescueTool:**

  Instala la EC2Rescue herramienta en el sistema operativo de la instancia para capturar los EC2Rescue registros que utiliza. AWS-ConfigureAWSPackage

- **RunEC2RescueTool:**

  Ejecuta la EC2Rescue herramienta en el sistema operativo de la instancia para capturar todos los registros necesarios. EC2Rescuecaptura solo los registros necesarios para ahorrar espacio.

- **BranchOnIfS3BucketProvided:**

  Se divide en función de los datos introducidos por el usuario LogUploadBucketName para comprobar si hay un nombre de depósito disponible para cargar los registros.

- **GetS3BucketPublicStatus:**

  Determina si se proporciona un bucket de Amazon S3 y, de ser así, confirma que el bucket de Amazon S3 no es público y está configurado con SSE.

- **UploadLogResult:**

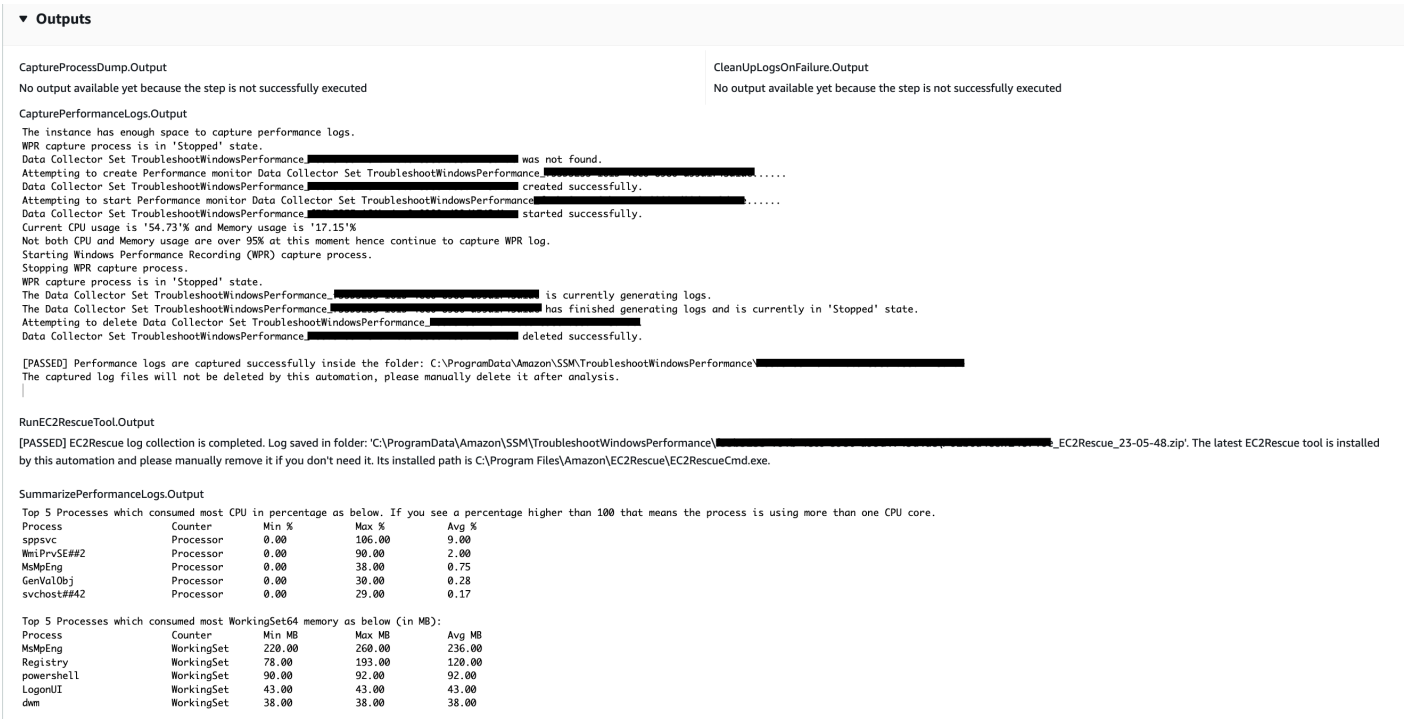
  Carga los registros en el bucket de Amazon S3 proporcionado. Si la PowerShell versión es 5.0 o superior, comprime los registros en un archivo ZIP y los carga. Elimina el archivo ZIP una vez finalizada la carga. Si la PowerShell versión es inferior a la 5.0, carga los archivos directamente a una carpeta.

- **CleanUpLogsOnFailure:**

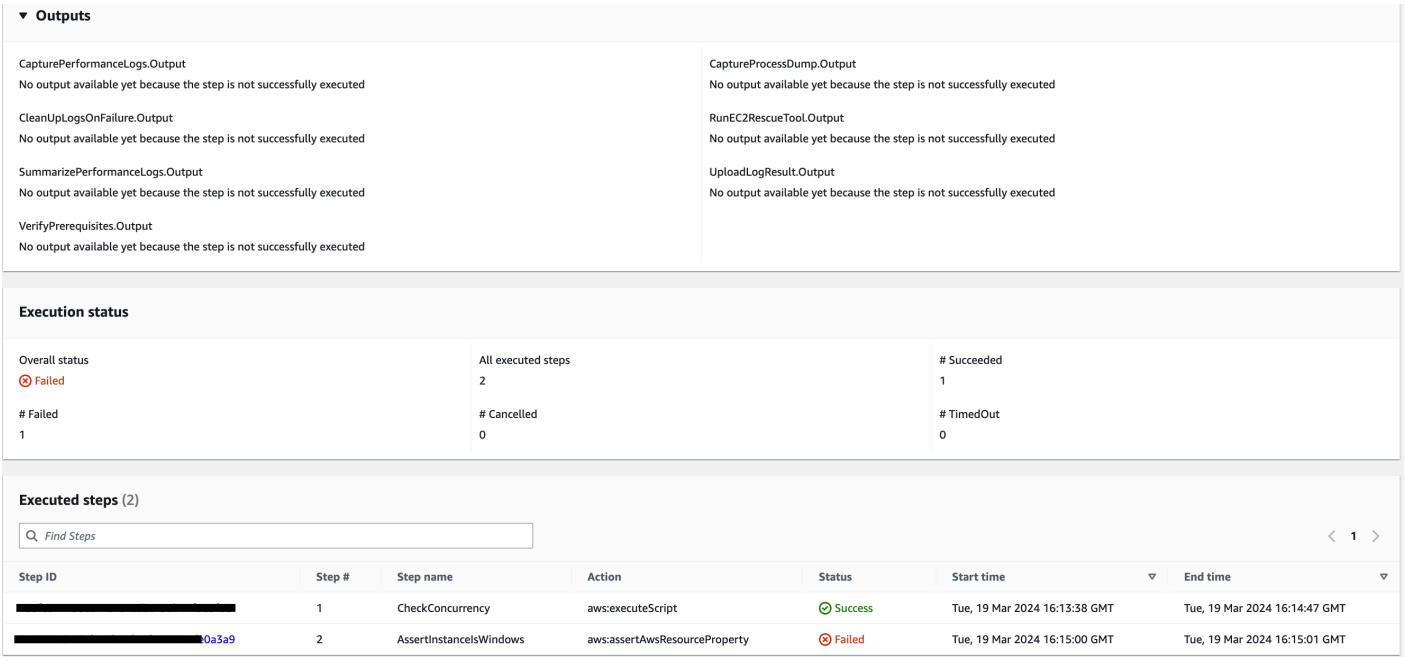
  Limpia todos los registros generados por el CapturePerformanceLogs paso cuando se produce un error. El CleanUpLogsOnFailure paso puede fallar o agotarse el tiempo de espera si el agente SSM no funciona correctamente o si el sistema Windows no responde.

7. Una vez finalizado, consulte la sección de resultados para ver los resultados detallados de la ejecución:

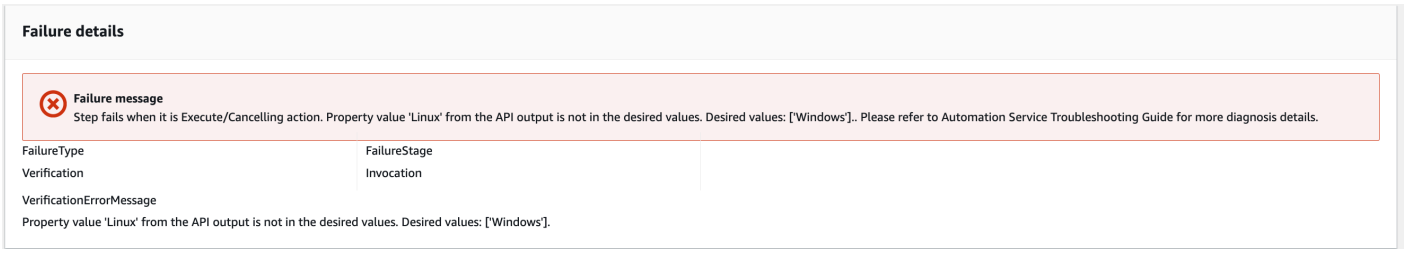
   Ejecución en la que la instancia de destino reúne todos los requisitos previos necesarios.



Ejecución en la que la instancia de destino está en una plataforma Linux y la ejecución ha fallado. Debe seleccionar el ID del paso para ver los detalles del error.



Los detalles de error del paso`AssertInstanceIsWindows`.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

`AWSSupport-TroubleshootWindowsUpdate`

Descripción

El `AWSSupport-TroubleshootWindowsUpdate` manual se utiliza para identificar los problemas que podrían fallar en las actualizaciones de Windows para las instancias de Windows de Amazon Elastic Compute Cloud (Amazon EC2).

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba si la instancia Amazon EC2 de destino está gestionada por. AWS Systems Manager
- Comprueba si las versiones AWS Systems Manager Agent (SSM Agent) y Windows Server son compatibles con las operaciones de aplicación de parches de Systems Manager.
- Comprueba el espacio en disco disponible recomendado para las actualizaciones de Windows y si hay un reinicio pendiente. Un reinicio pendiente normalmente indica que hay actualizaciones pendientes y es necesario reiniciarlo antes de realizar actualizaciones adicionales.
- Configura los ajustes del proxy a nivel del sistema operativo, lo que puede ayudar a solucionar problemas de conectividad.

- Realiza una prueba de conectividad de puntos finales del Amazon Simple Storage Service (Amazon S3) y llama a la operación de `GetDeployablePatchSnapshotForInstance`la API para recuperar la instantánea actual de la línea base del parche que utiliza el nodo gestionado.
- Si se produce un error en la conexión, ofrece la opción de ejecutar el `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analizar la conectividad de la instancia con los puntos de enlace de Amazon S3.
- Valida la configuración de actualizaciones de Windows y prueba Windows Server Update Services (WSUS) (si corresponde).

Important

- No se admiten los controladores de dominio de Active Directory.
- La versión 2008 R2 o las versiones anteriores de Windows Server no son compatibles.
- No se admiten SSM Agent 1.2.371 ni las versiones anteriores.
- El `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` manual se utiliza `VPC Reachability Analyzer`para analizar la conectividad de red entre una fuente y un punto final del servicio. Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte Precios de Amazon EFS.
- El `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` manual no está disponible en todas las regiones en las que se admite Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Para ejecutar el manual secundario`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, añada los permisos que se indican en este documento.

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-TroubleshootWindowsUpdate`Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
   - InstanceId (Obligatorio):

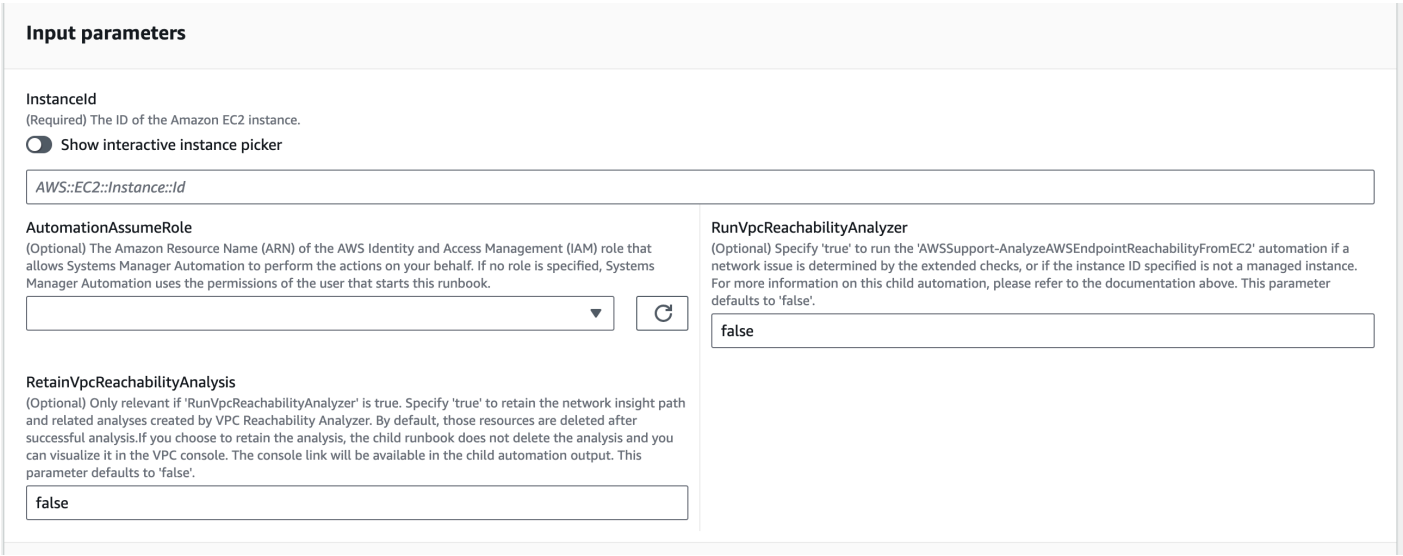
     Introduzca el ID de la instancia de Amazon EC2 en la que se produjo un error en la actualización de Windows.

- RunVpcReachabilityAnalyzer(Opcional):

  Especifique `true` que se ejecute la `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` automatización si las comprobaciones ampliadas determinan un problema de red o si el ID de instancia especificado no es una instancia administrada. Para obtener más información sobre esta automatización secundaria, consulta la documentación. El valor predeterminado es `false`.

- RetainVpcReachabilityAnalysis(Opcional):

  Solo relevante si lo `RunVpcReachabilityAnalyzer` es`true`. Especifique `true` conservar la ruta de conocimiento de la red y los análisis relacionados creados por`Reachability Analyzer`. De forma predeterminada, esos recursos se eliminan tras un análisis correcto. Si decide conservar el análisis, el manual secundario no elimina el análisis y puede visualizarlo en la consola de Amazon VPC. El enlace a la consola estará disponible en la salida de automatización secundaria. El valor predeterminado`false`.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:

   - **`getWindowsServerAndSSMAgentVersion:`**

     Comprueba que la instancia de destino esté gestionada por la versión del agente SSM AWS Systems Manager y la versión de Windows y obtiene detalles sobre ellas.

   - **`assertifInstanceIsSsmManaged:`**

Garantiza que la instancia de Amazon EC2 esté gestionada por AWS Systems Manager (SSM); de lo contrario, la automatización finaliza.

- **CheckProxy:**

  Comprueba todos los tipos de proxy de la instancia de Windows.

- **CheckPrerequisites:**

  Obtiene la versión del agente SSM y la versión de Windows y determina si se trata de un controlador de dominio (DC) de Active Directory. Si la instancia es una versión DC o no se admite la versión del agente SSM o Windows, el runbook se detiene.

- **CheckDiskSpace:**

  Obtiene y valida el espacio en disco disponible en la instancia de Windows si es suficiente para realizar la actualización de Windows.

- **CheckPendingReboot:**

  Comprueba si hay algún reinicio pendiente en la instancia de Windows.

- **CheckS3Connectivity:**

  Comprueba si la instancia puede llegar a los puntos de enlace de Amazon S3 para`Patchbaseline`.

- **branchOnRunVpcReachabilityAnalyzer:**

  Si `RunVpcReachabilityAnalyzer` es cierto, entonces ramifica la automatización para ejecutar un análisis más profundo de la depuración de la conectividad de Amazon S3.

- **GenerateEndpoints:**

  Genera un punto final para realizar una comprobación de conectividad ampliada para el punto final Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

  Llama al manual de automatización,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. para comprobar si la instancia seleccionada es accesible a los puntos de enlace necesarios.

- **CheckWindowsUpdateServices:**

  Comprueba el estado del servicio Windows Update y el tipo de inicio.

- **`CheckWindowsUpdateSettings:`**

  Comprueba las políticas de Windows Update configuradas en la instancia de Windows.

- **`CheckWSUSSettings:`**

  Comprueba si la actualización de Windows está configurada con WSUS o el catálogo de Microsoft Update y comprueba la conectividad.

- **`CheckWUGlobalSettings:`**

  Comprueba la configuración global de Windows Update configurada en la instancia de Windows.

- **`GenerateLogs:`**

  Descarga los registros de Windows Update y CBS en el escritorio de la instancia y comprueba si hay errores en los registros de eventos de Windows.

- **`FinalReport:`**

  Genera un informe completo de todos los pasos.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

```
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
"
```

Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización

- Configuración de Automation
- Página de inicio de Support Automation Workflows

Documentación relacionada con el AWS servicio

- Consulte el artículo TroubleShoot Windows Update para obtener más información.

AWSSupport-UpgradeWindowsAWSDrivers

Descripción

El manual de procedimientos `AWSSupport-UpgradeWindowsAWSDrivers`actualiza o repara controladores de AWSde almacenamiento y de red en la instancia EC2 especificada. El manual de procedimientos intenta instalar las versiones más recientes de AWSllamando al agente de SSM. Si el SSM Agent no responde, el manual de procedimientos puede llevar a cabo una instalación sin conexión de los controladores de AWSsi se especifica de forma explícita.

> **Note**
>
> Tanto la actualización online como la actualización sin conexión crearán una AMI antes de intentar realizar ninguna operación, que se conservará incluso después de que se complete la Automation. Es su responsabilidad proteger el acceso a la AMI o eliminarla. El método en línea reinicia la instancia como parte del proceso de actualización, mientras que el método sin conexión requiere detener y reiniciar la instancia EC2 proporcionada.

> **Important**
>
> Si sus instancias se conectan a AWS Systems Manager usando puntos de enlace de la VPC, este manual de procedimientos dará un error a menos que se utilice en la región us-east-1. Este manual de procedimientos también producirá un error en un controlador de dominio. Para actualizar los controladores PV de AWSen un controlador de dominio, consulte Actualización de controladores de dominio (actualización de controladores PV de AWS).

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AllowOffline

  Tipo: cadena

  Valores válidos: true | false

  Valor predeterminado: falso

  Descripción: (Opcional) establecer en true si se permite una actualización de los controladores sin conexión en caso de que no se puede llevar a cabo la instalación online. Nota: El método sin conexión requiere detener y volver a iniciar la instancia EC2 proporcionada. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.
- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- ForceUpgrade

  Tipo: cadena

  Valores válidos: true | false

  Valor predeterminado: falso

Descripción: (Opcional) Solo sin conexión: establecer en true si se permite la actualización de los controladores sin conexión para continuar incluso aunque la instancia ya tenga instalada la versión más reciente de los controladores.

- InstanceId

  Tipo: cadena

  Descripción: (Obligatorio) ID de la instancia EC2 para Windows Server.

- SubnetId

  Tipo: cadena

  Predeterminado: SelectedInstanceSubnet

  Descripción: (Opcional) solo sin conexión: el ID de subred para la instancia EC2Rescue utilizada para realizar la actualización de los controladores sin conexión. Si no se especifica el ID de subred, Systems Manager Automation creará una nueva VPC.

  > **Important**
  >
  > La subred debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales del SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

La instancia EC2 que reciba el comando debe tener, como mínimo, una función de IAM que incluya permisos para que ssm: StartAutomationExecution y ssm: ejecute la automatización y envíe el comando SendCommand a la instancia, además de ssm: GetAutomationExecution para poder leer el resultado de la automatización. Puede adjuntar la política administrada por Amazon `AmazonSSMManagedInstanceCore`a su rol de IAM para proporcionar estos permisos. Sin embargo, recomendamos utilizar el rol de IAM de Automation `AmazonSSMAutomationRole`para este propósito. Para obtener más información, consulte Uso de IAM para configurar roles para Automation.

Si está realizando una actualización sin conexión, consulte los permisos que requiere [AWSSupport-StartEC2RescueWorkflow].

Pasos de documentos

1. `aws:assertAwsResourceProperty` - Comprueba que la instancia de entrada sea Windows.
2. `aws:assertAwsResourceProperty` - Verifica que la instancia de entrada sea una instancia gestionada. En caso afirmativo, comienza la actualización online, de lo contrario, se evalúa la actualización sin conexión.
   a. (Actualización online) Si la instancia de entrada es una instancia administrada:
      i. `aws:createImage` - Crea una copia de seguridad de AMI.
      ii. `aws:createTags` - Etiqueta la copia de seguridad de AMI.
      iii. `aws:runCommand` - Instala el controlador de red ENA mediante `AWS-ConfigureAWSPackage`.
      iv. `aws:runCommand` - Instala el controlador NVMe mediante `AWS-ConfigureAWSPackage`.
      v. `aws:runCommand` - Instala el controlador PV de AWSmediante `AWS-ConfigureAWSPackage`.
   b. (Actualización sin conexión) Si la instancia de entrada no es una instancia administrada:
      i. `aws:assertAwsResourceProperty`- Verifica que el AllowOffline indicador esté establecido en. `true` En caso afirmativo, comienza la actualización sin conexión; de lo contrario, la automatización finaliza.
      ii. `aws:changeInstanceState` - Forzar la detención de la instancia
      iii. `aws:changeInstanceState` - Fuerza la detención de la instancia de origen.
      iv. `aws:createImage` - Crear una copia de seguridad de AMI de la instancia de origen.
      v. `aws:createTags` - Etiquetar la copia de seguridad de AMI de la instancia de origen.
      vi. `aws:executeAwsApi` - Habilita ENA para la instancia
      vii. `aws:assertAwsResourceProperty`- Haga valer la bandera. ForceUpgrade
      viii. Si ForceUpgrade = true (forzar la actualización sin conexión), ejecútelo `aws:executeAutomation` para invocarlo `AWSSupport-StartEC2RescueWorkflow` con el script Drivers Force Upgrade. Esto instala los controladores independientemente de la versión actual instalada.
      ix. (Actualización sin conexión) Si ForceUpgrade = false, ejecútelo `aws:executeAutomation` para invocarlo `AWSSupport-StartEC2RescueWorkflow` con el script de actualización de los controladores.

Salidas

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Salida

forceUpgradeDriversSalida fuera de línea

Amazon ECS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Container Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

`AWSSupport-CollectECSInstanceLogs`

Descripción

El manual de procedimientos `AWSSupport-CollectECSInstanceLogs` recopila archivos de registro relacionados con el sistema operativo y Amazon Elastic Container Service (Amazon ECS) de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para ayudarle a solucionar

problemas comunes de Amazon ECS. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en el sistema de archivos. Estos cambios incluyen la creación de directorios temporales y un directorio de registro, la copia de los archivos de registro a estos directorios y la compresión de los archivos de registro en un archivo.

Si especifica un valor para el parámetro `LogDestination`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia de Amazon EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users` Amazon S3, los registros no se cargan. Además, si el bucket proporcionado no está disponible en su cuenta, los registros no se cargarán. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los Grupos predefinidos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ECS InstanceId

  Tipo: cadena

Descripción: (obligatorio) ID de la instancia de la que desea recopilar los registros. La instancia que especifique debe ser administrada por Systems Manager.

- LogDestination

  Tipo: cadena

  Descripción: (opcional) El depósito de Amazon S3 en el Cuenta de AWS que debe cargar los registros archivados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Recomendamos que la instancia Amazon EC2 que recibe el comando `ECSInstanceId` tenga un rol de IAM con la política administrada Amazon de `AmazonSSMManagedInstanceCore` asociada. Para cargar el archivo de registro en el bucket de Amazon S3 que especifique en el parámetro `LogDestination`, debe añadir los siguientes permisos:

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

Pasos de documentos

- `assertInstanceIsManaged`: verifica si la instancia que especifique en el parámetro `ECSInstanceId`está gestionada por Systems Manager.
- `getInstancePlatform`: obtiene información acerca de la plataforma del sistema operativo (SO) de la instancia especificada en el parámetro `ECSInstanceId`.

- `verifyInstancePlatform`: ramifica la automatización en función de la plataforma del sistema operativo.
- `runLogCollectionScriptOnLinux`: recopila los archivos de registro relacionados con el sistema operativo y Amazon ECS en las instancias de Linux y crea un archivo de almacenamiento en el directorio `/var/log/collectECSlogs`.
- `runLogCollectionScriptOnWindows`: recopila los archivos de registro relacionados con el sistema operativo y Amazon ECS en las instancias de Windows y crea un archivo de almacenamiento en el directorio `C:\ProgramData\collectECSlogs`.
- `verifyIfS3BucketProvided`: verifica si se especificó un valor para el parámetro `LogDestination`.
- `runUploadScript`: ramifica el paso de automatización en función de la plataforma del sistema operativo.
- `runUploadScriptOnLinux`: carga el archivo de registro en el bucket de Amazon S3 especificado en el parámetro `LogDestination` y elimina el archivo de registro archivado del sistema operativo.
- `runUploadScriptOnWindows`: carga el archivo de registro en el bucket de Amazon S3 especificado en el parámetro `LogDestination` y elimina el archivo de registro archivado del sistema operativo.

AWS-InstallAmazonECSAgent

Descripción

El manual de procedimientos `AWS-InstallAmazonECSAgent` instala el agente de Amazon Elastic Container Service (Amazon ECS) en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos solo es compatible con instancias de Amazon Linux y Amazon Linux 2.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceIds

  Tipo: StringList

  Descripción: (obligatorio) los ID de las instancias de Amazon EC2 en las que desea instalar el agente de Amazon ECS.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Pasos de documentos

`aws:executeScript`: instala el agente de Amazon ECS en las instancias de Amazon EC2 que especifique en el parámetro `InstanceIds`.

Salidas

InstallAmazonAgente ECS. SuccessfulInstances - El ID de la instancia en la que se instaló correctamente el agente de Amazon ECS.

InstallAmazonAgente ECS. FailedInstances - El ID de la instancia en la que se produjo un error en la instalación del agente de Amazon ECS.

InstallAmazonAgente ECS. InProgressInstances - El ID de la instancia en la que se está instalando el agente Amazon ECS.

AWS-ECSRunTask

Descripción

El `AWS-ECSRunTask` manual ejecuta la tarea de Amazon Elastic Container Service (Amazon ECS) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- capacidad ProviderStrategy

  Tipo: cadena

Descripción: (opcional) La estrategia del proveedor de capacidad que se utilizará para la tarea.

- Clúster

  Tipo: cadena

  Descripción: (opcional) El nombre abreviado o el ARN del clúster en el que se ejecutará la tarea. Si no especifica un clúster, se utiliza el clúster predeterminado.

- count

  Tipo: cadena

  Descripción: (opcional) El número de instancias de la tarea especificada que se van a colocar en el clúster. Puedes especificar hasta 10 tareas para cada solicitud.

- Habilite ECS ManagedTags

  Tipo: Booleano

  Descripción: (opcional) Especifica si se van a utilizar etiquetas gestionadas de Amazon ECS para la tarea. Para obtener más información, consulte Etiquetado de los recursos de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

- habilitar ExecuteCommand

  Tipo: Booleano

  Descripción: (opcional) Determina si se debe activar la funcionalidad de ejecución de comandos para los contenedores de esta tarea. Si es cierto, se activa la función de ejecución de comandos en todos los contenedores de la tarea.

- grupo

  Tipo: cadena

  Descripción: (opcional) El nombre del grupo de tareas que se va a asociar a la tarea. El valor predeterminado es el apellido de la definición de la tarea. Por ejemplo, `family:my-family-name`.

- Tipo de lanzamiento

  Tipo: cadena

  Valores válidos: EC2 | FARGATE | EXTERNAL

Descripción: (opcional) La infraestructura en la que ejecutar la tarea independiente.

- networkConfiguration

  Tipo: cadena

  Descripción: (opcional) La configuración de red de la tarea. Este parámetro es necesario para las definiciones de tareas que utilizan el modo de `awsvpc` red para recibir su propia interfaz de red elástica y no se admite en otros modos de red.

- anula

  Tipo: cadena

  Descripción: (opcional) Una lista de anulaciones de contenedores en formato JSON que especifica el nombre de un contenedor en la definición de tarea especificada y las anulaciones que debe recibir. Puedes anular el comando predeterminado de un contenedor especificado en la definición de la tarea o en la imagen de Docker con una anulación de comandos. También puedes anular las variables de entorno existentes que se especifican en la definición de la tarea o en la imagen de Docker de un contenedor. Además, puedes añadir nuevas variables de entorno con una anulación de entorno.

- Restricciones de ubicación

  Tipo: cadena

  Descripción: (opcional) Una matriz de objetos de restricción de ubicación que se utilizarán en la tarea. Puede especificar hasta 10 restricciones para cada tarea, incluidas las restricciones en la definición de la tarea y las especificadas en tiempo de ejecución.

- Estrategia de colocación

  Tipo: cadena

  Descripción: (opcional) Los objetos de la estrategia de colocación que se utilizarán en la tarea. Puede especificar un máximo de 5 reglas de estrategia para cada tarea.

- platformVersion

  Tipo: cadena

Descripción: (opcional) La versión de plataforma que utiliza la tarea. Solo se especifica una versión de plataforma para las tareas alojadas en Fargate. Si no se especifica una versión de la plataforma, se utilizará la versión `LATEST`.

- propagateTags

  Tipo: cadena

  Descripción: (opcional) Determina si las etiquetas se propagan de la definición de la tarea a la tarea. Si no se especifica ningún valor, las etiquetas no se propagan. Las etiquetas solo se pueden propagar a la tarea durante la creación de tareas.

- referenceId

  Tipo: cadena

  Descripción: (opcional) El identificador de referencia que se va a utilizar en la tarea. El identificador de referencia puede tener una longitud máxima de 1024 caracteres.

- Empezado por

  Tipo: cadena

  Descripción: (opcional) Una etiqueta opcional que se especifica cuando se inicia una tarea. Esto le ayuda a identificar qué tareas pertenecen a un trabajo específico al filtrar los resultados de una operación de `ListTasks` API. Se permiten hasta 36 letras (mayúsculas y minúsculas), números, guiones (-) y guiones bajos (_).

- etiquetas

  Tipo: cadena

  Descripción: (opcional) Metadatos que desea aplicar a la tarea para ayudarle a categorizar y organizar las tareas. Cada etiqueta consta de una clave y un valor definidos por el usuario.

- Definición de tarea

  Tipo: cadena

  Descripción: (opcional) El `family` y `revision` (`family:revision`) o el ARN completo de la definición de tarea que se va a ejecutar. Si no se especifica una revisión, se utiliza la última `ACTIVE` revisión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ecs:RunTask`

Pasos de documentos

`aws:executeScript`- Ejecuta la tarea Amazon ECS en función de los valores que especifique para los parámetros de entrada del runbook.

`AWSSupport-TroubleshootECSContainerInstance`

Descripción

El manual de procedimientos `AWSSupport-TroubleshootECSContainerInstance` le ayuda a solucionar problemas de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que no se registra con un clúster de Amazon ECS. Esta automatización comprueba si los datos de usuario de la instancia contienen la información de clúster correcta, si el perfil de instancia contiene los permisos necesarios y si hay problemas de configuración de la red.

> **Important**
>
> Para ejecutar correctamente esta automatización, el estado de su instancia de Amazon EC2 debe ser `running` y el estado del clúster de Amazon ECS debe ser `ACTIVE`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon ECS en el que no se pudo registrar la instancia.
- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia Amazon EC2 que quiere resolver.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

aws:executeScript: comprueba si la instancia de Amazon EC2 cumple los requisitos previos necesarios para registrarse en un clúster de Amazon ECS.

AWSSupport-TroubleshootECSTaskFailedToStart

Descripción

El manual de procedimientos AWSSupport-TroubleshootECSTaskFailedToStart le ayuda a resolver por qué no se pudo iniciar una tarea de Amazon Elastic Container Service (Amazon ECS) en un clúster de Amazon ECS. Debe ejecutar este manual de ejecución de la Región de AWS misma manera que la tarea que no se pudo iniciar. El manual de procedimientos analiza los siguientes problemas comunes que pueden impedir el inicio de una tarea:

- Conectividad de red con el registro de contenedores configurado
- Faltan los permisos de IAM necesarios para la función de ejecución de la tarea
- Conectividad del punto de conexión de VPC
- Configuración de regla de grupo de seguridad
- AWS Secrets Manager secretos, referencias
- Configuración de registro

> **Note**
>
> Si el análisis determina que es necesario probar la conectividad de la red, se crean en su cuenta una función de Lambda y el rol de IAM necesario. Estos recursos se utilizan para simular la conectividad de red de su tarea fallida. La automatización elimina estos recursos cuando ya no son necesarios. Sin embargo, si la automatización no elimina los recursos, debe hacerlo manualmente.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon ECS donde no se pudo iniciar la tarea.
- CloudwatchRetentionPeríodo

  Tipo: entero

  Descripción: (opcional) El período de retención, en días, para que los registros de la función Lambda se almacenen en Amazon CloudWatch Logs. Esto solo es necesario si el análisis determina que es necesario probar la conectividad de la red.

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Valor predeterminado: 30
- TaskId

  Tipo: cadena

Descripción: (obligatorio) ID de la tarea fallida. Use la tarea fallida más reciente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeScript: comprueba que el usuario o rol que inició la automatización tiene los permisos de IAM necesarios. Si no tiene los permisos suficientes para usar este manual de procedimientos, los permisos necesarios que faltan se incluyen en el resultado de la automatización.
- aws:branch: se ramifica en función de si tiene permisos para todas las acciones necesarias para el manual de procedimientos.
- aws:executeScript: crea una función de Lambda en su VPC si el análisis determina que es necesario probar la conectividad de la red.
- aws:branch: se ramifica en función de los resultados del paso anterior.
- aws:executeScript: analiza las posibles causas del error al iniciar la tarea.
- aws:executeScript: elimina los recursos creados por esta automatización.
- aws:executeScript: formatea la salida de la automatización para regresar los resultados del análisis a la consola. Puede revisar el análisis después de este paso antes de que se complete la automatización.

- `aws:branch`: se ramifica en función de si la función de Lambda y los recursos asociados se crearon y si es necesario eliminarlos.
- `aws:sleep`: permanece en reposo durante 30 minutos para poder eliminar la interfaz de red elástica de la función de Lambda.
- `aws:executeScript`: elimina la interfaz de red de la función de Lambda.
- `aws:executeScript`: formatea la salida del paso de eliminación de la interfaz de red de la función de Lambda.

AWS-UpdateAmazonECSAgent

Descripción

El manual de procedimientos `AWS-UpdateAmazonECSAgent` actualiza el agente de Amazon Elastic Container Service (Amazon ECS) en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos solo es compatible con instancias de Amazon Linux y Amazon Linux 2.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterARN

  Tipo: StringList

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del clúster de Amazon ECS con el que están registradas las instancias de contenedor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Pasos de documentos

`aws:executeScript`: actualiza el agente de Amazon ECS en el clúster de Amazon ECS que especifique en los parámetros `ClusterARN`.

Salidas

UpdateAmazonAgente ECS. UpdatedContainers - El ID de la instancia en la que se realizó correctamente la actualización del agente de Amazon ECS.

UpdateAmazonAgente ECS. FailedContainers - El ID de la instancia en la que se produjo un error en la actualización del agente de Amazon ECS.

UpdateAmazonAgente ECS. InProgressContainers - El ID de la instancia en la que se está realizando la actualización del agente de Amazon ECS.

Amazon EFS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic File System. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-CheckAndMountEFS

AWSSupport-CheckAndMountEFS

Descripción

El manual de procedimientos `AWSSupport-CheckAndMountEFS` verifica los requisitos previos para montar su sistema de archivos Amazon Elastic File System (Amazon EFS) y lo monta en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos admite el montaje del sistema de archivos Amazon EFS con el nombre DNS o con la dirección IP del destino del montaje.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Acción

  Tipo: cadena

  Valores válidos: Check | CheckAndMount

  Descripción: (obligatorio) determina si el manual de procedimientos verifica los requisitos previos o si verifica los requisitos previos y monta el sistema de archivos.

- EfsId

  Tipo: cadena

  Descripción: (obligatorio) el ID del sistema de archivos que desea montar.

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la instancia de Amazon EC2 en la que desea montar el sistema de archivos.

- MountOptions

  Tipo: cadena

  Descripción: (opcional) las opciones compatibles con el asistente de montaje de Amazon EFS que desea utilizar al montar el sistema de archivos. Si especifica la opción `tls`, verifique que stunnel se haya actualizado en la instancia de destino.

- MountPoint

  Tipo: cadena

  Descripción: (opcional) el directorio en el que desea montar el sistema de archivos. Si especifica el valor `Check` del parámetro `Action`, no debe especificarse este parámetro.

- MountTargetIP

  Tipo: cadena

  Descripción: (opcional) la dirección IP del objetivo de montaje. El montaje por dirección IP funciona en entornos en los que el DNS está desactivado, como en el caso de las nubes privadas virtuales (VPC) con los nombres de host DNS desactivados. Además, puede utilizar esta opción si su entorno utiliza un proveedor de DNS distinto de Amazon Route 53 (Route 53).
- Región

  Tipo: cadena

  Descripción: (Obligatorio) El Región de AWS lugar donde se encuentran la instancia y el sistema de archivos de Amazon EC2.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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:*`

Pasos de documentos

- `aws:executeScript`: recopila detalles sobre la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.
- `aws:executeScript`: recopila detalles sobre el sistema de archivos que especifique en el parámetro `EfsId`.
- `aws:executeScript`: verifica que el grupo de seguridad asociado al sistema de archivos permita el tráfico en el puerto 2049 desde la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.
- `aws:assertAwsResourceProperty`: verifica que la instancia de Amazon EC2 que especifique en el parámetro `InstanceId` esté gestionada por Systems Manager y que su estado sea `Online`.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Action`.
- `aws:runCommand`: verifica los requisitos previos para montar el sistema de archivos que especifique en el parámetro `EfsId`.
- `aws:runCommand`: verifica los requisitos previos para montar el sistema de archivos que especifique en el parámetro `EfsId` y monta el sistema de archivos en la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.

Amazon EKS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Kubernetes Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-CollectEKSInstanceLogs

- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups

AWSSupport-CollectEKSInstanceLogs

Descripción

El manual de procedimientos `AWSSupport-CollectEKSInstanceLogs` recopila los archivos de registro relacionados con el sistema operativo y Amazon Elastic Kubernetes Service (Amazon EKS) de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para ayudarle a solucionar problemas comunes. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en la estructura del sistema de archivos, incluyendo la creación de directorios temporales, la copia de los archivos de registro en los directorios temporales y la compresión de los archivos de registro en un archivo. Esta actividad puede provocar un aumento de `CPUUtilization` en la instancia EC2. Para obtener más información`CPUUtilization`, consulta las métricas de instancias en la Guía del CloudWatch usuario de Amazon.

Si especifica un valor para el parámetro `LogDestination`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users` Amazon S3, los registros no se cargan. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los Grupos predefinidos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> Esta automatización requiere al menos un 10 por ciento del espacio de disco disponible en el volumen raíz de Amazon Elastic Block Store (Amazon EBS) adjuntado a su instancia de

EC2. Si no hay suficiente espacio en disco disponible en el volumen raíz, la automatización se detiene.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EKS InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia Amazon EKS EC2 de la que desea recopilar los registros.
- LogDestination

  Tipo: cadena

  Descripción: (opcional) el bucket de S3 de su cuenta en el que cargar los registros archivados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Recomendamos que la instancia EC2 que recibe el comando tenga una función de IAM con la política gestionada por Amazon de AmazonSSM ManagedInstance Core adjunta. Para cargar el archivo de registro en el bucket de S3 que especifique en el parámetro `LogDestination`, debe añadir el permiso `s3:PutObject`.

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el sistema operativo del valor especificado en el parámetro `EKSInstanceId` es Linux.
- `aws:runCommand`: recopila los archivos de registro relacionados con el sistema operativo y Amazon EKS y los comprime en un archivo del directorio `/var/log`.
- `aws:branch`: confirma si se especificó un valor para el parámetro `LogDestination`.
- `aws:runCommand`: carga el archivo de registro en el bucket de S3 que especifique en el parámetro `LogDestination`.

AWS-CreateEKSClusterWithFargateProfile

Descripción

El `AWS-CreateEKSClusterWithFargateProfile` manual crea un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante un. AWS Fargate

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) Un nombre único para el clúster.
- ClusterRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la función de IAM que proporciona permisos para que el plano de control de Kubernetes realice llamadas a AWS las operaciones de la API en su nombre.
- FargateProfileNombre

  Tipo: cadena

  Descripción: (Obligatorio) El nombre del perfil de Fargate.
- FargateProfileRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la función de IAM de ejecución del Amazon EKS Pod.
- FargateProfileSelectores

  Tipo: cadena

  Descripción: (Obligatorio) Los selectores hacen coincidir las cápsulas con el perfil de Fargate.
- SubnetIds

Tipo: StringList

Descripción: (Obligatorio) Los ID de las subredes que quiere usar para su clúster de Amazon EKS. Amazon EKS crea interfaces de red elásticas en estas subredes para la comunicación entre los nodos y el plano de control de Kubernetes. Debe especificar al menos dos ID de subredes.

- Acceso a EndpointPrivate EKS

  Tipo: Booleano

  Valor predeterminado: True

  Descripción: (opcional) Defina este valor para permitir el acceso privado `True` al punto final del servidor de la API de Kubernetes de su clúster. Si habilita el acceso privado, las solicitudes de la API de Kubernetes desde la VPC del clúster utilizan el punto de conexión de VPC privada. Si deshabilita el acceso privado y tiene nodos o AWS Fargate pods en el clúster, asegúrese de `publicAccessCidrs` incluir los bloques CIDR necesarios para la comunicación con los nodos o los pods de Fargate.

- Acceso a EKS EndpointPublic

  Tipo: Booleano

  Valor predeterminado: False

  Descripción: (opcional) Defina este valor para deshabilitar el acceso público `False` al punto final del servidor de la API de Kubernetes de su clúster. Si inhabilitas el acceso público, el servidor de API de Kubernetes de tu clúster solo podrá recibir solicitudes desde la VPC en la que se lanzó.

- PublicAccessCIDR

  Tipo: StringList

  Descripción: (opcional) El CIDR bloquea el acceso al punto final del servidor API de Kubernetes público de tu clúster. Se deniega la comunicación al punto de conexión desde direcciones fuera de los bloques de CIDR que se especifiquen. Si ha desactivado el acceso a los terminales privados y tiene nodos o pods de Fargate en el clúster, asegúrese de especificar los bloques CIDR necesarios.

- SecurityGroupID

  Tipo: StringList

Descripción: (opcional) Especifique uno o más grupos de seguridad para asociarlos a las interfaces de red elásticas creadas en su cuenta por Amazon EKS.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- CreateEksCluster (aws:execute): crea un clúster de Amazon AwsApi EKS.
- VerifyEKS ClusterIsActive (aws:wait): verifica el estado del clúster. ForAws ResourceProperty `ACTIVE`
- CreateFargateProfile (aws:executeAwsApi): crea un Fargate para el clúster.
- VerifyFargateProfileIsActive (aws:wait ForAwsResourceProperty) - Verifica que el estado del perfil de Fargate sea. `ACTIVE`

Salidas

`CreateEKSCluster.CreateClusterResponse`

Descripción: Respuesta recibida de la llamada a la API. `CreateCluster`

`CreateFargateProfile.CreateFargateProfileResponse`

Descripción: Respuesta recibida de la llamada a la `CreateFargateProfile` API.

AWS-CreateEKSClusterWithNodegroup

Descripción

El `AWS-CreateEKSClusterWithNodegroup` manual crea un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) utilizando un grupo de nodos para aumentar la capacidad.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) Nombre exclusivo para el clúster.

- ClusterRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la función de IAM que proporciona permisos para que el plano de control de Kubernetes realice llamadas a AWS las operaciones de la API en su nombre.

- NodegroupName

  Tipo: cadena

  Descripción: (obligatorio) Un nombre único para el grupo de nodos.

- NodegroupRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del rol de IAM que se va a asociar al grupo de nodos. El daemon kubelet del nodo de trabajo de Amazon EKS realiza llamadas a AWS las API en su nombre. Los nodos reciben permisos de dichas llamadas de API a través de políticas asociadas y de un perfil de instancias de IAM. Antes de poder lanzar nodos y registrarlos en un clúster, debe crear un rol de IAM para dichos nodos, para utilizarlo cuando se lancen.

- SubnetIds

  Tipo: StringList

  Descripción: (Obligatorio) Los ID de las subredes que quiere usar para su clúster de Amazon EKS. Amazon EKS crea interfaces de red elásticas en estas subredes para la comunicación entre los nodos y el plano de control de Kubernetes. Debe especificar al menos dos ID de subredes.

- Acceso a EndpointPrivate EKS

  Tipo: Booleano

  Valor predeterminado: True

  Descripción: (opcional) Defina este valor para permitir el acceso privado `True` al punto final del servidor de la API de Kubernetes de su clúster. Si habilita el acceso privado, las solicitudes de la API de Kubernetes desde la VPC del clúster utilizan el punto de conexión de VPC privada.

Si deshabilita el acceso privado y tiene nodos o AWS Fargate pods en el clúster, asegúrese de `publicAccessCidrs` incluir los bloques CIDR necesarios para la comunicación con los nodos o los pods de Fargate.

- Acceso a EKS EndpointPublic

  Tipo: Booleano

  Valor predeterminado: False

  Descripción: (opcional) Defina este valor para deshabilitar el acceso público `False` al punto final del servidor de la API de Kubernetes de su clúster. Si inhabilitas el acceso público, el servidor de API de Kubernetes de tu clúster solo podrá recibir solicitudes desde la VPC en la que se lanzó.

- PublicAccessCIDR

  Tipo: StringList

  Descripción: (opcional) El CIDR bloquea el acceso al punto final del servidor API de Kubernetes público de tu clúster. Se deniega la comunicación al punto de conexión desde direcciones fuera de los bloques de CIDR que se especifiquen. Si ha desactivado el acceso a los terminales privados y tiene nodos o pods de Fargate en el clúster, asegúrese de especificar los bloques CIDR necesarios.

- SecurityGroupID

  Tipo: StringList

  Descripción: (opcional) Especifique uno o más grupos de seguridad para asociarlos a las interfaces de red elásticas creadas en su cuenta por Amazon EKS.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`

- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Pasos de documentos

- CreateEksCluster (aws:execute): crea un clúster de Amazon AwsApi EKS.
- VerifyEKS ClusterIsActive (aws:wait): verifica el estado del clúster. ForAws ResourceProperty `ACTIVE`
- CreateNodegroup (aws:executeAwsApi): crea un grupo de nodos para el clúster.
- VerifyNodegroupIsActive (aws:wait ForAwsResourceProperty) - Verifica el estado del grupo de nodos. `ACTIVE`

Salidas

- `CreateEKSCluster.CreateClusterResponse`: Respuesta recibida de la llamada a la `CreateCluster` API.
- `CreateNodegroup.CreateNodegroupResponse`: Respuesta recibida de la llamada a la `CreateNodegroup` API.

AWS-DeleteEKSCluster

Descripción

Este manual de procedimientos elimina los recursos asociados a un clúster de Amazon EKS, incluyendo los grupos de nodos y los perfiles de Fargate. Si lo desea, puede optar por eliminar todos los nodos autogestionados, las AWS CloudFormation pilas utilizadas para crear los nodos y la CloudFormation pila de VPC de su clúster. Para obtener más información sobre cómo eliminar un clúster, consulte Eliminación de un clúster en la Guía del usuario de Amazon EKS.

> **Note**
>
> Si tiene en el clúster servicios activos asociados a un equilibrador de carga, deberá eliminar los servicios antes de eliminar el clúster. Si no lo hace, el sistema no podrá eliminar los equilibradores de carga. Utilice el siguiente procedimiento para buscar y eliminar servicios antes de ejecutar el manual de procedimientos `AWS-DeleteEKSCluster`.

Cómo localizar y eliminar los servicios del clúster

1. Instale la utilidad de línea de comandos de Kubernetes, `kubectl`. Para obtener más información, consulte Instalación del kubectl en la Guía del usuario de Amazon EKS.
2. Ejecute el siguiente comando para enumerar todos los servicios que se ejecutan en su clúster.

   ```
   kubectl get svc --all-namespaces
   ```

3. Ejecute el siguiente comando para eliminar cualquier servicio que tenga un valor de IP EXTERNO asociado. Estos servicios se presentan por medio de un equilibrador de carga de y debe eliminarlos en Kubernetes para que el equilibrador y los recursos asociados se liberen correctamente.

   ```
   kubectl delete svc
   service-name
   ```

Ahora puede ejecutar el manual de procedimientos `AWS-DeleteEKSCluster`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EKS ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon EKS que se va a eliminar.

- Pila de VPC CloudFormation

  Tipo: cadena

  Descripción: nombre de AWS CloudFormation pila (opcional) para la VPC del clúster de EKS que se va a eliminar. Esto elimina la AWS CloudFormation pila de la VPC y todos los recursos creados por la pila.

- VPC CloudFormation StackRole

  Tipo: cadena

  Descripción: (opcional) El ARN de una función de IAM que AWS CloudFormation supone eliminar la pila de VPC. CloudFormation AWS CloudFormation utiliza las credenciales del rol para realizar llamadas en tu nombre.

- SelfManagedNodeStacks

  Tipo: cadena

  Descripción: (opcional) Lista de nombres de AWS CloudFormation pila separados por comas para los nodos autogestionados. Esto eliminará las AWS CloudFormation pilas de los nodos autogestionados.

- SelfManagedNodeStacksFunción

Tipo: cadena

Descripción: (opcional) El ARN de una función de IAM que AWS CloudFormation asume la eliminación de las pilas de nodos autogestionadas. AWS CloudFormation utiliza las credenciales del rol para realizar llamadas en tu nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn:DeleteStack`

Pasos de documentos

- `aws:executeScript`- DeleteNodeGroups: Busque y elimine todos los grupos de nodos del clúster de EKS.
- `aws:executeScript`- DeleteFargateProfiles: Busque y elimine todos los perfiles de Fargate en el clúster EKS.
- `aws:executeScript`- DeleteSelfManagedNodes: Elimine todos los nodos autogestionados y las CloudFormation pilas utilizadas para crear los nodos.
- `aws:executeScript`: DeleteEKSCluster: eliminar el clúster EKS.
- `aws:executeScript`- Eliminar pila de VPC: elimina la CloudFormation pila de VPC. CloudFormation

AWS-MigrateToNewEKSSelfManagedNodeGroup

Descripción

El AWS-MigrateToNewEKSSelfManagedNodeGroup manual le ayuda a crear un nuevo grupo de nodos de Linux de Amazon Elastic Kubernetes Service (Amazon EKS) al que migrar la aplicación existente. Para obtener más información, consulte Migración a un nuevo grupo de nodos en la Guía del usuario de Amazon EKS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- OldStackNombre

  Tipo: cadena

  Descripción: (obligatorio) El nombre o el ID de pila de tu AWS CloudFormation pila existente.
- NewStackNombre

  Tipo: cadena

Descripción: (opcional) El nombre de la nueva AWS CloudFormation pila que se crea para el nuevo grupo de nodos. Si no especificas un valor para este parámetro, el nombre de la pila se crea con el formato:`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGrupo

  Tipo: cadena

  Descripción: (opcional) El ID del grupo de seguridad que desea que usen los nodos para comunicarse con el plano de control de Amazon EKS. Si no especifica un valor para este parámetro, se utilizará el grupo de seguridad especificado en la AWS CloudFormation pila existente.

- NodeInstanceEscriba

  Tipo: cadena

  Descripción: (opcional) El tipo de instancia que quieres usar para el nuevo grupo de nodos. Si no especificas un valor para este parámetro, se usará el tipo de instancia especificado en tu AWS CloudFormation pila existente.

- NodeGroupNombre

  Tipo: cadena

  Descripción: (opcional) El nombre del nuevo grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el nombre del grupo de nodos especificado en la AWS CloudFormation pila existente.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: cadena

  Descripción: (opcional) La cantidad de nodos a los que se debe escalar cuando se cree la nueva pila. Este número debe ser mayor o igual que el `NodeAutoScalingGroupMinSize` valor y menor o igual que`NodeAutoScalingGroupMaxSize`. Si no especificas un valor para este parámetro, se utilizará la capacidad deseada del grupo de nodos especificada en la AWS CloudFormation pila existente.

- NodeAutoScalingGroupMaxSize

  Tipo: cadena

Descripción: (opcional) El número máximo de nodos al que puede ampliarse tu grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el tamaño máximo del grupo de nodos especificado en la AWS CloudFormation pila existente.

- NodeAutoScalingGroupMinSize

  Tipo: cadena

  Descripción: (opcional) La cantidad mínima de nodos a la que puede ampliarse tu grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el tamaño mínimo del grupo de nodos especificado en la AWS CloudFormation pila existente.

- NodeImageID

  Tipo: cadena

  Descripción: (opcional) el ID del Amazon Machine Image (AMI) que desea que utilice el grupo de nodos.

- NodeImageDissmParam

  Tipo: cadena

  Descripción: (opcional) el parámetro público de Systems Manager para la AMI que desea que utilice el grupo de nodos.

- NodeVolumeTamaño

  Tipo: cadena

  Descripción: (opcional) El tamaño del volumen raíz de los nodos en GiB. Si no especificas un valor para este parámetro, se utilizará el tamaño del volumen de nodo especificado en la AWS CloudFormation pila existente.

- NodeVolumeEscriba

  Tipo: cadena

  Descripción: (opcional) El tipo de volumen de Amazon EBS que desea utilizar para el volumen raíz de sus nodos. Si no especifica un valor para este parámetro, se utilizará el tipo de volumen especificado en la AWS CloudFormation pila existente.

- KeyName

Tipo: cadena

Descripción: (opcional) El key pair que quieres asignar a tus nodos. Si no especificas un valor para este parámetro, se utilizará el par de claves especificado en la AWS CloudFormation pila existente.

- Subredes

  Tipo: StringList

  Descripción: (opcional) Una lista separada por comas de los ID de subred que quieres usar para tu nuevo grupo de nodos. Si no especificas un valor para este parámetro, se utilizarán las subredes especificadas en la pila existente AWS CloudFormation .

- DisableIMDSv1

  Tipo: Booleano

  Descripción: (opcional) Especifique si `true` desea deshabilitar la versión 1 del servicio de metadatos de instancia (IMDSv1). De forma predeterminada, los nodos admiten IMDSv1 e IMDSv2.

- BootstrapArguments

  Tipo: cadena

  Descripción: (opcional) Argumentos adicionales que desea pasar al script de arranque del nodo.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- DetermineParameterValuesForNewNodeGroup (AWS:ExecuteScript): recopila los valores de los parámetros que se utilizarán en el nuevo grupo de nodos.
- CreateStack (aws:CreateStack): crea la pila para el nuevo grupo de nodos. AWS CloudFormation
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - Obtiene el rol de instancia del nodo.
- GetNewStackSecurityGroup (aws:executeAwsApi): el paso obtiene el grupo de seguridad del nodo.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - Añade reglas de entrada al grupo de seguridad recién creado para que pueda aceptar el tráfico del grupo de nodos anterior asignado al grupo de nodos anterior.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi): agrega reglas de entrada al grupo de seguridad anterior para que pueda aceptar el tráfico del grupo de nodos asignado al grupo de nodos recién creado.
- VerifyStackComplete (aws:assert AwsResource Property): verifica que el estado de la nueva pila sea. CREATE_COMPLETE

Salidas

DetermineParameterValuesForNewNodeGrupo. NewStackParameters - Los parámetros utilizados para crear la nueva pila.

GetNewStackNodeInstanceRole. NewNodeInstanceRole - La función de instancia de nodo para el nuevo grupo de nodos.

GetNewStackSecurityGrupo. NewNodeSecurityGroup - El ID del grupo de seguridad del nuevo grupo de nodos.

DetermineParameterValuesForNewNodeGrupo. NewStackName - El nombre de la AWS CloudFormation pila del nuevo grupo de nodos.

CreateStack. StackId - El ID de AWS CloudFormation pila del nuevo grupo de nodos.

AWSPremiumSupport-TroubleshootEKSCluster

Descripción

El manual de procedimientos `AWSPremiumSupport-TroubleshootEKSCluster` diagnostica problemas comunes con un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) y la infraestructura subyacente y proporciona las medidas de corrección recomendadas.

> **Important**
>
> El acceso a los manuales de procedimientos de `AWSPremiumSupport-*` requiere una suscripción Enterprise o Business Support. Para obtener más información, consulte Compare AWS Support Plans.

Si especifica un valor para el parámetro `S3BucketName`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users` Amazon S3, los registros no se cargan. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los Grupos predefinidos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon EKS del que desea solucionar problemas.
- S3 BucketName

  Tipo: cadena

  Descripción: (opcional) el nombre del bucket privado de Amazon S3 en el que se debe cargar el informe generado por el manual de procedimientos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Además, la política AWS Identity and Access Management (IAM) asociada al usuario o rol que inicia la automatización debe permitir la ssm:GetParameter operación con los siguientes AWS Systems Manager parámetros públicos para obtener la última versión recomendada de Amazon EKS Amazon Machine Image (AMI) para los nodos de trabajo.

- 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 cargar el informe generado por el manual de procedimientos en un bucket de Amazon S3, se requieren los siguientes permisos para el bucket específico de Amazon S3 que especifique.

- s3:GetBucketPolicyStatus
- s3:GetBucketAcl

- s3:PutObject

Pasos de documentos

- aws:executeAwsApi: recopila detalles para el clúster de Amazon EKS especificado.
- aws:executeScript: recopila detalles de las instancias de Amazon Elastic Compute Cloud (Amazon EC2), los grupos de escalado automático, AMI y los tipos de instancias gráficas de GPU de Amazon EC2.
- aws:executeScript: recopila detalles de la nube privada virtual (VPC), las subredes, las puertas de enlace de traducción de direcciones de red (NAT), las rutas de subred, los grupos de seguridad y las listas de control de acceso (ACL) del clúster de Amazon EKS.
- aws:executeScript: recopila detalles de los perfiles de instancias y políticas de funciones de IAM adjuntos.
- aws:executeScript: recopila detalles del bucket de Amazon S3 que especifique en el parámetro S3BucketName.
- aws:executeScript: clasifica las subredes de Amazon VPC como públicas o privadas.
- aws:executeScript: comprueba las subredes de Amazon VPC en busca de las etiquetas que se requieren como parte de un clúster de Amazon EKS.
- aws:executeScript: comprueba las subredes de Amazon VPC en busca de las etiquetas necesarias para las subredes de Elastic Load Balancing.
- aws:executeScript: comprueba si las instancias de Amazon EC2 del nodo de trabajo utilizan la última versión optimizada de Amazon EKS AMI.
- aws:executeScript: comprueba si los grupos de seguridad de Amazon VPC conectados a los nodos de trabajo tienen las etiquetas necesarias.
- aws:executeScript: comprueba las reglas del grupo de seguridad del clúster de Amazon EKS y del nodo de trabajo de Amazon VPC para las reglas de entrada recomendadas para el clúster de Amazon EKS.
- aws:executeScript: comprueba las reglas del grupo de seguridad del clúster de Amazon EKS y del nodo de trabajo de Amazon VPC para las reglas de salida recomendadas desde el clúster de Amazon EKS.
- aws:executeScript: comprueba la configuración de ACL de red de las subredes de Amazon VPC.
- aws:executeScript: comprueba si las instancias Amazon EC2 del nodo de trabajo tienen las políticas gestionadas requeridas.

- `aws:executeScript`: comprueba si los grupos de escalado automático tienen las etiquetas necesarias para el escalado automático del clúster.
- `aws:executeScript`: comprueba si las instancias Amazon EC2 del nodo de trabajo están conectadas a Internet.
- `aws:executeScript`: genera un informe basado en los resultados de los pasos anteriores. Si se especifica un valor para el parámetro `S3BucketName`, el informe generado se carga en el bucket de Amazon S3.

AWSSupport-TroubleshootEKSWorkerNode

Descripción

El manual de procedimientos `AWSSupport-TroubleshootEKSWorkerNode` analiza un nodo de trabajo de Amazon Elastic Compute Cloud (Amazon EC2) y un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) para ayudarle a identificar y solucionar las causas comunes que impiden que los nodos de trabajo se unan a un clúster. El manual de procedimientos contiene una guía que le ayudará a resolver cualquier problema que identifique.

> **Important**
>
> Para ejecutar correctamente esta automatización, el estado del nodo de trabajo de Amazon EC2 debe ser `running`, y el estado del clúster de Amazon EKS debe ser `ACTIVE`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon EKS.
- WorkerID

  Tipo: cadena

  Descripción: (obligatorio) el ID del nodo de trabajo de Amazon EC2 que no pudo unirse al clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:assertAwsResourceProperty: confirma que el clúster de Amazon EKS que especifique en el parámetro ClusterName existe y se encuentra en un estado ACTIVE.
- aws:assertAwsResourceProperty: confirma que el nodo de trabajo de Amazon EC2 que especifique en el parámetro WorkerID existe y se encuentra en un estado running.
- aws:executeScript: ejecuta un script de Python que ayuda a identificar las posibles causas por las que el nodo de trabajo no se une al clúster.

AWS-UpdateEKSCluster

Descripción

El AWS-UpdateEKSCluster manual le ayuda a actualizar el clúster de Amazon Elastic Kubernetes Service (Amazon EKS) a la versión de Kubernetes que desee utilizar.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) El nombre del clúster de Amazon EKS.
- Versión

  Tipo: cadena

  Descripción: (Obligatoria) La versión de Kubernetes a la que desea actualizar el clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Actualiza la versión de Kubernetes que utiliza su clúster de Amazon EKS.
- `aws:waitForAwsResourceProperty`- Espera a que aparezca el estado de la actualización. `Successful`

AWS-UpdateEKSManagedNodeGroup

Descripción

El manual de procedimientos `AWS-UpdateEKSManagedNodeGroup` le ayuda a actualizar un grupo de nodos administrado de Amazon Elastic Kubernetes Service (Amazon EKS). Puede elegir entre una actualización de `Version` o `Configuration`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster cuyo grupo de nodos desea actualizar.
- NodeGroup¿Nombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre del grupo de nodos para actualizar.

- UpdateType

  Tipo: cadena

  Valores válidos: Update Node Group Version | Update Node Group Configurations

  Predeterminado: actualizar la versión del grupo de nodos

  Descripción: (obligatorio) el tipo de actualización que desea realizar en el grupo de nodos.

Los siguientes parámetros solo se aplican al tipo de actualización `Version`:

- AMI ReleaseVersion

  Tipo: cadena

  Descripción: (opcional) la versión optimizada de Amazon EKS AMI que desea utilizar. Por defecto, se utiliza la última versión.

- ForceUpgrade

  Tipo: Booleano

  Descripción: (opcional) si es cierto, la actualización no fallará en respuesta a una infracción del presupuesto por interrupción del pod.

- KubernetesVersion

  Tipo: cadena

  Descripción: (opcional) la versión de Kubernetes a la que actualizar el grupo de nodos.

- LaunchTemplateId

  Tipo: cadena

  Descripción: (opcional) el ID de la plantilla de lanzamiento.

- LaunchTemplateNombre

  Tipo: cadena

  Descripción: (opcional) el nombre de la plantilla de lanzamiento.

- LaunchTemplateVersión

Tipo: cadena

Descripción: (opcional) la versión de la plantilla de lanzamiento de Amazon Elastic Compute Cloud (Amazon EC2). Este parámetro solo es válido si se creó un grupo de nodos a partir de una plantilla de lanzamiento.

Los siguientes parámetros solo se aplican al tipo de actualización `Configuration`:

- AddOrUpdateNodeGroupLabels

  Tipo: StringMap

  Descripción: (opcional) etiquetas de Kubernetes que desea añadir o actualizar.
- AddOrUpdateKubernetesTaintsEffect

  Tipo: StringList

  Descripción: (opcional) las taints de Kubernetes que desea añadir o actualizar.
- MaxUnavailableNodeGroups

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) número máximo de nodos no disponibles a la vez durante una actualización de versión.
- MaxUnavailablePercentageNodeGrupo

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) el porcentaje de nodos que no están disponibles durante una actualización de versión.
- NodeGroupDesiredSize

  Tipo: entero

  Predeterminado: 0

Descripción: (opcional) cantidad actual de nodos que debería conservar el grupo de nodos administrados.

- NodeGroupMaxSize

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) cantidad máxima de nodos a los que puede escalar horizontalmente el grupo de nodos administrados.

- NodeGroupMinSize

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) cantidad mínima de nodos a los que puede reducir horizontalmente el grupo de nodos administrados.

- RemoveKubernetesTaintsEffect

  Tipo: StringList

  Descripción: (opcional) las taints de Kubernetes que desea eliminar.

- RemoveNodeGroupLabels

  Tipo: StringList

  Descripción: (opcional) una lista separada por comas de etiquetas que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Pasos de documentos

- `aws:executeScript`: actualiza un grupo de nodos de un clúster de Amazon EKS según los valores que especifique para los parámetros de entrada del manual de procedimientos.
- `aws:waitForAwsResourceProperty`: espera a que el estado de actualización del clúster sea `Successful`.

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descripción

El manual de procedimientos `AWS-UpdateEKSSelfManagedLinuxNodeGroups` actualiza los grupos de nodos autogestionados del clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante una pila AWS CloudFormation .

Si su clúster usa el escalado automático, le recomendamos que escale la implementación a dos réplicas antes de usar este manual de procedimientos.

Cómo escalar una implementación a dos réplicas

1. Instale la utilidad de línea de comandos de Kubernetes, `kubectl`. Para obtener más información, consulte Instalación del kubectl en la Guía del usuario de Amazon EKS.
2. Ejecute el siguiente comando de la .

   ```
   kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
   ```
3. Ejecute el manual de procedimientos `AWS-UpdateEKSSelfManagedLinuxNodeGroups`.
4. Escale la implementación de regreso al número deseado de réplicas ejecutando el siguiente comando.

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

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del clúster de Amazon EKS.
- NodeGroupNombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre del grupo de nodos administrados.
- ClusterControlPlaneSecurityGrupo

  Tipo: cadena

  Descripción: (obligatorio) el ID del grupo de seguridad del plano de control.
- DisableIMDSv1

  Tipo: Booleano

  Descripción: (opcional) determina si desea permitir la versión 1 del servicio de metadatos de instancia (IMDSv1) e IMDSv2.
- KeyName

  Tipo: cadena

  Descripción: (opcional) nombre de la clave para las instancias.
- NodeAutoScalingGroupDesiredCapacity

Tipo: cadena

Descripción: (opcional) el número de nodos que debe conservar el grupo de nodos.

- NodeAutoScalingGroupMaxSize

  Tipo: cadena

  Descripción: (opcional) cantidad máxima de nodos a los que puede escalar horizontalmente el grupo de nodos.

- NodeAutoScalingGroupMinSize

  Tipo: cadena

  Descripción: (opcional) cantidad mínima de nodos a los que puede reducir horizontalmente el grupo de nodos.

- NodeInstanceTipo

  Tipo: cadena

  Valor predeterminado: t3.large

  Descripción: (opcional) el tipo de instancia que desea usar para el grupo de nodos.

- NodeImageID

  Tipo: cadena

  Descripción: (opcional) el ID del Amazon Machine Image (AMI) que desea que utilice el grupo de nodos.

- NodeImageDissmParam

  Tipo: cadena

  Predeterminado: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Descripción: (opcional) el parámetro público de Systems Manager para la AMI que desea que utilice el grupo de nodos.

- StackName

  Tipo: cadena

Descripción: (obligatorio) El nombre de la AWS CloudFormation pila utilizada para actualizar el grupo de nodos.

- Subredes

  Tipo: cadena

  Descripción: (obligatorio) lista separada por comas de los ID de las subredes que desea que utilice su clúster.

- VpcId

  Tipo: cadena

  Valor predeterminado: Default

  Descripción: (obligatorio) la nube privada virtual (VPC) donde se implementa el clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Pasos de documentos

- `aws:executeScript`: actualiza un grupo de nodos de un clúster de Amazon EKS según los valores que especifique para los parámetros de entrada del manual de procedimientos.

- `aws:waitForAwsResourceProperty`- Espera a que se devuelva el estado de actualización de la AWS CloudFormation pila.

Elastic Beanstalk

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Elastic Beanstalk Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

`AWSSupport-CollectElasticBeanstalkLogs`

Descripción

El manual de procedimientos `AWSSupport-CollectElasticBeanstalkLogs` recopila archivos de registro AWS Elastic Beanstalk relacionados de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) Windows Server lanzada por Elastic Beanstalk para ayudarle a solucionar problemas comunes. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en la estructura del sistema de archivos, incluyendo la creación de directorios temporales, la copia de los archivos de registro en los directorios temporales y la compresión de los archivos de registro en un archivo. Esta actividad puede provocar un aumento de `CPUUtilization` en la instancia de Amazon EC2. Para obtener más información`CPUUtilization`, consulta las métricas de instancias en la Guía del CloudWatch usuario de Amazon.

Si especifica un valor para el parámetro `S3BucketName`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia de Amazon EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users` Amazon S3, los registros no se cargan. Para

obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los Grupos predefinidos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Si no especifica un valor para el parámetro `S3BucketName`, la automatización carga el paquete de registros en el bucket predeterminado Amazon S3 de Elastic Beanstalk, en la Región de AWS en la que ejecuta la automatización. El nombre del directorio se basa en la siguiente estructura,. `elasticbeanstalk-` *`region`* `-` *`accountID`* . Los valores de la *`región`* y *`accountID`* diferirán en función de la región y Cuenta de AWS en la que ejecute la automatización. El paquete de registros se guardará en el directorio `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* . Los valores de *`environmentID`* e *`instanceID`* diferirán en función de su entorno de Elastic Beanstalk y de la instancia de Amazon EC2 de la que esté recopilando los registros.

De forma predeterminada, el perfil de instancia AWS Identity and Access Management (IAM) adjunto a las instancias de Amazon EC2 del entorno de Elastic Beanstalk tiene los permisos necesarios para cargar el paquete en el bucket Amazon S3 de Elastic Beanstalk predeterminado de su entorno. Si especifica un valor para el parámetro `S3BucketName`, el perfil de instancia adjunto a la instancia de Amazon EC2 debe permitir las acciones `s3:GetBucketAcl`, `s3:GetBucketPolicy`, `s3:GetBucketPolicyStatus` y `s3:PutObject` para el bucket y la ruta de Amazon S3 especificados.

> **Note**
>
> Esta automatización requiere al menos 500 MB de espacio de disco disponible en el volumen raíz de Amazon Elastic Block Store (Amazon EBS) adjuntado a su instancia de Amazon EC2. Si no hay suficiente espacio en disco disponible en el volumen raíz, la automatización se detiene.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EnvironmentId

  Tipo: cadena

  Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk del que desea recopilar el paquete de registros.
- InstanceId

  Tipo: cadena

  (obligatorio) el ID de la instancia de Amazon EC2 del entorno de Elastic Beanstalk del que desea recopilar el paquete de registro.
- S3 BucketName

  Tipo: cadena

  (opcional) el bucket de Amazon S3 en el que desea cargar los registros archivados.
- S3 BucketPath

  Tipo: cadena

  (opcional) la ruta del bucket de Amazon S3 en la que desea cargar el paquete de registros. Este parámetro es ignorado si especifica un valor para el parámetro `S3BucketName`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

Pasos de documentos

- aws:assertAwsResourceProperty: confirma que la instancia de Amazon EC2 que especifique en el parámetro InstanceId está gestionada por AWS Systems Manager.
- aws:assertAwsResourceProperty: confirma que la instancia de Amazon EC2 que especifique en el parámetro InstanceId es una instancia Windows Server.
- aws:runCommand: comprueba si la instancia forma parte de un entorno de Elastic Beanstalk, si hay suficiente espacio en disco para agrupar los registros y si el bucket de Amazon S3 en el que se cargarían los registros es público.
- aws:runCommand: recopila los archivos de registro y carga el archivo en el bucket de Amazon S3 especificado en el parámetro S3BucketName o en el bucket predeterminado de su entorno de Elastic Beanstalk si no se especifica ningún valor.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Descripción

El AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming runbook permite iniciar sesión en el entorno AWS Elastic Beanstalk (Elastic Beanstalk) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- EnvironmentId

  Tipo: cadena

  Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk en el que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Pasos de documentos

- `aws:executeAwsApi`: permite el registro en el entorno de Elastic Beanstalk que especifique en el parámetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del entorno cambie a `Ready`.
- `aws:executeScript`: verifica que el registro está habilitado en el entorno de Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descripción

El `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook habilita las notificaciones para el entorno AWS Elastic Beanstalk (Elastic Beanstalk) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EnvironmentId

  Tipo: cadena

  Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk para el que desea habilitar las notificaciones.

- TopicArn

  Tipo: cadena

Descripción: (obligatorio) el ARN del tema de Amazon Simple Notification Service (Amazon SNS) al que desea enviar notificaciones.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Pasos de documentos

- `aws:executeAwsApi`: activa las notificaciones para el entorno de Elastic Beanstalk que especifique en el parámetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del entorno cambie a `Ready`.
- `aws:executeScript`: verifica que las notificaciones estén habilitadas para el entorno de Elastic Beanstalk.

AWSSupport-TroubleshootElasticBeanstalk

Descripción

El `AWSSupport-TroubleshootElasticBeanstalk` manual le ayuda a solucionar los posibles motivos por los que su AWS Elastic Beanstalk entorno se encuentra en un estado `Degraded` o`Severe`. Esta automatización comprueba los siguientes AWS recursos asociados al entorno de Elastic Beanstalk:

- Detalles de configuración para un balanceador de carga, una AWS CloudFormation pila, un grupo de Amazon EC2 Auto Scaling, instancias de Amazon Elastic Compute Cloud (Amazon EC2) y nube privada virtual (VPC).

- Problemas de configuración de red con las reglas del grupo de seguridad asociado, las tablas de enrutamiento y las listas de control de acceso (ACL) asociadas a sus subredes.
- Verifica la conectividad con los puntos de conexión de Elastic Beanstalk y el acceso público a Internet.
- Verifica el estado del equilibrador de carga.
- Verifica el estado de las instancias de Amazon EC2.
- Recupera un paquete de registros del entorno de Elastic Beanstalk y, si lo desea, carga los archivos en él. AWS Support

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ApplicationName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de su aplicación Elastic Beanstalk.
- EnvironmentName

Tipo: cadena

Descripción: (obligatorio) el nombre de su entorno de Elastic Beanstalk.

- AWSS3UploaderLink

  Tipo: cadena

  Descripción: (opcional) URL que le proporcionó AWS Support para cargar el paquete de registros desde su entorno de Elastic Beanstalk a. Esta opción solo está disponible para los clientes que hayan comprado un AWS Support plan y hayan abierto un caso de Support.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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*`

Pasos de documentos

- `aws:executeScript`- Comprueba que el director AWS Identity and Access Management (IAM) que inició la automatización tiene los permisos necesarios para realizar todas las acciones definidas en el manual.
- `aws:branch`: ramifica el flujo de trabajo en función de los resultados del paso anterior.
- `aws:executeScript`- Recopila información sobre el entorno de Elastic Beanstalk, incluidos el balanceador de carga AWS CloudFormation , la pila, el grupo de Auto Scaling, las instancias de Amazon EC2 y la configuración de la VPC.
- `aws:executeScript`: comprueba si hay problemas de conectividad de red con las tablas de enrutamiento y las ACL asociadas a las subredes de su VPC.
- `aws:executeScript`: comprueba si hay problemas de conectividad de red con las reglas del grupo de seguridad asociadas a sus instancias de Amazon EC2.
- `aws:executeScript`: verifica las comprobaciones de estado de las instancias de Amazon EC2.
- `aws:executeScript`: genera un enlace para un paquete de registros de su entorno de Elastic Beanstalk.
- `aws:executeScript`- Carga el paquete de registros a. AWS Support
- `aws:executeScript`: genera un informe de las medidas a tomar para ayudarle a solucionar problemas que podrían estar afectando al estado de su entorno de Elastic Beanstalk.

Elastic Load Balancing

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para Elastic Load Balancing. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- Modo AWS-UpdateALB DesyncMitigation
- Modo AWS-UpdateCLB DesyncMitigation

AWSConfigRemediation-DropInvalidHeadersForALB

Descripción

El manual `AWSConfigRemediation-DropInvalidHeadersForALB` de procedimientos permite que el equilibrador de carga de aplicación que especifique elimine los encabezados HTTP con encabezados no válidos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LoadBalancerArn

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del equilibrador de carga del que desea eliminar los encabezados no válidos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita la opción de eliminar encabezados no válidos para el equilibrador de carga que especifique en el parámetro `LoadBalancerArn`.
- `aws:executeScript`: verifica que la opción de eliminar encabezados no válidos esté habilitada en el equilibrador de carga que especifique en el parámetro `LoadBalancerArn`.

AWS-EnableCLBAccessLogs

Descripción

El `AWS-EnableCLBAccessLogs` runbook permite acceder a los registros de acceso de un Classic Load Balancer.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EmitInterval

  Tipo: entero

  Valores válidos: 5 | 60

  Predeterminado: 60

  Descripción: (opcional) El intervalo de publicación de los registros de acceso en minutos.
- LoadBalancerNombres

  Tipo: cadena

  Descripción: (Obligatorio) Una lista separada por comas de los balanceadores de carga clásicos para los que quieres habilitar los registros de acceso.
- S3 BucketName

  Tipo: cadena

  Descripción: (Obligatorio) El nombre del depósito de Amazon Simple Storage Service (Amazon S3) en el que se almacenan los registros de acceso.

- S3 BucketPrefix

  Tipo: cadena

  Descripción: (opcional) La jerarquía lógica que creó para su bucket de Amazon S3, por ejemplomy`-bucket-prefix/prod`. Si no se ha proporcionado el prefijo, el registro se colocan en el nivel raíz del bucket.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`- Habilita los registros de acceso para los balanceadores de carga clásicos que especifique en el `LoadBalancerNames` parámetro.

Salidas

Habilite CLBAccessLogs. SuccessesLoadBalancers - Lista de nombres de balanceadores de carga en los que los registros de acceso se habilitaron correctamente.

Habilite CLBAccessLogs. FailedLoadBalancers - MapList de los nombres de los balanceadores de carga en los que no se pudo habilitar los registros de acceso y el motivo del error.

`AWS-EnableCLBConnectionDraining`

Descripción

El `AWS-EnableCLBConnectionDraining` runbook permite agotar la conexión en un Classic Load Balancer (CLB) hasta el valor de tiempo de espera especificado. El agotamiento de las conexiones permite al CLB completar las solicitudes en curso realizadas a instancias que se están cancelando el registro o en mal estado, y el tiempo de espera especificado es el tiempo que mantiene activas las conexiones antes de informar que la instancia está cancelada. Para obtener más información sobre el drenaje de conexiones en los CLB, consulte Configurar el drenaje de conexiones para el Classic Load Balancer en la Guía del usuario de Classic Load Balancers.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LoadBalancerNombre

  Tipo: cadena

  Descripción: (obligatorio) El nombre del equilibrador de carga en el que quieres activar el agotamiento de la conexión.
- ConnectionTimeout

  Tipo: entero

  Valores válidos: 1-3600

  Predeterminado: 300

  Descripción: (obligatorio) El valor de tiempo de espera de conexión del balanceador de cargas. El valor de tiempo de espera se puede establecer entre 1 y 3600 segundos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): habilita el agotamiento de la conexión y establece el valor de tiempo de espera especificado para el balanceador de carga que especifique.
- VerifyLoadBalancerConnectionDrainingEnabled(AwsResourcepropiedad aws:assert): verifica que el drenaje de conexiones esté habilitado para el balanceador de cargas.
- VerifyLoadBalancerConnectionDrainingTimeout(AwsResourcepropiedad aws:assert): verifica que el valor del tiempo de espera de conexión del balanceador de cargas coincida con el valor que especificó.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` permite el equilibrio de carga entre zonas para el Equilibrador de carga clásico (CLB) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- LoadBalancerNombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre del CLB en el que desea habilitar el equilibrio de carga entre zonas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita el equilibrio de carga entre zonas para el CLB que especifique en el parámetro `LoadBalancerName`.
- `aws:assertAwsResourceProperty`: verifica que el equilibrio de carga entre zonas esté habilitado en el CLB.

AWSConfigRemediation-EnableELBDeletionProtection

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableELBDeletionProtection` habilita la protección contra la eliminación para el equilibrador de carga elástico (ELB) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- LoadBalancerArn

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del ELB en el que desea habilitar la protección de eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeScript`: habilita la protección contra la eliminación en el ELB que especifique en el parámetro `LoadBalancerArn`.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descripción

El `AWSConfigRemediation-EnableLoggingForALBAndCLB` runbook permite registrar el AWS Application Load Balancer o el Classic Load Balancer (CLB) especificados.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- LoadBalancerID

  Tipo: cadena

Descripción: (obligatorio) el nombre del equilibrador de carga clásico o el ARN del equilibrador de carga de aplicación.

- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3.

- S3 BucketPrefix

  Tipo: cadena

  Descripción: (opcional) la jerarquía lógica que creó para su bucket de Amazon Simple Storage Service (Amazon S3), por ejemplo `my-bucket-prefix/prod`. Si no se ha proporcionado el prefijo, el registro se colocan en el nivel raíz del bucket.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeScript`: habilita y verifica el registro del equilibrador de carga clásico o el equilibrador de carga de aplicación.

AWSSupport-TroubleshootCLBConnectivity

Descripción

El manual de procedimientos `AWSSupport-TroubleshootCLBConnectivity` le ayudará a solucionar problemas de conectividad entre instancias de un equilibrador de carga clásico (CLB) y Amazon Elastic Compute Cloud (Amazon EC2). Además, se revisan los problemas de conectividad

entre un cliente y el CLB. Este manual de procedimientos también revisa las comprobaciones de estado del CLB, verifica que se estén siguiendo las mejores prácticas y crea un panel de solución de problemas para usted. Si lo desea, puede cargar la salida de automatización en un bucket de Amazon Simple Storage Service (Amazon S3). Sin embargo, este manual de procedimientos no admite la carga de salida en buckets de S3 que son de acceso público. Recomendamos crear un bucket de S3 temporal para esta automatización.

> **Important**
>
> El uso de este manual de procedimientos puede conllevar gastos por el panel que se cree. Para obtener más información, consulta los CloudWatchprecios de Amazon

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InvestigationType

  Tipo: cadena

Valores válidos: Best Practices | Connectivity Issues | Troubleshooting Dashboard

Descripción: (obligatorio) las operaciones que desea que realice el manual de procedimientos.

- LoadBalancerNombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre del CLB.

- S3Location

  Tipo: cadena

  Descripción: (opcional) el nombre del bucket de S3 al que desea enviar los resultados de la automatización. No se admiten los buckets de acceso público. Si su bucket de S3 usa el cifrado del lado del servidor, el usuario o rol que ejecute esta automatización debe tener permisos `kms:GenerateDataKey` para la clave AWS KMS .

- S3 LocationPrefix

  Tipo: cadena

  Descripción: (opcional) el prefijo clave de Amazon S3 (subcarpeta) en el que desea cargar el resultado de la automatización. *El formato de salida se almacena en el siguiente formato: DOC-EXAMPLE-BUCKET/ S3 LocationPrefix/{{}} _ {{automation: InvestigationTypeEXECUTION_ID}} .txt.*

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeScript: verifica que existe el CLB que especifique en el parámetro LoadBalancerName.
- aws:branch: se ramifica en función del valor especificado para el parámetro InvestigationType.
- aws:executeScript: realiza comprobaciones de conectividad con el CLB.

- `aws:executeScript`: verifica que la configuración de CLB cumpla con las mejores prácticas de Elastic Load Balancing.
- `aws:executeScript`- Crea un CloudWatch panel de Amazon para tu CLB.
- `aws:executeScript`: crea un archivo de texto con los resultados de la automatización y lo carga en el bucket de Amazon S3 que especifique en el parámetro `S3Location`.

Salidas

RunBestPrácticas. Resumen

RunConnectivityComprobaciones. Resumen

CreateTroubleshootingPanel de mandos. Resultado

UploadOutputSalida S3.

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` permite el equilibrio de carga entre zonas para el Equilibrador de carga de red (NLB) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LoadBalancerArn

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del NLB en el que desea habilitar el equilibrio de carga entre zonas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita el equilibrio de carga entre zonas para el NLB que especifique en el parámetro `LoadBalancerArn`.
- `aws:executeScript`: verifica que el equilibrador de carga entre zonas esté habilitado en el NLB.

Modo AWS-UpdateALB DesyncMitigation

Descripción

El `AWS-UpdateALBDesyncMitigationMode` manual actualizará el modo de mitigación desincronizado de un Application Load Balancer (ALB) al modo de mitigación especificado. El modo de mitigación desincronizado determina la forma en que el balanceador de cargas gestiona las solicitudes que puedan suponer un riesgo de seguridad para la aplicación.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LoadBalancerArn

  Tipo: cadena

  Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) del ALB del que desea modificar el modo de mitigación de desincronización.
- DesyncMitigationModo

  Tipo: cadena

  Valores válidos: monitor | defensivo | estricto

  Descripción: (Obligatorio) El modo de mitigación que desea que utilice el ALB. Para obtener información sobre los modos de mitigación desincronizados, consulte el modo de mitigación desincronizado en la Guía del usuario de los balanceadores de carga de aplicaciones.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- VerifyLoadBalancerType (AwsResourcepropiedad aws:assert): comprueba que el valor especificado para el parámetro de `LoadBalancerArn` entrada corresponde a un balanceador de carga de aplicaciones antes de continuar con el siguiente paso.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi): actualiza el ALB para usar lo especificado. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (AWS:Executescript) - Verifica que el modo de mitigación de desincronización se haya actualizado para el ALB de destino.

Salidas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil del mensaje del script que verifica la modificación en su ALB.

Modo AWS-UpdateCLB DesyncMitigation

Descripción

El `AWS-UpdateCLBDesyncMitigationMode` manual actualizará el modo de mitigación desincronizado de un Classic Load Balancer (CLB) al modo de mitigación especificado. El modo de mitigación desincronizado determina la forma en que el balanceador de cargas gestiona las solicitudes que puedan suponer un riesgo de seguridad para la aplicación.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LoadBalancerNombre

  Tipo: cadena

  Descripción: (obligatorio) El nombre del CLB del que desea modificar el modo de mitigación de desincronización.
- DesyncMitigationModo

  Tipo: cadena

  Valores válidos: monitor | defensivo | estricto

  Descripción: (obligatorio) El modo de mitigación que desea que utilice el CLB. Para obtener información sobre los modos de mitigación desincronizados, consulte el modo de mitigación desincronizado en la Guía del usuario de los balanceadores de carga de aplicaciones.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi): actualiza el CLB para usar el especificado. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (AWS:Executescript) - Verifica que se haya actualizado el modo de mitigación de desincronización para el CLB de destino.

Salidas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil del mensaje del script que verifica la modificación de su CLB.

Amazon EMR

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon EMR. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

`AWSSupport-AnalyzeEMRLogs`

Descripción

Este manual de procedimientos ayuda a identificar los errores al ejecutar un trabajo en un clúster de Amazon EMR. El manual de procedimientos analiza una lista de registros definidos en el sistema de archivos y busca una lista de palabras clave predefinidas. Estas entradas de registro se utilizan para crear CloudWatch eventos de Amazon Events para que pueda realizar las acciones necesarias en función de los eventos. Si lo desea, el runbook publica las entradas de registro en el grupo de CloudWatch registros de Amazon Logs que elija. Actualmente, este manual de procedimientos busca los siguientes errores y patrones en los archivos de registro:

- container_out_of_memory: el contenedor YARN se quedó sin memoria, por lo que es posible que no se ejecute el trabajo.

- yarn_nodemanager_health: el nodo MAESTRO o de TAREA se está quedando sin espacio en disco y no podrá ejecutar tareas.
- node_state_change: el nodo MAESTRO no puede acceder al nodo MAESTRO o de TAREA.
- step_failure: falló un paso de EMR.
- no_core_nodes_running: actualmente no hay nodos PRINCIPALES en ejecución, el clúster no está en buen estado.
- hdfs_missing_blocks: faltan bloques de HDFS, lo que podría provocar la pérdida de datos.
- hdfs_high_util: el uso del HDFS es elevado, lo que puede afectar a los trabajos y al buen estado del clúster.
- instance_controller_restart: el proceso del controlador de instancias se ha reiniciado. Este proceso es esencial para el buen estado del clúster.
- instance_controller_restart_legacy: el proceso del controlador de instancias se ha reiniciado. Este proceso es esencial para el buen estado del clúster.
- high_load: se detectó un promedio de carga alto, lo que puede afectar a los informes sobre el estado de los nodos o provocar tiempos de espera o ralentizaciones.
- yarn_node_blacklisted: YARN ha incluido en la lista negra el nodo MAESTRO o de TAREA para que no pueda ejecutar tareas.
- yarn_node_lost: YARN ha marcado el nodo MAESTRO o de TAREA como PERDIDO, posibles problemas de conectividad.

Las instancias asociadas al `ClusterID` que especifique deben ser administradas por AWS Systems Manager. Puede ejecutar esta automatización una vez, programar la automatización para que se ejecute en un intervalo de tiempo específico o eliminar una programación creada previamente por una automatización. Este manual de procedimientos es compatible con las versiones 5.20 a 6.30 de Amazon EMR.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ID del clúster

  Tipo: cadena

  Descripción: (obligatorio) el ID del clúster cuyos registros de nodos desea analizar.
- Operación

  Tipo: cadena

  Valores válidos: Run Once | Schedule | Remove Schedule

  Descripción: (obligatoria) la operación que se debe realizar en el clúster.
- IntervalTime

  Tipo: cadena

  Valores válidos: 5 minutes | 10 minutes | 15 minutes

  Descripción: (opcional) el tiempo transcurrido entre la ejecución de la automatización. Este parámetro solo se aplica si especifica `Schedule` para el parámetro `Operation`.
- LogToCloudWatchRegistros

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (opcional) Si especificas `yes` el valor de este parámetro, la automatización crea un grupo de CloudWatch registros con el nombre especificado en el `CloudWatchLogGroup` parámetro para almacenar cualquier entrada de registro coincidente.

- CloudWatchLogGroup

  Tipo: cadena

  Descripción: (opcional) El nombre del grupo de CloudWatch registros en el que desea almacenar las entradas de registro coincidentes. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.
- CreateLogInsightsDashboard

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (opcional) Si lo especifica`yes`, se crea el CloudWatch panel si aún no existe. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.
- CreateMetricFiltros

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (opcional) Especifique `yes` si desea crear filtros de métricas para el grupo de CloudWatch registros. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeAwsApi: recopila información sobre el clúster de Amazon EMR especificado en el parámetro ClusterID.
- aws:branch: se ramifica en función de la entrada.
  - Si la operación proporcionada es Run Once o Schedule:
    - aws:assertAwsResourceProperty: verifica que el clúster esté disponible.
    - aws:executeAwsApi: recopila los ID de todas las instancias que se ejecutan en el clúster.

- `aws:assertAwsResourceProperty`: verifica que el agente SSM se esté ejecutando en todas las instancias del clúster.
- `aws:branch`: se ramifica en función de si especificó ejecutar la automatización una vez o de forma programada.
  - Si la operación proporcionada es `Run Once`:
    - `aws:branch`: se ramifica en función del valor especificado en el parámetro `LogToCloudWatchLogs`.
      - Si el valor `LogToCloudWatchLogs` es `yes`:
        - `aws:executeScript`- Comprueba si `CloudWatchLogGroup` ya existe un grupo de CloudWatch registros con el nombre especificado en el parámetro. De lo contrario, el grupo se crea con el nombre especificado.
        - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateMetricFilters`.
          - Si el valor `CreateMetricFilters` es `yes`:
            - `aws:executeAwsApi`: se ejecutan 12 pasos para cada filtro métrico
            - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateLogInsightsDashboard`.
              - Si el valor `CreateLogInsightsDashboard` es `yes`:
                - `aws:executeAwsApi`- Crea un CloudWatch panel con el mismo nombre especificado en el `CloudWatchLogGroup` parámetro, si aún no existe.
              - Si el valor `CreateLogInsightsDashboard` es no:
                - `aws:runCommand`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.
          - Si el valor `CreateMetricFilters` es no:
            - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateLogInsightsDashboard`.
              - Si el valor `CreateLogInsightsDashboard` es `yes`:
                - `aws:executeAwsApi`- Crea un CloudWatch panel con el mismo nombre especificado en el `CloudWatchLogGroup` parámetro, si aún no existe.
              - Si el valor `CreateLogInsightsDashboard` es no:
                - `aws:runCommand`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.

- Si el valor `LogToCloudWatchLogs` es no:
  - `aws:executeAwsApi`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.
- Si la operación proporcionada es `Schedule`:
  - `aws:createStack`- Crea un EventBridge evento de Amazon dirigido a este runbook.
- Si la operación proporcionada es `Remove Schedule`:
  - `aws:executeAwsApi`: verifica la existencia de un horario para el clúster.
  - `aws:deleteStack`: elimina la programación.

Salidas

GetClusterInformación. ClusterName

GetClusterInformación. ClusterState

ListingClusterInstancias.ID de instancia

CreatingScheduleCloudFormationPila. StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExiste. Salida

FindLogPatternOnEMR Node. CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Descripción

El `AWSSupport-DiagnoseEMRLogsWithAthena` manual ayuda a diagnosticar los registros de Amazon EMR mediante Amazon Athena en integración con Data Catalog. AWS Glue Amazon Athena se utiliza para consultar los archivos de registro de Amazon EMR en busca de contenedores, registros de nodos o ambos, con parámetros opcionales para intervalos de fechas específicos o búsquedas basadas en palabras clave.

El runbook puede recuperar automáticamente la ubicación del registro de Amazon EMR de un clúster existente, o puede especificar la ubicación del registro de Amazon S3. Para analizar los registros, el runbook:

- Crea una AWS Glue base de datos y ejecuta consultas del lenguaje de definición de datos (DDL) de Amazon Athena en la ubicación del registro Amazon S3 de Amazon EMR para crear tablas para los registros del clúster y una lista de problemas conocidos.
- Ejecuta consultas de lenguaje de manipulación de datos (DML) para buscar patrones de problemas conocidos en los registros de Amazon EMR. Las consultas devuelven una lista de los problemas detectados, su número de incidencias y el número de palabras clave coincidentes por ruta de archivo de Amazon S3.
- Los resultados se cargan en un bucket de Amazon S3 que especifique bajo el prefijo`osaw_diagnose_EMR_known_issues`.
- El manual muestra los resultados de las consultas de Amazon Athena y destaca los hallazgos, recomendaciones y referencias a los artículos del Amazon Knowledge Center (KC) procedentes de un subconjunto predefinido.
- Al finalizar o fallar, se eliminan la AWS Glue base de datos y los archivos de problemas conocidos cargados en el bucket de Amazon S3.

¿Cómo funciona?

`AWSSupport-DiagnoseEMRLogsWithAthena`Realice un análisis de los registros de Amazon EMR con Amazon Athena para detectar errores y destacar los hallazgos, recomendaciones y artículos relevantes del Knowledge Center.

El manual lleva a cabo los siguientes pasos:

- Obtenga la ubicación del registro del clúster de Amazon EMR mediante el ID del clúster o introduzca la ubicación de Amazon S3 para recuperar la ubicación y el tamaño del registro.
- Proporcione a Athena una estimación de los costos en función del tamaño de la ubicación del registro.
- Obtenga la aprobación para continuar solicitando la aprobación de los directores de IAM designados antes de ejecutar las consultas de Athena y continuar con los siguientes pasos.
- Sube los problemas conocidos al bucket de Amazon S3 especificado y crea una AWS Glue base de datos y tablas.
- Ejecute consultas de Athena en los datos de los registros de Amazon EMR. Las consultas se pueden buscar por intervalo de fechas, palabras clave o ambos criterios o ejecutarse sin filtros en función de las entradas proporcionadas.
- Analice los resultados para destacar los hallazgos, las recomendaciones y los artículos relevantes de KC.

- Enlaces de salida para los resultados de las consultas de Amazon Athena DML.
- Limpie el entorno eliminando la base de datos creada, las tablas y los problemas conocidos cargados.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

El AutomationAssumeRole parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- athena: Ejecución GetQuery
- athena: Ejecución StartQuery
- athena: Declaración GetPrepared
- athena: Declaración CreatePrepared
- pegamento: GetDatabase
- pegamento: CreateDatabase
- pegamento: DeleteDatabase
- pegamento: CreateTable
- pegamento: GetTable
- pegamento: DeleteTable
- elasticmapreduce: DescribeCluster
- s3: ListBucket
- s3: GetBucket Control de versiones
- s3: Versiones ListBucket
- s3: GetBucket PublicAccess Bloquear
- s3: GetBucket PolicyStatus
- s3: GetObject

- s3: GetBucket Ubicación
- precios: GetProducts
- precios: GetAttribute valores
- precios: DescribeServices
- precios: ListPrice Listas

> **Important**
>
> Para restringir el acceso únicamente a los recursos que necesita esta automatización, asocie la siguiente política a la función de IAM que confía en el servicio SSM. Sustituya la partición, la región y la cuenta por los valores adecuados para la partición, la región y el número de cuenta en los que se ejecuta el libro de ejecuciones.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "RestrictPutObjects",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:{Partition}:s3:::*/*/results/*",
        "arn:{partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Sid": "RestrictDeleteAccess",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:{Partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:userDefinedFunction/
saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:CreateTable",
        "glue:GetTable",
```

```
        "glue:DeleteTable"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_known_issues",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_logs_table",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
j_*",
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    }
  ]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue AWSSupport- Diagnostique al Sr. LogsWith Athena en la parte inferior de Documentos. AWS Systems Manager
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
   - ClusteriD (obligatorio):

     El ID del clúster de Amazon EMR.
   - S3 LogLocation (opcional):

     La ubicación del registro de Amazon EMR de Amazon S3. Introduzca la URL de estilo Path (ubicación de Amazon S3), por ejemplo:`s3://mybucket/myfolder/j-1K48XXXXXXHCB/`. Proporcione este parámetro si el clúster de Amazon EMR ha estado cerrado durante más `30` de unos días.
   - S3 BucketName (obligatorio):

El nombre del bucket de Amazon S3 para cargar una lista de problemas conocidos y el resultado de las consultas de Amazon Athena. El bucket debe tener activado el acceso público en bloque y estar en la misma AWS región y cuenta que el clúster de Amazon EMR.

- Aprobadores (obligatorio):

  La lista de directores AWS autenticados que pueden aprobar o rechazar la acción. Puede especificar los principales mediante cualquiera de los siguientes formatos: nombre de usuario, ARN de usuario, ARN del rol de IAM o ARN de asumir rol de IAM. El número máximo de aprobadores es 10.

- FetchNodeLogsOnly (Opcional):

  Si se establece en`true`, la automatización diagnostica los registros de contenedores de la aplicación Amazon EMR. El valor predeterminado es `false`.

- FetchContainersLogsOnly (Opcional):

  Si se establece en`true`, la automatización diagnostica los registros de contenedores de Amazon EMR. El valor predeterminado es `false`.

- EndSearchDate (Opcional):

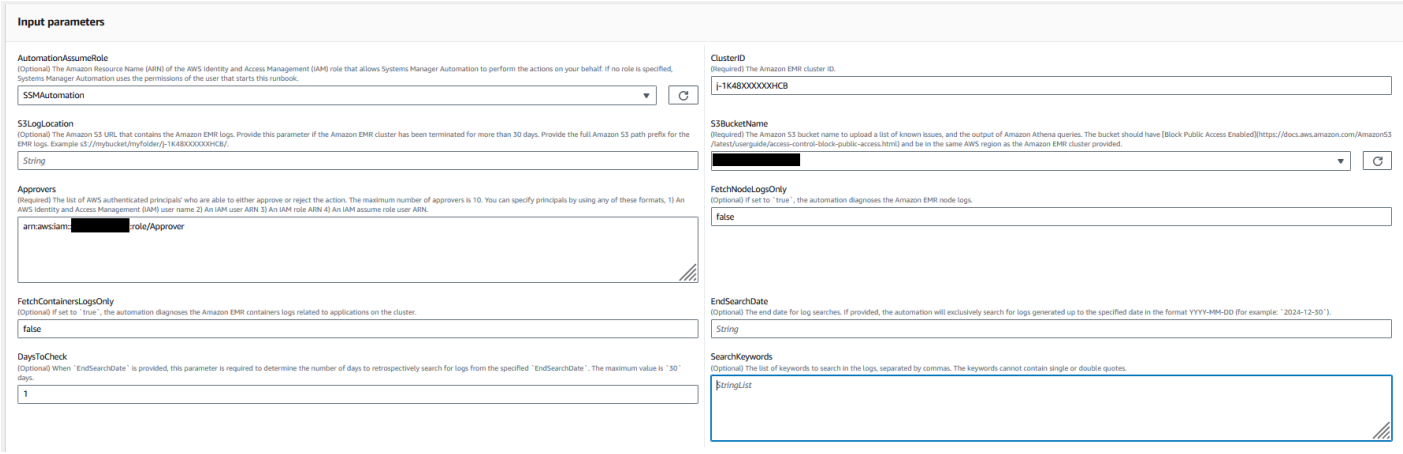
  La fecha de finalización de las búsquedas en los registros. Si se proporciona, la automatización buscará exclusivamente los registros generados hasta la fecha especificada en el formato AAAA-MM-DD (por ejemplo:). `2024-12-30`

- DaysToCheck (Opcional):

  Si `EndSearchDate` se proporciona, este parámetro es necesario para determinar el número de días necesarios para buscar retrospectivamente los registros especificados`EndSearchDate`. El valor máximo es de `30` días. El valor predeterminado es `1`.

- SearchKeywords (Opcional):

  La lista de palabras clave para buscar en los registros, separadas por comas. Las palabras clave no pueden contener comillas simples o dobles.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - obtenerLogLocation:

     Recupera la ubicación del registro de Amazon S3 consultando el ID de clúster de Amazon EMR especificado. Si la automatización no puede consultar la ubicación del registro desde el ID del clúster de Amazon EMR, el runbook utiliza el `S3LogLocation` parámetro de entrada.
   - Registro de sucursalOnValid:

     Verifica la ubicación de los registros de Amazon EMR. Si la ubicación es válida, proceda a estimar los posibles costes de Amazon Athena al ejecutar consultas en los registros de Amazon EMR.
   - estimación: AthenaCosts

     Determina el tamaño de los registros de Amazon EMR y proporciona una estimación del costo de ejecutar los escaneos de Athena en el conjunto de datos de registros. Para las regiones no comerciales (sin AWS particiones), este paso solo proporciona el tamaño del registro sin estimar los costos. Los costes se pueden calcular utilizando la documentación de precios de Athena en la región especificada.
   - Apruebe la automatización:

     Espera la aprobación del director de IAM designado para continuar con los siguientes pasos de la automatización. La notificación de aprobación contiene el costo estimado del escaneo de Amazon Athena en los registros de Amazon EMR y detalles sobre los recursos que aprovisiona la automatización.

- subir consultas: KnownIssues ExecuteAthena

  Carga los problemas conocidos predefinidos en el bucket de Amazon S3 especificado en el `S3BucketName` parámetro. Crea AWS Glue bases de datos y tablas. Ejecuta las consultas de Amazon Athena en AWS Glue la base de datos en función de los parámetros de entrada.

- obtener el estadoQueryExecution:

  Espera hasta que la ejecución de la consulta de Amazon Athena esté `SUCCEEDED` activa. La consulta DML de Amazon Athena busca errores y excepciones en los registros del clúster de Amazon EMR.

- analizar: AthenaResults

  Analiza los resultados de Amazon Athena para proporcionar hallazgos, recomendaciones y artículos del Knowledge Center (KC) procedentes de un conjunto predefinido de mapeos.

- obtenga Query1: AnalyzeResults ExecutionStatus

  Espera hasta que la ejecución de la consulta esté en estado. `SUCCEEDED` La consulta de DML de Amazon Athena analiza los resultados de la consulta de DML anterior. Esta consulta de análisis devolverá las excepciones coincidentes con las resoluciones y los artículos de KC

- obtenga AnalyzeResults Query2: ExecutionStatus

  Espera hasta que la ejecución de la consulta esté en estado. `SUCCEEDED` La consulta de DML de Amazon Athena analiza los resultados de la consulta de DML anterior. Esta consulta de análisis devolverá una lista de excepciones o errores detectados en cada ruta de registro de Amazon S3.

- imprimir mensaje: AthenaQueries

  Imprime enlaces para los resultados de las consultas de Amazon Athena DML.

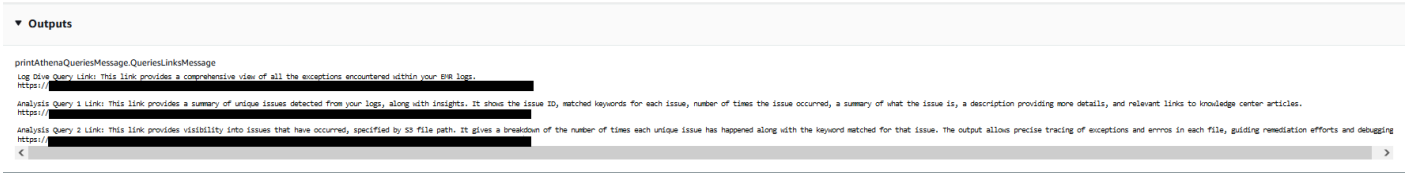
- Recursos de limpieza:

  Limpia los recursos eliminando la AWS Glue base de datos creada y eliminando los archivos de problemas conocidos que se crearon en el depósito de registros de Amazon EMR.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

   El resultado proporciona tres enlaces para los resultados de las consultas de Athena:

- Lista de todos los errores y excepciones frecuentes que se encuentran en los registros del clúster de Amazon EMR, junto con las ubicaciones de registro correspondientes (prefijo Amazon S3).
- Resumen de las excepciones conocidas únicas que coinciden en los registros de Amazon EMR, junto con las resoluciones recomendadas y los artículos de KC para ayudar a solucionar problemas.
- Detalles sobre dónde aparecen errores y excepciones específicos en las rutas de registro de Amazon S3, para facilitar un diagnóstico más detallado.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automatización
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- Consulte Solución de problemas de clústeres de Amazon EMR para obtener más información

OpenSearch Servicio Amazon

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon OpenSearch Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-DeleteOpenSearchDomain

- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

AWSConfigRemediation-DeleteOpenSearchDomain

Descripción

El `AWSConfigRemediation-DeleteOpenSearchDomain` runbook elimina el dominio de Amazon OpenSearch Service en cuestión mediante la DeleteDomainAPI.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- DomainName

  Tipo: cadena

  Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  Descripción: (Obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres eliminar.

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Pasos de documentos

- `aws:executeScript`- Acepta el nombre de dominio de Amazon OpenSearch Service como entrada, lo elimina y verifica la eliminación.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descripción

El `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` runbook se habilita `EnforceHTTPS` en un dominio de Amazon OpenSearch Service determinado mediante la API UpdateDomainConfig.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- DomainName

  Tipo: cadena

  Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  Descripción: (Obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres usar para aplicar HTTPS.
- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Pasos de documentos

- `aws:executeScript`- Activa la opción de `EnforceHTTPS` punto final en el dominio OpenSearch de Amazon Service que especifiques en el `DomainName` parámetro.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Descripción

El `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` runbook actualiza la configuración del grupo de seguridad en un dominio de Amazon OpenSearch Service determinado mediante la API UpdateDomainConfig.

> **Note**
>
> AWS Los grupos de seguridad solo se pueden aplicar a los dominios de Amazon OpenSearch Service configurados para Amazon Virtual Private Cloud (VPC) y no a los dominios de Amazon OpenSearch Service configurados para Public Access.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- DomainName

  Tipo: cadena

  Descripción: (obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres usar para actualizar los grupos de seguridad.

- SecurityGroupLista

Tipo: StringList

Descripción: (Obligatorio) Los ID de los grupos de seguridad que quieres asignar al dominio de Amazon OpenSearch Service.

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Pasos de documentos

- `aws:executeScript`- Actualiza la configuración del grupo de seguridad en el dominio OpenSearch de Amazon Service que especifiques en el `DomainName` parámetro.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Descripción

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`El manual de automatización se utiliza para identificar la causa del estado de salud de los clústeres rojos o amarillos y sirve de guía para cambiar el clúster a verde.

¿Cómo funciona?

El manual le `AWSSupport-TroubleshootOpenSearchRedYellowCluster` ayuda a solucionar la causa del clúster rojo o amarillo y proporciona los siguientes pasos para resolver este problema mediante el análisis de la configuración del clúster y el uso de los recursos.

El manual de ejecución lleva a cabo los siguientes pasos:

- Llama a la DescribeDomainAPI en el dominio de destino para obtener la configuración del clúster.
- Comprueba si el dominio del OpenSearch servicio está basado en Internet (público) o en Amazon Virtual Private Cloud (VPC).
- Crea una función pública o basada en Amazon VPC en AWS Lambda función de la configuración del clúster. Nota: La función Lambda contiene el código de solución de problemas que ejecuta las API de OpenSearch servicio en el clúster para determinar por qué el clúster está en rojo o amarillo.
- Elimina la función Lambda.
- Muestra las comprobaciones realizadas y los siguientes pasos recomendados para resolver el problema del clúster rojo o amarillo.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

El LambdaExecutionRole parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

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

Descripción general de la LambdaExecutionRole política:

A continuación, se muestra un ejemplo del rol de ejecución de una función Lambda (rol AWS Identity and Access Management (IAM)) que otorga a la función permiso para acceder a los AWS servicios y recursos que requiere este manual. Para obtener más información, consulte Rol de ejecución de Lambda.

> **Note**
>
> Los `ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface`, y solo `ec2:DeleteNetworkInterface` son necesarios si el clúster de OpenSearch servicio está basado en Amazon VPC para permitir que la función Lambda cree y gestione las interfaces de red de Amazon VPC. Para obtener más información, consulte Conexión de redes salientes a recursos en una función de ejecución de Amazon VPC y 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"
            }

        ]
    }
```

Instrucciones

Siga estos pasos para configurar la automatización:

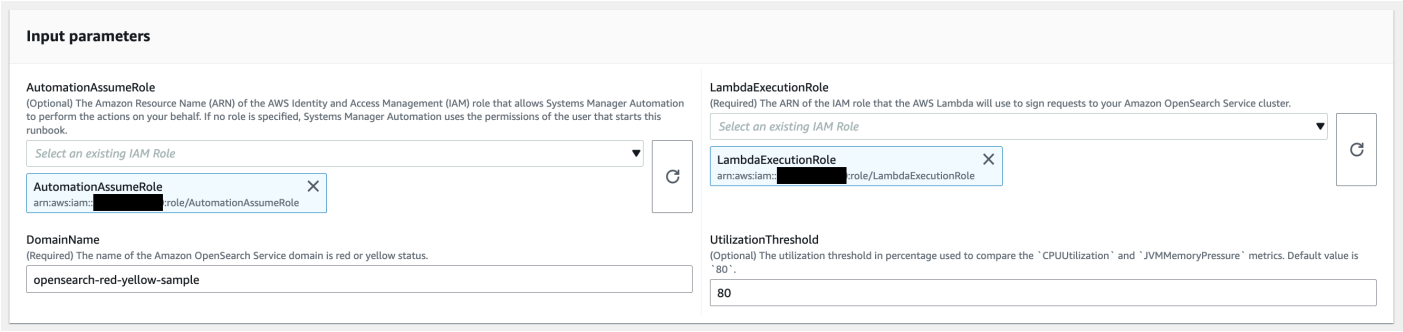
1. Navegue hasta el AWSSupport- TroubleshootOpenSearchRedYellowCluster en la consola. AWS Systems Manager
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
   - LambdaExecutionRole (Obligatorio):

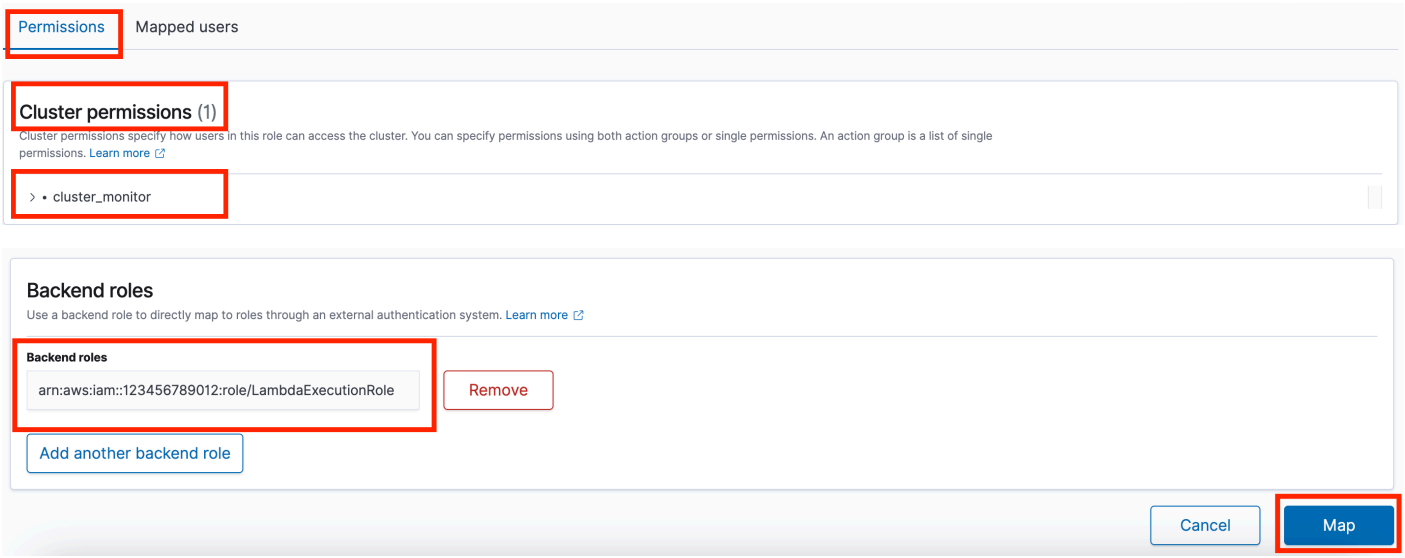
     El ARN de la función de IAM que Lambda utilizará para firmar las solicitudes a tu clúster de Amazon Service. OpenSearch
   - DomainName (Obligatorio):

     El nombre del dominio del OpenSearch servicio con el estado de salud del clúster en rojo o amarillo.
   - UtilizationThreshold (Opcional):

     El porcentaje del umbral de utilización utilizado para comparar las métricas de utilización de la CPU y de MemoryPressure JVM. El valor predeterminado es 80.



4. Si ha habilitado un control de acceso detallado en un clúster de OpenSearch servicios, asegúrese de que el `LambdaExecutionRole` rol arn esté asignado a un rol con al menos permiso. `cluster_monitor`



5. Seleccione Ejecutar.
6. Se inicia la automatización.
7. El manual de procedimientos de automatización realiza los siguientes pasos:
   - GetClusterConfiguration:

     Obtiene la configuración del clúster de servicios. OpenSearch
   - CreaAWSLambdaFunctionStack:

     Crea una función Lambda temporal en su cuenta mediante. AWS CloudFormation La función Lambda se utiliza para ejecutar las API de OpenSearch servicio.
   - WaitForAWSLambdaFunctionStack:

     Espera a que se complete la CloudFormation pila.

- GetClusterMetricsFromCloudWatch:

  Obtiene las métricas relacionadas con los clústeres de Amazon CloudWatch ClusterStatus, CPUUtilization y JVM MemoryPressure OpenSearch Service y su fecha de creación.

- RunOpenSearchAPIs:

  Utiliza la función Lambda para llamar a las API de OpenSearch servicio y analizar los datos de las métricas del clúster para diagnosticar la causa del estado rojo o amarillo del clúster.

- EliminarAWSLambdaFunctionStack:

  Elimina la función Lambda creada por esta automatización en su cuenta.

8. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

   - RootCause:

     Proporciona una descripción general de la causa identificada por la que el estado del clúster está en rojo o amarillo.

   - IssueDescription:

     Proporciona detalles sobre por qué el clúster está en estado rojo o amarillo y las posibles medidas para devolverlo al estado verde.

Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- Consulta Solución de problemas de Amazon OpenSearch Service para obtener más información

AWSSupport-TroubleshootOpenSearchHighCPU

Descripción

El AWSSupport-TroubleshootOpenSearchHighCPU manual proporciona una solución automatizada para recopilar datos de diagnóstico de un dominio de Amazon OpenSearch Service a fin de solucionar problemas de CPU elevados.

¿Cómo funciona?

El AWSSupport-TroubleshootOpenSearchHighCPU runbook ayuda a solucionar problemas de uso elevado de la CPU en el dominio de Amazon OpenSearch Service.

El manual de ejecución lleva a cabo los siguientes pasos:

- Ejecuta la DescribeDomainAPI en el dominio de Amazon OpenSearch Service proporcionado para obtener los metadatos del clúster.
- Comprueba si el dominio de Amazon OpenSearch Service es público o está basado en Amazon VPC y, con la ayuda de AWS CloudFormation, crea una función pública o basada en Amazon AWS Lambda VPC.
- La función Lambda obtiene datos de diagnóstico de los dominios de Amazon OpenSearch Service.
- Utiliza una máquina de AWS Step Functions estados para organizar múltiples ejecuciones de funciones Lambda a fin de recopilar datos más completos.
- De forma predeterminada, almacena los datos recopilados en un grupo de CloudWatch registros de Amazon durante 24 horas.
- Elimina los recursos creados, excepto el grupo de CloudWatch registros.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

El `LambdaExecutionRole` parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

La función de ejecución de Lambda otorga a la función permiso para acceder a AWS los servicios y recursos que requiere este manual. Para obtener más información, consulte Rol de ejecución de Lambda.

> **Note**
>
> Los `ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface`, y solo `ec2:DeleteNetworkInterface` son necesarios si el clúster de OpenSearch servicio está basado en Amazon VPC para permitir que la función Lambda cree y gestione las interfaces de red de Amazon VPC. Para obtener más información, consulte Conexión de redes salientes a recursos en una función de ejecución de Amazon VPC y Lambda.

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta la TroubleshootOpenSearchHighCPU AWSSupport - de la consola. AWS Systems Manager
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- DomainName (Obligatorio):

  El nombre del dominio de Amazon OpenSearch Service que quieres solucionar en caso de problemas de CPU elevada.

- LambdaExecutionRoleForOpenSearch (Obligatorio):

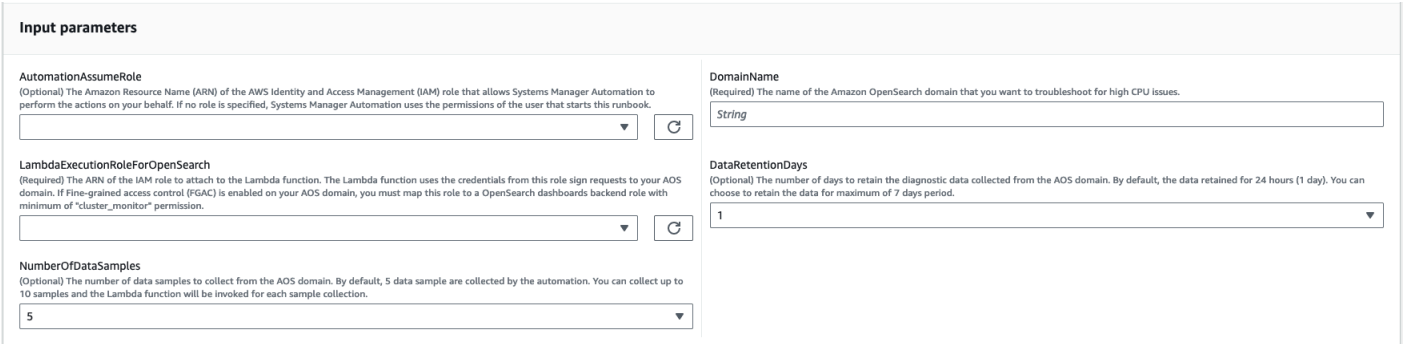
  El ARN de la función de IAM que se va a adjuntar a la función Lambda. La función Lambda usa las credenciales de este rol para firmar las solicitudes al dominio de Amazon OpenSearch Service. Si el control de acceso detallado está habilitado en el dominio de Amazon OpenSearch Service, debes asignar este rol a un rol de backend de OpenSearch Service Dashboards con un permiso mínimo de «cluster_monitor».

- DataRetentionDays (Opcional):

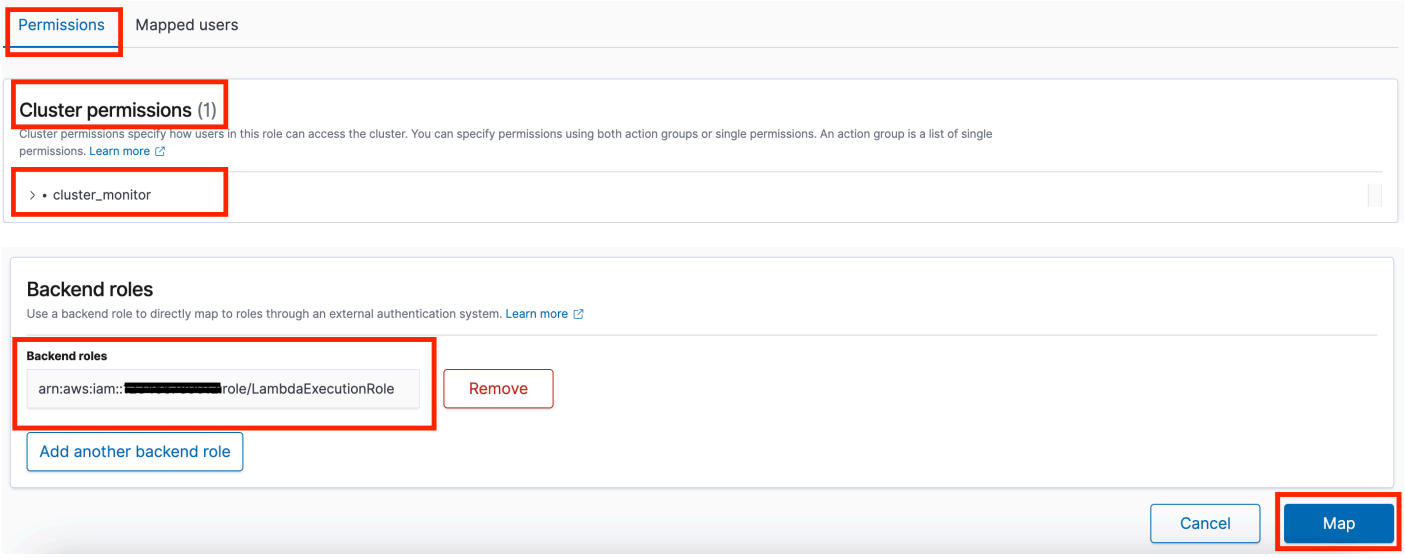
  El número de días que se conservarán los datos de diagnóstico recopilados del dominio de Amazon OpenSearch Service. De forma predeterminada, los datos se conservan durante 24 horas (un día). Puede optar por conservar los datos durante un máximo de 30 días.

- NumberOfDataSamples (Opcional):

  El número de muestras de datos que se van a recopilar del dominio OpenSearch de Amazon Service. De forma predeterminada, se recopilan 5 muestras de datos. Puede recopilar hasta 10 muestras y se invocará la función Lambda para cada colección de muestras.



4. Si ha habilitado un control de acceso detallado en un clúster de OpenSearch servicios, asegúrese de que el `LambdaExecutionRole` rol arn esté asignado a un rol con al menos permiso. `cluster_monitor`



5. Seleccione Ejecutar.
6. Se inicia la automatización.
7. El manual de procedimientos de automatización realiza los siguientes pasos:
   - Compruebe la simultaneidad:

     Garantiza que solo haya una ejecución de este runbook dirigida al dominio de Amazon OpenSearch Service especificado. Si el runbook encuentra otra ejecución dirigida al mismo nombre de dominio, devuelve un error y finaliza.
   - getDomainConfig:

     Obtiene los detalles de configuración del dominio de OpenSearch servicio de destino.
   - Recursos de aprovisionamiento:

     Aprovisiona los recursos para la recopilación de datos mediante AWS CloudFormation.
   - waitForStackCreación:

     Espera a que se complete la AWS CloudFormation pila.
   - describeStackResources:

     Describe la AWS CloudFormation pila y obtiene el ARN de la máquina de estados.
   - runStateMachine:

     Invoca la función Lambda del recopilador de datos una o más veces mediante la ejecución de una máquina de estados Step Functions.

- describeErrorsFromStackEvents:

  Describe los errores de la AWS CloudFormation pila de errores.

- unstageOpenSearchAlta automatización de la CPU:

  Elimina la pila. `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation

- describeErrorsFromStackDeletion:

  Describe los errores encontrados al eliminar la AWS CloudFormation pila.

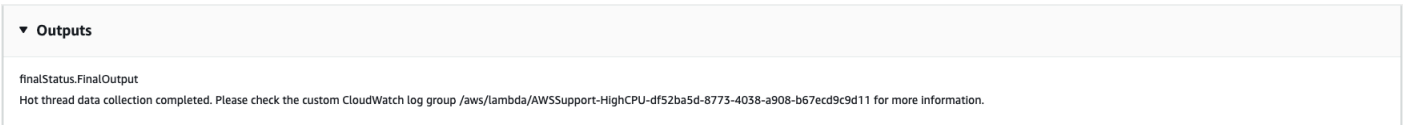
- Estado final:

  Devuelve el resultado final del runbook. `AWSSupport-TroubleshootOpenSearchHighCPU`

8. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

   - Estado final. FinalOutput:

     Proporciona el grupo de CloudWatch registros en el que se almacenan los datos de diagnóstico.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- Consulta Solución de problemas de Amazon OpenSearch Service para obtener más información

EventBridge

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon EventBridge. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

Descripción

El `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook añade una cadena de deduplicación para todas las AWS Systems Manager OpsItems asociadas a una regla de Amazon EventBridge . Este manual de procedimientos no agrega una cadena de deduplicación si una regla ya tiene una. Para obtener más información sobre las cadenas de deduplicación OpsItems, consulte Reducir la duplicación OpsItems en la Guía del AWS Systems Manager usuario.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DedupString

  Tipo: cadena

  Descripción: (obligatorio) la cadena de deduplicación que desea agregar a la regla.

- RuleName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la regla a la que desea agregar la cadena de deduplicación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Pasos de documentos

- `aws:executeScript`- Añade una cadena de deduplicación a la EventBridge regla que especifique en el `RuleName` parámetro.

AWS-DisableEventBridgeRule

Descripción

El *`AWS-DisableEventBridgeRule`* manual desactiva la EventBridge regla de Amazon que especifiques. Para obtener más información sobre las reglas EventBridge , consulta las reglas de Amazon EventBridge en la Guía del usuario de Amazon. EventBridge

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- EventBusNombre

  Tipo: cadena

  Valor predeterminado: default

  Descripción: (opcional) el bus de eventos asociado a la regla que desea deshabilitar.
- RuleName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la regla que desea deshabilitar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Pasos de documentos

- `aws:executeAwsApi`- Desactiva la EventBridge regla que especifique en el `RuleName` parámetro.

GuardDuty

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon GuardDuty. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-CreateGuardDutyDetector

`AWSConfigRemediation-CreateGuardDutyDetector`

Descripción

El `AWSConfigRemediation-CreateGuardDutyDetector` manual crea un detector Amazon GuardDuty (GuardDuty) en el Región de AWS lugar donde se ejecuta la automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Pasos de documentos

- `aws:executeAwsApi`- Crea un GuardDuty detector.
- `aws:assertAwsResourceProperty`: verifica que el `Status` del detector sea `ENABLED`.

IAM

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Identity and Access Management Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- 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

Descripción

Adjunta un rol AWS Identity and Access Management (de IAM) a una instancia gestionada.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ForceReplace

  Tipo: Booleano

  Descripción: (opcional) marcar para especificar si reemplazar el perfil de existente o no.

  Predeterminado: true

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia en la que desea asignar un rol de IAM.

- RoleName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del rol de IAM que se va a añadir a la instancia administrada.

Pasos de documentos

1. `aws:executeAwsApi`- DescribeInstanceProfile - Busque el perfil de instancia de IAM adjunto a la instancia EC2.
2. `aws:branch`- CheckInstanceProfileAssociations - Compruebe el perfil de instancia de IAM adjunto a la instancia EC2.
   a. Si un perfil de instancia de IAM se encuentra adjunto y `ForceReplace` está establecido en `true`:
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Desasocie el perfil de instancia de IAM de la instancia EC2.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Enumere los perfiles de instancia para la función de IAM proporcionada.
   c. `aws:branch`- CheckInstanceProfileCreated - Compruebe si el rol de IAM proporcionado tiene un perfil de instancia asociado.

i. Si el rol de IAM tiene un perfil de instancia asociado:

   A. `aws:executeAwsApi`- attachiAMProfileToInstance : asocie el rol de perfil de instancia de IAM a la instancia EC2.

i. Si el rol de IAM no tiene un perfil de instancia asociado:

   A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Cree un rol de perfil de instancia para el rol de IAM especificado.

   B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Adjunta el rol del perfil de instancia al rol de IAM especificado.

   C. `aws:executeAwsApi`- GetInstanceProfile - Obtenga los datos del perfil de la instancia para el rol de IAM especificado.

   D. `aws:executeAwsApi`- attachiAMProfileToInstanceWithRetry : asocie el rol de perfil de instancia de IAM a la instancia EC2.

Salidas

Vuelva a intentarlo con ProfileTo InstanceWith AttachiAM. AssociationId

GetInstancePerfil. InstanceProfileNombre

GetInstancePerfil. InstanceProfileArn

En una instancia de AttachiamProfileTo. AssociationId

ListInstanceProfilesForFunción. InstanceProfileNombre

ListInstanceProfilesForRol. InstanceProfileArn

`AWS-DeleteIAMInlinePolicy`

Descripción

El `AWS-DeleteIAMInlinePolicy` manual elimina todas las políticas integradas AWS Identity and Access Management (IAM) asociadas a las identidades de IAM que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- IamArns

  Tipo: cadena

  Descripción: (Obligatorio) Lista de ARN separados por comas para las identidades de IAM de las que desea eliminar las políticas integradas. Esta lista puede incluir usuarios, grupos o roles de IAM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Pasos de documentos

- `aws:executeScript`- Elimina las políticas integradas de IAM asociadas a las identidades de IAM de destino.

`AWSConfigRemediation-DeleteIAMRole`

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteIAMRole` elimina el rol de AWS Identity and Access Management (IAM) que especifique. Esta automatización no elimina los perfiles de instancia asociados al rol de IAM ni los roles vinculados al servicio.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAMRoleID

  Tipo: cadena

  Descripción: (obligatorio) el ID del rol de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Pasos de documentos

- `aws:executeScript`: recopila el nombre del rol de IAM que especifique en el parámetro `IAMRoleID`.
- `aws:executeScript`: recopila las políticas y los perfiles de instancia asociados al rol de IAM.
- `aws:executeScript`: elimina las políticas adjuntas.
- `aws:executeScript`: elimina el rol de IAM y verifica que el rol se haya eliminado.

AWSConfigRemediation-DeleteIAMUser

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteIAMUser` elimina el usuario de AWS Identity and Access Management (IAM) que especifique. Esta automatización elimina o separa los siguientes recursos asociados al usuario de IAM:

- Claves de acceso
- Políticas administradas asociadas
- Credenciales de Git
- Membresías a grupos de IAM

- Contraseña de usuario de IAM
- Políticas insertadas
- Uso de dispositivos de autenticación multifactor (MFA)
- Firma de certificados
- Clave SSH pública

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAM UserId

  Tipo: cadena

  Descripción: (obligatorio) el ID del usuario de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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

Pasos de documentos

- aws:executeScript: recopila el nombre de usuario del usuario de IAM que especifique en el parámetro IAMUserId.
- aws:executeScript: recopila las claves de acceso, los certificados, las credenciales, los dispositivos MFA y las claves SSH asociadas al usuario de IAM.

- `aws:executeScript`: recopila las membresías a grupos y las políticas del usuario de IAM.
- `aws:executeScript`: elimina las claves de acceso, los certificados, las credenciales, los dispositivos MFA y las claves SSH asociadas al usuario de IAM.
- `aws:executeScript`: elimina las membresías a grupos y las políticas del usuario de IAM.
- `aws:executeScript`: elimina el usuario de IAM y verifica que el usuario se haya eliminado.

AWSConfigRemediation-DeleteUnusedIAMGroup

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedIAMGroup` elimina un grupo de IAM que no contenga ningún usuario.

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedIAMGroup` elimina un grupo de IAM que no contenga ningún usuario.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- GroupName

Tipo: cadena

Descripción: (obligatorio) el nombre del grupo de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Pasos de documentos

- `aws:executeScript`: elimina las políticas de IAM gestionadas e insertadas asociadas al grupo de IAM de destino y, a continuación, elimina el grupo de IAM.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedIAMPolicy` elimina una política (de IAM) AWS Identity and Access Management que no está asociada a ningún usuario, grupo o función.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAM ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recurso de la política de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DeletePolicy`
- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Pasos de documentos

- `aws:executeScript`: elimina la política que especifique en el parámetro `IAMResourceId` y verifica que se haya eliminado.

AWSConfigRemediation-DetachIAMPolicy

Descripción

El manual de procedimientos `AWSConfigRemediation-DetachIAMPolicy` desvincula la política (de IAM) AWS Identity and Access Management que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAM ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la política de IAM que desea separar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`

- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy
- iam:DetachUserPolicy
- iam:GetPolicy
- iam:ListEntitiesForPolicy

Pasos de documentos

- aws:executeScript: separa la política de IAM de todos los recursos.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descripción

El AWSConfigRemediation-EnableAccountAccessAnalyzer manual crea un analizador de acceso AWS Identity and Access Management (IAM) en su. Cuenta de AWS Para obtener información acerca de Access Analyzer, consulte Cómo utilizar IAM Access Analyzer de AWS en la Guía del usuario de IAM.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AnalyzerName

  Tipo: cadena

  Descripción: (obligatorio) nombre de la analizadora que se va a crear.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Pasos de documentos

- `aws:executeAwsApi`: crea un analizador de acceso para su cuenta.
- `aws:waitForAwsResourceProperty`: espera a que el estado del analizador de acceso sea `ACTIVE`.
- `aws:assertAwsResourceProperty`: confirma que el estado del analizador de acceso sea `ACTIVE`.

AWSSupport-GrantPermissionsToIAMUser

Descripción

Este manual de procedimientos concede los permisos especificados a un grupo de IAM (nuevo o existente) y añade el usuario de IAM existente. Las políticas que puede elegir: Billing o Support. Para

habilitar el acceso de facturación para IAM, recuerde activar también el acceso del usuario de IAM y del usuario federado a las páginas de facturación y administración de costos.

> **Important**
>
> Si proporciona un grupo de IAM existente, todos los usuarios actuales de IAM en el grupo de reciben los nuevos permisos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- IAM GroupName

  Tipo: cadena

  Predeterminado: ExampleSupportAndBillingGroup

  Descripción: (obligatorio) puede ser un grupo nuevo o existente. Debe cumplir con Límites de nombres de entidades de IAM.
- IAM UserName

Tipo: cadena

Predeterminado: ExampleUser

Descripción: (obligatorio) debe ser un usuario existente.

- LambdaAssumeRol

  Tipo: cadena

  Descripción: (opcional) el ARN del rol asumido por Lambda.

- Permisos

  Tipo: cadena

  Valores válidos: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  Predeterminado: SupportAndBillingFullAccess

  Descripción: (obligatorio) elija una de estas opciones: `SupportFullAccess` concede acceso completo al centro de soporte | `BillingFullAccess` concede acceso completo al panel de facturación | `SupportAndBillingFullAccess` concede acceso completo tanto al centro de soporte como al panel de facturación. Más información sobre las políticas en Detalles del documento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Los permisos necesarios dependen de cómo se ejecute `AWSSupport-GrantPermissionsToIAMUser`.

En ejecución como usuario o rol que ha iniciado sesión actualmente

Se recomienda tener asociada la política administrada `AmazonSSMAutomationRole` de Amazon y los siguientes permisos adicionales para poder crear la función de Lambda y el rol de IAM que pasar a 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" : "*"
                        }
                    ]
                }
```

Uso AutomationAssumeRole y LambdaAssumeRole

El usuario debe tener los permisos ssm: StartAutomation Execution en el runbook e iam: PassRole en las funciones de IAM, transferidas como AutomationAssume rol y rol. LambdaAssume A continuación se incluyen los permisos que necesita cada rol de IAM:

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

Pasos de documentos

1. `aws:createStack`- Ejecute la AWS CloudFormation plantilla para crear una función Lambda.
2. `aws:invokeLambdaFunction`: para configurar permisos de IAM para Lambda.
3. `aws:deleteStack`- Eliminar CloudFormation plantilla.

Salidas

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

Descripción

El manual de procedimientos `AWSConfigRemediation-RemoveUserPolicies` elimina las políticas insertadas de AWS Identity and Access Management (IAM) y separa las políticas gestionadas asociadas al usuario que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAMUserID

  Tipo: cadena

  Descripción: (obligatorio) el ID del usuario del que desea eliminar políticas.
- PolicyType

Tipo: cadena

Valores válidos: All | Inline | Managed

Valor predeterminado: All

Descripción: (obligatorio) el tipo de políticas de IAM que desea eliminar del usuario.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Pasos de documentos

- `aws:executeScript`: elimina y separa las políticas de IAM del usuario que especifique en el parámetro `IAMUserID`.

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descripción

El `AWSConfigRemediation-ReplaceIAMInlinePolicy` manual reemplaza una política en línea AWS Identity and Access Management (IAM) por una política de IAM administrada replicada. En el caso de una política insertada asociada a un usuario, grupo o función, los permisos de la política insertada se clonan en una política de IAM gestionada. La política de IAM gestionada se añade al recurso y la política integrada se elimina. AWS Config debe estar habilitada en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- InlinePolicyNombre

  Tipo: StringList

  Descripción: (obligatoria) la política de IAM insertada que desea reemplazar.
- ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el ID del usuario, grupo o rol de IAM cuya política insertada desea reemplazar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- aws:executeScript: sustituya la política de IAM insertada por una política AWS replicada en el recurso que especifique.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Descripción

El AWSConfigRemediation-RevokeUnusedIAMUserCredentials manual revoca las contraseñas no utilizadas AWS Identity and Access Management (IAM) y las claves de acceso activas. Este manual también desactiva las claves de acceso caducadas y elimina los perfiles de inicio de sesión caducados. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- IAM ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el ID del recurso de IAM del que desea revocar las credenciales no utilizadas.
- MaxCredentialUsageAge

  Tipo: cadena

  Predeterminado: 90

  Descripción: (obligatorio) el número de días en los que se debe haber utilizado la credencial.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`

- iam:DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

Pasos de documentos

- aws:executeScript: revoca las credenciales de IAM del usuario especificado en el parámetro IAMResourceId. Las claves de acceso caducadas se desactivan y los perfiles de inicio de sesión caducados se eliminan.

> **Note**
>
> Asegúrese de configurar el MaxCredentialUsageAge parámetro de esta acción correctiva para que coincida con el maxAccessKeyAge parámetro de la AWS Config regla que utiliza para activar esta acción: access-keys-rotated.

AWSConfigRemediation-SetIAMPasswordPolicy

Descripción

El manual de procedimientos AWSConfigRemediation-SetIAMPasswordPolicy establece la política de contraseñas de usuario de AWS Identity and Access Management (IAM) para su Cuenta de AWS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- AllowUsersToChangeContraseña

  Tipo: Booleano

  Predeterminado: false

  Descripción: (Opcional) Si se establece en`true`, todos los usuarios de IAM de su Cuenta de AWS cuenta pueden utilizarla AWS Management Console para cambiar sus contraseñas.
- HardExpiry

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si se establece en `true`, los usuarios de IAM no pueden restablecer sus contraseñas una vez caducada la contraseña.
- MaxPasswordEdad

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) el número de días que la contraseña de un usuario de IAM es válida.
- MinimumPasswordLongitud

  Tipo: entero

  Valor predeterminado: 6

Descripción: (opcional) el número mínimo de caracteres que puede tener la contraseña de un usuario de IAM.

- PasswordReusePrevención

  Tipo: entero

  Predeterminado: 0

  Descripción: (opcional) el número de contraseñas anteriores que un usuario de IAM no puede reutilizar.

- RequireLowercasePersonajes

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener una minúscula del alfabeto latino básico ISO (de la a a la z).

- RequireNumbers

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter numérico (del 0 al 9).

- RequireSymbols

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter que no sea alfanumérico (! @ # $ % ^ * ( ) _ + - = [ ] { } | ').

- RequireUppercasePersonajes

  Tipo: Booleano

  Predeterminado: false

Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter en mayúscula del alfabeto latino básico ISO (de la A a la Z).

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Pasos de documentos

- `aws:executeScript`: establece la política de contraseñas de usuario de IAM en función de los valores que especifique para los parámetros del manual de procedimientos de su Cuenta de AWS.

Amazon Kinesis Data Streams

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Kinesis Data Streams. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableKinesisStreamEncryption

`AWS-EnableKinesisStreamEncryption`

Descripción

El `AWS-EnableKinesisStreamEncryption` manual permite el cifrado en Amazon Kinesis Data Streams (Kinesis Data Streams). Las aplicaciones de los productores que escriban en una

transmisión cifrada encontrarán errores si no tienen acceso a la clave AWS Key Management Service ()AWS KMS.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- KinesisStreamName

  Tipo: cadena

  Descripción: (obligatorio) El nombre de la transmisión en la que quieres activar el cifrado.
- KeyId

  Tipo: cadena

  Predeterminado: alias/aws/kinesis

  Descripción: (Obligatoria) La AWS KMS clave gestionada por el cliente que desea utilizar para el cifrado. Este valor puede ser un identificador único global, un ARN para un alias o una clave, o un nombre de alias con el prefijo «alias/». También puede utilizar la clave AWS gestionada mediante el valor predeterminado del parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Pasos de documentos

- VerifyKinesisStreamStatus (aws: waitforAwsResource Property): comprueba el estado de Kinesis Data Streams.
- EnableKinesisStreamEncryption (aws:executeAwsApi) - Habilita el cifrado de Kinesis Data Streams.
- VerifyKinesisStreamUpdateComplete (aws: waitForAwsResourceProperty) - Espera a que el estado de Kinesis Data Streams vuelva a ser. `ACTIVE`
- VerifyKinesisStreamEncryption (aws: assertAwsResource Property): verifica que el cifrado esté habilitado para Kinesis Data Streams.

AWS KMS

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Key Management Service Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

AWSConfigRemediation-CancelKeyDeletion

Descripción

El `AWSConfigRemediation-CancelKeyDeletion` manual cancela la eliminación de la clave gestionada por el cliente AWS Key Management Service (AWS KMS) que especifiques.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- KeyId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la clave gestionada por el cliente cuya eliminación desea cancelar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion
- kms:DescribeKey

Pasos de documentos

- aws:executeAwsApi: cancela la eliminación de la clave gestionada por el cliente que especifique en el parámetro KeyId.
- aws:assertAwsResourceProperty: confirma que la eliminación de claves está deshabilitada en la clave gestionada por el cliente.

AWSConfigRemediation-EnableKeyRotation

Descripción

El AWSConfigRemediation-EnableKeyRotation manual permite la rotación automática de claves para la clave simétrica AWS Key Management Service (AWS KMS) gestionada por el cliente.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KeyId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la clave gestionada por el cliente en la que desea activar la rotación automática de claves.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Pasos de documentos

- `aws:executeAwsApi`: habilita la rotación automática de claves en la clave gestionada por el cliente que especifique en el parámetro `KeyId`.
- `aws:assertAwsResourceProperty`: confirma que la rotación automática de claves está habilitada en su clave administrada por el cliente.

Lambda

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Lambda Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

Descripción

El `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` manual de ejecución permite el rastreo AWS X-Ray en tiempo real de la AWS Lambda función que especifique en el parámetro. `FunctionName`

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- FunctionName

  Tipo: cadena

  Descripción: (obligatorio) el nombre o ARN de la función de Lambda en la que se habilitará el seguimiento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: permite el trazado de X-Ray en la función de Lambda que especifique en el parámetro `FunctionName`.
- `aws:assertAwsResourceProperty`: verifica que el trazado de X-Ray esté activado en la función de Lambda.

Salidas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Respuesta de la llamada a la `UpdateFunctionConfiguration` API.

AWSConfigRemediation-DeleteLambdaFunction

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteLambdaFunction` elimina la función AWS Lambda que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- LambdaFunctionNombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la función de Lambda que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Pasos de documentos

- `aws:executeAwsApi`: elimina la función de Lambda especificada en el parámetro `LambdaFunctionName`.

- `aws:executeScript`: verifica que se ha eliminado la función de Lambda.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Descripción

El `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook cifra, en reposo, las variables de entorno de la función (AWS Lambda Lambda) que especifique mediante una clave AWS Key Management Service (AWS KMS) gestionada por el cliente. Este manual de procedimientos solo debe usarse como referencia para garantizar que las variables de entorno de la función de Lambda estén cifradas de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varias funciones con diferentes claves administradas por el cliente.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- FunctionName

  Tipo: cadena

Descripción: (obligatorio) el nombre o ARN de la función de Lambda cuyas variables de entorno desea cifrar.

- KMS KeyArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la clave gestionada por el AWS KMS cliente que desea utilizar para cifrar las variables de entorno de la función Lambda.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Pasos de documentos

- `aws:waitForAwsResourceProperty`: espera a que el `LastUpdateStatus` de la propiedad sea `Successful`.
- `aws:executeAwsApi`- Cifra las variables de entorno de la función Lambda que especifique en `FunctionName` el parámetro mediante la clave gestionada por AWS KMS el cliente que especifique en `KMSKeyArn` el parámetro.
- `aws:assertAwsResourceProperty`: confirma que el cifrado está habilitado en las variables de entorno de la función de Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descripción

El manual de procedimientos `AWSConfigRemediation-MoveLambdaToVPC` mueve una función de AWS Lambda (Lambda) a una Amazon Virtual Private Cloud (Amazon VPC).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- FunctionName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la función de Lambda que se va a migrar a una Amazon VPC.
- SecurityGroupIds

  Tipo: cadena

  Descripción: (obligatorio) los ID de los grupos de seguridad que desea asignar a las interfaces de red elásticas (ENI) asociadas a su función de Lambda.
- SubnetIds

  Tipo: cadena

  Descripción: (obligatorio) los ID de subred que desea crear para las interfaces de red elásticas (ENI) asociadas a su función de Lambda.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Pasos de documentos

- `aws:executeAwsApi`: actualiza la configuración de Amazon VPC para la función de Lambda que especifique en el parámetro `FunctionName`.
- `aws:waitForAwsResourceProperty`: espera a que el `LastUpdateStatus` de la función de Lambda sea `successful`.
- `aws:executeScript`: verifica que la configuración de Amazon VPC de la función de Lambda se haya actualizado correctamente.

AWSSupport-RemediateLambdaS3Event

Descripción

El `AWSSupport-TroubleshootLambdaS3Event` manual proporciona una solución automatizada para los procedimientos descritos en los artículos del AWS Knowledge Center ¿Por qué mi notificación de eventos de Amazon S3 no activa mi función Lambda? y ¿Por qué aparece el error «No se pueden validar las siguientes configuraciones de destino» al crear una notificación de evento de Amazon S3 para activar mi función Lambda? Este manual le ayuda a identificar y solucionar los motivos por los que una notificación de evento de Amazon Simple Storage Service (Amazon S3) no pudo activar la función que especificó. AWS Lambda Si el resultado del manual de procedimientos sugiere validar y configurar la simultaneidad de la función de Lambda, consulte Invocación asíncrona y Escalado de funciones de AWS Lambda.

> **Note**
>
> Los errores “Unable to validate the following destination configurations” también pueden producirse debido a configuraciones de eventos incorrectas de Amazon S3 de Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Queue Service (Amazon SQS). Este manual de procedimientos solo comprueba las configuraciones de la función de Lambda. Si, después de usar el manual de procedimientos sigue recibiendo el error “Unable to validate the following destination configurations”, por favor revise las configuraciones de eventos de Amazon S3 de Amazon SNS y Amazon SQS existentes.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LambdaFunctionArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN de la función de Lambda.

- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuyas notificaciones de eventos activan la función de Lambda.

- Acción

  Tipo: cadena

  Valores válidos: Troubleshoot | Remediate

  Descripción: (obligatoria) la acción que desea que realice el manual de procedimientos. La opción `Troubleshoot` ayuda a identificar cualquier problema, pero no realiza ninguna acción de mutación para resolver el problema. La opción `Remediate` ayuda a identificar los problemas e intenta resolverlos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Pasos de documentos

- `aws:branch`: se ramifica en función de la entrada especificada para el parámetro `Action`.

  Si el valor especificado es `Troubleshoot`:

- `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSSupport-TroubleshootLambdaS3Event`.
- `aws:executeAwsApi`: comprueba el resultado del manual de procedimientos `AWSSupport-TroubleshootLambdaS3Event`que se ejecutó en el paso anterior.

Si el valor especificado es `Remediate`:

- `aws:executeScript`: ejecuta un script para solucionar los problemas descritos en la sección ¿Por qué mi notificación de eventos de Amazon S3 no activa mi función de Lambda? y ¿Por qué aparece el error “Unable to validate the following destination configurations” al crear una notificación de evento de Amazon S3 para activar mi función de Lambda? Artículos del Centro de conocimientos.

Salidas

checkoutput.Output

remediatelambdas3event.Output

AWSSupport-TroubleshootLambdaInternetAccess

Descripción

El `AWSSupport-TroubleshootLambdaInternetAccess` manual le ayuda a solucionar problemas de acceso a Internet para una AWS Lambda función que se lanzó en Amazon Virtual Private Cloud (Amazon VPC). Se revisan recursos como las rutas de subred, las reglas de los grupos de seguridad y las reglas de la lista de control de acceso (ACL) de red para confirmar que se permite el acceso saliente a Internet.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- FunctionName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la función de Lambda para la que desea solucionar problemas de acceso a Internet.
- destinationIp

  Tipo: cadena

  Descripción: (obligatoria) la dirección IP de destino con la que desea establecer una conexión saliente.
- destinationPort

  Tipo: cadena

  Predeterminado: 443

  Descripción: (opcional) el puerto de destino en el que desea establecer una conexión saliente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`

- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls

Pasos de documentos

- aws:executeScript: verifica la configuración de varios recursos de VPC en la que se lanzó la función de Lambda.
- aws:branch: se ramifica en función de si la función de Lambda especificada está en una VPC o no.
- aws:executeScript: revisa las rutas de la tabla de enrutamiento de la subred en la que se lanzó la función de Lambda y verifica que estén presentes las rutas a una puerta de enlace de traducción de direcciones de red (NAT) y a una puerta de enlace de Internet. Confirma que la función de Lambda no está en una subred pública.
- aws:executeScript: verifica que el grupo de seguridad asociado a la función de Lambda permita el acceso saliente a Internet en función de los valores especificados para los parámetros destinationIp y destinationPort.
- aws:executeScript: verifica las reglas de ACL asociadas a las subredes de la función de Lambda y la puerta de enlace NAT que permiten el acceso saliente a Internet en función de los valores especificados para los parámetros destinationIp y destinationPort.

Salidas

checkVpc.vpc: el ID de VPC en la que se lanzó la función de Lambda.

checkVpc.subnet: los ID de las subredes en las que se lanzó la función de Lambda.

checkVpc.securityGroups: grupos de seguridad asociados a la función de Lambda.

checkNACL.NACL: mensaje de análisis con nombres de recursos. LambdaIp hace referencia a la dirección IP privada de la interfaz de red elástica de la función de Lambda. El objeto LambdaIpRules solo se genera para las subredes que tienen una ruta a una puerta de enlace NAT. A continuación se muestra un ejemplo de la salida.

```
{
   "subnet-1234567890":{
      "NACL":"acl-1234567890",
      "destinationIp_Egress":"Allowed",
```

```
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule",
      "LambdaIpRules":{
         "{LambdaIp}":{
            "Egress":"notAllowed",
            "Ingress":"notAllowed",
            "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
 rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
 IP in your egress and ingress NACL rules"
         }
      }
   },
   "subnet-0987654321":{
      "NACL":"acl-0987654321",
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule"
   }
}
```

check SecurityGroups .secgrps: análisis del grupo de seguridad asociado a la función Lambda. A continuación se muestra un ejemplo de la salida.

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets: análisis de las subredes de su VPC asociadas con su función de Lambda. A continuación se muestra un ejemplo de la salida.

```
{
   "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

Descripción

El `AWSSupport-TroubleshootLambdaS3Event` manual proporciona una solución automatizada para los procedimientos descritos en los artículos del AWS Knowledge Center ¿Por qué mi notificación de eventos de Amazon S3 no activa mi función Lambda? y ¿Por qué aparece el error «No se pueden validar las siguientes configuraciones de destino» al crear una notificación de evento de Amazon S3 para activar mi función Lambda? Este manual le ayuda a identificar por qué una notificación de evento de Amazon Simple Storage Service (Amazon S3) no pudo activar AWS Lambda la función que especificó. Si el resultado del manual de procedimientos sugiere validar y configurar la simultaneidad de la función de Lambda, consulte Invocación asíncrona y Escalado de funciones de AWS Lambda.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LambdaFunctionArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN de la función de Lambda que activa la notificación de eventos de Amazon S3.

- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuyas notificaciones de eventos activan la función de Lambda.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Pasos de documentos

- `aws:executeScript`: ejecuta el script para validar los ajustes de configuración de la notificación de eventos de Amazon S3. Valida la política de IAM basada en recursos para la función Lambda y genera un comando AWS Command Line Interface (AWS CLI) para añadir los permisos necesarios si faltan los permisos necesarios en la política. Valida las políticas de recursos de otras funciones de Lambda que forman parte de las notificaciones de eventos para el mismo bucket de S3 y genera AWS CLI un comando como resultado si faltan los permisos necesarios.

Salidas

lambdaS3Event.output

Amazon Managed Workflows para Apache Airflow

AWS Systems Manager Automation proporciona manuales predefinidos para Amazon Managed Workflows para Apache Airflow. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSSupport-TroubleshootMWAAEnvironmentCreation

AWSSupport-TroubleshootMWAAEnvironmentCreation

Descripción

El `AWSSupport-TroubleshootMWAAEnvironmentCreation` manual proporciona información para depurar los problemas de creación del entorno Amazon Managed Workflows for Apache Airflow (Amazon MWAA) y realizar comprobaciones junto con los motivos documentados haciendo todo lo posible para ayudar a identificar el error.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Recupera los detalles del entorno de Amazon MWAA.
- Verifica los permisos de la función de ejecución.
- Comprueba si el entorno tiene permisos para usar la AWS KMS clave proporcionada para el registro y si existe el grupo de CloudWatch registros requerido.
- Analiza los registros del grupo de registros proporcionado para localizar cualquier error.
- Comprueba la configuración de la red para comprobar si el entorno Amazon MWAA tiene acceso a los puntos de conexión necesarios.
- Genera un informe con los resultados.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

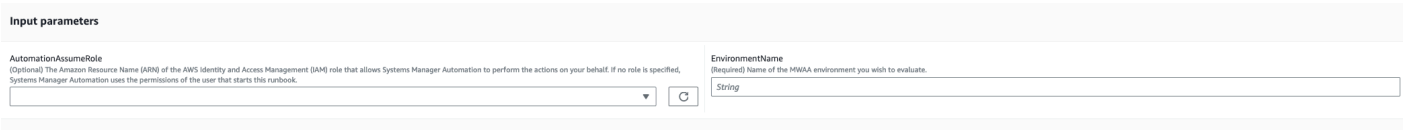
Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-TroubleshootMWAAEnvironmentCreation`Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
   - EnvironmentName (Obligatorio):

     Nombre del entorno de Amazon MWAA que desea evaluar.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - **`GetMWAAEnvironmentDetails:`**

     Recupera los detalles del entorno de Amazon MWAA. Si este paso no funciona, el proceso de automatización se detendrá y aparecerá como. `Failed`
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Verifica que la función de ejecución tenga los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Si detecta una clave gestionada por el cliente AWS Key Management Service (AWS KMS),

la automatización valida los permisos necesarios de la clave. En este paso, se emplea la `iam:SimulateCustomPolicy` API para determinar si la función de ejecución de la automatización cumple con todos los permisos necesarios.

- **`CheckKMSPolicyOnKMSKey:`**

  Comprueba si la política de AWS KMS claves permite que el entorno MWAA de Amazon utilice la clave para cifrar CloudWatch los registros. Si la AWS KMS clave está AWS gestionada, la automatización omite esta comprobación.

- **`CheckIfRequiredLogGroupsExists:`**

  Comprueba si existen los grupos de CloudWatch registros necesarios para el entorno Amazon MWAA. Si no es así, la automatización comprueba si hay CloudTrail eventos`CreateLogGroup`. `DeleteLogGroup` En este paso también se comprueban los `CreateLogGroup` eventos.

- **`BranchOnLogGroupsFindings:`**

  Las ramificaciones se basan en la existencia de grupos de CloudWatch registros relacionados con el entorno de Amazon MWAA. Si existe al menos un grupo de registros, la automatización lo analiza para localizar los errores. Si no hay ningún grupo de registros, la automatización omite el siguiente paso.

- **`CheckForErrorsInLogGroups:`**

  Analiza los grupos de CloudWatch registros para localizar los errores.

- **`GetRequiredEndPointsDetails:`**

  Recupera los puntos de enlace del servicio utilizados por el entorno Amazon MWAA.

- **`CheckNetworkConfiguration:`**

  Verifica que la configuración de red del entorno Amazon MWAA cumpla con los requisitos, incluidas las comprobaciones de los grupos de seguridad, las ACL de red, las subredes y las configuraciones de las tablas de enrutamiento.

- **`CheckEndpointsConnectivity:`**

  Invoca la automatización `AWSSupport-ConnectivityTroubleshooter` secundaria para validar la conectividad de la MWAA de Amazon con los puntos de conexión necesarios.

- **`CheckS3BlockPublicAccess:`**

Comprueba si el bucket Amazon S3 del entorno de Amazon MWAA está `Block Public Access` activado y también revisa la configuración general de Amazon S3 Block Public Access de la cuenta.

- **`GenerateReport:`**

  Recopila información de la automatización e imprime el resultado o la salida de cada paso.

7. Una vez completado, revise la sección de resultados para ver los resultados detallados de la ejecución:
   - Comprobación de los permisos de ejecución del entorno Amazon MWAA:

     Comprueba si la función de ejecución tiene los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Si se detecta una AWS KMS clave gestionada por el cliente, la automatización valida los permisos necesarios de la clave.
   - Comprobación de la política AWS KMS clave del entorno de Amazon MWAA:

     Comprueba si la función de ejecución posee los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Además, si se detecta una AWS KMS clave administrada por el cliente, la automatización comprueba los permisos necesarios para la clave.
   - Comprobar los grupos de CloudWatch registros del entorno de Amazon MWAA:

     Comprueba si existen los grupos de CloudWatch registros necesarios para el entorno Amazon MWAA. Si no es así, la automatización comprueba la ubicación de CloudTrail `CreateLogGroup` los `DeleteLogGroup` eventos.
   - Comprobación de las tablas de enrutamiento del entorno Amazon MWAA:

     Comprueba si las tablas de enrutamiento de Amazon VPC del entorno Amazon MWAA están configuradas correctamente.
   - Comprobación de los grupos de seguridad del entorno Amazon MWAA:

     Comprueba si los grupos de seguridad de Amazon VPC del entorno MWAA están configurados correctamente.
   - Comprobación de las ACL de red del entorno Amazon MWAA:

     Comprueba si los grupos de seguridad de Amazon VPC del entorno de Amazon MWAA están configurados correctamente.

- Comprobación de las subredes del entorno Amazon MWAA:

  Comprueba si las subredes del entorno Amazon MWAA son privadas.

- Para comprobar el entorno de Amazon MWAA, se requería la conectividad de los puntos finales:

  Verifica si el entorno Amazon MWAA puede acceder a los puntos de enlace necesarios. Para ello, la automatización invoca la automatización. `AWSSupport-ConnectivityTroubleshooter`

- Comprobación del entorno Amazon MWAA (bucket de Amazon S3):

  Comprueba si el bucket Amazon S3 del entorno de Amazon MWAA está `Block Public Access` activado y también revisa la configuración de Amazon S3 Block Public Access de la cuenta.

- La comprobación de los CloudWatch registros del entorno de Amazon MWAA agrupa errores:

  Analiza los grupos de CloudWatch registros existentes del entorno Amazon MWAA para localizar los errores.

Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

Neptune

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Neptune. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Descripción

El `AWS-EnableNeptuneDbAuditLogsToCloudWatch` runbook le ayuda a enviar los registros de auditoría de un clúster de base de datos de Amazon Neptune a Amazon CloudWatch Logs.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- DbClusterResourceId

  Tipo: cadena

  Descripción: (obligatorio) El ID de recurso del clúster de base de datos de Neptune para el que desea habilitar los registros de auditoría.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Devuelve el ID del clúster de base de datos de Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property): verifica que el tipo de motor Neptune DB sea. `neptune`
- EnableNeptuneDbAuditLogs (aws:executeAwsApi) - Permite enviar CloudWatch registros de auditoría para el clúster de base de datos de Neptune.
- VerifyNeptuneDbStatus (aws: waitAwsResource Property): verifica que el estado del clúster de base de datos de Neptune sea. `available`
- VerifyNeptuneDbAuditLogs (AWS:Executescript): verifica que los registros de auditoría se hayan configurado correctamente para enviarlos a Logs. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

Descripción

El AWS-EnableNeptuneDbBackupRetentionPeriod runbook le ayuda a habilitar las copias de seguridad automatizadas con un período de retención de las copias de seguridad de entre 7 y 35 días para un clúster de base de datos de Amazon Neptune.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- DbClusterResourceId

  Tipo: cadena

  Descripción: (Obligatorio) El ID de recurso del clúster de base de datos de Neptune para el que desea habilitar las copias de seguridad.
- BackupRetentionPeriod

  Tipo: entero

  Valores válidos: 7-35

Descripción: (Obligatorio) El número de días que se conservan las copias de seguridad.

- PreferredBackupWindow

  Tipo: cadena

  Descripción: (opcional) Un período de tiempo diario de al menos 30 minutos para realizar las copias de seguridad. El valor debe estar en hora universal coordinada (UTC) y usar el formato:`hh24:mm-hh24:mm`. El período de retención de la copia de seguridad no puede entrar en conflicto con el período de mantenimiento preferido.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Devuelve el ID del clúster de base de datos de Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property): verifica que el tipo de motor Neptune DB sea. `neptune`
- VerifyNeptuneDbStatus (aws: waitAwsResource Property): verifica que el estado del clúster de base de datos de Neptune sea. `available`
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Establece el período de retención del clúster de base de datos Neptune.
- VerifyNeptuneDbBackupsEnabled (AWS:Executescript) - Verifica que el período de retención y la ventana de respaldo se hayan establecido correctamente.

AWS-EnableNeptuneClusterDeletionProtection

Descripción

El `AWS-EnableNeptuneClusterDeletionProtection` runbook permite la protección contra la eliminación del clúster de Amazon Neptune que especifique.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Management que permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- DbClusterResourceId

  Tipo: cadena

  Descripción: (Obligatorio) El ID del clúster de Neptune en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Devuelve el ID del clúster de base de datos de Neptune.
- VerifyNeptuneDbEngine (aws: assertAwsResource Property): verifica el tipo de motor del clúster de base de datos especificado. `neptune`
- VerifyNeptuneStatus (aws: waitForAwsResourceProperty) - Verifica que el estado del clúster sea. `available`
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi) - Habilita la protección contra la eliminación en el clúster de base de datos Neptune.
- VerifyNeptuneDbDeletionProtection (aws: assertAwsResource Property) - Verifica que la protección contra la eliminación esté habilitada en el clúster de base de datos.

Salidas

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - El resultado de la operación de la API.

Amazon RDS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Relational Database Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- 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

Descripción

El `AWS-CreateEncryptedRdsSnapshot` runbook crea una instantánea cifrada a partir de una instancia no cifrada de Amazon Relational Database Service (Amazon RDS).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BASE DE DATOS InstanceIdentifier

  Tipo: cadena

  Descripción: (obligatorio) El ID de la instancia de Amazon RDS de la que desea crear una instantánea.

- BASE DE DATOS SnapshotIdentifier

  Tipo: cadena

  Descripción: (opcional) La plantilla de nombres de la instantánea de Amazon RDS. La plantilla de nombres predeterminada es *`DB InstanceIdentifier -yyyymmddhhmmss`*.

- DB cifrada SnapshotIdentifier

Tipo: cadena

Descripción: (opcional) Nombre de la instantánea cifrada. El nombre predeterminado es el valor que especifique para el `DBSnapshotIdentifier` parámetro adjunto. `-encrypted`

- InstanceTags

  Tipo: cadena

  Descripción: etiquetas (opcionales) para añadir a la instancia de base de datos. (Ejemplo: key=tagkey1, value=tagvalue1; key=tagkey2, value=tagValue2) '

- KmsKeyId.

  Tipo: cadena

  Valor predeterminado: `alias/aws/rds`

  Descripción: (opcional) El ARN, el identificador de clave o el alias de la clave gestionada por el cliente que desee utilizar para cifrar la instantánea.

- SnapshotTags

  Tipo: cadena

  Descripción: (opcional) Etiquetas para añadir a la instantánea. (Ejemplo: key=tagKey1, value=tagValue1; key=TagKey2, value=tagValue2) '

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Pasos de documentos

- `aws:executeScript`- Crea una instantánea de la instancia de base de datos que especifique en el parámetro. `DBInstanceIdentifier`
- `aws:executeScript`- Comprueba que la instantánea creada en el paso anterior existe y existe`available`.
- `aws:executeScript`- Copia la instantánea creada anteriormente en una instantánea cifrada.
- `aws:executeScript`- Verifica la existencia de la instantánea cifrada creada en el paso anterior.

Salidas

CopyRdsSnapshotToEncryptedRdsInstantánea. EncryptedSnapshotId - El ID de la instantánea cifrada de Amazon RDS.

AWS-CreateRdsSnapshot

Descripción

Crea una instantánea de Amazon Relational Database Service (Amazon RDS) de una instancia de Amazon RDS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DB InstanceIdentifier

  Tipo: cadena

  Descripción: (obligatorio) El InstanceId ID de base de datos de la instancia de RDS desde la que se va a crear la instantánea.

- Base de datos SnapshotIdentifier

  Tipo: cadena

  Descripción: (opcional) El SnapshotIdentifier ID de base de datos de la instantánea de RDS que se va a crear.

- InstanceTags

  Tipo: cadena

  Descripción: (opcional) etiquetas que se van a crear para la instancia.

- SnapshotTags

  Tipo: cadena

  Descripción: (opcional) etiquetas que se van a crear para la instantánea.

Pasos de documentos

createRDSSnapshot: crea la instantánea de RDS y devuelve el ID de la instantánea.

verifyRDSSnapshot: comprueba que existe la instantánea creada en el paso anterior.

Salidas

Creador: DSSnapshot. SnapshotId — El ID de la instantánea creada.

AWSConfigRemediation-DeleteRDSCluster

Descripción

El `AWSConfigRemediation-DeleteRDSCluster` runbook elimina el clúster de Amazon Relational Database Service (Amazon RDS) que especifique. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DB ClusterId

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- config:GetResourceConfigHistory
- rds:DeleteDBCluster
- rds:DeleteDBInstance
- rds:DescribeDBClusters

Pasos de documentos

- aws:executeScript: elimina el clúster de base de datos que especifique en el parámetro DBClusterId.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteRDSClusterSnapshot elimina la instantánea del clúster de Amazon Relational Database Service (Amazon RDS) determinada.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterSnapshotID de base de datos

  Tipo: cadena

  Descripción: (obligatorio) el identificador de la instantánea del clúster de Amazon RDS que se va a eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Pasos de documentos

- `aws:branch`: comprueba si la instantánea del clúster está en estado `available`. Si no está disponible, el flujo finaliza.
- `aws:executeAwsApi`: elimina la instantánea de clúster de Amazon RDS determinada mediante el identificador de la instantánea del clúster de la base de datos (DB).
- `aws:executeScript`: verifica que se haya eliminado la instantánea determinada del clúster de Amazon RDS.

AWSConfigRemediation-DeleteRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRDSInstance` elimina la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Al eliminar una instancia de base de datos (DB), se eliminan todas las copias de seguridad automatizadas para esa instancia y no se pueden recuperar. Las instantáneas DB manuales no se eliminan. Si la instancia de base de datos que desea eliminar se encuentra en estado `failed`, `incompatible-network` o `incompatible-restore`, debe establecer el parámetro `SkipFinalSnapshot` en `true`.

> **Note**
>
> Si la instancia de base de datos que desea eliminar está en un clúster de base de datos de Amazon Aurora, el manual de procedimientos no eliminará la instancia de base de datos si es una réplica de lectura y la única instancia del clúster de base de datos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbiResourceID

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recurso de la instancia de base de datos que desea eliminar.
- SkipFinalCaptura instantánea

  Tipo: Booleano

  Predeterminado: false

Descripción: (opcional) si se establece en `true`, no se crea una instantánea final antes de eliminar la instancia de base de datos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Pasos de documentos

- `aws:executeAwsApi`: recopila el nombre de la instancia de base de datos a partir del valor que especifique en el parámetro `DbiResourceId`.
- `aws:branch`: se ramifica en función del valor que especifique en el parámetro `SkipFinalSnapshot`.
- `aws:executeAwsApi`: elimina la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:executeAwsApi`: elimina la instancia de base de datos que especifique en el parámetro `DbiResourceId` una vez creada la instantánea final.
- `aws:assertAwsResourceProperty`: verifica que la instancia de base de datos se haya eliminado.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRDSInstanceSnapshot` elimina la instantánea de la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Solo se eliminan las instantáneas que estén en estado `available`. Este manual de procedimientos no admite la eliminación de instantáneas de las instancias de bases de datos de Amazon Aurora.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbSnapshotID

  Tipo: cadena

  Descripción: (obligatorio) ID de la instantánea que quiere eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Pasos de documentos

- `aws:executeAwsApi`: recopila el estado de la instantánea especificada en el parámetro `DbSnapshotId`.
- `aws:assertAwsResourceProperty`: confirma que el estado de la instantánea es `available`.
- `aws:executeAwsApi`: elimina la instantánea especificada en el parámetro `DbSnapshotId`.
- `aws:executeScript`: verifica que se haya eliminado la instantánea.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-DisablePublicAccessToRDSInstance` deshabilita la accesibilidad pública de la instancia de base de datos (DB) de Amazon Relational Database Service (Amazon RDS) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbiResourceID

  Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos para la que desea deshabilitar la accesibilidad pública.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: verifica que las instancias de base de datos estén en un estado `AVAILABLE`.
- `aws:executeAwsApi`: deshabilita la accesibilidad pública en su instancia de base de datos.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos cambie al estado `MODIFYING`.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos cambie al estado `AVAILABLE`.
- `aws:assertAwsResourceProperty`: confirma que la accesibilidad pública está deshabilitada en la instancia de base de datos.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` habilita la configuración `CopyTagsToSnapshot`

del clúster de Amazon Relational Database Service (Amazon RDS) que especifique. Al habilitar esta configuración, se copian todas las etiquetas del clúster de base de datos en instantáneas del clúster de base de datos. El valor predeterminado es no copiarlos. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- ApplyImmediately

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente del valor de `PreferredMaintenanceWindow` del clúster de base de datos.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbClusterResourceId

  Tipo: cadena

Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la configuración `CopyTagsToSnapshot`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador del clúster de base de datos a partir del identificador de recursos del clúster de base de datos.
- `aws:assertAwsResourceProperty`: confirma que el clúster de base de datos está en un estado `AVAILABLE`.
- `aws:executeAwsApi`: activa la configuración `CopyTagsToSnapshot` en su clúster de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la configuración `CopyTagsToSnapshot` está habilitada en su clúster de base de datos.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` habilita la configuración `CopyTagsToSnapshot` en la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Al habilitar esta configuración, se copian todas las etiquetas de la instancia de base de

datos en instantáneas de la instancia de base de datos. El valor predeterminado es no copiarlos. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- ApplyImmediately

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbiResourceID

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar la configuración `CopyTagsToSnapshot`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `AVAILABLE`.
- `aws:executeAwsApi`: activa la configuración `CopyTagsToSnapshot` en su instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la configuración `CopyTagsToSnapshot` está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` permite la monitorización mejorada en la instancia de base de datos de Amazon RDS que especifique. Para obtener información sobre la monitorización mejorada, consulte la Monitorización mejorada en la Guía del usuario de Amazon RDS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- MonitoringInterval

  Tipo: entero

  Valores válidos: 1 | 5 | 10 | 15 | 30 | 60

  Descripción: (obligatorio) el intervalo en segundos en el que se recopilan las métricas de supervisión mejoradas de la instancia de base de datos.
- MonitoringRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Amazon RDS enviar métricas de monitorización mejorada a Amazon Logs. CloudWatch
- ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea activar la supervisión mejorada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `AVAILABLE`.
- `aws:executeAwsApi`: permite una supervisión mejorada en su instancia de base de datos.
- `aws:executeScript`: confirma que la supervisión mejorada está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` habilita la configuración `AutoMinorVersionUpgrade` en la instancia de base de datos de Amazon RDS que especifique. Habilitar esta opción indica que las actualizaciones de versión secundarias se aplican automáticamente a la instancia de base de datos durante el periodo de mantenimiento.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbiResourceID

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos que desea configurar `AutoMinorVersionUpgrade`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `AVAILABLE`.
- `aws:executeAwsApi`: activa la configuración `AutoMinorVersionUpgrade` en su instancia de base de datos.
- `aws:executeScript`: confirma que la configuración `AutoMinorVersionUpgrade` está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableMultiAZOnRDSInstance` cambia su instancia de base de datos (DB) de Amazon Relational Database Service (Amazon RDS) a una implementación multi-AZ. Cambiar este ajuste no produce una interrupción. El cambio se aplicará durante el siguiente período de mantenimiento, salvo que el parámetro `ApplyImmediately` esté establecido en `true`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- ApplyImmediately

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DbiResourceID

  Tipo: cadena

  Descripción: (obligatorio) El identificador Región de AWSúnico e inmutable de la instancia de base de datos para habilitar la configuración. `MultiAZ`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Pasos de documentos

- `aws:executeAwsApi`: recupera el nombre de la instancia de base de datos mediante el valor proporcionado en el parámetro `DBInstanceId`.
- `aws:executeAwsApi`: verifica que `DBInstanceStatus` esté `available`.
- `aws:branch`: comprueba si `MultiAZ` ya está establecido `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:executeAwsApi`: cambia la configuración `MultiAZ` a `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:assertAwsResourceProperty`: verifica que `MultiAZ` esté configurado como `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` habilita Performance Insights en la instancia de base de datos de Amazon RDS que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbiResourceID

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar Performance Insights.
- PerformanceInsightsKMS KeyId

  Tipo: cadena

  Valor predeterminado: `alias/aws/rds`

  Descripción: (opcional) El nombre del recurso de Amazon (ARN), el identificador de clave o el alias clave de la AWS Key Management Service (AWS KMS) clave gestionada por el cliente que

desea que Performance Insights utilice para cifrar todos los datos potencialmente confidenciales. Si introduce el alias de la clave para este parámetro, ponga el prefijo **alias/** al valor. Si no especifica un valor para este parámetro, Clave administrada de AWS se utiliza el.

- PerformanceInsightsRetentionPeriod

  Tipo: entero

  Valores válidos: 7, 731

  Valor predeterminado: 7

  Descripción (opcional): el número de días durante los que se retienen los datos de Información de rendimiento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de base de datos sea `available`.
- `aws:executeAwsApi`- Recopila el ARN de la clave gestionada AWS KMS por el cliente especificada en `PerformanceInsightsKMSKeyId` el parámetro.
- `aws:branch`: comprueba si ya hay un valor asignado a la propiedad `PerformanceInsightsKMSKeyId` de la instancia de base de datos.

- `aws:executeAwsApi`: habilita Performance Insights en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:assertAwsResourceProperty`: confirma que el valor especificado para el parámetro `PerformanceInsightsKMSKeyId` se utilizó para habilitar el cifrado de Performance Insights en la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que Performance Insights está habilitado en la instancia de base de datos.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descripción

El `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook permite la protección contra la eliminación en el clúster de Amazon Relational Database Service (Amazon RDS) que especifique. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- ClusterId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `aws:executeAwsApi`: recopila el nombre del clúster de base de datos a partir del identificador de recursos del clúster de base de datos.
- `aws:assertAwsResourceProperty`: verifica que el estado del clúster de base de datos sea `available`.
- `aws:executeAwsApi`: activa la protección contra la eliminación en el clúster de base de datos que especifique en el parámetro `ClusterId`.
- `aws:assertAwsResourceProperty`: verifica que la protección contra la eliminación esté habilitada en el clúster de base de datos.

AWSConfigRemediation-EnableRDSInstanceBackup

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRDSInstanceBackup` permite realizar copias de seguridad para la instancia de base de datos de Amazon Relational Database Service (Amazon RDS) que especifique. Este manual de procedimientos no admite la habilitación de copias de seguridad para las instancias de bases de datos de Amazon Aurora.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- ApplyImmediately

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- BackupRetentionPeríodo

  Tipo: entero

  Valores válidos: 1-35

  Descripción: (obligatorio) el número de días que se conservan las copias de seguridad.
- DbiResourceID

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos para la que desea habilitar las copias de seguridad.

- PreferredBackupVentana

  Tipo: cadena

  Descripción: (opcional) el intervalo de tiempo diario (en UTC) durante el cual se crean las copias de seguridad.

  Restricciones:

  - Tiene que tener el formato `hh24:mi-hh24:mi`
  - Debe estar en tiempo universal coordinado (UTC)
  - No debe entrar en conflicto con la ventana de mantenimiento preferida.
  - Debe durar al menos 30 minutos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeScript`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos. Habilita las copias de seguridad para su instancia de base de datos. Confirma que las copias de seguridad estén habilitadas en la instancia de base de datos.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` permite la protección contra la eliminación en la instancia de base de datos de Amazon RDS que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- ApplyImmediately

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DbInstanceResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:executeAwsApi`: activa la protección contra la eliminación en su instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la protección contra la eliminación está habilitada en la instancia de base de datos.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRDSInstancePortNumber` modifica el número de puerto en el que la instancia de Amazon Relational Database Service (Amazon RDS) acepta conexiones. Al ejecutar esta automatización se reiniciará la base de datos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- PortNumber

  Tipo: cadena

  Descripción: (opcional) el número de puerto en el que desea que la instancia de base de datos acepte conexiones.
- ID de RDSDB InstanceResource

  Tipo: cadena

  Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos cuyo número de puerto de entrada desea modificar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `AVAILABLE`.
- `aws:executeAwsApi`: modifica el número de puerto de entrada en el que la instancia de base de datos acepta conexiones.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos esté en estado `MODIFYING`.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos esté en estado `AVAILABLE`.

AWSSupport-ModifyRDSSnapshotPermission

Descripción

El manual de procedimientos `AWSSupport-ModifyRDSSnapshotPermission` le ayuda a modificar permisos para varias instantáneas de Amazon Relational Database Service (Amazon RDS). Con este manual de procedimientos, puede crear instantáneas `Public` o `Private` y compartirlas con otras Cuentas de AWS. Las instantáneas cifradas con una clave de KMS predeterminada no se pueden compartir con otras cuentas que utilicen este manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AccountIds

  Tipo: StringList

  Predeterminado: none

  Descripción: (opcional) los ID de las cuentas con las que desea compartir instantáneas. Este parámetro es obligatorio si especifica un valor No para el parámetro `Private`.

- AccountPermissionOperación

  Tipo: cadena

  Valores válidos: add | remove

  Predeterminado: none

  Descripción: (opcional) el tipo de operación que se va a realizar.

- Private

  Tipo: cadena

  Valores válidos: Yes | No

  Descripción: (obligatorio) introduzca No para el valor si desea compartir instantáneas con cuentas específicas.

- SnapshotIdentifiers

  Tipo: StringList

  Descripción: (obligatorio) los nombres de las instantáneas de Amazon RDS cuyo permiso desea modificar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Pasos de documentos

1. `aws:executeScript`: verifica los ID de las instantáneas proporcionadas en el parámetro `SnapshotIdentifiers`. Tras comprobar los ID, el script comprueba si hay instantáneas cifradas y genera una lista si encuentra alguna.
2. `aws:branch`: ramifica la automatización en función del valor que introduzca para el parámetro `Private`.
3. `aws:executeScript`: modifica los permisos de las instantáneas especificadas para compartirlas con las cuentas especificadas.
4. `aws:executeScript`: modifica los permisos de las instantáneas para cambiarlos de `Public` a `Private`.

Salidas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherCuentas. Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSPremiumSupport-PostgreSQLWorkloadReview

Descripción

El manual de procedimientos `AWSPremiumSupport-PostgreSQLWorkloadReview` captura varias instantáneas de las estadísticas de uso de base de datos de PostgreSQL de Amazon Relational Database Service (Amazon RDS). Las estadísticas recopiladas son necesarias para que

un experto de AWS Support Proactive Services realice una revisión operativa. Las estadísticas se recopilan mediante un conjunto de scripts SQL y de intérprete de comandos personalizados. Estos scripts se descargan en una instancia temporal de Amazon Elastic Compute Cloud (Amazon EC2) creada por este runbook. Cuenta de AWS El manual de procedimientos requiere que proporcione credenciales mediante un secreto AWS Secrets Manager que contenga un par de clave-valor de nombre de usuario y contraseña. El nombre de usuario debe tener permisos para consultar las vistas y funciones de estadísticas estándar de PostgreSQL.

Este manual crea automáticamente los siguientes AWS recursos Cuenta de AWS mediante una pila. AWS CloudFormation Puede supervisar la creación de la pila mediante la consola AWS CloudFormation .

- Una nube privada virtual (VPC) y una instancia de Amazon EC2 lanzadas en una subred privada de VPC con conectividad opcional a Internet mediante una puerta de enlace NAT.
- Un rol AWS Identity and Access Management (IAM) asociado a la instancia temporal de Amazon EC2 con permisos para recuperar el valor secreto de Secrets Manager. El rol también proporciona permisos para cargar archivos en un bucket de Amazon Simple Storage Service (Amazon S3) que elija y, opcionalmente, en un caso. AWS Support
- Una conexión de emparejamiento de VPC para permitir la conectividad entre la instancia de base de datos y la instancia temporal de Amazon EC2.
- Puntos de conexión de VPC Systems Manager, Secrets Manager y Amazon S3 que están conectados a la VPC temporal.
- Un período de mantenimiento con tareas registradas que inician y detienen periódicamente la instancia temporal de Amazon EC2, ejecutan scripts de recopilación de datos y suben archivos a un bucket de Amazon S3. También se crea un rol de IAM para la ventana de mantenimiento que proporciona permisos para realizar las tareas registradas.

Cuando se complete el runbook, se eliminará la AWS CloudFormation pila que se utilizó para crear los AWS recursos necesarios y el informe se cargará en el bucket de Amazon S3 que elija y, opcionalmente, en un AWS Support caso.

> **Note**
>
> De forma predeterminada, se conserva el volumen raíz de Amazon EBS de la instancia temporal de Amazon EC2. Puede invalidar esta configuración seleccionando el `EbsVolumeDeleteOnTermination` con el parámetro `true`.

Requisitos previos

- Suscripción a Enterprise Support Este manual de procedimientos y los diagnósticos y revisiones de la carga de trabajo de Proactive Services requieren una suscripción a Enterprise Support. Antes de utilizar este manual de procedimientos, póngase en contacto con su administrador técnico de cuentas (TAM) o con un especialista en TAM (STAM) para obtener instrucciones. Para obtener más información, consulte Servicios proactivos de AWS Support.
- Cuenta y Región de AWS cuotas Asegúrese de no haber alcanzado el número máximo de instancias o VPC de Amazon EC2 que puede crear en su cuenta y región en las que utiliza este runbook. Si necesita solicitar un aumento de los límites, utilice el formulario de aumento de los límites de servicio.
- Configuración de las bases de datos

  1. La base de datos que especifique en el parámetro `DatabaseName` debe tener la extensión `pg_stat_statements` configurada. Si no ha configurado `pg_stat_statements` en `shared_preload_libraries`, debe editar el valor en el grupo de parámetros de base de datos y aplicar los cambios. Los cambios en el parámetro `shared_preload_libraries` requieren que reinicie su instancia de base de datos. Para obtener más información, consulte Trabajo con los grupos de parámetros. Si se añade `pg_stat_statements` a `shared_preload_libraries`, se añadirá cierta sobrecarga de rendimiento. Sin embargo, esto es útil para realizar un seguimiento del rendimiento de las declaraciones individuales. Para obtener más información acerca de la extensión `pg_stat_statements`, consulte la documentación de PostgreSQL. Si no configura la extensión `pg_stat_statements` o si la extensión no está presente en la base de datos que se utiliza para la recopilación de estadísticas, el análisis a nivel de declaración no se presentará en la revisión operativa.
  2. Asegúrese de que los parámetros `track_counts` y `track_activities` no estén desactivados. Si estos parámetros están desactivados en el grupo de parámetros de la base de datos, no habrá estadísticas significativas disponibles. Para cambiar estos parámetros, deberá reiniciar su instancia de base de datos. Para obtener más información, consulte Uso de parámetros en su instancia de base de datos de Amazon RDS para PostgreSQL.
  3. Si el parámetro `track_io_timing` está desactivado, las estadísticas del nivel de E/S no se incluirán en la revisión operativa. El cambio `track_io_timing` requerirá reiniciar la instancia de base de datos y generará una sobrecarga de rendimiento adicional en función de la carga de trabajo de la instancia de base de datos. A pesar de la sobrecarga de rendimiento de las cargas de trabajo críticas, este parámetro proporciona información útil relacionada con el tiempo de E/S por consulta.

Facturación y cargos Se le Cuenta de AWS cobrarán los costos asociados a la instancia temporal de Amazon EC2, el volumen de Amazon EBS asociado, la puerta de enlace NAT y los datos transferidos durante la ejecución de esta automatización. De forma predeterminada, este manual de procedimientos crea una instancia de `t3.micro` Amazon Linux 2 para recopilar las estadísticas. El manual de procedimientos inicia y detiene la instancia entre los pasos para reducir los costos.

Seguridad y gobernanza de datos Este manual de procedimientos recopila estadísticas consultando las vistas y funciones estadísticas de PostgreSQL. Asegúrese de que las credenciales proporcionadas en el parámetro `SecretId` solo concedan permisos de solo lectura para las vistas y funciones de estadísticas. Como parte de la automatización, los scripts de recopilación se cargan en su bucket de Amazon S3 y se pueden encontrar en `s3://DOC-EXAMPLE-BUCKET/automation execution id/queries/`.

Estos scripts recopilan datos que un AWS especialista utiliza para revisar los indicadores clave de rendimiento a nivel de objeto. El script recopila información como el nombre de la tabla, el nombre del esquema y el nombre del índice. Si parte de esta información contiene información confidencial, como indicadores de ingresos, nombre de usuario, dirección de correo electrónico o cualquier otra información de identificación personal, le recomendamos que deje de revisar la carga de trabajo. Póngase en contacto con su AWS TAM para analizar un enfoque alternativo para la revisión de la carga de trabajo.

Asegúrese de contar con la aprobación y la autorización necesarias para compartir con usted las estadísticas y los metadatos recopilados por esta automatización AWS.

Consideraciones de seguridad Si establece el parámetro `UpdateRdsSecurityGroup` en `yes`, el manual de procedimientos actualiza el grupo de seguridad asociado a la instancia de base de datos para permitir el tráfico entrante desde la dirección IP privada de la instancia temporal de Amazon EC2.

Si establece el parámetro `UpdateRdsRouteTable` en `yes`, el manual de procedimientos actualiza la tabla de enrutamiento asociada a la subred en la que se ejecuta su instancia de base de datos para permitir el tráfico a la instancia temporal de Amazon EC2 a través de la conexión de emparejamiento de VPC.

Creación de usuarios Para permitir que el script de recopilación se conecte a su base de datos de Amazon RDS, debe configurar un usuario con permisos para leer las vistas de las estadísticas. Debe almacenar estas credenciales en Secrets Manager. Recomendamos crear un nuevo usuario dedicado para esta automatización. La creación de un usuario independiente le permite auditar y realizar un seguimiento de las actividades realizadas por esta automatización.

1. Cree un nuevo usuario.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Asegúrese de que este usuario solo pueda realizar conexiones de solo lectura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Establezca límites a nivel de usuario.

```
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. Conceda permisos `pg_monitor` al nuevo usuario para que pueda acceder a las estadísticas de la base de datos. (El rol `pg_monitor` es miembro de `pg_read_all_settings`, `pg_read_all_stats` y `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Permisos añadidos al perfil de instancia temporal de Amazon EC2 por esta automatización de Systems Manager Los siguientes permisos se añaden al rol de IAM asociado a la instancia temporal de Amazon EC2. La política `AmazonSSMManagedInstanceCore` gestionada también está asociada al rol de IAM para permitir que Systems Manager gestione la instancia de Amazon EC2.

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

Permisos agregados a la ventana de mantenimiento temporal por esta automatización de Systems Manager Los siguientes permisos se agregan automáticamente al rol de IAM asociado a las tareas de mantenimiento de Windows. Las tareas de mantenimiento de Windows inician, detienen y envían comandos a la instancia temporal de 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"
        }
    ]
}
```

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BASE DE DATOS InstanceIdentifier

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia DB.
- DatabaseName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la base de datos alojada en su instancia de base de datos.
- SecretId

  Tipo: cadena

  Descripción: (obligatorio) el ARN de su secreto de Secrets Manager que contenga un par de clave-valor de nombre de usuario y contraseña. La AWS CloudFormation pila crea una política de IAM con permisos para la `GetSecretValue` operación en este ARN. Las credenciales se utilizan para permitir que la instancia temporal recopile las estadísticas de la base de datos. Póngase en contacto con su TAM o STAM para hablar sobre los permisos mínimos requeridos.
- Acknowledge

Tipo: cadena

Descripción: (obligatorio) introduzca **yes** si reconoce que este manual de procedimientos creará recursos temporales en su cuenta para recopilar estadísticas de su instancia de base de datos. Le recomendamos que se ponga en contacto con su TAM o STAM antes de ejecutar esta automatización.

- SupportCase

  Tipo: cadena

  Descripción: (opcional) El número de AWS Support caso proporcionado por su TAM o STAM. Si se proporciona, el manual de procedimientos actualiza el caso y adjunta los datos recopilados. Esta opción requiere que la instancia temporal de Amazon EC2 tenga conectividad a Internet para acceder al punto final de la AWS Support API. El parámetro `AllowVpcInternetAccess` debe estar establecido en `true`. El asunto del caso debe contener la frase `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 de su cuenta en la que desea cargar los datos recopilados por la automatización. Verifique que la política del bucket no conceda permisos de lectura o escritura innecesarios a las entidades principales que no necesiten acceso al contenido del bucket. Recomendamos crear un nuevo bucket temporal de Amazon S3 para esta automatización. El manual de procedimientos proporciona permisos para la operación API de `s3:PutObject` al rol de IAM asociado a la instancia de Amazon EC2 temporal. Los archivos cargados se ubicarán en `s3://`*`bucket name`*`/`*`automation execution id`*`/`.

- InstanceType

  Tipo: cadena

  Descripción: (opcional) el tipo de instancia temporal de Amazon EC2 que ejecutará los scripts SQL y de intérprete de comandos personalizados.

  Valores válidos: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Valor predeterminado: t3.micro

- VpcCidr

Tipo: cadena

Descripción: (opcional) el rango de dirección IP en notación CIDR para la nueva VPC (por ejemplo, `172.31.0.0/16`). Asegúrese de seleccionar un CIDR que no se superponga ni coincida con ninguna VPC existente con conectividad a su instancia de base de datos. La VPC más pequeña que puede crear utiliza una máscara de subred /28 y la VPC mayor utiliza una máscara de subred /16.

Valor predeterminado: 172.31.0.0/16

- StackResourcesNamePrefix

  Tipo: cadena

  Descripción: (opcional) El nombre, el prefijo y la etiqueta de los recursos de la AWS CloudFormation pila. El manual crea los recursos de la AWS CloudFormation pila utilizando este prefijo como parte del nombre y la etiqueta que se aplican a los recursos. La estructura del par clave-valor de etiqueta es *`StackResourcesNamePrefix`*`:{{automation:EXECUTION_ID}}`.

  Predeterminado: AWSPostgreSQLWorkloadReview

- Programación

  Tipo: cadena

  Descripción: (opcional) el horario del período de mantenimiento. Especifica la frecuencia con la que la ventana de mantenimiento ejecuta las tareas. El valor predeterminado es `1 hour`.

  Valores válidos: 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 12 hours | 1 day | 2 days | 4 days

  Valor predeterminado: 1 hora

- Duración

  Tipo: entero

  Descripción: (opcional) el tiempo máximo, en minutos, que desea permitir que se ejecute la automatización. La duración máxima admitida es de 8640 minutos (6 días). El valor predeterminado es 4320 minutos (3 días).

  Valores válidos: 30-8640

Predeterminado: 4320

- UpdateRdsRouteTable

  Tipo: cadena

  Descripción: (opcional) si se establece en `true`, el manual de procedimientos actualiza la tabla de enrutamiento asociada a la subred en la que se ejecuta la instancia de base de datos. Se agrega una ruta IPv4 para enrutar el tráfico a la dirección IPV4 privada de la instancia temporal de Amazon EC2 a través de la conexión de emparejamiento de VPC recién creada.

  Valores válidos: true | false

  Predeterminado: false

- AllowVpcInternetAccess

  Tipo: cadena

  Descripción: (Opcional) Si se establece en`true`, el runbook crea una puerta de enlace NAT para proporcionar conectividad a Internet a la instancia temporal de Amazon EC2 para comunicarse con AWS Support el punto de enlace de la API. Puede dejar este parámetro como `false` si solo quiere que el manual de procedimientos cargue la salida en su bucket de Amazon S3.

  Valores válidos: true | false

  Predeterminado: false

- UpdateRdsSecurityGroup

  Tipo: cadena

  Descripción: (opcional) si se establece en `true`, el manual de procedimientos actualiza el grupo de seguridad asociado a su instancia de base de datos para permitir el tráfico desde la dirección IP privada de la instancia temporal.

  Valores válidos: Falso | Verdadero

  Predeterminado: false

- EbsVolumeDeleteOnTerminación

  Tipo: cadena

Descripción: (Opcional) Si se establece en`true`, el volumen raíz de la instancia temporal de Amazon EC2 se elimina una vez que el runbook complete y elimine la pila. AWS CloudFormation

Valores válidos: Falso | Verdadero

Predeterminado: false

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

1. aws:assertAwsResourceProperty: confirma que la instancia de base de datos está en estado available.
2. aws:executeAwsApi: recopila detalles sobre la instancia de base de datos.
3. aws:executeScript: comprueba si el bucket de Amazon S3 especificado en el campo S3BucketName permite permisos de acceso de lectura o escritura públicos o anónimos.
4. aws:executeScript- Obtiene el contenido de la AWS CloudFormation plantilla del archivo adjunto del manual de automatización que se utiliza para crear los recursos temporales AWS en su archivo. Cuenta de AWS
5. aws:createStack- Crea la AWS CloudFormation pila de recursos.
6. aws:waitForAwsResourceProperty- Espera a que se ejecute la instancia Amazon EC2 creada por AWS CloudFormation la plantilla.
7. aws:executeAwsApi: obtiene los ID de la instancia temporal de Amazon EC2 y de la conexión de emparejamiento de VPC creada por AWS CloudFormation.
8. aws:executeAwsApi: obtiene la dirección IP de la instancia temporal de Amazon EC2 para configurar la conectividad con su instancia de base de datos.
9. aws:executeAwsApi: etiqueta el volumen de Amazon EBS adjunto a la instancia temporal de Amazon EC2.
10. aws:waitForAwsResourceProperty: espera hasta que la instancia temporal de Amazon EC2 supere las comprobaciones de estado.
11. aws:waitForAwsResourceProperty: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2. Si se agota el tiempo de espera de este paso o se produce un error, el manual de procedimientos reinicia la instancia.
    a. aws:executeAwsApi: reinicia la instancia temporal de Amazon EC2 si el paso anterior ha fallado o se ha agotado el tiempo de espera.
    b. aws:waitForAwsResourceProperty: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2 tras el reinicio.
12. aws:runCommand: instala los requisitos de la aplicación recopiladora de metadatos en la instancia temporal de Amazon EC2.

13. `aws:runCommand`: configura el acceso a la instancia de base de datos mediante la creación de un archivo de configuración en la instancia temporal de Amazon EC2.
14. `aws:executeAwsApi`: crea una ventana de mantenimiento para ejecutar periódicamente la aplicación recopiladora de metadatos mediante Run Command. La ventana de mantenimiento inicia y detiene la instancia entre comandos.
15. `aws:waitForAwsResourceProperty`- Espera a que la ventana de mantenimiento creada por la AWS CloudFormation plantilla esté lista.
16. `aws:executeAwsApi`- Obtiene los ID de la ventana de mantenimiento y el calendario de cambios creados por AWS CloudFormation.
17. `aws:sleep`: espera hasta la fecha de finalización del período de mantenimiento.
18. `aws:executeAwsApi`: desactiva la ventana de mantenimiento.
19. `aws:executeScript`: obtiene los resultados de las tareas ejecutadas durante el período de mantenimiento.
20. `aws:waitForAwsResourceProperty`: espera a que el período de mantenimiento finalice la última tarea antes de continuar.
21. `aws:branch`: ramifica el flujo de trabajo en función de si ha proporcionado un valor para el parámetro `SupportCase`.
    a. `aws:changeInstanceState`: inicia la instancia temporal de Amazon EC2 y espera a que se superen las comprobaciones de estado antes de cargar el informe.
    b. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2. Si se agota el tiempo de espera de este paso o se produce un error, el manual de procedimientos reinicia la instancia.
        i. `aws:executeAwsApi`: reinicia la instancia temporal de Amazon EC2 si el paso anterior ha fallado o se ha agotado el tiempo de espera.
        ii. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2 tras el reinicio.
    c. `aws:runCommand`: adjunta el informe de metadatos al caso AWS Support si ha proporcionado un valor para el parámetro `SupportCase`. El script comprime y divide el informe en archivos de 5 MB. El número máximo de archivos que el script adjunta a un caso AWS Support es 12.
22. `aws:changeInstanceState`- Detiene la instancia temporal de Amazon EC2 en caso de que la AWS CloudFormation pila no se elimine.
23. `aws:executeAwsApi`- Describe los eventos de la AWS CloudFormation pila si los runbooks no pueden crear o actualizar la AWS CloudFormation pila.

24. `aws:waitForAwsResourceProperty`- Espera a que la AWS CloudFormation pila esté en estado terminal antes de eliminarla.
25. `aws:executeAwsApi`- Elimina la AWS CloudFormation pila excluyendo la ventana de mantenimiento. El volumen raíz de Amazon EBS asociado a la instancia temporal de Amazon EC2 se conserva si el valor del parámetro `EbsVolumeDeleteOnTermination` se estableció en `false`.

AWS-RebootRdsInstance

Descripción

El manual de procedimientos `AWS-RebootRdsInstance` reinicia una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) si aún no se está reiniciando.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon RDS DB que desea reiniciar.

Pasos de documentos

RebootInstance - Reinicia la instancia de base de datos si aún no se está reiniciando.

WaitForAvailableState - Espera a que la instancia de base de datos complete el proceso de reinicio.

Salidas

Esta automatización no tiene salidas.

AWSSupport-ShareRDSSnapshot

Descripción

El manual de procedimientos `AWSSupport-ShareRDSSnapshot` proporciona una solución automatizada para el procedimiento descrito en el artículo del Centro de Conocimiento ¿Cómo puedo compartir una instantánea de base de datos de Amazon RDS cifrada con otra cuenta? Si la instantánea de Amazon Relational Database Service (Amazon RDS) se cifró con la Clave administrada de AWS configuración predeterminada, no podrá compartir la instantánea. En este caso, debe copiar la instantánea con una clave administrada por el cliente y, a continuación, compartir la instantánea con la cuenta de destino. Esta automatización realiza estos pasos utilizando el valor que especifique en el parámetro `SnapshotName` o la última instantánea encontrada para la instancia de base de datos o el clúster de base de datos de Amazon RDS seleccionados.

> **Note**
>
> Si no especifica un valor para el `KMSKey` parámetro, la automatización crea una nueva clave administrada por el AWS KMS cliente en su cuenta que se utiliza para cifrar la instantánea.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AccountIds

  Tipo: StringList

  Descripción: (obligatorio) lista de identificadores de cuenta separados por comas con los que compartir la instantánea.

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Base de datos

  Tipo: cadena

  Descripción: (obligatorio) el nombre de la instancia de base de datos o el clúster de Amazon RDS cuya instantánea desea compartir. Este parámetro es opcional si especifica un valor para el parámetro `SnapshotName`.

- KMSKey

  Tipo: cadena

  Descripción: (opcional) el nombre de recurso de Amazon (ARN) completo de la clave de AWS KMS administrada por el cliente que se utiliza para cifrar la instantánea.

- SnapshotName

  Tipo: cadena

Descripción: (opcional) el ID del clúster o instantánea de instancia de base de datos que desea utilizar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

`AutomationAssumeRole` requiere las siguientes acciones para iniciar correctamente el manual de procedimientos de un clúster de base de datos.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

El rol de IAM utilizado para ejecutar la automatización debe agregarse como usuario clave para usar la clave de KMS especificada en el parámetro `ARNKmsKey`. Para obtener información sobre cómo añadir usuarios de clave a la clave KMS, consulte Modificación de una política de claves en la Guía del desarrollador de AWS Key Management Service .

Si no se especifica un valor para el parámetro `KMSKey`, `AutomationAssumeRole` requiere realizar las siguientes acciones adicionales para iniciar correctamente el manual de procedimientos.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`

- kms:DescribeKey

Pasos de documentos

1. aws:executeScript- Comprueba si se ha proporcionado un valor para el KMSKey parámetro y crea una clave gestionada por el AWS KMS cliente si no se encuentra ningún valor.
2. aws:branch: comprueba si se ha proporcionado un valor para el parámetro SnapshotName y se ramifica en consecuencia.
3. aws:executeAwsApi: comprueba si la instantánea proporcionada proviene de una instancia de base de datos.
4. aws:executeScript: formatea el parámetro SnapshotName sustituyendo los dos puntos por un guion.
5. aws:executeAwsApi: copia la instantánea utilizando el KMSKey especificado.
6. aws:waitForAwsResourceProperty: espera a que finalice la operación de copia de la instantánea.
7. aws:executeAwsApi: comparte la nueva instantánea con la AccountIds especificada.
8. aws:executeAwsApi: comprueba si la instantánea proporcionada proviene de un clúster de base de datos.
9. aws:executeScript: formatea el parámetro SnapshotName sustituyendo los dos puntos por un guion.
10. aws:executeAwsApi: copia la instantánea utilizando el KMSKey especificado.
11. aws:waitForAwsResourceProperty: espera a que finalice la operación de copia de la instantánea.
12. aws:executeAwsApi: comparte la nueva instantánea con la AccountIds especificada.
13. aws:executeAwsApi: comprueba si el valor proporcionado para el parámetro Database es una instancia de base de datos.
14. aws:executeAwsApi: comprueba si el valor proporcionado para el parámetro Database es un clúster de base de datos.
15. aws:executeAwsApi: recupera una lista de instantáneas de la Database especificada.
16. aws:executeScript: determina la última instantánea disponible de la lista recopilada en el paso anterior.
17. aws:executeAwsApi: copia la instantánea de la instancia de base de datos utilizando la KMSKey especificada.

18. `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
19. `aws:executeAwsApi`: comparte la nueva instantánea con la `AccountIds` especificada.
20. `aws:executeAwsApi`: recupera una lista de instantáneas de la `Database` especificada.
21. `aws:executeScript`: determina la última instantánea disponible de la lista recopilada en el paso anterior.
22. `aws:executeAwsApi`: copia la instantánea de la instancia de base de datos utilizando la `KMSKey` especificada.
23. `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
24. `aws:executeAwsApi`: comparte la nueva instantánea con la `AccountIds` especificada.
25. `aws:executeScript`- Elimina la clave gestionada por el AWS KMS cliente creada por la automatización si no se especificó un valor para el `KMSKey` parámetro y la automatización falla.

AWS-StartRdsInstance

Descripción

Inicia una instancia de Amazon Relational Database Service (Amazon RDS).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia Amazon RDS que comenzar.

AWS-StartStopAuroraCluster

Descripción

Este manual inicia o detiene un clúster de Amazon Aurora.

> **Note**
>
> Para iniciar un clúster, debe estar en un `stopped` estado. Para detener un clúster, debe estar en un `available` estado. Este manual de ejecución no se puede utilizar para iniciar o detener un clúster que sea un clúster Aurora Serverless, un clúster de varios maestros de Aurora, parte de una base de datos global de Aurora o un clúster que utilice Aurora parallel Query.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- ClusterName

  Tipo: cadena

  Descripción: (Obligatorio) El nombre del clúster de Aurora que desea detener o iniciar.
- Acción

  Tipo: cadena

  Valores válidos: Start | Stop

  Predeterminado: Inicio

  Descripción: (Obligatorio) El nombre del clúster de Aurora que desea detener o iniciar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

Pasos de documentos

- `aws:executeScript`- Inicia o detiene el clúster en función de los valores que especifique para el.

Salidas

StartStopAuroraCluster. ClusterName - El nombre del cúmulo de Aurora

StartStopAuroraCluster. CurrentStatus - El estado actual del cúmulo Aurora

StartStopAuroraCluster.Message: detalles de la automatización

AWS-StopRdsInstance

Descripción

Detenga una instancia de Amazon Relational Database Service (Amazon RDS).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: cadena

Descripción: (obligatorio) ID de la instancia de Amazon RDS que se va a detener.

AWSSupport-TroubleshootConnectivityToRDS

Descripción

El manual de procedimientos `AWSSupport-TroubleshootConnectivityToRDS` diagnostica los problemas de conectividad entre una instancia EC2 y una instancia de Amazon Relational Database Service. La automatización garantiza que la instancia de base de datos esté disponible y, a continuación, comprueba las reglas de grupo de seguridad asociadas, las listas de control de acceso a la red (ACL de red) y las tablas de ruteo para detectar posibles problemas de conectividad.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BASE DE DATOS InstanceIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el ID de instancia de base de datos para probar la conectividad.

- SourceInstance

  Tipo: cadena

  Patrón permitido: ^i-[a-z0-9]{8,17}$

  Descripción: (obligatorio) el ID de la instancia EC2 desde la que probar la conectividad.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de base de datos sea `available`.
- `aws:executeAwsApi`: obtiene información de resumen acerca de la instancia DB.
- `aws:executeAwsApi`: obtiene información sobre las ACL de la red de instancia DB.
- `aws:executeAwsApi`: obtiene el CIDR de la subred de la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información acerca de la instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre las ACL de la red de instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre los grupos de seguridad asociados a la instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre los grupos de seguridad asociados a la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información sobre las tablas de ruteo asociadas a la instancia EC2.

- `aws:executeAwsApi`: obtiene información sobre la tabla de enrutamiento principal asociada con el Amazon VPC para la instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre las tablas de enrutamiento asociadas a la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información sobre la tabla de enrutamiento principal asociada con el Amazon VPC para la instancia de base de datos.
- `aws:executeScript`: evalúa las reglas de los grupos de seguridad.
- `aws:executeScript`: evalúa las ACL de la red.
- `aws:executeScript`: evalúa las tablas de enrutamiento.
- `aws:sleep`: finaliza la automatización.

Salidas

getRDS InstanceProperties .DBInstanceIdentifier : la instancia de base de datos utilizada en la automatización.

getRDS InstanceProperties .DBInstanceStatus : el estado actual de la instancia de base de datos.

evalSecurityGroupReglas. SecurityGroupEvaluation - Resultados de la comparación de las reglas del grupo `SourceInstance` de seguridad con las reglas del grupo de seguridad de la instancia de base de datos.

evalNetworkAclReglas. NetworkAclEvaluation - Resultados de la comparación de las ACL de `SourceInstance` red con las ACL de red de la instancia de base de datos.

evalRouteTableEntradas. RouteTableEvaluation - Resultados de la comparación de la tabla de `SourceInstance` rutas con las rutas de la instancia de base de datos.

AWSSupport-TroubleshootRDSIAMAuthentication

Descripción

`AWSSupport-TroubleshootRDSIAMAuthentication`Ayuda a solucionar problemas de autenticación AWS Identity and Access Management (IAM) para instancias de Amazon RDS for PostgreSQL, Amazon RDS for MySQL, Amazon RDS for MariaDB, Amazon Aurora PostgreSQL y Amazon Aurora MySQL. Utilice este manual para comprobar la configuración necesaria para la autenticación de IAM con una instancia de Amazon RDS o un clúster Aurora. También proporciona pasos para corregir los problemas de conectividad con la instancia Amazon RDS o el clúster Aurora.

Important

Este manual no es compatible con Amazon RDS for Oracle ni Amazon RDS for Microsoft SQL Server.

Important

Si se proporciona una instancia Amazon EC2 de origen y la base de datos de destino es Amazon RDS, `AWSSupport-TroubleshootConnectivityToRDS` se invoca una automatización secundaria para solucionar los problemas de conectividad TCP. El resultado también proporciona comandos que puede ejecutar en su instancia Amazon EC2 o máquina de origen para conectarse a las instancias de Amazon RDS mediante la autenticación de IAM.

¿Cómo funciona?

Este manual consta de seis pasos:

- Paso 1: ValidateInputs: valida las entradas de la automatización.
- Paso 2: branchOnSource proporcionado por EC2: verifica si se proporciona un ID de instancia de Amazon EC2 de origen en los parámetros de entrada.
- Paso 3: ValidaterDSConnectivity: valida la conectividad de Amazon RDS desde la instancia Amazon EC2 de origen, si se proporciona.
- Paso 4: ValidatersSiamAuthentication: valida si la función de autenticación de IAM está habilitada.
- Paso 5: Validar las políticas de IAM: verifica si los permisos de IAM necesarios están presentes en el usuario o rol de IAM proporcionado.
- Paso 6: Generar un informe: genera un informe con los resultados de los pasos ejecutados anteriormente.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- Tipo RDS

  Tipo: cadena

  Descripción: (Obligatorio): Seleccione el tipo de base de datos relacional a la que intenta conectarse y autenticarse.

  Valores permitidos: o `Amazon RDS` `Amazon Aurora Cluster.`
- DB InstanceIdentifier

  Tipo: cadena

  Descripción: (obligatorio) El identificador de la instancia de base de datos Amazon RDS o del clúster de base de datos Aurora de destino.

  Valor permitido: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  Número máximo de caracteres: 63
- SourceEc2 InstanceIdentifier

  Tipo: `AWS::EC2::Instance::Id`

  Descripción: (opcional) El ID de instancia de Amazon EC2 si se conecta a la instancia de base de datos Amazon RDS desde una instancia de Amazon EC2 que se ejecuta en la misma cuenta y

región. No especifique este parámetro si la fuente no es una instancia de Amazon EC2 o si el tipo de Amazon RDS de destino es un clúster de base de datos Aurora.

Valor predeterminado: ""

- DBIAM RoleName

  Tipo: cadena

  Descripción: (opcional) El nombre de la función de IAM que se utiliza para la autenticación basada en IAM. Indíquelo solo si no `DBIAMUserName` se proporciona el parámetro; de lo contrario, déjelo vacío. Se `DBIAMUserName` debe proporcionar `DBIAMRoleName` o se debe proporcionar.

  Valor permitido: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Número máximo de caracteres: 64

  Valor predeterminado: ""

- DIBAM UserName

  Tipo: cadena

  Descripción: (opcional) El nombre de usuario de IAM utilizado para la autenticación basada en IAM. Indíquelo solo si no se proporciona el `DBIAMRoleName` parámetro; de lo contrario, déjelo vacío. Se `DBIAMUserName` debe proporcionar `DBIAMRoleName` o se debe proporcionar.

  Valor permitido: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Número máximo de caracteres: 64

  Valor predeterminado: ""

- DB UserName

  Tipo: cadena

  Descripción: (opcional) El nombre de usuario de la base de datos asignado a un rol o usuario de IAM para la autenticación basada en IAM dentro de la base de datos. La opción predeterminada * evalúa si el `rds-db:connect` permiso está permitido para todos los usuarios de la base de datos.

  Valor permitido: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Número máximo de caracteres: 64

Valor predeterminado: *

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Instrucciones

1. Navegue hasta la opción de AWSSupportsolución de problemas de autenticación RDSIAM en la consola. AWS Systems Manager
2. Elija Execute automation (Ejecutar automatización)
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

  El nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- Tipo RDS (obligatorio):

  Seleccione el tipo de Amazon RDS al que intenta conectarse y autenticarse. Elija uno de los dos valores permitidos: o `Amazon RDS` `Amazon Aurora Cluster.`

- DB InstanceIdentifier (obligatorio):

  Introduzca el identificador de la instancia de base de datos Amazon RDS de destino o del clúster Aurora al que intenta conectarse y utilice las credenciales de IAM para la autenticación.

- SourceEc2 InstanceIdentifier (opcional):

  Proporcione el ID de instancia de Amazon EC2 si se conecta a la instancia de base de datos de Amazon RDS desde una instancia de Amazon EC2 presente en la misma cuenta y región. Déjelo en blanco si el origen no es Amazon EC2 o si el tipo de Amazon RDS de destino es un clúster Aurora.

- DBIAM RoleName (opcional):

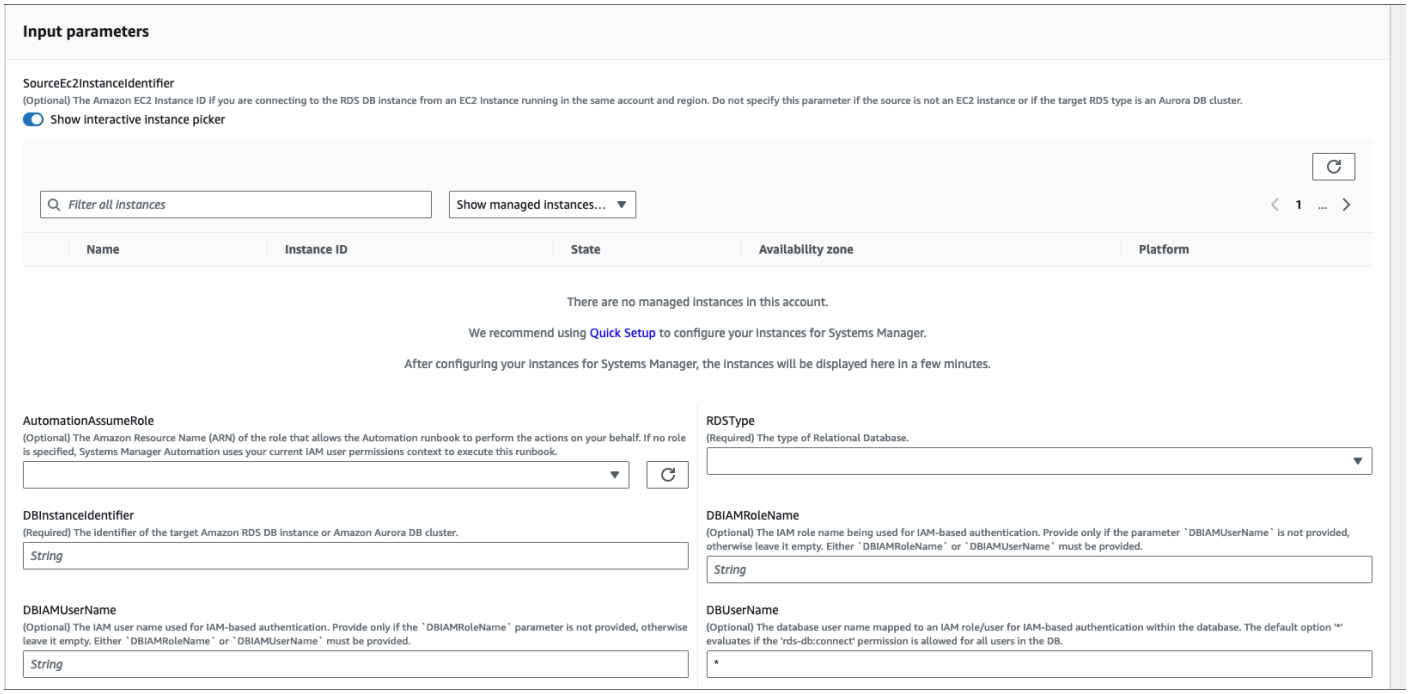
  Introduzca el nombre del rol de IAM utilizado para la autenticación basada en IAM. Indíquelo solo si no `DBIAMUserName` se proporciona; de lo contrario, déjelo en blanco. Se `DBIAMUserName` debe proporcionar `DBIAMRoleName` o se debe proporcionar.

- DBIAM UserName (opcional):

  Introduzca el usuario de IAM utilizado para la autenticación basada en IAM. Indique solo si no `DBIAMRoleName` se proporciona; de lo contrario, déjelo en blanco. Se `DBIAMUserName` debe proporcionar `DBIAMRoleName` o se debe proporcionar.

- Base de datos UserName (opcional):

  Introduzca el usuario de la base de datos asignado a un rol o usuario de IAM para la autenticación basada en IAM dentro de la base de datos. La opción predeterminada * se utiliza para evaluar; no se proporciona nada en este campo.



4. Seleccione Ejecutar.
5. Observe que se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - Paso 1: Validar las entradas:

     Valida las entradas de la automatización: `SourceEC2InstanceIdentifier` (opcional), `DBInstanceIdentifier` o, y o`ClusterID`. `DBIAMRoleName` `DBIAMUserName` Verifica si los parámetros de entrada ingresados están presentes en su cuenta y región. También verifica si el usuario ingresó uno de los parámetros de IAM (por ejemplo, `DBIAMRoleName` o). `DBIAMUserName` Además, realiza otras verificaciones, por ejemplo, si la base de datos mencionada está en estado Disponible.
   - Paso 2: branchOnSource EC2 proporcionó:

     Verifica si se proporciona Amazon EC2 de origen en los parámetros de entrada y si la base de datos es Amazon RDS. En caso afirmativo, continúa con el paso 3. De lo contrario, se salta el paso 3, que es la validación de la conectividad entre Amazon EC2 y Amazon RDS, y pasa al paso 4.
   - Paso 3: Validar la conectividad de RDS:

     Si se proporciona el Amazon EC2 de origen en los parámetros de entrada y la base de datos es Amazon RDS, el paso 2 inicia el paso 3. En este paso, `AWSSupport-`

`TroubleshootConnectivityToRDS` se invoca la automatización secundaria para validar la conectividad de Amazon RDS desde Amazon EC2 de origen. El manual de automatización secundaria `AWSSupport-TroubleshootConnectivityToRDS` verifica si las configuraciones de red requeridas (Amazon Virtual Private Cloud [Amazon VPC], grupos de seguridad, lista de control de acceso a la red [NACL], disponibilidad de Amazon RDS) están implementadas para que pueda conectarse desde la instancia de Amazon EC2 a la instancia de Amazon RDS.

- Paso 4: Validar la autenticación de DSIAMAuthentication:

  Valida si la función de autenticación de IAM está habilitada en la instancia de Amazon RDS o en el clúster Aurora.

- Paso 5: Validar las políticas de IAM:

  Comprueba si los permisos de IAM necesarios están presentes en el usuario o rol de IAM transferido para permitir que las credenciales de IAM se autentiquen en la instancia de Amazon RDS para el usuario de base de datos especificado (si lo hubiera).

- Paso 6: Generar un informe:

  Obtiene toda la información de los pasos anteriores e imprime el resultado o la salida de cada paso. También se enumeran los pasos a seguir y realizar para conectarse a la instancia de Amazon RDS mediante las credenciales de IAM.

7. Cuando se complete la automatización, consulte la sección de resultados para ver los resultados detallados:

   - Comprobar el permiso de usuario o rol de IAM para conectarse a la base de datos:

     Comprueba si los permisos de IAM necesarios están presentes en el usuario o rol de IAM transferido para permitir que las credenciales de IAM se autentiquen en la instancia de Amazon RDS para el usuario de base de datos especificado (si lo hubiera).

   - Comprobación del atributo de autenticación basado en IAM para la base de datos:

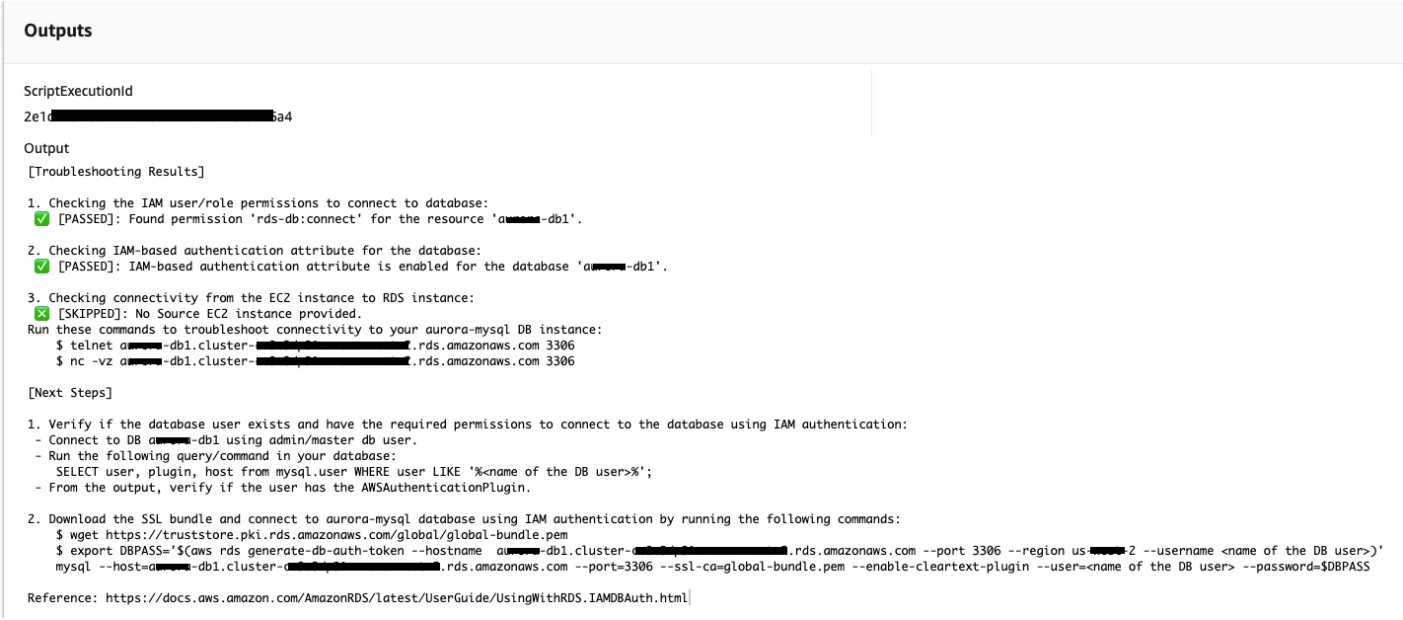
     Comprueba si la función de autenticación de IAM está habilitada para la base de datos Amazon RDS o el clúster Aurora especificados.

   - Comprobación de la conectividad de una instancia de Amazon EC2 a una instancia de Amazon RDS:

     Verifica si las configuraciones de red requeridas (Amazon VPC, grupos de seguridad, NACL, disponibilidad de Amazon RDS) están implementadas para que pueda conectarse desde la instancia de Amazon EC2 a la instancia de Amazon RDS.

- Pasos siguientes:

  Muestra los comandos y los pasos que se deben consultar y ejecutar para conectarse a la instancia de Amazon RDS mediante las credenciales de IAM.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWSSupport-ValidateRdsNetworkConfiguration

Descripción

`AWSSupport-ValidateRdsNetworkConfiguration`la automatización ayuda a evitar un estado de red incompatible para su instancia existente de Amazon Relational Database Service (Amazon RDS), Amazon Aurora o Amazon DocumentDB antes de realizar u operar. `ModifyDBInstance` `StartDBInstance` Si la instancia ya se encuentra en un estado de red incompatible, el manual explicará el motivo.

¿Cómo funciona?

Este manual determina si la instancia de base de datos de Amazon RDS pasará a un estado de red incompatible o, si lo ha hecho, determina el motivo por el que se encuentra en un estado de red incompatible.

El runbook realiza las siguientes comprobaciones en la instancia de base de datos de Amazon RDS:

- Cuota de Amazon Elastic Network Interface (ENI) por región.
- Existen todas las subredes del grupo de subredes de la base de datos.
- Hay suficientes direcciones IP libres disponibles para las subredes.
- (Para instancias de Amazon RDS de acceso público) Configuración de los atributos de VPC `enableDnsSupport` (`enableDnsHostnamesy`).

> **Important**
>
> Cuando utilice este documento en clústeres de Amazon Aurora o Amazon DocumentDB, asegúrese de utilizar `DBInstanceIdentifier` en lugar de. `ClusterIdentifier` De lo contrario, el documento fallará en el primer paso.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Bases de datos

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:DescribeDBInstances`

- servicequotas:GetServiceQuota
- ec2:DescribeNetworkInterfaces
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets

Ejemplo de política:

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

Instrucciones

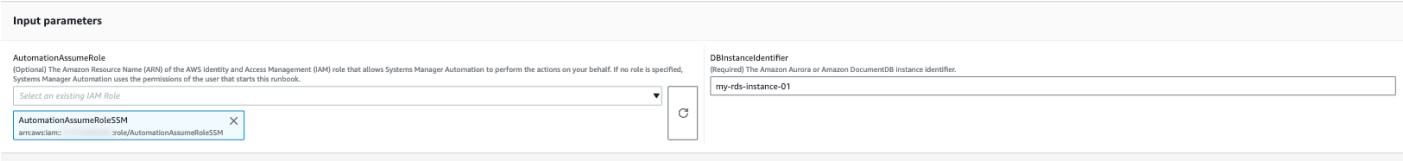
1. Navegue hasta el AWSSupport- ValidateRdsNetworkConfiguration en la AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización)
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se

especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- Base de datos InstanceIdentifier (obligatorio):

  Introduzca el identificador de instancia de Amazon Relational Database Service.



4. Seleccione Ejecutar.
5. Observe que se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - Paso 1: assertRdsState

     Comprueba si el identificador de instancia proporcionado existe y tiene alguno de los siguientes estados:`available`,`stopped`, `oincompatible-network`.
   - Paso 2 gatherRdsInformation:

     Recopila la información necesaria sobre la instancia de Amazon RDS para utilizarla más adelante en la automatización.
   - Paso 3: checkEniQuota

     Comprueba la cuota actual disponible de Amazon ENI para la región.
   - Paso 4 validateVpcAttributes:

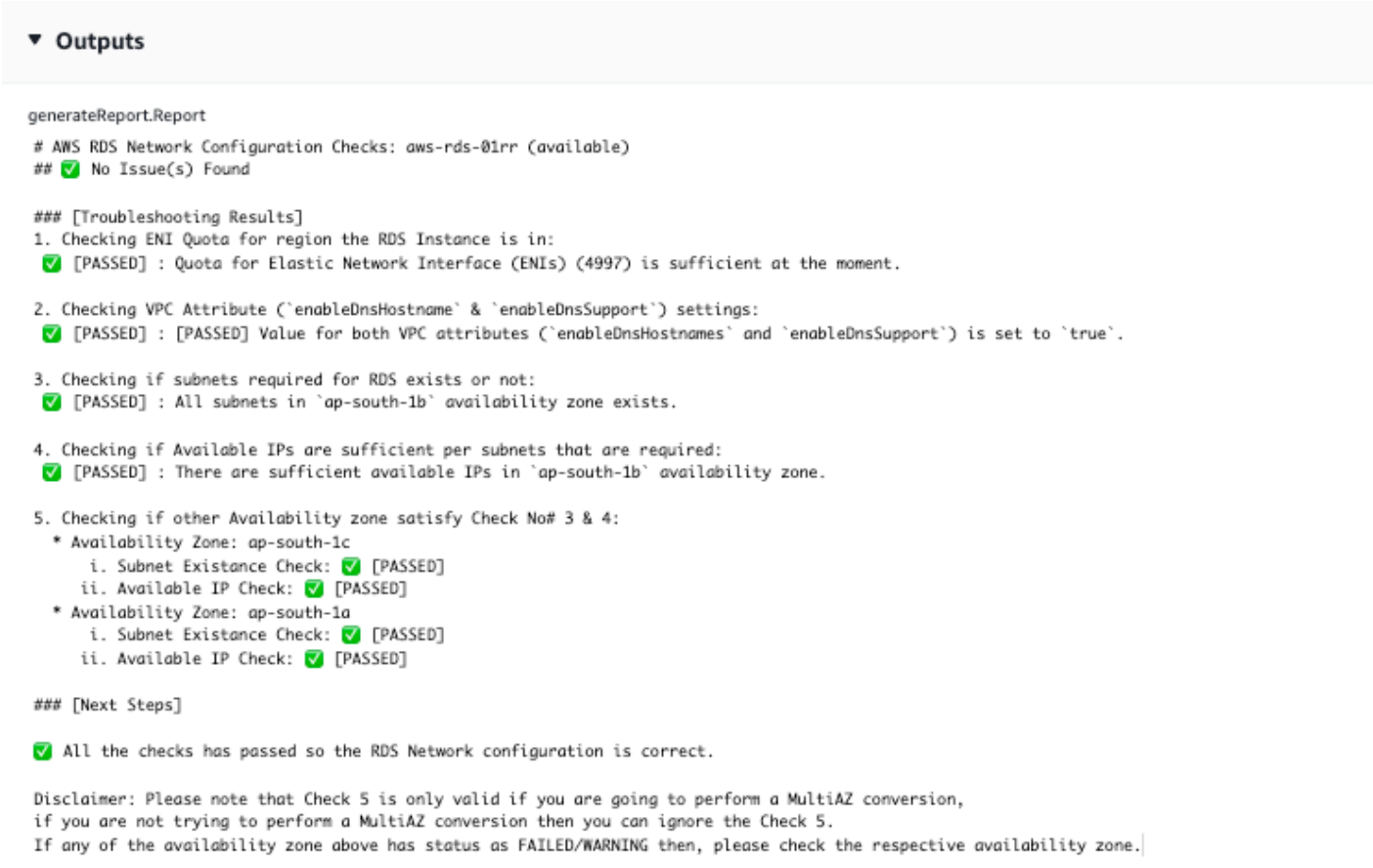
     Valida que los parámetros de DNS (`enableDnsSupportyenableDnsHostnames`) de la VPC de Amazon estén configurados en true (o no si la instancia de Amazon RDS lo está). `PubliclyAccessible`
   - Paso 5: validateSubnetAttributes

     Valida la existencia de subredes `DBSubnetGroup` y comprueba las IP disponibles para cada subred.
   - Paso 6: Generar un informe:

     Obtiene toda la información de los pasos anteriores e imprime el resultado o la salida de cada paso. También se enumeran los pasos que se deben seguir y realizar para conectarse a la instancia de Amazon RDS mediante las credenciales de IAM.

7. Cuando se complete la automatización, consulte la sección de resultados para ver los resultados detallados:

   Instancia de Amazon RDS con una configuración de red 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.
```

   Instancia de Amazon RDS con una configuración de red incorrecta (el enableDnsHostnames atributo de VPC está establecido en false):

Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- ¿Cómo resuelvo los problemas con una base de datos de Amazon RDS que se encuentra en un estado de red incompatible?
- ¿Cómo resuelvo los problemas con una instancia de Amazon DocumentDB que se encuentra en un estado de red incompatible?

Amazon Redshift

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Redshift. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

`AWSConfigRemediation-DeleteRedshiftCluster`

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRedshiftCluster` elimina el clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el ID del clúster de Amazon Redshift que desea eliminar.

- SkipFinalClusterSnapshot

  Tipo: Booleano

  Predeterminado: false

  Descripción: (opcional) si se establece en `false`, la automatización crea una instantánea antes de eliminar el clúster de Amazon Redshift. Si se establece en `true`, no se crea una instantánea final del clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Pasos de documentos

- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `SkipFinalClusterSnapshot`.

- `aws:executeAwsApi`: elimina el clúster de Amazon Redshift especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el clúster de Amazon Redshift se haya eliminado.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` deshabilita la accesibilidad pública para el clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- ClusterIdentifier

  Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster para el que desea deshabilitar la accesibilidad pública.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: desactiva la accesibilidad pública para el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del clúster cambie a `available`.
- `aws:assertAwsResourceProperty`: confirma que la configuración de accesibilidad pública está deshabilitada en el clúster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` permite el registro de auditorías para el clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon Simple Storage Service (Amazon S3) al que desea cargar los registros.

- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el registro de auditoría.

- S3 KeyPrefix

  Tipo: cadena

  Descripción: (opcional) el prefijo clave de Amazon S3 (subcarpeta) en el que desea cargar los registros.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Pasos de documentos

- `aws:branch`: se ramifica en función de si se especificó un valor para el parámetro `S3KeyPrefix`.
- `aws:executeAwsApi`: habilita el registro de auditoría en el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el registro de auditoría fue habilitado en el clúster.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` permite realizar instantáneas automatizadas para el clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- AutomatedSnapshotRetentionPeriod

  Tipo: entero

  Valores válidos: 1-35

  Descripción: (obligatorio) el número de días que se conservan las instantáneas automatizadas.
- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar las instantáneas automatizadas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: activa las instantáneas de automatización en el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del clúster cambie a `available`.
- `aws:executeScript`: confirma que las instantáneas automatizadas estaban habilitadas en el clúster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descripción

El `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook permite el cifrado en el clúster de Amazon Redshift que especifique mediante AWS Key Management Service una clave gestionada por el cliente AWS KMS(). Este manual de procedimientos solo debe utilizarse como referencia para garantizar que los clústeres de Amazon Redshift estén cifrados de acuerdo con las prácticas recomendadas de seguridad mínimas. Recomendamos cifrar varios clústeres con diferentes claves administradas por el cliente. Este manual no puede cambiar la clave administrada por el AWS KMS cliente que se utiliza en un clúster ya cifrado. Para cambiar la clave gestionada por el AWS KMS cliente que se utiliza para cifrar un clúster, primero debe deshabilitar el cifrado en el clúster.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterIdentifier

  Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el cifrado.

- KMSKeyArn

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la clave AWS KMS administrada por el cliente que desea utilizar para cifrar los datos del clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: habilita el cifrado en el clúster de Amazon Redshift especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el cifrado esté habilitado en el clúster.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` permite un enrutamiento mejorado de la nube privada virtual (VPC) para el clúster de Amazon Redshift que especifique. Para obtener información acerca del enrutamiento mejorado de VPC, consulte Enrutamiento mejorado VPC de Amazon Redshift en la Guía de administración de Amazon Redshift.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: permite un enrutamiento de VPC mejorado en el clúster especificado en el parámetro `ClusterIdentifier`.
- `assertAwsResourceProperty`: confirma que el enrutamiento de VPC mejorado estaba habilitado en el clúster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` requiere que las conexiones entrantes usen SSL para el clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- ClusterIdentifier

  Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Pasos de documentos

- `aws:executeAwsApi`: recopila los detalles de los parámetros del clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:executeAwsApi`: activa la configuración `require_ssl` en el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: confirma que la configuración `require_ssl` estaba habilitada en el clúster.
- `aws:executeScript`: verifica la configuración `require_ssl` del clúster.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` modifica la configuración de mantenimiento del clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AllowVersionActualización

  Tipo: Booleano

  Descripción: (obligatorio) si se establece en `true`, las actualizaciones de las versiones principales se aplican automáticamente al clúster durante el período de mantenimiento.
- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- AutomatedSnapshotRetentionPeriod

  Tipo: entero

  Valores válidos: 1-35

  Descripción: (obligatorio) el número de días que se conservan las instantáneas automatizadas.
- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.
- PreferredMaintenanceVentana

Tipo: cadena

Descripción: (obligatorio) el intervalo de tiempo semanal (en UTC) durante el cual puede llevarse a cabo el mantenimiento del sistema.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: modifica la configuración de mantenimiento del clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: confirma que los ajustes de mantenimiento modificados se configuraron para el clúster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRedshiftClusterNodeType` modifica el tipo de nodo y la cantidad de nodos del clúster de Amazon Redshift que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- Classic

  Tipo: Booleano

  Descripción: (opcional) si se establece en `true`, la operación de cambio de tamaño utiliza el proceso de cambio de tamaño clásico.
- ClusterIdentifier

  Tipo: cadena

  Descripción: (obligatorio) el identificador único del clúster cuyo tipo de nodo desea modificar.
- ClusterType

  Tipo: cadena

  Valores válidos: single-node | multi-node

  Descripción: (obligatorio) el tipo de clúster que desea asignar a su clúster.
- NodeType

  Tipo: cadena

  Valores válidos: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  Descripción: (obligatorio) el tipo de nodo que desea asignar a su clúster.

- NumberOfNodos

  Tipo: entero

  Valores válidos: 2-100

  Descripción: (opcional) la cantidad de nodos que desea asignar a su clúster. Si su clúster es de un tipo `single-node`, no especifique un valor para este parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Pasos de documentos

- `aws:executeScript`: modifica el tipo de nodo y el número de nodos del clúster especificados en el parámetro `ClusterIdentifier`.

Amazon S3

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Storage Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-ArchiveS3BucketToIntelligentTiering
- AWS-ConfigureS3BucketLogging
- AWS-ConfigureS3BucketVersioning

- AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock
- AWSConfigRemediation-ConfigureS3PublicAccessBlock
- AWS-CreateS3PolicyToExpireMultipartUploads
- AWS-DisableS3BucketPublicReadWrite
- AWS-EnableS3BucketEncryption
- AWS-EnableS3BucketKeys
- AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy
- AWSConfigRemediation-RestrictBucketSSLRequestsOnly
- AWSSupport-TroubleshootS3PublicRead

AWS-ArchiveS3BucketToIntelligentTiering

Descripción

El `AWS-ArchiveS3BucketToIntelligentTiering` runbook crea o reemplaza una configuración de organización inteligente por niveles para el bucket de Amazon Simple Storage Service (Amazon S3) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) El nombre del depósito de S3 para el que desea crear una configuración de estratificación inteligente.

- ConfigurationId

  Tipo: cadena

  Descripción: (obligatorio) El ID de la configuración de organización inteligente por niveles. Puede ser un ID de configuración nuevo o el ID de una configuración existente.

- NumberOfDaysToArchivar

  Tipo: cadena

  Valores válidos: 90-730

  Descripción: (obligatorio) El número de días consecutivos transcurridos desde que un objeto de su depósito pueda pasar al nivel Archive Access.

- NumberOfDaysToDeepArchive

  Tipo: cadena

  Valores válidos: 180-730

  Descripción: (obligatorio) El número de días consecutivos transcurridos desde que un objeto de tu depósito pueda pasar al nivel de Deep Archive Access.

- S3Prefix

  Tipo: cadena

  Descripción: (opcional) El prefijo del nombre clave de los objetos a los que desea aplicar la configuración.

- Etiquetas

Tipo: MapList

Descripción: (opcional) Metadatos asignados a los objetos a los que desea aplicar la configuración. Las etiquetas constan de una clave y un valor definidos por el usuario.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Pasos de documentos

- PutsBucketIntelligentTieringConfiguration (AWS:ExecuteScript): crea o actualiza una configuración de Amazon S3 Intelligent-Tiering para el bucket especificado.
- VerifyBucketIntelligentTieringConfiguración (AwsResourcepropiedad aws:assert): verifica que la configuración inteligente del bucket de S3 se haya aplicado al bucket especificado.

AWS-ConfigureS3BucketLogging

Descripción

Activa el registro en un bucket de Amazon Simple Storage Service (Amazon S3).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 para el que desea configurar el registro.

- GrantedPermission

  Tipo: cadena

  Valores permitidos: FULL_CONTROL | READ | WRITE

  Descripción: (obligatorio) permisos de registro asignados al beneficiario para el bucket.

- GranteeEmailDirección

  Tipo: cadena

  (Opcional) Dirección de correo electrónico del beneficiario.

- GranteeId

  Tipo: cadena

  Descripción: (opcional) ID de usuario canónico del beneficiario.

- GranteeType

  Tipo: cadena

Valores válidos: CanonicalUser | AmazonCustomerByEmail | Grupo

Descripción: (obligatorio) tipo de beneficiario.

- GranteeUri

  Tipo: cadena

  Descripción: (opcional) URI del grupo de beneficiarios.

- TargetBucket

  Tipo: cadena

  Descripción: (obligatorio) especifica el bucket en el que desea que Amazon S3 almacene los registros de acceso al servidor. Puede hacer que los registros se entreguen en cualquier bucket de su propiedad. También puede configurar varios buckets para entregar sus registros en el mismo bucket de destino. En este caso, debe elegir uno diferente TargetPrefix para cada depósito de origen, de modo que los archivos de registro entregados se puedan distinguir por clave.

- TargetPrefix

  Tipo: cadena

  Valor predeterminado: /

  Descripción: (opcional) especifica un prefijo para las claves en las que se almacenarán los archivos de registro.

AWS-ConfigureS3BucketVersioning

Descripción

Configure el control de versiones para un bucket de Amazon Simple Storage Service (Amazon S3).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 para el que desea configurar el control de versiones.

- VersioningState

  Tipo: cadena

  Valores permitidos: Enabled | Suspended

  Valor predeterminado: Enabled

  Descripción: (opcional) Aplicada al VersioningConfiguration .Status. Cuando se establece en “Enabled”, este proceso permite el control de versiones para los objetos en el bucket, todos los objetos agregados al bucket reciben un ID de versión único. Cuando se establece en `Suspended`, este proceso deshabilita el control de versiones para los objetos en el bucket. Todos los objetos añadidos al bucket reciben el ID de versión `null`.

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Descripción

El manual de procedimientos `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` configura los ajustes del bloque de acceso público de Amazon Simple Storage Service (Amazon S3) para un bucket de Amazon S3 en función de los valores que especifique en los parámetros del manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- BlockPublicAcls

  Tipo: Booleano

  Predeterminado: true

  Descripción: (opcional) si se establece en `true`, Amazon S3 bloquea las listas de control de acceso público (ACL) del bucket de S3 y los objetos almacenados en el bucket de S3 que especifique en el parámetro `BucketName`.
- BlockPublicPolítica

  Tipo: Booleano

  Predeterminado: true

Descripción: (opcional) si se establece en `true`, Amazon S3 bloquea las políticas de bucket públicos para el bucket de S3 que especifique en el parámetro `BucketName`.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de S3 que desea configurar.

- IgnorePublicAcls

  Tipo: Booleano

  Predeterminado: true

  Descripción: (opcional) si se establece en `true`, Amazon S3 ignora todas las ACL públicas del bucket de S3 que especifique en el parámetro `BucketName`.

- RestrictPublicCubos

  Tipo: Booleano

  Predeterminado: true

  Descripción: (opcional) si se establece en `true`, Amazon S3 restringe las políticas de bucket públicos para el bucket de S3 que especifique en el parámetro `BucketName`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Pasos de documentos

- `aws:executeAwsApi`: crea o modifica la configuración `PublicAccessBlock` del bucket de S3 especificado en el parámetro `BucketName`.
- `aws:executeScript`: regresa la configuración `PublicAccessBlock` del bucket de S3 especificado en el parámetro `BucketName` y verifica que los cambios se hayan realizado correctamente en función de los valores especificados en los parámetros del manual de procedimientos.

`AWSConfigRemediation-ConfigureS3PublicAccessBlock`

Descripción

El `AWSConfigRemediation-ConfigureS3PublicAccessBlock` runbook configura los ajustes de un bloque de acceso público de Cuenta de AWS Amazon Simple Storage Service (Amazon S3) en función de los valores que especifique en los parámetros del runbook.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AccountId

  Tipo: cadena

  Descripción: (obligatorio) El ID del propietario del bucket de S3 Cuenta de AWS que está configurando.
- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BlockPublicAcls

  Tipo: Booleano

  Predeterminado: true

  Descripción: (Opcional) Si se establece en`true`, Amazon S3 bloquea las listas de control de acceso público (ACL) de los buckets S3 que pertenezcan a los Cuenta de AWS que especifique en el `AccountId` parámetro.

- BlockPublicPolítica

  Tipo: Booleano

  Predeterminado: true

  Descripción: (Opcional) Si se establece en`true`, Amazon S3 bloquea las políticas de bucket públicos para los buckets S3 propiedad de los Cuenta de AWS que especifique en el `AccountId` parámetro.

- IgnorePublicACL

  Tipo: Booleano

  Predeterminado: true

  Descripción: (Opcional) Si se establece en`true`, Amazon S3 ignora todas las ACL públicas de los buckets de S3 que sean propiedad de los Cuenta de AWS que especifique en el parámetro. `AccountId`

- RestrictPublicBuckets

  Tipo: Booleano

  Predeterminado: true

  Descripción: (Opcional) Si se establece en`true`, Amazon S3 restringe las políticas de bucket públicos para los buckets S3 propiedad de los Cuenta de AWS que especifique en el `AccountId` parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Pasos de documentos

- `aws:executeAwsApi`: crea o modifica la configuración `PublicAccessBlock` de la Cuenta de AWS especificada en el parámetro `AccountId`.
- `aws:executeScript`- Devuelve la `PublicAccessBlock` configuración de lo Cuenta de AWS especificado en el `AccountId` parámetro y verifica que los cambios se hayan realizado correctamente en función de los valores especificados en los parámetros del runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descripción

El `AWS-CreateS3PolicyToExpireMultipartUploads` manual crea una política de ciclo de vida para un segmento específico que vence de forma incompleta y las cargas de varias partes en curso transcurridos un número de días definido. Este manual combina la nueva política de ciclo de vida con cualquier política de ciclo de vida existente que ya exista.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de S3 que desea configurar.
- DaysUntilCaducar

  Tipo: entero

  Descripción: (Obligatorio) El número de días que Amazon S3 espera antes de eliminar permanentemente todas las partes de la carga.
- RuleId

  Tipo: cadena

  Descripción: (obligatorio) El identificador utilizado para identificar la regla del ciclo de vida. Debe ser un valor único.
- S3Prefix

  Tipo: cadena

  Descripción: (opcional) El prefijo del nombre clave de los objetos a los que desea aplicar la configuración.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Pasos de documentos

- ConfigureExpireMultipartUploads (AWS:ExecuteScript): configura la política de ciclo de vida del depósito.
- VerifyExpireMultipartUploads (AWS:ExecuteScript): verifica que la política de ciclo de vida se haya configurado para el depósito.

Salidas

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

AWS-DisableS3BucketPublicReadWrite

Descripción

Use Amazon Simple Storage Service (Amazon S3) `Block Public Access` para deshabilitar el acceso de lectura y escritura a un bucket de S3 público. Para obtener más información, consulte Uso de Bloqueo de acceso público de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) bucket de S3 cuyo acceso desea restringir.

AWS-EnableS3BucketEncryption

Descripción

Configura el cifrado por defecto de un bucket de Amazon Simple Storage Service (Amazon S3).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de S3 donde desea cifrar el contenido.

- SSEAlgorithm

  Tipo: cadena

  Valor predeterminado: AES256

  Descripción: (opcional) el algoritmo de cifrado del lado del servidor que se va a utilizar para el cifrado predeterminado.

AWS-EnableS3BucketKeys

Descripción

El `AWS-EnableS3BucketKeys` runbook habilita las claves de bucket en el bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Esta clave de nivel de depósito crea claves de datos para nuevos objetos durante su ciclo de vida. Si no especifica un valor para el `KmsKeyId` parámetro, se utiliza el cifrado del lado del servidor mediante claves gestionadas de Amazon S3 (SSE-S3) como configuración de cifrado predeterminada.

> **Note**
>
> Las claves de bucket de Amazon S3 no son compatibles con el cifrado de doble capa del lado del servidor con claves AWS Key Management Service (AWS KMS) (DSSE-KMS).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BucketName

  Tipo: cadena

  Descripción: (obligatorio) El nombre del bucket de S3 para el que desea habilitar las claves de bucket.
- KMS KeyId

  Tipo: cadena

  Descripción: (opcional) El nombre del recurso de Amazon (ARN), el ID de clave o el alias de clave de la clave gestionada por el cliente AWS Key Management Service (AWS KMS) que desea utilizar para el cifrado del lado del servidor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`

- `s3:PutEncryptionConfiguration`

Pasos de documentos

- ChooseEncryptionType (aws:branch): evalúa el valor proporcionado para el `KmsKeyId` parámetro para determinar si se utilizará SSE-S3 (AES256) o SSE-KMS.
- PutBucketkeysKMS (aws:executeAwsApi): establece la propiedad en el bucket S3 especificado utilizando el valor especificado. `BucketKeyEnabled` `true` `KmsKeyId`
- PutBucketkeySaes256 (aws:executeAwsApi): establece la `BucketKeyEnabled` propiedad en el bucket de S3 especificado con cifrado AES256. `true`
- VerifyS3 BucketKeysEnabled (AwsResourcepropiedad aws:assert): verifica que las claves de bucket estén habilitadas en el bucket S3 de destino.

`AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy`

Descripción

El manual de procedimientos `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` elimina las principales declaraciones de políticas que contienen caracteres comodín (`Principal: *` o `Principal: "AWS": *`) para acciones `Allow` de su política de bucket de Amazon Simple Storage Service (Amazon S3). También se eliminan las declaraciones de política con condiciones.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuya política desea modificar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Pasos de documentos

- `aws:executeScript`: modifica la política del bucket y verifica que las principales declaraciones de política con caracteres comodín se hayan eliminado del bucket de Amazon S3 que especificó en el parámetro `BucketName`.

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Descripción

El manual de procedimientos `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` crea una declaración de política de bucket de Amazon Simple Storage Service (Amazon S3) que deniega de forma explícita las solicitudes HTTP al bucket de Amazon S3 que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket de S3 al que desea denegar las solicitudes HTTP.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Pasos de documentos

- `aws:executeScript`: crea una política de bucket para el bucket de S3 especificado en el parámetro `BucketName` que deniega de forma explícita las solicitudes HTTP.

AWSSupport-TroubleshootS3PublicRead

Descripción

El manual de procedimientos `AWSSupport-TroubleshootS3PublicRead` diagnostica problemas al leer objetos del bucket público de Amazon Simple Storage Service (Amazon S3) que especifique en el parámetro `S3BucketName`. También se analiza un subconjunto de configuraciones para detectar los objetos del bucket de S3.

Ejecuta esta automatización (consola)

Limitaciones

- Esta automatización no comprueba los puntos de acceso que permiten el acceso público a los objetos.
- Esta automatización no evalúa las claves de condición de la política de bucket de S3.
- Si la utiliza AWS Organizations, esta automatización no evalúa las políticas de control de servicios para confirmar que se permite el acceso a Amazon S3.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CloudWatchLogGroupNombre

  Tipo: cadena

  Descripción: (opcional) El grupo de CloudWatch registros de Amazon Logs al que desea enviar el resultado de la automatización. Si no se encuentra ningún grupo de registro que coincida con el valor que ha especificado, la automatización creará un grupo de registro con este valor de parámetro. El período de retención del grupo de registro creado por esta automatización es de 14 días.

- CloudWatchLogStreamNombre

  Tipo: cadena

  Descripción: (opcional) El flujo de registro de CloudWatch registros al que desea enviar el resultado de la automatización. Si no se encuentra un flujo de registro que coincida con el valor especificado, la automatización creará un flujo de registro con este valor de parámetro. Si no especifica un valor para este parámetro, la automatización utilizará el `ExecutionId` como nombre del flujo de registro.

- HttpGet

  Tipo: Booleano

  Valores válidos: true | false

  Predeterminado: true

  Descripción: (opcional) si este parámetro está establecido en `true`, la automatización realiza una solicitud HTTP parcial a los objetos en el `S3BucketName` que especifique. Solo se regresa el primer byte del objeto mediante el encabezado HTTP Range.

- IgnoreBlockPublicAccess

  Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) si este parámetro está establecido en `true`, la automatización ignora la configuración del bloque de acceso público del bucket de S3 que especifique en el parámetro `S3BucketName`. No se recomienda cambiar este parámetro del valor predeterminado.

- MaxObjects

  Tipo: entero

  Valores válidos: 1-25

  Predeterminado: 5

  Descripción: (opcional) el número de objetos que se van a analizar en el bucket de S3 que especifique en el parámetro `S3BucketName`.

- S3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el nombre del bucket S3 para solucionar problemas.

- S3 PrefixName

  Tipo: cadena

  Descripción: (opcional) el prefijo del nombre clave de los objetos que desea analizar en su bucket de S3. Para obtener más información, consulte el tema para Claves de objetos en la Guía del usuario de Amazon Simple Storage Service.

- StartAfter

  Tipo: cadena

  Descripción: (opcional) el nombre de la clave del objeto en el que desea que la automatización comience a analizar los objetos del bucket de S3.

- ResourcePartition

  Tipo: cadena

Valores válidos: `aws` | `aws-us-gov` | `aws-cn`

Valor predeterminado: `aws`

Descripción: (obligatorio) la partición donde está ubicado su bucket de S3.

- Detallado

  Tipo: Booleano

  Valores válidos: true | false

  Predeterminado: false

  Descripción: (opcional) para obtener información más detallada durante la automatización, defina este parámetro en `true`. Si el parámetro está establecido en `false`, solo se regresarán los mensajes de advertencia y error.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Los `logs:PutLogEvents` permisos `logs:CreateLogGrouplogs:CreateLogStream`, y solo son necesarios si deseas que la automatización envíe datos de registro a 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"
        }
    ]
}
```

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el bucket de S3 existe y es accesible.
- `aws:executeScript`: regresa la ubicación del bucket de S3 y su ID de usuario canónico.
- `aws:executeScript`: regresa la configuración de bloqueo de acceso público de su cuenta y del bucket de S3.
- `aws:assertAwsResourceProperty`: confirma que el pagador de bucket de S3 está configurado en `BucketOwner`. Si `Requester Pays` está habilitado en el bucket de S3, la automatización finaliza.
- `aws:executeScript`: regresa el estado de la política del bucket de S3 y determina si se considera público. Para obtener más información acerca de los buckets S3 públicos, consulte El significado de “público” en la Guía del usuario de Amazon Simple Storage Service.
- `aws:executeAwsApi`: regresa la política de bucket de S3.

- `aws:executeAwsApi`: regresa todas las claves de contexto que se encuentran en la política de bucket de S3.
- `aws:assertAwsResourceProperty`: confirma si hay una denegación explícita en la política del bucket de S3 para la acción de la API `GetObject`.
- `aws:executeAwsApi`: regresa la lista de control de acceso (ACL) para el bucket de S3.
- `aws:executeScript`- Crea un grupo de CloudWatch registros y un flujo de registros si se especifica un valor para el `CloudWatchLogGroupName` parámetro.
- `aws:executeScript`: en función de los valores que especifique en los parámetros de entrada del manual de procedimientos, evalúa si alguna de las configuraciones del bucket de S3 recopiladas durante la automatización impide que el público acceda a los objetos. Este script realiza las siguientes funciones:
  - Evalúa la configuración de los bloques de acceso público
  - Regresa los objetos de su bucket de S3 en función de los valores que especifique en los parámetros `MaxObjects`, `S3PrefixName` y `StartAfter`.
  - Regresa la política del bucket de S3 para simular una política de IAM personalizada para los objetos regresados desde su bucket de S3.
  - Realiza una solicitud HTTP parcial a los objetos regresados si el parámetro `HttpGet` está establecido en `true`. Solo se regresa el primer byte del objeto mediante el encabezado HTTP Range.
  - Comprueba el nombre clave del objeto regresado para confirmar si termina con uno o dos puntos. Los nombres de claves de objeto que terminan en puntos no se pueden descargar de la consola de Amazon S3.
  - Comprueba si el propietario del objeto regresado coincide con el propietario del bucket de S3.
  - Comprueba si la ACL del objeto concede permisos de `READ` o `FULL_CONTROL` a usuarios anónimos.
  - Regresa las etiquetas asociadas al objeto.
  - Utiliza la política de IAM simulada para confirmar si hay una denegación explícita de este objeto en la política de bucket de S3 para la acción de la API `GetObject`.
  - Regresa los metadatos del objeto para confirmar que se admite la clase de almacenamiento.
  - Comprueba la configuración de cifrado del lado del servidor del objeto para confirmar si el objeto está cifrado mediante una AWS Key Management Service (AWS KMS) clave gestionada por el cliente.

Salidas

AnalyzeObjects.bucket

AnalyzeObjects.objeto

SageMaker

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon SageMaker. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-DisableSageMakerNotebookRootAccess

AWS-DisableSageMakerNotebookRootAccess

Descripción

El `AWS-DisableSageMakerNotebookRootAccess` runbook deshabilita el acceso root en una instancia de Amazon SageMaker Notebook. Durante la automatización, la instancia del bloc de notas se detiene para realizar los cambios necesarios. SageMaker No se admiten las instancias de Studio Notebook.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- NotebookInstanceNombre

  Tipo: cadena

  Descripción: (obligatorio) El nombre de la instancia del SageMaker bloc de notas a la que se va a deshabilitar el acceso root.

- StartInstanceAfterUpdate

  Tipo: Booleano

  Predeterminado: true

  Descripción: (opcional) Determina si la instancia del bloc de notas se inicia después de deshabilitar el acceso raíz. La configuración predeterminada de este parámetro es`true`. Si se establece en`true`, la instancia se inicia cuando se deshabilita el acceso a la raíz. Si se establece en`false`, la instancia permanece en ese `stopped` estado después de deshabilitar el acceso raíz.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Pasos de documentos

- CheckNotebookInstanceStatus (aws:executeAwsApi): comprueba el estado actual de la instancia del bloc de notas.
- StopOrUpdateNotebookInstance (aws:branch): se ramifica según el estado de la instancia del bloc de notas.
- StopNotebookInstance (aws:executeAwsApi): inicia la instancia si el estado es. `stopped`
- WaitForInstanceToStop (aws:wait ForAwsResourceProperty): verifica que la instancia sea. `stopped`
- UpdateNotebookInstance (aws:executeAwsApi): inhabilita el acceso root en la instancia del bloc de notas.
- WaitForNotebookUpdate (aws:wait ForAwsResourceProperty): verifica que el acceso a la raíz se haya deshabilitado y que la instancia esté en estado. `stopped`
- ChooseInstanceStart (aws:branch): se ramifica en función de si la instancia debe iniciarse.
- StartNotebookInstance (aws:executeAwsApi): inicia la instancia del bloc de notas.
- VerifyNotebookInstanceStatus (aws:wait ForAwsResourceProperty): Comprueba si la instancia está `available` activa antes de deshabilitar el acceso root.
- VerifyNotebookInstanceRootAccess (aws:assert AwsResource Property): verifica que la configuración de acceso raíz de la instancia del bloc de notas esté deshabilitada correctamente.

Secrets Manager

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Secrets Manager Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

AWSConfigRemediation-DeleteSecret

Descripción

El `AWSConfigRemediation-DeleteSecret` runbook elimina un secreto y todas las versiones almacenadas en él. AWS Secrets Manager Si lo desea, puede especificar el período de recuperación durante el cual puede restaurar el secreto. Si no especifica un valor para el parámetro `RecoveryWindowInDays`, la operación se establece de forma predeterminada en 30 días.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- RecoveryWindowInDays

  Tipo: entero

  Valores válidos: 7-30

  Valor predeterminado: 30

  Descripción: (opcional) el número de días durante los que puede restaurar el secreto.
- SecretId

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del secreto que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

Pasos de documentos

- `aws:executeAwsApi`: elimina el secreto que especifique en el parámetro `SecretId`.
- `aws:executeScript`: verifica que se ha programado la eliminación del secreto.

`AWSConfigRemediation-RotateSecret`

Descripción

El `AWSConfigRemediation-RotateSecret` runbook rota un secreto almacenado en. AWS Secrets Manager

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- RotationInterval

  Tipo: Interval

  Valores válidos: 1-365

  Descripción: (obligatorio) el número de días entre las rotaciones del secreto.

- RotationLambdaArn

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la función AWS Lambda que puede rotar el secreto.

- SecretId

  Tipo: cadena

  Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del secreto que desea rotar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Pasos de documentos

- `aws:executeAwsApi`: rota el secreto que especifique en el parámetro `SecretId`.
- `aws:executeScript`: verifica que la rotación esté habilitada en el secreto.

Security Hub

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Security Hub Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

Descripción

El `AWSConfigRemediation-EnableSecurityHub` manual habilita AWS Security Hub (Security Hub) para la automatización Cuenta de AWS y el Región de AWS lugar donde se ejecuta. Para obtener información sobre Security Hub, consulte ¿Qué es AWS Security Hub? en la Guía AWS Security Hub del usuario.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EnableDefaultEstándares

  Tipo: Booleano

  Predeterminado: true

  Descripción: (obligatorio) si se establece en `true`, se habilitan los estándares de seguridad predeterminados designados por Security Hub.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Pasos de documentos

- `aws:executeAwsApi`: activa Security Hub en la cuenta y región actuales.
- `aws:executeAwsApi`: verifica que se haya habilitado Security Hub.

AWS Shield

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Shield Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSPremiumSupport-DDoSResiliencyAssessment

AWSPremiumSupport-DDoSResiliencyAssessment

Descripción

El manual de procedimientos `AWSPremiumSupport-DDoSResiliencyAssessment`de automatización AWS Systems Managerle ayuda a comprobar las vulnerabilidades DDoS y a configurar los recursos de acuerdo con la protección AWS Shield Advancedpara su Cuenta de AWS. Proporciona un informe sobre los ajustes de configuración de los recursos que son vulnerables a los ataques de Distributed Denial of Service (DDoS). Se utiliza para recopilar, analizar y evaluar los siguientes recursos: Amazon Route 53, Amazon Load Balancers, CloudFront distribuciones de Amazon AWS Global Accelerator e IP AWS elásticas para sus ajustes de configuración, de acuerdo con las prácticas recomendadas de protección. AWS Shield Advanced El informe de configuración final está disponible en el bucket de Amazon S3 de su elección como archivo HTML.

¿Cómo funciona?

Este manual de procedimientos contiene una serie de comprobaciones para los distintos tipos de recursos que están habilitados para el acceso público y si tienen las protecciones configuradas según las recomendaciones del AWSDocumento técnico sobre las mejores prácticas de DDoS. El manual de procedimientos realiza lo siguiente:

- Comprueba si una suscripción a AWS Shield Advancedestá habilitada.
- Si está habilitada, busca si hay algún recurso protegido por Shield Advanced.
- Busca todos los recursos mundiales y regionales en Cuenta de AWSy comprueba si están protegidos por Shield.
- Requiere los parámetros del tipo de recurso para la evaluación, el nombre del bucket de Amazon S3 y el Cuenta de AWS ID del bucket de Amazon S3 (S3BucketOwner).
- Regresa los resultados como un informe HTML almacenado en el bucket de Amazon S3 proporcionado.

Los parámetros de entrada `AssessmentType`deciden si se realizarán las comprobaciones de todos los recursos. De forma predeterminada, el manual de procedimientos comprueba todos los tipos de recursos. Si solo se selecciona el parámetro `GlobalResource`so `RegionalResources`, el manual de procedimientos comprueba únicamente los tipos de recursos seleccionados.

> **Important**
>
> - El acceso a los manuales de procedimientos de `AWSPremiumSupport-*` requiere una suscripción a Enterprise o Business Support. Para obtener más información, consulte Comparar AWS Supportplanes.
> - Este manual de procedimientos requiere una AWS Shield Advancedsuscripción `ACTIVE`.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- AssessmentType

  Tipo: cadena

  Descripción: (Opcional) Determina el tipo de recursos que se van a evaluar para la evaluación de resiliencia de DDoS. De forma predeterminada, el manual de procedimientos evaluará los recursos tanto globales como regionales. Para los recursos regionales, el manual de procedimientos

describe todos los equilibradores de carga de aplicaciones (ALB) y redes (NLB), así como todo el grupo de escalado automático de su Cuenta de AWS/región.

Valores válidos: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

Predeterminado: recursos globales y regionales

- S3 BucketName

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

  Descripción: (Obligatorio) El nombre del bucket de Amazon S3 en el que se cargará el informe.

  Valor permitido: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  Tipo: cadena

  Descripción: (Opcional) La Cuenta de AWSpropietaria del bucket de Amazon S3. Por favor especifique este parámetro si el bucket de Amazon S3 pertenece a una Cuenta de AWSdistinta; de lo contrario puede dejar este parámetro en blanco.

  Valor permitido: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  Tipo: `AWS::IAM::Role::Arn`

  Descripción: (Opcional) El ARN de un rol de IAM con permisos para describir el bucket de Amazon S3 y Cuenta de AWSbloquear la configuración de acceso público si el bucket está en otra Cuenta de AWS. Si no se especifica este parámetro, el manual de procedimientos utilizará `AutomationAssumeRole`o el usuario de IAM que inició este manual de procedimientos (si `AutomationAssumeRole`no se especifica). Por favor consulte la sección de permisos necesarios en la descripción del manual de procedimientos.

  Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

  Tipo: cadena

Descripción: (Opcional) El prefijo de la ruta dentro de Amazon S3 para almacenar los resultados.

Valor permitido: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Ejemplo de política de IAM para el rol 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"
                        }
                    ]
                }
```

Instrucciones

1. Navegue hasta el AWSPremiumSupport-DDoS ResiliencyAssessment en la AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización)
3. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

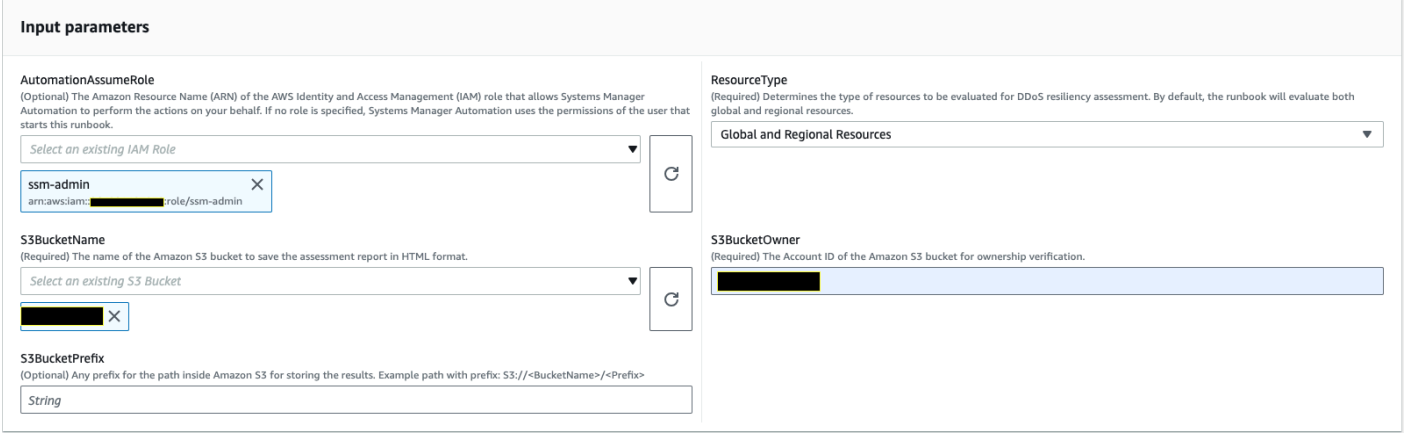
     El nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
   - AssessmentType (Opcional):

     Determina el tipo de recursos que se van a evaluar para la evaluación de resiliencia de DDoS. De forma predeterminada, el manual de procedimientos evalúa tanto los recursos globales como los regionales.
   - S3 BucketName (obligatorio):

     El nombre del bucket de Amazon S3 para guardar el informe de evaluación en formato HTML.
   - S3 BucketOwner (opcional):

     El ID de la Cuenta de AWSdel bucket de Amazon S3 para verificar la propiedad. El ID de la Cuenta de AWSes obligatorio si el informe debe publicarse en un bucket de Amazon S3 multicuenta y es opcional si el bucket de Amazon S3 se encuentra en la misma Cuenta de AWSdonde se inició la automatización.
   - S3 BucketPrefix (opcional):

     Cualquier prefijo de la ruta dentro de Amazon S3 para almacenar los resultados.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - CheckShieldAdvancedState:

     Comprueba si el bucket de Amazon S3 especificado en «S3BucketName» permite permisos de acceso de lectura o escritura anónimos o públicos, si el bucket tiene activado el cifrado en reposo y si el Cuenta de AWS ID proporcionado en «S3BucketOwner» es el propietario del bucket de Amazon S3.
   - S3BucketSecurityChecks:

     Comprueba si el bucket de Amazon S3 especificado en «S3BucketName» permite permisos de acceso de lectura o escritura anónimos o públicos, si el bucket tiene activado el cifrado en reposo y si el Cuenta de AWS ID proporcionado en «S3BucketOwner» es el propietario del bucket de Amazon S3.
   - BranchOnShieldAdvancedStatus:

     Ramifica los pasos del documento en función del estado de la suscripción AWS Shield Advancedo del estado de propiedad del bucket de Amazon S3.
   - ShieldAdvancedConfigurationReview:

     Revisa las configuraciones de Shield Advanced para garantizar que estén presentes los detalles mínimos requeridos. Por ejemplo: el equipo de IAM Access para AWS ShieldResponse Team (SRT), los detalles de la lista de contactos y el estado de participación proactiva del SRT.
   - ListShieldAdvancedProtections:

     Muestra los recursos protegidos de Shield y crea un grupo de recursos protegidos para cada servicio.
   - BranchOnResourceTypeAndCount:

     Ramifica los pasos del documento según el valor del parámetro Resource Type y la cantidad de recursos globales protegidos por Shield.
   - ReviewGlobalResources:

     Revisa los recursos globales protegidos de Shield Advanced, como las zonas alojadas, las CloudFront distribuciones y los aceleradores globales de Route 53.
   - BranchOnResourceType:

Ramifica los pasos del documento en función de las selecciones de tipo de recurso, ya sean globales, regionales o ambas.

- ReviewRegionalResources:

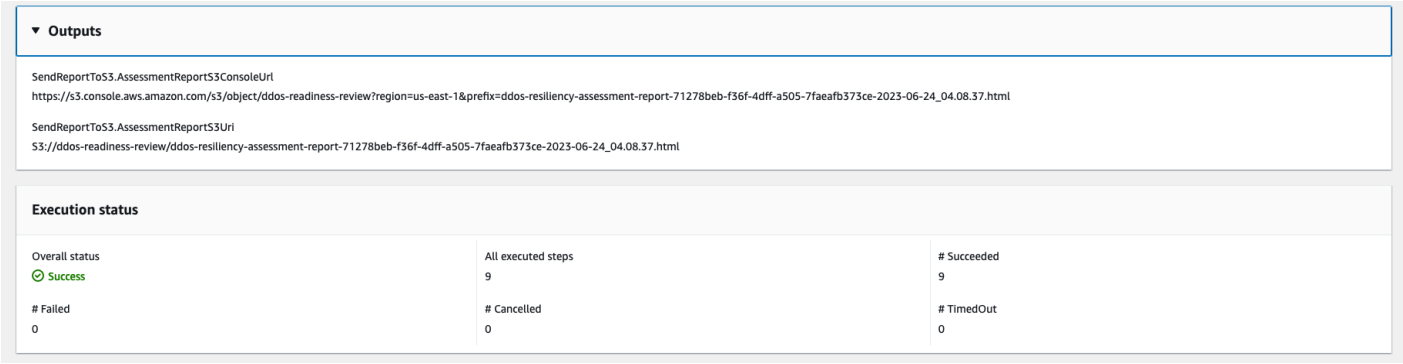
  Revisa los recursos regionales protegidos de Shield Advanced, como los equilibradores de carga de aplicaciones, los equilibradores de carga de red, los equilibradores de carga clásicos y las instancias de Amazon Elastic Compute Cloud (Amazon EC2) (Elastic IPs).

- SendReportToS3:

  Carga los detalles del informe de evaluación de DDoS en el bucket de Amazon S3.

7. Una vez completado, el URI del archivo HTML del informe de evaluación se proporciona en el bucket de Amazon S3:

   Enlace a la consola S3 y URI de Amazon S3 para el informe sobre la ejecución correcta del manual de procedimientos



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Notification Service. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

AWS-EnableSNSTopicDeliveryStatusLogging

Descripción

El `AWS-EnableSNSTopicDeliveryStatusLogging` manual configura el registro del estado de la entrega para un punto HTTP final de Amazon Data Firehose, Lambda o Amazon Simple `Platform application` Queue Service (Amazon SQS). Esto permite a Amazon SNS registrar las alertas fallidas y una muestra del porcentaje de notificaciones de alertas que se han enviado correctamente a Amazon. CloudWatch Si el registro del estado de entrega ya está configurado para el tema, el manual sustituirá la configuración existente por los nuevos valores que especifique para los parámetros de entrada.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EndpointType

  Tipo: cadena

  Valores válidos:

  - HTTP
  - Firehose
  - Lambda
  - Aplicación
  - SQS

  Descripción: (Obligatorio) El tipo de punto final temático de Amazon SNS para el que desea registrar los mensajes de notificación del estado de la entrega.

- TopicArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del tema de Amazon SNS para el que desea configurar el registro del estado de entrega.

- SuccessFeedbackRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la función de IAM que Amazon SNS utiliza para enviar los registros de los mensajes de notificación correctos. CloudWatch

- SuccessFeedbackSampleRate

  Tipo: cadena

Valores válidos: 0-100

Descripción: (Obligatorio) El porcentaje de mensajes correctos que se deben muestrear para el tema de Amazon SNS especificado.

- FailureFeedbackRoleArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la función de IAM que Amazon SNS utiliza para enviar los registros de los mensajes de notificación de errores. CloudWatch

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Pasos de documentos

- `aws:executeAwsApi`- Aplica el valor del `SuccessFeedbackRoleArn` parámetro al tema de Amazon SNS.
- `aws:executeAwsApi`- Aplica el valor del `SuccessFeedbackSampleRate` parámetro al tema de Amazon SNS.
- `aws:executeAwsApi`- Aplica el valor del `FailureFeedbackRoleArn` parámetro al tema de Amazon SNS.
- `aws:executeScript`- Confirma que el registro del estado de la entrega está habilitado en el tema Amazon SNS.

Salidas

VerifyDeliveryStatusLoggingActivado. GetTopicAttributesResponse - Respuesta de las operaciones de la `GetTopicAttributes` API.

VerifyDeliveryStatusLoggingHabilitado. VerifyDeliveryStatusLoggingEnabled - Mensaje que indica que se ha verificado correctamente el registro del estado de la entrega.

AWSConfigRemediation-EncryptSNSTopic

Descripción

El `AWSConfigRemediation-EncryptSNSTopic` manual permite el cifrado en el tema del Amazon Simple Notification Service (Amazon SNS) que especifique mediante una clave gestionada por el cliente AWS Key Management Service (AWS KMS). Este manual de procedimientos solo debe usarse como referencia para garantizar que los temas de Amazon SNS estén cifrados de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varios temas con diferentes claves administradas por el cliente.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- KmsKeyArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la clave de AWS KMS administrada por el cliente que desea utilizar para cifrar el tema de Amazon SNS.

- TopicArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN del tema de Amazon SNS que desea cifrar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Pasos de documentos

- `aws:executeAwsApi`: cifra el tema de Amazon SNS que especifique en el parámetro `TopicArn`.
- `aws:assertAwsResourceProperty`: confirma que el cifrado está habilitado en el tema de Amazon SNS.

AWS-PublishSNSNotification

Descripción

Publicar una notificación en Amazon SNS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Mensaje

  Tipo: cadena

  Descripción: (obligatorio) el mensaje que se incluirá en la notificación de SNS.
- TopicArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN del tema de SNS en el que se publicará la notificación.

Amazon SQS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Queue Service (Amazon SQS). Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

Descripción

El `AWS-EnableSQSEncryption` runbook permite el cifrado en reposo para una cola del Amazon Simple Queue Service (Amazon SQS). Una cola de Amazon SQS se puede cifrar con claves administradas de Amazon SQS (SSE-SQS) o con AWS Key Management Service claves administradas () (SSE-KMS). AWS KMS La clave que asigne a la cola debe tener una política de claves que incluya permisos para todos los principales que estén autorizados a utilizar la cola. Con el cifrado activado, se rechazan `ReceiveMessage` las solicitudes anónimas `SendMessage` y las dirigidas a la cola cifrada.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- QueueUrl

  Tipo: cadena

  Descripción: (Obligatorio) La URL de la cola de Amazon SQS en la que desea activar el cifrado.

- KmsKeyId

  Tipo: cadena

  Descripción: (opcional) La AWS KMS clave que se utilizará para el cifrado. Este valor puede ser un identificador único global, un ARN para un alias o una clave, o un nombre de alias con el prefijo «alias/». También puede usar la clave AWS administrada especificando el alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

  Tipo: cadena

  Valores válidos: 60-86400

  Predeterminado: 300

  Descripción: (opcional) El tiempo, en segundos, que una cola de Amazon SQS puede reutilizar una clave de datos para cifrar o descifrar los mensajes antes de volver a llamar. AWS KMS

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Pasos de documentos

- SelectKeyType (aws:branch): se ramifica según la clave especificada.
- PutAttributeSseKms (aws:executeAwsApi) - Actualiza la cola de Amazon SQS para usar la AWS KMS clave especificada para el cifrado.
- PutAttributeSseSqs (aws:executeAwsApi) - Actualiza la cola de Amazon SQS para utilizar la clave de cifrado predeterminada.
- VerifySqsEncryptionKms (aws: assertAwsResource Property): verifica que el cifrado esté habilitado en la cola de Amazon SQS.

- VerifySqsEncryptionDefault (aws: assertAwsResource Property): verifica que el cifrado esté habilitado en la cola de Amazon SQS.

Step Functions

AWS Systems Manager La automatización proporciona manuales predefinidos para AWS Step Functions (Step Functions). Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-EnableStepFunctionsStateMachineLogging

AWS-EnableStepFunctionsStateMachineLogging

Descripción

El `AWS-EnableStepFunctionsStateMachineLogging` runbook habilita o actualiza el registro en la máquina de AWS Step Functions estados que especifique. El nivel de registro mínimo debe estar establecido en `ALL`ERROR, o`FATAL`.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.

- Nivel

  Tipo: cadena

  Valores válidos: ALL | ERROR | FATAL

  Descripción: (Obligatorio) La URL de la cola de Amazon SQS en la que desea activar el cifrado.

- LogGroupArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del grupo de CloudWatch registros de Amazon Logs al que desea enviar los registros de las máquinas de estado.

- StateMachineArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN de la máquina de estado en la que desea habilitar el inicio de sesión.

- IncludeExecutionData

  Tipo: Booleano

  Valor predeterminado: False

  Descripción: (opcional) Determina si los datos de ejecución se incluyen en los registros.

- TracingConfiguration

  Tipo: Booleano

  Valor predeterminado: False

  Descripción: (opcional) Determina si AWS X-Ray el rastreo está habilitado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Pasos de documentos

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- Actualiza la máquina de estados especificada con la configuración de registro especificada.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- Verifica que el registro esté habilitado en la máquina de estado especificada.

Salidas

- EnableStepFunctionsStateMachineLogging.Response: respuesta de la llamada a la UpdateStateMachine API.

Systems Manager

AWS Systems Manager La automatización proporciona manuales predefinidos para Systems Manager. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- 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

Descripción

El manual de procedimientos `AWS-BulkDeleteAssociation` le ayuda a eliminar hasta 50 asociaciones de administradores de estados de Systems Manager a la vez.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AssociationIds

  Tipo: StringList

  Descripción: (obligatorio) lista separada por comas de los ID de las asociaciones que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:DeleteAssociation`

Pasos de documentos

- `aws:executeScript`: elimina las asociaciones especificadas en el parámetro `AssociationIds`.

AWS-BulkEditOpsItems

Descripción

El `AWS-BulkEditOpsItems` manual le ayuda a editar el estado, la gravedad, la categoría o la prioridad de AWS Systems Manager OpsItems. Esta automatización puede editar un máximo de 50 OpsItems a la vez.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Categoría

  Tipo: cadena

  Valores válidos:
  - Disponibilidad
  - Costo
  - Sin cambios
  - Rendimiento
  - Recuperación
  - Seguridad

  Predeterminado: sin cambios

  Descripción: (opcional) La nueva categoría que desea especificar para los editados OpsItems.
- OpsItemIds

  Tipo: StringList

  Descripción: (Obligatorio) Lista de OpsItems identificadores separados por comas que deseas editar (por ejemplo, OI-xxxxxxxxxxxx, OI-xxxxxxxxxxxx).
- Priority (Prioridad)

  Tipo: cadena

  Valores válidos:
  - Sin cambios

- 1
- 2
- 3
- 4
- 5

Predeterminado: sin cambios

Descripción: (opcional) La importancia de lo editado en relación con otros elementos del sistema. OpsItems OpsItems

- Gravedad

  Tipo: cadena

  Valores válidos:

  - Sin cambios
  - 1
  - 2
  - 3
  - 4

  Predeterminado: sin cambios

  Descripción: (opcional) La gravedad de lo editado OpsItems.

- WaitTimeBetweenEditsInSecs

  Tipo: cadena

  Valores válidos: 0.0-2.0

  Valor predeterminado: 0,8

  Descripción: (opcional) el tiempo que espera la automatización entre las llamadas a la operación `UpdateOpsItems`.

- Status

  Tipo: cadena

Valores válidos:

- InProgress
- Sin cambios
- Abra
- Resolved (Resuelto)

Predeterminado: sin cambios

Descripción: (opcional) El nuevo estado de lo editado OpsItems.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Pasos de documentos

- `aws:executeScript`- Edita OpsItems lo que especificó en el `OpsItemIds` parámetro en función de los valores que especifique para los `Status` parámetros `CategoryPriority`,`Severity`, y.

AWS-BulkResolveOpsItems

Descripción

El `AWS-BulkResolveOpsItems` manual resuelve los filtros AWS Systems Manager OpsItems que coincidan con el filtro que especifique. También puede especificar un elemento OpsItemId para añadirlo al resuelto OpsItems mediante el `OpsInsightsId` parámetro. Si especifica un valor para el parámetro `S3BucketName`, se envía un resumen de los resultados al bucket de Amazon Simple Storage Service (Amazon S3). Para recibir una notificación una vez que se haya enviado el resumen de los resultados al bucket de Amazon S3, especifique un valor para el parámetro `SnsTopicArn`. Esta automatización resolverá un máximo de 1000 OpsItems a la vez.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Filtros

  Tipo: cadena

  Descripción: (Obligatorio) Los pares de filtros clave-valor para devolver OpsItems lo que desea resolver. Por ejemplo, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Para obtener más información sobre las opciones disponibles para filtrar OpsItems las respuestas, consulta OpsItemlos filtros en la referencia de la AWS Systems Manager API.
- OpsInsightID

  Tipo: cadena

  Descripción: (opcional) El identificador de recurso relacionado que quieres añadir a Resolved OpsItems.
- S3 BucketName

  Tipo: cadena

Descripción: (opcional) el nombre del bucket de Amazon S3 al que desea enviar el resumen de resultados.

- SnsMessage

  Tipo: cadena

  Descripción: (opcional) la notificación que desea que Amazon Simple Notification Service (Amazon SNS) envíe cuando se complete la automatización.

- SnsTopicArn

  Tipo: cadena

  Descripción: (opcional) el ARN del tema de Amazon SNS que desea notificar cuando se envíe el resumen de resultados a Amazon S3.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Pasos de documentos

- `aws:executeScript`- Recopila y resuelve en OpsItems función de los filtros que especifique. Si especificó un valor para el parámetro `OpsInsightId`, el valor se añade como un recurso relacionado.
- `aws:executeScript`: si especificó un valor para el parámetro `S3BucketName`, se enviará un resumen de los resultados al bucket de Amazon S3.

- `aws:executeScript`: si especificó un valor para el parámetro `SnsTopicArn`, se enviará una notificación al tema de Amazon SNS después de enviar el resumen de los resultados a Amazon S3, incluyendo el valor del parámetro `SnsMessage` si se ha especificado.

AWS-ConfigureMaintenanceWindows

Descripción

El manual de procedimientos `AWS-ConfigureMaintenanceWindows` le ayuda a habilitar o deshabilitar varias ventanas de mantenimiento de Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- MaintenanceWindows

  Tipo: StringList

  Descripción: (obligatorio) lista separada por comas de los ID de las ventanas de mantenimiento que desea habilitar o deshabilitar.

- MaintenanceWindowsEstado

  Tipo: cadena

  Valores válidos: “True” | “False”

  Valor predeterminado: “False”

  Descripción: (obligatorio) determina si las ventanas de mantenimiento están habilitadas o deshabilitadas. Especifique “Verdadero” para habilitar las ventanas de mantenimiento y “Falso” para deshabilitarlas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Pasos de documentos

- `aws:executeScript`: recopila el estado de las ventanas de mantenimiento que especifique en el parámetro `MaintenanceWindows` y habilita o deshabilita las ventanas de mantenimiento.

AWS-CreateManagedLinuxInstance

Descripción

Cree una instancia EC2 para Linux que esté configurada para Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AmiId

  Tipo: cadena

  Descripción: (obligatorio) ID AMI que se va a utilizar para lanzar la instancia.
- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- GroupName

  Tipo: cadena

  Predeterminado: instancias SSM SecurityGroup ForLinux

  Descripción: (obligatorio) nombre de grupo de seguridad que se va a crear.
- HttpTokens

  Tipo: cadena

  Valores válidos: opcional | obligatorio

  Predeterminado: opcional

  Descripción: (opcional) IMDSv2 utiliza sesiones basadas en token. Defina el uso de los tokens HTTP a `optional` o `required` para determinar si IMDSv2 es opcional u obligatorio.
- InstanceType

  Tipo: cadena

  Valor predeterminado: t2.medium

Descripción: (obligatorio) tipo de instancia que se va a lanzar. El valor predeterminado es t2.medium.

- KeyPairNombre

  Tipo: cadena

  Descripción: (obligatorio) par de claves que se utilizará al crear una instancia.

- RemoteAccessCidr

  Tipo: cadena

  Valor predeterminado: 0.0.0.0/0

  Descripción: (obligatorio) crea un grupo de seguridad con puerto para SSH(Rango de puerto 22) abierto a las IP especificadas por CIDR (el valor predeterminado es 0.0.0.0/0). Si el grupo de seguridad ya existe no será modificado y no se cambiarán las reglas.

- RoleName

  Tipo: cadena

  Predeterminado: SSM ManagedInstance ProfileRole

  Descripción: (obligatorio) nombre de rol que se va a crear.

- StackName

  Tipo: cadena

  Predeterminado: CreateManagedInstanceStack {{Automation:EXECUTION_ID}}

  Descripción: (opcional) especificar el nombre de pila que utiliza este manual de procedimientos

- SubnetId

  Tipo: cadena

  Valor predeterminado: Default

  Descripción: (obligatorio) una nueva instancia se implementará en esta subred o en la subred predeterminada si no se especifica.

- VpcId

Tipo: cadena

Valor predeterminado: Default

Descripción: (obligatorio) una nueva instancia se implementará en este Amazon Virtual Private Cloud (Amazon VPC) o en la Amazon VPC predeterminada si no se especifica.

AWS-CreateManagedWindowsInstance

Descripción

Cree una instancia EC2 para la Windows Server que esté configurada para Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Parámetros

- AmiId

  Tipo: cadena

  Valor predeterminado: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

  Descripción: (obligatorio) ID AMI que se va a utilizar para lanzar la instancia.
- AutomationAssumeRole

  Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- GroupName

  Tipo: cadena

  SecurityGroupForLinuxPredeterminado: instancias SSM

  Descripción: (obligatorio) nombre de grupo de seguridad que se va a crear.

- HttpTokens

  Tipo: cadena

  Valores válidos: opcional | obligatorio

  Predeterminado: opcional

  Descripción: (opcional) IMDSv2 utiliza sesiones basadas en token. Defina el uso de los tokens HTTP a `optional` o `required` para determinar si IMDSv2 es opcional u obligatorio.

- InstanceType

  Tipo: cadena

  Valor predeterminado: t2.medium

  Descripción: (obligatorio) tipo de instancia que se va a lanzar. El valor predeterminado es t2.medium.

- KeyPairNombre

  Tipo: cadena

  Descripción: (obligatorio) par de claves que se utilizará al crear una instancia.

- RemoteAccessCidr

  Tipo: cadena

  Valor predeterminado: 0.0.0.0/0

Descripción: (obligatorio) crea un grupo de seguridad con puerto para RDP (Rango de puerto 3389) abierto a las IP especificadas por CIDR (el valor predeterminado es 0.0.0.0/0). Si el grupo de seguridad ya existe no será modificado y no se cambiarán las reglas.

- RoleName

  Tipo: cadena

  Predeterminado: SSM ManagedInstance ProfileRole

  Descripción: (obligatorio) nombre de rol que se va a crear.

- StackName

  Tipo: cadena

  Predeterminado: CreateManagedInstanceStack {{Automation:EXECUTION_ID}}

  Descripción: (opcional) especificar el nombre de pila que utiliza este manual de procedimientos

- SubnetId

  Tipo: cadena

  Valor predeterminado: Default

  Descripción: (obligatorio) una nueva instancia se implementará en esta subred o en la subred predeterminada si no se especifica.

- VpcId

  Tipo: cadena

  Valor predeterminado: Default

  Descripción: (obligatorio) una nueva instancia se implementará en este Amazon Virtual Private Cloud (Amazon VPC) o en la Amazon VPC predeterminada si no se especifica.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descripción

El `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook permite que las AWS Systems Manager sesiones del administrador de sesiones (administrador de sesiones) almacenen los registros de salida en un grupo de registros de Amazon CloudWatch (CloudWatch).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- DestinationLogGrupo

  Tipo: cadena

  Descripción: (obligatorio) El nombre del grupo de CloudWatch registros.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Pasos de documentos

- `aws:executeScript`- Acepta el grupo de CloudWatch registros para actualizar el documento que almacena las preferencias de los registros de salida de las sesiones del Administrador de sesiones, o crea uno si no existe.

AWS-ExportOpsDataToS3

Descripción

Este runbook recupera una lista de OpsData resúmenes en AWS Systems Manager Explorer y los exporta a un objeto de un bucket específico de Amazon Simple Storage Service (Amazon S3).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- columnFields

  Tipo: StringList

  Descripción: (obligatorio) campos de la columna para escribir en el archivo de salida.

- filters

  Tipo: cadena

  Descripción: filtros (opcionales) para la getOpsSummary solicitud.

- resultAttribute

  Tipo: cadena

  Descripción: (opcional) El atributo de resultado de la getOpsSummary solicitud.

- s3 BucketName

  Tipo: cadena

  Descripción: (obligatorio) el bucket de S3 donde desea descargar el archivo de salida.

- sns SuccessMessage

  Tipo: cadena

  Descripción: (opcional) mensaje que se envía cuando termine el manual de procedimientos.

- sns TopicArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN del tema de Amazon Simple Notification Service (Amazon SNS) para notificar cuando se complete la descarga.

- SyncName

  Tipo: cadena

  Descripción: (opcional) el nombre de la sincronización de datos de recursos.

Pasos de documentos

getOpsSummaryStep : ahora recupera hasta 5000 resúmenes de operaciones para exportarlos a un archivo CSV.

Salidas

OpsData objeto: si el manual se ejecuta correctamente, encontrarás el OpsData objeto exportado en el depósito S3 de destino.

AWS-ExportPatchReportToS3

Descripción

Este manual de procedimientos recupera listas de datos de resúmenes y detalles de parches en AWS Systems Manager Patch Manager y los exporta a archivos.csv en un bucket de Amazon Simple Storage Service (Amazon S3) específico.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- assumeRole

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que ejecuta este documento.
- s3 BucketName

Tipo: cadena

Descripción: (obligatorio) el bucket de S3 donde desea descargar el archivo de salida.

- sns TopicArn

  Tipo: cadena

  Descripción: (opcional) el nombre de recurso de Amazon (ARN) del tema de Amazon Simple Notification Service (Amazon SNS) para notificar cuando se completa la descarga.

- sns SuccessMessage

  Tipo: cadena

  Descripción: (opcional) el texto del mensaje que se enviará cuando finalice el manual de procedimientos.

- destinos

  Tipo: cadena

  Descripción: (obligatorio) el ID de la instancia o un carácter comodín (*) para indicar si se deben informar los datos de los parches de una instancia específica o de todas las instancias.

Pasos de documentos

ExportReportStep — La acción de este paso depende del valor del `targets` parámetro. Si `targets` tiene el formato de `instanceids=*`, el paso recupera hasta 10.000 resúmenes de parches para las instancias de su cuenta y exporta los datos a un archivo .csv.

Si `targets` tiene el formato de `instanceids=<instance-id>`, el paso recupera tanto el resumen del parche como todos los parches de la instancia especificada en su cuenta y los exporta a un archivo .csv.

Salidas

PatchSummaryObjeto /Patches: si el runbook se ejecuta correctamente, el objeto de informe de parches exportado se descarga en el depósito S3 de destino.

AWS-SetupInventory

Descripción

Cree una asociación de Systems Manager Inventory para una o varias instancias administradas. El sistema recopila metadatos de sus instancias de acuerdo con la programación en la asociación. Para obtener más información, consulte AWS Systems Manager Inventory.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- Aplicaciones

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional) recopilar metadatos de las aplicaciones instaladas.
- AssociatedDocNombre

  Tipo: cadena

  Valor predeterminado: `AWS-GatherSoftwareInventory`

  Descripción: (opcional) nombre del manual de procedimientos de SSM utilizado para recopilar datos del inventario desde la instancia administrada.
- AssociationName

  Tipo: cadena

  Descripción: (opcional) un nombre para la asociación de inventario que se asignará a la instancia.
- AssocWaitHora

  Tipo: cadena

Valor predeterminado: PT5M

Descripción: (opcional) cantidad de tiempo que debe ponerse en pausa la recopilación de inventario cuando se alcanza la hora de inicio de la asociación del inventario. La hora usa el formato ISO 8601.

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `AwsComponents`

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (Opcional) Recopile metadatos para AWS componentes como amazon-ssm-agent.

- CustomInventory

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional) recopilar los metadatos de inventario personalizado.

- Archivos

  Tipo: cadena

  Descripción: (opcional) recopilar metadatos acerca de archivos en las instancias. Para obtener más información sobre cómo recopilar este tipo de datos de inventario, consulte Trabajar con el inventario de archivos y del registro de Windows. Requiere la versión 2.2.64.0 del SSMAgent o posterior. Ejemplo de 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}]`

- InstanceDetailedInformación

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional) recopilar información adicional acerca de la instancia, incluido el modelo de CPU, la velocidad y el número de núcleos, por mencionar algunos.

- InstanceIds

  Tipo: cadena

  Valor predeterminado: *

  Descripción: (obligatorio) instancias EC2 de las que desea crear un inventario.

- LambdaAssumeFunción

  Tipo: cadena

  Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- NetworkConfig

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional) recopilar metadatos de las configuraciones de red.

- Salidas 3 BucketName

  Tipo: cadena

  Descripción: (opcional) nombre de un bucket de Amazon S3 en el que desea escribir los datos de registro del inventario.

- Salidas 3 KeyPrefix

  Tipo: cadena

Descripción: (opcional) un prefijo de clave de Amazon S3 (subcarpeta) en el que desea escribir los datos de registro del inventario.

- OutputS3Region

  Tipo: cadena

  Descripción: (opcional) El nombre del Región de AWS lugar donde se encuentra Amazon S3.

- Programación

  Tipo: cadena

  Valor predeterminado: cron(0 */30 * * * ? *)

  Descripción: (opcional) una expresión cron para la programación de asociación de inventario. El valor predeterminado es cada 30 minutos.

- Servicios

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional, solo SO Windows, requiere la versión 2.2.64.0 de SSMAgent o superior) recopile datos para configuraciones de servicio.

- WindowsRegistry

  Tipo: cadena

  Descripción: (opcional) recopilar metadatos acerca de claves del Registro de Microsoft Windows. Para obtener más información sobre cómo recopilar este tipo de datos de inventario, consulte Trabajar con el inventario de archivos y del registro de Windows. Requiere la versión 2.2.64.0 del SSM Agent o posterior. Ejemplo: [{"Path» :"HKEY_CURRENT_CONFIG\ System», "Recursive» :true}, {"Path» :"HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ «," «: [" amiName "]}] MachineImage ValueNames

- WindowsRoles

  Tipo: cadena

  Valor predeterminado: Enabled

Descripción: (opcional) recopilar información acerca de roles de Windows en la instancia. Se aplica solo a sistemas operativos Windows. Requiere la versión 2.2.64.0 del SSMAgent o posterior.

- WindowsUpdates

  Tipo: cadena

  Valor predeterminado: Enabled

  Descripción: (opcional) recopilar datos acerca de todas las actualizaciones de Windows en la instancia.

AWS-SetupManagedInstance

Descripción

Configure una instancia con un rol AWS Identity and Access Management (IAM) para el acceso a Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia EC2 que se va a configurar.

- LambdaAssumeRol

  Tipo: cadena

  Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- RoleName

  Tipo: cadena

  Predeterminado: SSM RoleFor ManagedInstance

  Descripción: (opcional) nombre del rol de IAM para la instancia EC2. Si este rol no existe, se creará. Al especificar este valor, compruebe que el rol contenga la política gestionada ManagedInstanceprincipal de AmazonSSM.

AWS-SetupManagedRoleOnEC2Instance

Descripción

Configure una instancia con la función de IAM RoleForManagedInstance gestionada por SSM para el acceso a Systems Manager.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia EC2 que se va a configurar.
- LambdaAssumeRol

  Tipo: cadena

  Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.
- RoleName

  Tipo: cadena

  Predeterminado: SSM RoleFor ManagedInstance

  Descripción: (opcional) nombre del rol de IAM para la instancia EC2. Si este rol no existe, se creará. Al especificar este valor, compruebe que el rol contenga la política gestionada ManagedInstanceprincipal de AmazonSSM.

AWSSupport-TroubleshootManagedInstance

Descripción

El manual de procedimientos `AWSSupport-TroubleshootManagedInstance`le ayuda a determinar por qué una instancia de Amazon Elastic Compute Cloud (Amazon EC2) no se

presenta como administrada por AWS Systems Manager. Este manual de procedimientos revisa la configuración de VPC de la instancia, incluyendo las reglas de los grupos de seguridad, los puntos de conexión de VPC, las reglas de la lista de control de acceso (ACL) y las tablas de enrutamiento. También confirma que un perfil de instancia AWS Identity and Access Management(de IAM) que contiene los permisos necesarios se asocia a la instancia.

> **Important**
>
> Este manual de automatización no evalúa las reglas de IPv6.

Ejecuta esta automatización (consola)

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- InstanceId

  Tipo: cadena

  Descripción: (Obligatorio) El ID de la instancia de Amazon EC2 que no informa como gestionada por Systems Manager.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript` - Recopila el `PingStatus`de la instancia.
- `aws:branch` - Se ramifica en función de si la instancia ya está informando como gestionada por Systems Manager.
- `aws:executeAwsApi` - Recopila detalles sobre la instancia, incluyendo la configuración de la VPC.
- `aws:executeScript` - Si corresponde, recopila detalles adicionales relacionados con los puntos de conexión de VPC que se han implementado para usarlos con Systems Manager y confirma que

los grupos de seguridad conectados al punto de conexión de VPC permiten el tráfico entrante en el puerto TCP 443 desde la instancia.

- `aws:executeScript` - Comprueba si la tabla de enrutamiento permite el tráfico al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript` - Comprueba si las reglas de ACL de la red permiten el tráfico al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript` - Comprueba si el grupo de seguridad asociado a la instancia permite el tráfico saliente al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript` - Comprueba si el perfil de instancia adjunto a la instancia incluye una política gestionada que proporcione los permisos necesarios.
- `aws:branch` - Se ramifica en función del sistema operativo de la instancia.
- `aws:executeScript` - Proporciona una referencia al script de `ssmagent-toolkit-linux`del intérprete de comandos.
- `aws:executeScript`- Proporciona una referencia al script. `ssmagent-toolkit-windows` PowerShell
- `aws:executeScript` - Genera el resultado final para la automatización.
- `aws:executeScript` - Si el `PingStatus`de la instancia es `Online`, regresa que la instancia ya está gestionada por Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descripción

El `AWSSupport-TroubleshootPatchManagerLinux` manual resuelve los problemas más comunes que pueden provocar un error en los parches en los nodos gestionados basados en Linux mediante la función «Administrador de parches»AWS Systems Manager. El objetivo principal de este manual es identificar la causa raíz del fallo del comando de parche y sugerir un plan de remediación.

¿Cómo funciona?

El `AWSSupport-TroubleshootPatchManagerLinux` manual tiene en cuenta el par de identificadores de instancia y de comando proporcionados por usted para solucionar problemas. Si no se proporciona ningún identificador de comando, selecciona el último comando de parche fallido en los últimos 30 días en la instancia proporcionada. Tras comprobar el estado del comando, el cumplimiento de los requisitos previos y la distribución del sistema operativo, el runbook descarga y

ejecuta un paquete analizador de registros. El resultado incluye la causa raíz del problema, así como las medidas necesarias para solucionarlo.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

- Amazon Linux 2 y 2023
- Red Hat Enterprise Linux 8.X y 9.X
- Centos 8.X y 9.X
- SUSE 15.X

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instrucciones

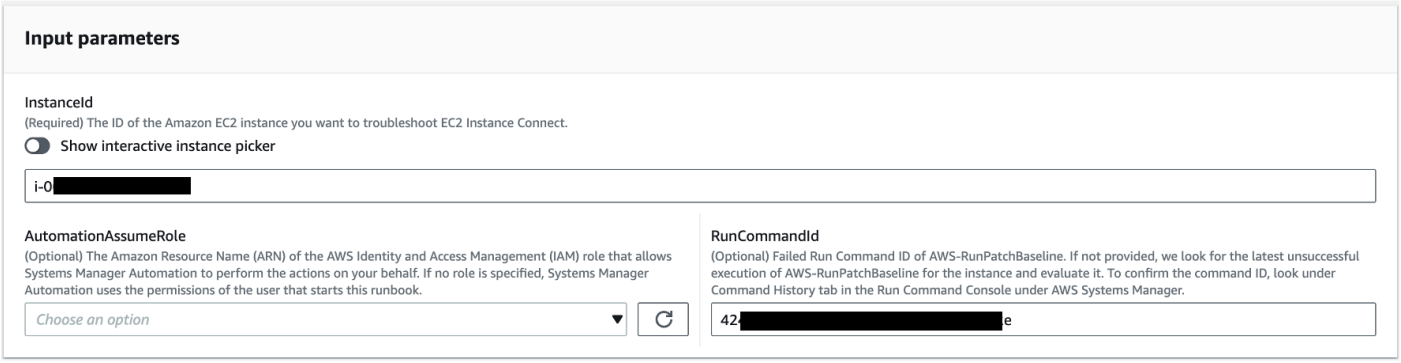
Siga estos pasos para configurar la automatización:

1. Navegue hasta AWSSupport-TroubleshootPatchManagerLinuxla AWS Systems Manager consola.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
   - InstanceId (Obligatorio):

     Usa el selector de instancias interactivo para elegir el ID del nodo gestionado por SSM basado en Linux (Amazon Elastic Compute Cloud (Amazon EC2) o servidor activado híbrido) contra el que falló el comando de parche, o introduce manualmente el ID de la instancia gestionada por SSM.
   - AutomationAssumeRole (Opcional):

     Introduzca el ARN del rol de IAM que permite a Automation realizar acciones en su nombre. Si no se especifica ningún rol, Automation usa los permisos del usuario que inicia este manual.
   - RunCommandId (Opcional):

     Introduzca el identificador del `AWS-RunPatchBaseline` documento con el comando de ejecución fallido. Si no proporciona un identificador de comando, el runbook buscará el último comando de parche fallido en los últimos 30 días en la instancia seleccionada.



4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
   - CheckConcurrency:

     Garantiza que solo haya una ejecución de este runbook dirigida a la misma instancia. Si el runbook encuentra otra ejecución en curso dirigida a la misma instancia, devuelve un error y finaliza.
   - ValidateCommandID:

Valida si el ID de comando proporcionado, como parámetro de entrada, se ejecutó para el documento `AWS-RunPatchBaseline` SSM. Si no se proporciona ningún identificador de comando, el manual considerará la última ejecución fallida de los `AWS-RunPatchBaseline` últimos 30 días en la instancia seleccionada.

- BranchOnCommandStatus:

  Confirma que el estado del comando proporcionado ha fallado. De lo contrario, el manual finaliza la ejecución y genera un informe en el que se indica que el comando proporcionado se ejecutó correctamente.

- VerifyPrerequistes:

  Confirma que se cumplen los requisitos previos mencionados anteriormente.

- GetPlatformDetails:

  Recupera la distribución y la versión del sistema operativo (SO).

- GetDownloadURL:

  Recupera la URL de descarga del paquete PatchManager Log Analyzer.

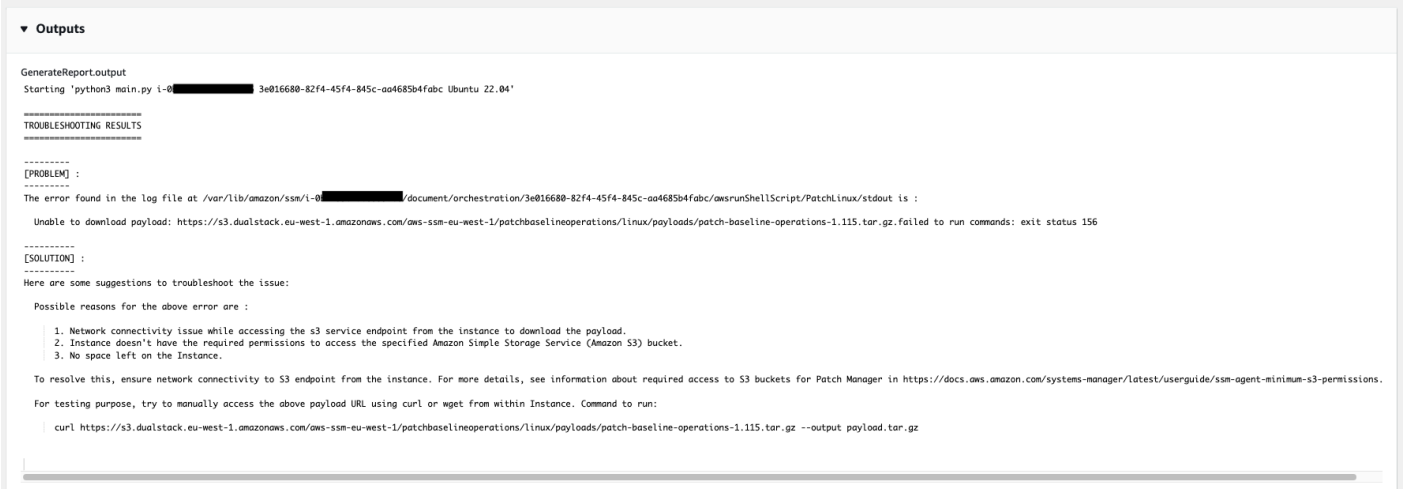
- EvaluatePatchManagerLogs:

  Descarga y ejecuta el paquete python de PatchManager Log Analyzer en la instancia para evaluar el archivo de registro.

- GenerateReport:

  Genera un informe final de la ejecución del manual de ejecución que incluye el problema identificado y la solución sugerida.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

`AWSSupport-TroubleshootSessionManager`

Descripción

El manual de procedimientos `AWSSupport-TroubleshootSessionManager` le ayuda a solucionar problemas comunes que le impiden conectarse a instancias administradas de Amazon Elastic Compute Cloud (Amazon EC2) mediante Session Manager. El administrador de sesiones es una capacidad de. AWS Systems Manager Este manual de procedimientos comprueba lo siguiente:

- Comprueba si la instancia se está ejecutando e informando como gestionada por Systems Manager.
- Ejecuta el manual de procedimientos `AWSSupport-TroubleshootManagedInstance` si la instancia no informa como gestionada por Systems Manager.
- Comprueba la versión del agente SSM instalada en la instancia.
- Comprueba si un perfil de instancia que contiene una política de AWS Identity and Access Management (IAM) recomendada para Session Manager está adjunto a la instancia Amazon EC2.

- Recopila los registros del agente SSM de la instancia.
- Analiza sus preferencias de Session Manager.
- Ejecuta el `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analizar la conectividad de la instancia con los puntos de conexión de Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) y CloudWatch Amazon Logs (Logs). CloudWatch

Consideraciones

- No se admiten los nodos gestionados híbridos.
- Este manual de procedimientos solo comprueba si hay una política de IAM administrada recomendada asociada al perfil de instancia. No analiza la IAM ni los permisos AWS KMS que se incluyen en su perfil de instancia.

> **Important**
>
> El manual de procedimientos `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` utiliza el Analizador de accesibilidad de VPC para analizar la conectividad de red entre una fuente y un punto de conexión de servicio. Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte Precios de Amazon EFS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

  Tipo: cadena

  Descripción: (obligatorio) el ID de la instancia de Amazon EC2 a la que no puede conectarse mediante Session Manager.

- SessionPreferenceDocumento

  Tipo: cadena

  Predeterminado: SSM- SessionManager RunShell

  Descripción: (opcional) el nombre de su documento de preferencias de sesión. Si no especifica un documento de preferencias de sesión personalizado al iniciar las sesiones, utilice el valor predeterminado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

1. aws:waitForAwsResourceProperty: espera hasta 6 minutos para que su instancia de destino supere las comprobaciones de estado.
2. aws:executeScript: analiza el documento de preferencias de sesión.
3. aws:executeAwsApi: obtiene el ARN del perfil de instancia asociado a su instancia.

4. `aws:executeAwsApi`: comprueba si su instancia informa como gestionada por Systems Manager.
5. `aws:branch`: se ramifica en función de si su instancia genera informes según la gestión de Systems Manager.
6. `aws:executeScript`: comprueba si el agente SSM instalado en su instancia es compatible con Session Manager.
7. `aws:branch`: se ramifican según la plataforma de su instancia para recopilar registros `ssm-cli`.
8. `aws:runCommand`: recopila la salida de los registros `ssm-cli` de una instancia Linux o macOS.
9. `aws:runCommand`: recopila la salida de los registros `ssm-cli` de una instancia Windows.
10. `aws:executeScript`: analiza los registros `ssm-cli`.
11. `aws:executeScript`: comprueba si hay una política de IAM recomendada asociada al perfil de instancia.
12. `aws:branch`: determina si se debe evaluar la conectividad del punto de conexión `ssmmessages` en función de los registros `ssm-cli`.
13. `aws:executeAutomation`: evalúa si la instancia se puede conectar a un punto de conexión `ssmmessages`.
14. `aws:branch`: determina si se debe evaluar la conectividad del punto de conexión de Amazon S3 en función de los registros `ssm-cli` y sus preferencias de sesión.
15. `aws:executeAutomation`: evalúa si la instancia se puede conectar a un punto de conexión de Amazon S3.
16. `aws:branch`: Determina si se debe evaluar la conectividad del AWS KMS punto final en función de `ssm-cli` los registros y las preferencias de la sesión.
17. `aws:executeAutomation`: Evalúa si la instancia se puede conectar a un AWS KMS punto final.
18. `aws:branch`: Determina si se debe evaluar la conectividad de CloudWatch los puntos finales de `ssm-cli` Logs en función de los registros y de sus preferencias de sesión.
19. `aws:executeAutomation`: Evalúa si la instancia se puede conectar a un punto final de CloudWatch Logs.
20. `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSSupport-TroubleshootManagedInstance`.
21. `aws:executeScript`: compila el resultado de los pasos anteriores y genera un informe.

Salidas

- `generateReport.EvalReport`: los resultados de las comprobaciones realizadas por el manual de procedimientos en texto sin formato.

De terceros

AWS Systems Manager La automatización proporciona manuales predefinidos para productos y servicios de terceros. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

`AWS-CreateJiraIssue`

Descripción

Cree un problema en Jira.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AssigneeName

Tipo: cadena

Descripción: (opcional) el nombre de usuario de la persona a la que debe asignarse el problema.

- DueDate

  Tipo: cadena

  Descripción: (opcional) yyyy-mm-dd Formato de la fecha límite de publicación.

- IssueDescription

  Tipo: cadena

  Descripción: (obligatorio) una descripción detallada del problema.

- IssueSummary

  Tipo: cadena

  Descripción: (obligatorio) un breve resumen del problema.

- IssueTypeNombre

  Tipo: cadena

  Descripción: (obligatorio) el nombre del tipo de problema que desea crear (por ejemplo, Task, Sub-task, Bug, etc.).

- JiraURL

  Tipo: cadena

  Descripción: (obligatorio) la URL de la instancia de Jira.

- JiraUsername

  Tipo: cadena

  Descripción: (obligatorio) el nombre del usuario con el que se creará el problema.

- PriorityName

  Tipo: cadena

  Descripción: (opcional) el nombre de la prioridad del problema.

- ProjectKey

  Tipo: cadena

  Descripción: (obligatorio) la clave del proyecto en el que se debe crear el problema.
- SSM ParameterName

  Tipo: cadena

  Descripción: (obligatorio) el nombre de un parámetro SSM cifrado que contiene la clave de API o la contraseña del usuario de Jira.

Pasos de documentos

`aws:createStack`- Cree una CloudFormation pila para crear el rol y la función de Lambda IAM.

`aws:invokeLambdaFunction`: invoca la función de Lambda para crear el problema de Jira

`aws:deleteStack`- Elimine la CloudFormation pila creada.

Salidas

IssueId: ID de la edición de Jira recién creada

AWS-CreateServiceNowIncident

Descripción

Cree un incidente en la tabla de ServiceNow incidentes.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Categoría

  Tipo: cadena

  Descripción: (opcional) la categoría del incidente.

  Valores válidos: Ninguno | Consulta/Ayuda | Software | Hardware | Red | Base de datos

  Valor predeterminado: None
- Descripción

  Tipo: cadena

  Descripción: (obligatorio) una explicación detallada sobre el incidente.
- Impact

  Tipo: cadena

  Descripción: (opcional) el efecto que un incidente tiene en el negocio.

  Valores válidos: Alto | Medio | Bajo

  Valor predeterminado: bajo
- ServiceNowInstanceUsername

  Tipo: cadena

  Descripción: (obligatorio) el nombre del usuario con el que se creará el incidente.
- ServiceNowInstancePassword

  Tipo: cadena

Descripción: (obligatorio) El nombre de un parámetro SSM cifrado que contiene la contraseña del ServiceNow usuario.

- ServiceNowURL de la instancia

  Tipo: cadena

  Descripción: (obligatorio) La URL de la instancia ServiceNow

- ShortDescription

  Tipo: cadena

  Descripción: (obligatorio) una breve descripción del incidente.

- Subcategory

  Tipo: cadena

  Descripción: (opcional) la subcategoría del incidente.

  Valores válidos: Ninguno | Antivirus | Email | Aplicación interna | Sistema operativo | CPU | Disco | Teclado | Hardware | Memoria | Monitor | Ratón | DHCP | DNS | Dirección IP | VPN | Inalámbrico | DB2 | MS SQL Server | Oracle

  Valor predeterminado: None

Pasos de documentos

PUSH_incident: envía la información del incidente a. ServiceNow

Salidas

Push_incident.incidentID: el ID del incidente creado.

AWS-RunPacker

Descripción

Este manual utiliza la herramienta HashiCorp Packer para validar, corregir o crear plantillas de empaquetador que se utilizan para crear imágenes de máquinas. Este manual de procedimientos utiliza Packer v1.7.2.

> **Note**
>
> Si especifica un valor `vpc_id`, también debe especificar el valor `subnet_id` de una subred pública. A menos que modifique el atributo de direccionamiento público IPv4 de la subred, también debe establecerse `associate_public_ip_address` en true.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- Force

  Tipo: Booleano

  Descripción: una opción de Packer para forzar la ejecución de un generador cuando artefactos de una compilación anterior impiden la ejecución de una compilación.
- Mode

  Tipo: cadena

Descripción: el modo, o comando, en el que utilizar Packer al realizar la validación respecto a la plantilla. Las opciones incluyen `Build`, `Validate` y `Fix`.

- TemplateFileNombre

  Tipo: cadena

  Descripción: el nombre, o clave, del archivo de plantilla en el bucket de S3.

- Plantillas 3 BucketName

  Tipo: cadena

  Descripción: el nombre del bucket de S3 que contiene la plantilla de empaquetador.

Pasos de documentos

RunPackerProcessTemplate — Ejecuta el modo seleccionado en la plantilla mediante la herramienta Packer.

Salidas

RunPackerProcessTemplate.output: la salida estándar de la herramienta Packer.

RunPackerProcessTemplate.fixed_template_key: el nombre de la plantilla almacenada en un bucket de S3 para usarla solo cuando se ejecuta en modo «Fix».

RunPackerProcessTemplate.s3_bucket: el nombre del bucket de S3 que contiene la plantilla fija para usarla solo cuando se ejecuta en modo «Fix».

Amazon VPC

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Virtual Private Cloud. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-CloseSecurityGroup

- AWSSupport-ConfigureDNSQueryLogging
- AWSSupport-ConfigureTrafficMirroring
- AWSSupport-ConnectivityTroubleshooter
- AWSSupport-TroubleshootVPN
- AWSConfigRemediation-DeleteEgressOnlyInternetGateway
- AWSConfigRemediation-DeleteUnusedENI
- AWSConfigRemediation-DeleteUnusedSecurityGroup
- AWSConfigRemediation-DeleteUnusedVPCNetworkACL
- AWSConfigRemediation-DeleteVPCFlowLog
- AWSConfigRemediation-DetachAndDeleteInternetGateway
- AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway
- AWS-DisableIncomingSSHOnPort22
- AWS-DisablePublicAccessForSecurityGroup
- AWSConfigRemediation-DisableSubnetAutoAssignPublicIP
- AWSSupport-EnableVPCFlowLogs
- AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch
- AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket
- AWS-ReleaseElasticIP
- AWS-RemoveNetworkACLUnrestrictedSSHRDP
- AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules
- AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules
- AWSSupport-SetupIPMonitoringFromVPC
- AWSSupport-TerminateIPMonitoringFromVPC

AWS-CloseSecurityGroup

Descripción

Este manual elimina todas las reglas de entrada y salida del grupo de seguridad que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- SecurityGroupID

  Tipo: cadena

  Descripción: (obligatorio) El ID del grupo de seguridad que desea cerrar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Pasos de documentos

- `aws:executeScript`- Elimina todas las reglas de entrada y salida del grupo de seguridad que especifique en el `SecurityGroupId` parámetro.

AWSSupport-ConfigureDNSQueryLogging

Descripción

El manual de procedimientos `AWSSupport-ConfigureDNSQueryLogging` configura el registro de las consultas de DNS que se originan en su nube privada virtual (VPC) o en las zonas alojadas de Amazon Route 53. Puede optar por publicar los registros de consultas en Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose. Para obtener más información sobre el registro de consultas y el solucionador de registros de consultas, consulte Registro de consultas de DNS público y Solucionador de registro de consultas .

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- LogDestinationArn

  Tipo: cadena

  Descripción: (opcional) El ARN del grupo CloudWatch Logs, el bucket de Amazon S3 o la transmisión Firehose a los que desea enviar los registros de consultas. Tenga en cuenta que el

registro de consultas de DNS público de Route 53 solo admite grupos de CloudWatch registros. Si no especifica un valor para este parámetro, la automatización crea un grupo de CloudWatch registros con el formato `AWSSupport-ConfigureDNSQueryLogging-{automation:EXECUTION_ID}` y una política de recursos de IAM para publicar los registros de consultas. El grupo de CloudWatch registros creado por la automatización tiene un período de retención de 14 días.

- QueryLogTipo

  Tipo: cadena

  Descripción: (opcional) los tipos de consultas que desea registrar.

  Valores válidos: Public | Resolver/Private

  Predeterminado: Public

- ResourceId

  Tipo: cadena

  Descripción: (obligatorio) el ID del recurso cuyas consultas desea registrar. Si especifica `Public` para el parámetro `QueryLogType`, el recurso debe ser el ID de una zona alojada privada de Route 53. Si especifica `Resolver/Private` para el parámetro `QueryLogType`, el recurso debe ser el ID de una VPC.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Pasos de documentos

- `aws:executeScript`: verifica que el recurso que especificó para el parámetro `ResourceId` existe y comprueba si el tipo de recurso coincide con la opción requerida `QueryLogType`.
- `aws:executeScript`: comprueba que el valor especificado para el parámetro `LogDestinationArn` coincide con el `QueryLogType` requerido.
- `aws:executeScript`- Verifica los permisos necesarios para que Route 53 publique registros en el grupo de CloudWatch registros y crea la política de recursos de IAM requerida si no existe.
- `aws:executeScript`: habilita el registro de consulta de DNS en el destino seleccionado.

AWSSupport-ConfigureTrafficMirroring

Descripción

El manual de procedimientos `AWSSupport-ConfigureTrafficMirroring` configura la duplicación de tráfico para ayudarle a resolver problemas de conectividad entre un equilibrador de carga e instancias de Amazon Elastic Compute Cloud (Amazon EC2). La duplicación del tráfico copia el tráfico entrante y saliente de las interfaces de red que están conectadas a sus instancias. Para configurar la duplicación de tráfico, este manual de procedimientos crea los destinos, filtros y sesiones necesarios. De forma predeterminada, el manual de procedimientos configura la duplicación de todo el tráfico entrante y saliente de todos los protocolos, excepto Amazon DNS. Si desea reflejar el tráfico de fuentes y destinos específicos, puede modificar las reglas de entrada y salida una vez finalizada la automatización.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- SourceENI

  Tipo: cadena

  Descripción: (obligatorio) la interfaz de red elástica para la que desea configurar la duplicación de tráfico.

- Destino

  Tipo: cadena

  Descripción: (obligatorio) el destino del tráfico reflejado. Debe especificar el ID de una interfaz de red, un punto de conexión de equilibrador de carga de red o equilibrador de carga de puerta de enlace. Si especifica un equilibrador de carga de red, debe haber receptores UDP en el puerto 4789.

- SessionNumber

  Tipo: cadena

  Valores válidos: 1-32766

  Descripción: (obligatorio) el número de la sesión duplicada que desea utilizar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorSession`

- ec2:DeleteTrafficMirrorFilter
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

Pasos de documentos

- aws:executeScript: ejecuta un script para crear un objetivo.
- aws:executeAwsApi: crea una regla de filtro.
- aws:executeAwsApi: crea una regla de filtro espejo para todo el tráfico entrante.
- aws:executeAwsApi: crea una regla de filtro espejo para todo el tráfico saliente.
- aws:executeAwsApi: crea una sesión de reflejo de tráfico.
- aws:executeAwsApi: elimina el filtro si se produce un error al crear el filtro o la sesión.
- aws:executeAwsApi: elimina el objetivo si se produce un error al crear el filtro o la sesión.

Salidas

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget. Salida de TargetID

AWSSupport-ConnectivityTroubleshooter

Descripción

El manual de procedimientos AWSSupport-ConnectivityTroubleshooter diagnostica los problemas de conectividad entre los siguientes:

- AWS recursos dentro de una Amazon Virtual Private Cloud (Amazon VPC)
- AWS recursos en diferentes VPC de Amazon dentro de la misma Región de AWS que están conectados mediante el emparejamiento de VPC

- AWS recursos en una Amazon VPC y un recurso de Internet mediante una puerta de enlace de Internet
- AWS recursos en una Amazon VPC y un recurso de Internet mediante una puerta de enlace de traducción de direcciones de red (NAT)

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- DestinationIp

  Tipo: cadena

  Descripción: (obligatorio) la dirección IPv4 del recurso al que desea conectarse.
- DestinationPort

  Tipo: cadena

  Predeterminado: true

  Descripción: (obligatorio) el número de puerto al que desea conectarse en el recurso de destino.

- DestinationVpc

  Tipo: cadena

  Valor predeterminado: All

  Descripción: (opcional) el ID de la Amazon VPC con la que desea probar la conectividad.

- SourceIp

  Tipo: cadena

  Descripción: (Obligatoria) La dirección IPv4 privada del AWS recurso de su Amazon VPC desde el que desea probar la conectividad.

- SourcePortRango

  Tipo: cadena

  Descripción: (opcional) El rango de puertos que utiliza el AWS recurso de tu Amazon VPC desde el que quieres probar la conectividad.

- SourceVpc

  Tipo: cadena

  Valor predeterminado: All

  Descripción: (opcional) el ID de la Amazon VPC desde la que desea probar la conectividad.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Recopila detalles sobre el AWS recurso que especifique en el `SourceIP` parámetro.
- `aws:executeScript`- Determina el destino del tráfico de red procedente del AWS recurso utilizando las rutas recopiladas en el paso anterior.
- `aws:branch`: se ramifican en función del destino del tráfico de la red.
- `aws:executeAwsApi`: recopila detalles sobre el recurso de destino.
- `aws:executeScript`: confirma que el ID regresado para la Amazon VPC de destino coincide con el valor especificado, si lo hubiera, en el parámetro `DestinationVpc`.
- `aws:executeAwsApi`: recopila las reglas del grupo de seguridad para los recursos de origen y destino.
- `aws:executeScript`: confirma si las reglas del grupo de seguridad permiten el tráfico necesario entre los recursos de origen y destino.
- `aws:executeAwsApi`: reúne las listas de control de acceso a la red (NACL) asociadas a las subredes de los recursos de origen y destino.
- `aws:executeScript`: confirma si las NACL permiten el tráfico necesario entre los recursos de origen y destino.
- `aws:executeScript`: confirma si la fuente tiene una dirección IP pública asociada al recurso, si el destino de la ruta es una puerta de enlace de Internet.
- `aws:executeAwsApi`: recopila las reglas del grupo de seguridad para el recurso fuente.
- `aws:executeScript`: confirma si las reglas del grupo de seguridad permiten el tráfico necesario desde el recurso de origen al de destino.
- `aws:executeAwsApi`: reúne las NACL asociadas a la subred del recurso de origen.
- `aws:executeScript`: confirma si las NACL permiten el tráfico necesario desde el recurso fuente.
- `aws:executeAwsApi`: recopila detalles sobre la puerta de enlace de NAT.
- `aws:executeAwsApi`: recopila las NACL asociadas a la subred de la puerta de enlace NAT.
- `aws:executeScript`: confirma si las NACL permiten el tráfico necesario desde la subred para la puerta de enlace NAT.
- `aws:executeScript`: recopila las rutas asociadas a la subred de la puerta de enlace NAT.
- `aws:executeScript`: confirma si la puerta de enlace NAT tiene una ruta hacia una puerta de enlace de Internet.

- `aws:executeAwsApi`: recopila detalles sobre la conexión de emparejamiento de VPC.
- `aws:executeScript`: confirma que ambas VPC están en la misma región y que el ID regresado para la VPC de destino coincide con el valor especificado, si lo hubiera, en el parámetro `DestinationVpc`.
- `aws:executeAwsApi`: regresa la subred del recurso de destino.
- `aws:executeScript`: recopila las rutas asociadas a la subred de la VPC interconectada.
- `aws:executeScript`: confirma si la VPC interconectada tiene una ruta hacia la conexión de intercambio de tráfico.
- `aws:executeScript`: confirma si el tráfico está permitido desde el recurso de origen si la automatización no admite el destino.

AWSSupport-TroubleshootVPN

Descripción

El manual de procedimientos `AWSSupport-TroubleshootVPN`le ayuda a rastrear y resolver los errores de una conexión AWS Site-to-Site VPN. La automatización incluye varias comprobaciones automatizadas diseñadas para rastrear los errores `IKEv1`o `IKEv2`relacionados con los túneles de conexión AWS Site-to-Site VPN. La automatización intenta hacer coincidir errores específicos y su correspondiente resolución para formar una lista de problemas comunes.

Nota: Esta automatización no corrige los errores. Se ejecuta durante el intervalo de tiempo mencionado y escanea el grupo de registros en busca de errores en el grupo de CloudWatch registros de la VPN.

¿Cómo funciona?

El runbook ejecuta una validación de parámetros para confirmar si el grupo de CloudWatch registros de Amazon incluido en el parámetro de entrada existe, si hay algún flujo de registro en el grupo de registros que corresponda al registro del túnel VPN, si existe el identificador de conexión VPN y si existe la dirección IP del túnel. Realiza llamadas a la API de Logs Insights en su grupo de CloudWatch registros que está configurado para el registro de VPN.

Tipo de documento

Automation

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (Opcional) el Nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
- LogGroupName

  Tipo: cadena

  Descripción: (obligatorio) El nombre del grupo de CloudWatch registros de Amazon configurado para el registro de AWS Site-to-Site VPN conexiones

  Valor permitido: `^[\.\-_/#A-Za-z0-9]{1,512}`
- VpnConnectionId

  Tipo: cadena

  Descripción: (Obligatorio) el ID de conexión AWS Site-to-Site VPNpara ser solucionado.

  Valor permitido: `^vpn-[0-9a-f]{8,17}$`
- TunnelAIPAddress

  Tipo: cadena

  Descripción: (Obligatorio) La dirección IPv4 número 1 del túnel asociada a su AWS Site-to-Site VPN.

  Valor permitido: `^((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: cadena

Descripción: (Opcional) La dirección IPv4 número 2 del túnel asociada a su AWS Site-to-Site VPN.

Valor permitido: `^((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: cadena

  Descripción: (Obligatorio) Seleccione la versión de IKE que está utilizando. Valores permitidos: IKEv1, IKEv2

  Valores válidos: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  Tipo: cadena

  Descripción: (Opcional) Hora de inicio para el análisis de registro. Puede usar StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod para el análisis de registros

  Valor permitido: `^\d{10}|^$`

- EndTimeinEpoch

  Tipo: cadena

  Descripción: (Opcional) Hora de finalización para el análisis de registro. Puede usar StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod para el análisis de registros. Si se proporcionan tanto StartTimeinEpoch/EndTimeinEpoch como LookBackPeriod , entonces, LookBackPeriod tiene prioridad

  Valor permitido: `^\d{10}|^$`

- LookBackPeriod

  Tipo: cadena

  Descripción: (Opcional) Tiempo de dos dígitos en horas para analizar el registro. Rango válido: 01 - 99. Este valor tiene prioridad si también se da y StartTimeinEpoch EndTime

  Valor permitido: `^(\d?[1-9]|[1-9]0)|^$`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Instrucciones

Nota: Esta automatización funciona en los grupos de CloudWatch registros que están configurados para el registro del túnel de la VPN, cuando el formato de salida del registro es JSON.

Siga estos pasos para configurar la automatización:

1. Ve a AWSSupport-TroubleShootVPN en la consola. AWS Systems Manager
2. Para los parámetros de entrada, introduzca lo siguiente:
   - AutomationAssumeRole (Opcional):

     El nombre de recurso de Amazon (ARN) del rol (IAM) AWS Identity and Access Managementque permite a System Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utilizará los permisos del usuario que ejecuta este manual de procedimientos.
   - LogGroupName (Obligatorio):

     El nombre del grupo de CloudWatch registros de Amazon que se va a validar. Debe ser el grupo de CloudWatch registros que está configurado para que la VPN envíe los registros.
   - VpnConnectionId (Obligatorio):

     El identificador de conexión AWS Site-to-Site VPNcuyo grupo de registro se rastrea para detectar un error de VPN.
   - TunnelAIPAddress (Obligatorio):

     La dirección IP del túnel A asociada a su conexión AWS Site-to-Site VPN.

- TunnelBIPAddress (Opcional):

  La dirección IP del túnel B asociada a su conexión AWS Site-to-Site VPN.
- IKEVersion (Obligatorio):

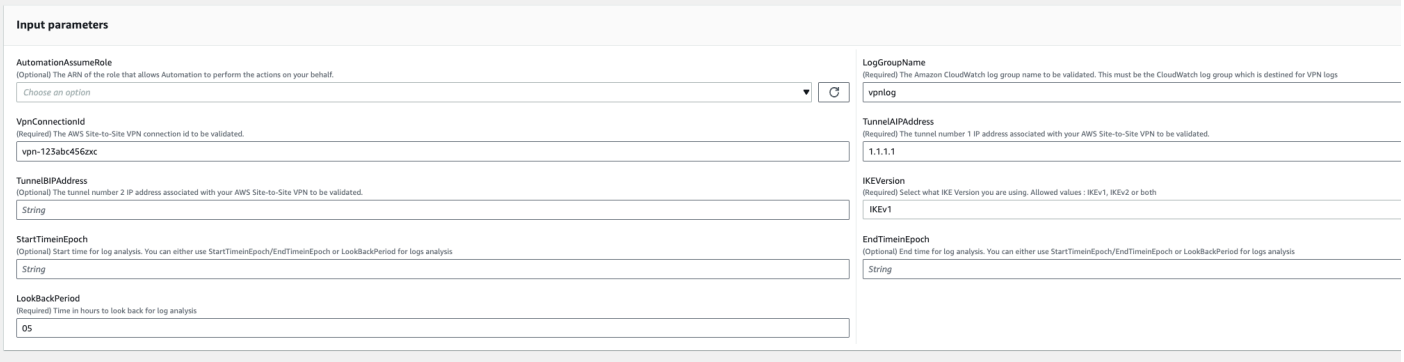
  Selecciona qué IKEversion está usando. Valores permitidos: IKEv1, IKEv2.
- StartTimeinEpoch (Opcional):

  El comienzo del intervalo de tiempo para realizar la consulta en busca de errores. El rango es inclusivo, por lo que la hora de inicio especificada se incluye en la consulta. Se especifica como tiempo de época el número de segundos desde el 1 de enero de 1970 a las 00:00:00 UTC.
- EndTimeinEpoch (Opcional):

  El final del intervalo de tiempo para buscar errores. El intervalo es inclusivo, por lo que la hora de finalización especificada se incluye en la consulta. Se especifica como tiempo de época el número de segundos desde el 1 de enero de 1970 a las 00:00:00 UTC.
- LookBackPeriod (Obligatorio):

  Tiempo en horas para revisar la consulta en busca de errores.

Nota: Configure un StartTimeinEpoch EndTimeinEpoch, o LookBackPeriod para fijar el intervalo de tiempo para el análisis de registros. Indique un número de dos dígitos en horas para comprobar si hay errores en el pasado desde la hora de inicio de la automatización. O bien, si el error se produjo en el pasado dentro de un intervalo de tiempo específico, incluya StartTimeinEpoch y EndTimeinEpoch, en lugar de LookBackPeriod.



3. Seleccione Ejecutar.
4. Se inicia la automatización.
5. El manual de procedimientos de automatización realiza los siguientes pasos:
   - parameterValidation:

Ejecuta una serie de validaciones de los parámetros de entrada incluidos en la automatización.

- branchOnValidationOfLogGroup:

  Comprueba si el grupo de registro mencionado en el parámetro es válido. Si no es válido, detiene los siguientes pasos de la automatización.

- branchOnValidationOfLogStream:

  Comprueba si el flujo de registros existe en el grupo de CloudWatch registros incluido. Si no es válido, detiene los siguientes pasos de la automatización.

- branchOnValidationOfVpnConnectionId:

  Comprueba si el identificador de conexión VPN incluido en el parámetro es válido. Si no es válido, detiene los siguientes pasos de la automatización.

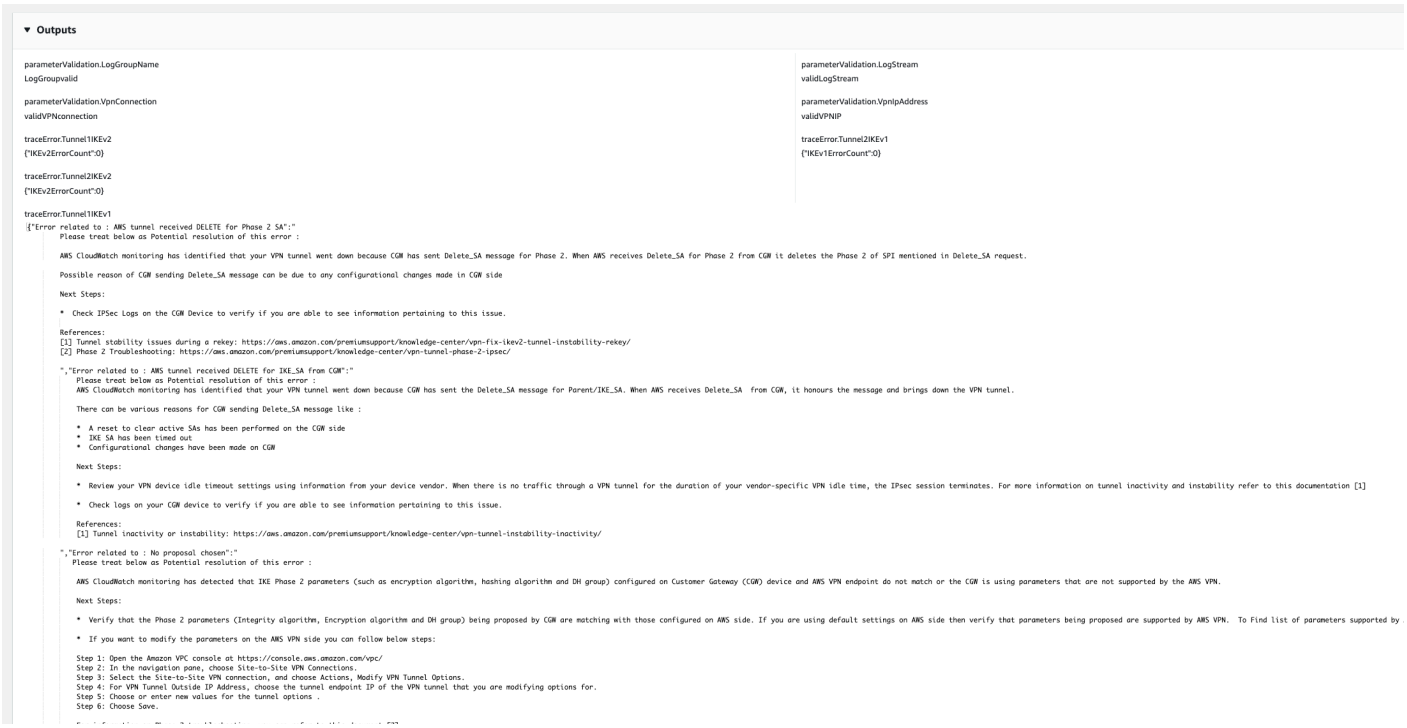
- branchOnValidationOfVpnIp:

  Comprueba si la dirección IP del túnel mencionada en el parámetro es válida o no. Si no es válida, detiene la ejecución posterior de los pasos de automatización.

- traceError:

  Realiza una llamada a la API de logs Insight en el grupo de registros incluido CloudWatch y busca el error relacionado con IKEv1/IKEv2 junto con una sugerencia de resolución relacionada.

6. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.



Referencias

Automatización de Systems Manager

- Ejecuta esta automatización (consola)
- Ejecución de una automatización
- Configuración de Automation
- Página de inicio de Support Automation Workflows

AWS documentación de servicio

- Contenido de los registros de Site-to-Site VPN

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descripción

El manual de procedimientos de `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` elimina la puerta de enlace de Internet de solo salida especificada.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- EgressOnlyInternetGatewayID

  Tipo: cadena

  Descripción: (obligatorio) el ID de la puerta de enlace de Internet de solo salida que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Pasos de documentos

- `aws:executeScript`: elimina la puerta de enlace de Internet de solo salida especificada en el parámetro `EgressOnlyInternetGatewayId`.
- `aws:executeScript`: verifica que se haya eliminado la puerta de enlace de Internet de solo salida.

`AWSConfigRemediation-DeleteUnusedENI`

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedENI` elimina una interfaz de red elástica (ENI) que tiene un estado de conexión de `detached`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- NetworkInterfaceID

  Tipo: cadena

  Descripción: (obligatorio) ID de la instancia de ENI que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Pasos de documentos

- `aws:executeAwsApi`: elimina el ENI que especifique en el parámetro `NetworkInterfaceId`.
- `aws:executeScript`: verifica que se haya eliminado el ENI.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedSecurityGroup` elimina el grupo de seguridad que especifique en el parámetro `GroupId`. Si intenta eliminar un grupo de seguridad asociado a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o si otro grupo de seguridad hace referencia a este, falla la automatización. Esta automatización no elimina un grupo de seguridad predeterminado.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- GroupId

  Tipo: cadena

  Descripción: (obligatorio) el ID del grupo de seguridad que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Pasos de documentos

- `aws:executeAwsApi`: regresa el nombre del grupo de seguridad utilizando el valor que haya proporcionado en el parámetro `GroupId`.
- `aws:branch`: confirma que el nombre del grupo no es “predeterminado”.
- `aws:executeAwsApi`: elimina el grupo de seguridad especificado en el parámetro `GroupId`.
- `aws:executeScript`: confirma que se ha eliminado el grupo de seguridad.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` elimina una lista de control de acceso (ACL) de red que no está asociada a una subred.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- NetworkAclID

  Tipo: cadena

  Descripción: (obligatorio) el ID de la ACL de red que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Pasos de documentos

- `aws:executeAwsApi`: elimina la ACL de red especificada en el parámetro `NetworkAclId`.
- `aws:executeScript`: confirma que se ha eliminado la ACL de red especificada en el parámetro `NetworkAclId`.

AWSConfigRemediation-DeleteVPCFlowLog

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteVPCFlowLog` elimina el registro de flujo de nube privada virtual (VPC) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- FlowLogID

  Tipo: cadena

  Descripción: (obligatorio) ID del registro de flujo que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: elimina el registro de flujo que especifique en el parámetro `FlowLogId`.
- `aws:executeScript`: verifica que se haya eliminado el registro de flujo.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Descripción

El manual de procedimientos `AWSConfigRemediation-DetachAndDeleteInternetGateway` separa y elimina la puerta de enlace de Internet que especifique. Si alguna instancia de Amazon EC2 de su nube privada virtual (VPC) tiene direcciones IP elásticas o direcciones IPv4 públicas asociadas, se produce un error en el manual de procedimientos.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- InternetGatewayID

  Tipo: cadena

  Descripción: (obligatorio) el ID de la puerta de enlace de Internet que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Pasos de documentos

- `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad estatal de la puerta de enlace privada virtual cambie a `available` o se agote el tiempo de espera.
- `aws:executeAwsApi`: recupera una configuración de puerta de enlace privada virtual específica.
- `aws:branch`- Se ramifican según el valor del parámetro VpcAttachments .state.

- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie `attached` o se agote el tiempo de espera.
- `aws:executeAwsApi`: acepta el ID de la puerta de enlace virtual privada y el ID de Amazon VPC como entrada y separa la puerta de enlace virtual privada de la Amazon VPC.

- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie o se agote el tiempo de espera. `detached`

- `aws:executeAwsApi`: acepta el ID de la puerta de enlace privada virtual como entrada y lo elimina.

- `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual como entrada y verifica su eliminación.

  `aws:executeAwsApi`: recopila el ID de VPC del ID de la puerta de enlace de Internet.
- `aws:executeAwsApi`: separa el ID de la puerta de enlace de Internet de la VPC.
- `aws:executeAwsApi`: elimina la puerta de enlace de Internet.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Descripción

El manual de procedimientos `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` separa y elimina una determinada puerta de enlace privada virtual de Amazon Elastic Compute Cloud (Amazon EC2) asociada a una nube privada virtual (VPC) creada con Amazon Virtual Private Cloud (Amazon VPC).

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- VpnGatewayID

  Tipo: cadena

  Descripción: (obligatorio) el ID de la puerta de enlace privada virtual que se va a eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Pasos de documentos

- `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad estatal de la puerta de enlace privada virtual cambie a `available` o se agote el tiempo de espera.
- `aws:executeAwsApi`: recupera una configuración de puerta de enlace privada virtual específica.
- `aws:branch`- Se ramifican según el valor del parámetro VpcAttachments .state.

- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie `attached` o se agote el tiempo de espera.

- `aws:executeAwsApi`: acepta el ID de la puerta de enlace virtual privada y el ID de Amazon VPC como entrada y separa la puerta de enlace virtual privada de la Amazon VPC.
- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie o se agote el tiempo de espera. `detached`

- `aws:executeAwsApi`: acepta el ID de la puerta de enlace privada virtual como entrada y lo elimina.

- `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual como entrada y verifica su eliminación.

AWS-DisableIncomingSSHOnPort22

Descripción

El `AWS-DisableIncomingSSHOnPort22` manual elimina las reglas que permiten el tráfico SSH entrante sin restricciones en el puerto TCP 22 para los grupos de seguridad.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- SecurityGroupID

  Tipo: cadena

  Descripción: (Obligatorio) Una lista separada por comas de los ID de los grupos de seguridad a los que desea restringir el tráfico SSH.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Pasos de documentos

- `aws:executeAwsApi`- Elimina todas las reglas que permiten el tráfico SSH entrante en el puerto TCP 22 de los grupos de seguridad que especifique en el parámetro. `SecurityGroupIds`

Salidas

DisableIncomingPlantilla SSH. RestrictedSecurityGroupIds - Una lista de los ID de los grupos de seguridad a los que se les han eliminado las reglas de SSH entrantes.

AWS-DisablePublicAccessForSecurityGroup

Descripción

Este manual de procedimientos deshabilita los puertos SSH y RDP predeterminados que se abren a todas las direcciones IP.

> **Important**
>
> Este manual no funciona con un». InvalidPermission NotFound«error para los grupos de seguridad que cumplen los dos criterios siguientes: 1) El grupo de seguridad está ubicado

en una VPC no predeterminada; y 2) Las reglas de entrada del grupo de seguridad no especifican los puertos abiertos mediante los cuatro patrones siguientes:

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

> **Note**
>
> Este manual no está disponible en China. Regiones de AWS

[Ejecuta esta automatización (consola)]

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- GroupId

  Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad para el que los puertos deben estar deshabilitados.

- IpAddressToBlock

  Tipo: cadena

  Descripción: (opcional) las direcciones IPv4 adicionales desde las que el acceso debe estar bloqueado, con el formato `1.2.3.4/32`.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descripción

El manual de procedimientos `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` deshabilita el atributo de direccionamiento público IPv4 para la subred que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- SubnetId

Tipo: cadena

Descripción: (obligatorio) el ID de la subred en la que desea deshabilitar la asignación automática del atributo de dirección IPv4 público.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Pasos de documentos

- `aws:executeAwsApi`: desactiva el atributo de asignación automática de direcciones IPv4 públicas para la subred que especificó en el parámetro `SubnetId`.
- `aws:assertAwsResourceProperty`: verifica que el atributo se ha desactivado.

AWSSupport-EnableVPCFlowLogs

Descripción

El manual de procedimientos `AWSSupport-EnableVPCFlowLogs` crea registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) para las subredes, las interfaces de red y las VPC en su Cuenta de AWS. Si crea un log de flujo para una subred o VPC, se supervisará cada interfaz de red elástica de Amazon VPC o la subred. Los datos del registro de flujo se publican en el grupo de CloudWatch registros de Amazon Logs o en el depósito de Amazon Simple Storage Service (Amazon S3) que especifique. Para obtener más información sobre los registros de flujo, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Important

Los cargos por ingesta y archivado de datos para los registros vendidos se aplican cuando publica los CloudWatch registros de flujo en Logs o en Amazon S3. Para obtener más información, consulte Registros de flujo de precios.

Ejecuta esta automatización (consola)

Note

s3Al seleccionar el destino del registro, asegúrese de que la política de compartimentos permita al servicio de entrega de registros acceder al depósito. Para obtener más información, consulte Permisos de bucket de Amazon S3 para registros de flujo.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- DeliverLogsPermissionArn

  Tipo: cadena

Descripción: (opcional) El ARN de la función de IAM que permite a Amazon Elastic Compute Cloud (Amazon EC2) publicar registros de flujo en CloudWatch el grupo de registros de su cuenta. Si especifica `s3` para el parámetro `LogDestinationType`, no proporcione un valor para este parámetro. Para obtener más información, consulte Publicar registros de flujo en CloudWatch registros en la Guía del usuario de Amazon VPC.

- LogDestinationARN

  Tipo: cadena

  Descripción: (opcional) el ARN del recurso en el que se publican los datos del registro de flujo. Si `cloud-watch-logs` se especifica para el `LogDestinationType` parámetro, proporcione el ARN del grupo de CloudWatch registros en el que desea publicar los datos del registro de flujo. También puede utilizar `LogGroupName` en su lugar. Si se especifica `s3` para el parámetro `LogDestinationType`, debe especificar el ARN del bucket de Amazon S3 en el que desea publicar los datos del registro de flujo para este parámetro. También puede especificar una carpeta de bucket.

  > **Important**
  >
  > `s3`Al elegir uno, `LogDestinationType` debe asegurarse de que el bucket seleccionado siga las prácticas recomendadas de seguridad de Amazon S3 Bucket y de que cumpla con las leyes de privacidad de datos de su organización y región geográfica.

- LogDestinationType

  Tipo: cadena

  Valores válidos: cloud-watch-logs | s3

  Descripción: (obligatorio) determina dónde se publican los datos del registro de flujo. Si especifica `LogDestinationType` como `s3`, no especifique `DeliverLogsPermissionArn` ni `LogGroupName`.

- LogFormat

  Tipo: cadena

  Descripción: (opcional) los campos que se van a incluir en el registro de logs de flujo, en el orden en que deben aparecer. Para obtener una lista de los campos disponibles, consulte Entradas de

registros de flujo en la Guía del usuario de Amazon VPC. Si no proporciona un valor para este parámetro, el registro de flujo se crea con el formato predeterminado. Si especifica este parámetro, debe especificar al menos un campo.

- LogGroupName

  Tipo: cadena

  Descripción: (opcional) Nombre del grupo de CloudWatch registros donde se publican los datos del registro de flujo. Si especifica `s3` para el parámetro `LogDestinationType`, no proporcione un valor para este parámetro.

- ResourceIds

  Tipo: StringList

  Descripción: (obligatorio) una lista separada por comas de los ID de las subredes, interfaces de red elásticas o VPC para las que desea crear un registro de flujo.

- TrafficType

  Tipo: cadena

  Valores válidos: ACCEPT | REJECT | ALL

  Descripción: (obligatorio) el tipo de tráfico que se va a registrar. Puede registrar el tráfico que el recurso acepta o rechaza, o todo el tráfico.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`
- `iam:AttachRolePolicy`
- `iam:CreateRole`

- iam:CreatePolicy
- iam:DeletePolicy
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:TagRole
- iam:PassRole
- iam:PutRolePolicy
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

Ejemplo de política

```
       {
           "Version": "2012-10-17",
           "Statement": [
               {
                   "Sid": "SSM Execution Permissions",
                   "Effect": "Allow",
```

```
                    "Action": [
                        "ssm:StartAutomationExecution",
                        "ssm:GetAutomationExecution"
                    ],
                    "Resource": "*"
                },
                {
                    "Sid": "EC2 FlowLogs Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:CreateFlowLogs",
                        "ec2:DeleteFlowLogs",
                        "ec2:DescribeFlowLogs"
                    ],
                    "Resource": "arn:{partition}:ec2:{region}:{account-id}:{instance|
subnet|vpc|transit-gateway|transit-gateway-attachment}/{resource ID}"
                },
                {
                    "Sid": "IAM CreateRole Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "iam:AttachRolePolicy",
                        "iam:CreateRole",
                        "iam:CreatePolicy",
                        "iam:DeletePolicy",
                        "iam:DeleteRole",
                        "iam:DeleteRolePolicy",
                        "iam:GetPolicy",
                        "iam:GetRole",
                        "iam:TagRole",
                        "iam:PassRole",
                        "iam:PutRolePolicy",
                        "iam:UpdateRole"
                    ],
                    "Resource": [
                        "arn:{partition}:iam::{account-id}:role/{role name}",
                        "arn:{partition}:iam::{account-id}:role/
AWSSupportCreateFlowLogsRole"
                    ]
                },
                {
                    "Sid": "CloudWatch Logs Permissions",
                    "Effect": "Allow",
                    "Action": [
```

```
                        "logs:CreateLogDelivery",
                        "logs:CreateLogGroup",
                        "logs:DeleteLogDelivery",
                        "logs:DeleteLogGroup",
                        "logs:DescribeLogGroups",
                        "logs:DescribeLogStreams"
                    ],
                    "Resource": [
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}",
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}:*"
                    ]
                },
                {
                    "Sid": "S3 Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "s3:GetBucketLocation",
                        "s3:GetBucketPublicAccessBlock",
                        "s3:GetAccountPublicAccessBlock",
                        "s3:GetBucketPolicyStatus",
                        "s3:GetBucketAcl",
                        "s3:ListBucket",
                        "s3:PutObject"
                    ],
                    "Resource": [
                        "arn:{partition}:s3:::{bucket name}",
                        "arn:{partition}:s3:::{bucket name}/*"
                    ]
                }
            ]
        }
```

Pasos de documentos

- `aws:branch`: se ramifica en función del valor especificado para el parámetro `LogDestinationType`.
- `aws:executeScript`- Comprueba si el Amazon Simple Storage Service (Amazon S3) de destino puede conceder acceso de lectura o `public` escritura a sus objetos.

- `aws:executeScript`: crea un grupo de registro si no se especifica ningún valor para el parámetro `LogDestinationARN`, y se especifica `cloud-watch-logs` para el parámetro `LogDestinationType`.
- `aws:executeScript`: crea registros de flujo en función de los valores especificados en los parámetros del manual de procedimientos.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Descripción

El `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook reemplaza un registro de flujo de Amazon VPC existente que publica los datos del registro de flujo en Amazon Simple Storage Service (Amazon S3) por un registro de flujo que publica los datos del registro de flujo en el grupo de registros de CloudWatch Amazon Logs CloudWatch (Logs) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DestinationLogGrupo

Tipo: cadena

Descripción: (obligatorio) El nombre del grupo de CloudWatch registros en el que desea publicar los datos del registro de flujo.

- DeliverLogsPermissionArn

  Tipo: cadena

  Descripción: (obligatorio) El ARN del rol AWS Identity and Access Management (IAM) que desea utilizar y que proporciona a Amazon Elastic Compute Cloud (Amazon EC2) los permisos necesarios para publicar datos de registros de flujo en Logs. CloudWatch

- FlowLogID

  Tipo: cadena

  Descripción: (obligatorio) el ID del registro de flujo que publica en Amazon S3 que desea reemplazar.

- MaxAggregationIntervalo

  Tipo: entero

  Valores válidos: 60 | 600

  Descripción: (opcional) el intervalo máximo de tiempo durante el cual se captura un flujo de paquetes y se agrega un registro de logs de flujo.

- TrafficType

  Tipo: cadena

  Valores válidos: ACCEPT | REJECT | ALL

  Descripción: (obligatorio) el tipo de datos del registro de flujo que desea registrar y publicar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre su VPC a partir del valor que especifique en el parámetro `FlowLogId`.
- `aws:executeAwsApi`: crea un registro de flujo en función de los valores que especifique para los parámetros del manual de procedimientos.
- `aws:assertAwsResourceProperty`- Verifica que el registro de flujo recién creado se publique en CloudWatch Logs.
- `aws:executeAwsApi`: elimina el registro de flujo que se publica en Amazon S3.
- `aws:executeScript`: confirma que se ha eliminado el registro de flujo publicado en Amazon S3.

`AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket`

Descripción

El `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook reemplaza un registro de flujo de Amazon VPC existente que publica los datos del registro de flujo en CloudWatch Amazon Logs CloudWatch (Logs) por un registro de flujo que publica los datos del registro de flujo en el depósito de Amazon Simple Storage Service (Amazon S3) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- Destinos 3 BucketArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN del bucket de Amazon S3 en el que desea publicar los datos del registro de flujo.

- FlowLogID

  Tipo: cadena

  Descripción: (obligatorio) El ID del registro de flujo que se publica en los CloudWatch registros que desea reemplazar.

- MaxAggregationIntervalo

  Tipo: entero

  Valores válidos: 60 | 600

  Descripción: (opcional) el intervalo máximo de tiempo durante el cual se captura un flujo de paquetes y se agrega un registro de logs de flujo.

- TrafficType

  Tipo: cadena

  Valores válidos: ACCEPT | REJECT | ALL

  Descripción: (obligatorio) el tipo de datos del registro de flujo que desea registrar y publicar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre su VPC a partir del valor que especifique en el parámetro `FlowLogId`.
- `aws:executeAwsApi`: crea un registro de flujo en función de los valores que especifique para los parámetros del manual de procedimientos.
- `aws:assertAwsResourceProperty`: verifica que el registro de flujo recién creado se publique en Amazon S3.
- `aws:executeAwsApi`- Elimina el registro de flujo que se publica en CloudWatch Logs.
- `aws:executeScript`- Confirma que se ha eliminado el registro de flujo publicado en CloudWatch Logs.

AWS-ReleaseElasticIP

Descripción

Libere la dirección IP elástica especificada utilizando el ID de asignación.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- AllocationId

  Tipo: cadena

  Descripción: (obligatorio) el ID de asignación de la dirección IP elástica.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descripción

El AWS-RemoveNetworkACLUnrestrictedSSHRDP manual elimina todas las reglas de la lista de control de acceso a la red (ACL) de la ACL de red especificada que permiten la entrada de tráfico desde todas las direcciones de origen a los puertos SSH y RDP predeterminados. No se eliminan las reglas que incluyen rangos de puertos que se superponen con los puertos SSH y RDP predeterminados.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- NetworkAclID

  Tipo: cadena

  Descripción: (obligatorio) El ID de la ACL de la red que desea eliminar, las reglas sin restricciones que permiten la entrada de tráfico desde todas las direcciones de origen a los puertos SSH y RDP predeterminados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Pasos de documentos

- `aws:executeScript`: elimina todas las reglas de entrada que permiten el tráfico de todas las direcciones de origen del grupo de seguridad que especificó en el parámetro `SecurityGroupId`.

Salidas

RemoveNaclEntriesAndVerifica. VerificationMessage - Mensajes de verificación de las reglas de ACL de la red eliminadas correctamente.

RemoveNaclEntriesAndVerificar. RulesDeletedAndApiResponses - Las reglas de ACL de la red que se eliminaron y las respuestas de la operación de la `DeleteNetworkAclEntry` API.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Descripción

El manual de procedimientos `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` elimina todas las reglas de entrada del grupo de seguridad que especifique que permiten el tráfico desde todas las direcciones de origen.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- SecurityGroupID

  Tipo: cadena

  Descripción: (obligatorio) el ID del grupo de seguridad del que desea eliminar las reglas de entrada que permiten el tráfico desde todas las direcciones de origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Pasos de documentos

- `aws:executeScript`: elimina todas las reglas de entrada que permiten el tráfico de todas las direcciones de origen del grupo de seguridad que especificó en el parámetro `SecurityGroupId`.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Descripción

El manual de procedimientos `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` elimina todas las reglas del grupo de seguridad predeterminado de la nube privada virtual (VPC) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- GroupId

  Tipo: cadena

  Descripción: (obligatorio) el ID del grupo de seguridad del que desea eliminar todas las reglas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el grupo de seguridad que especificó en el parámetro `GroupId` se denomina predeterminado.
- `aws:executeScript`: elimina todas las reglas del grupo de seguridad que especificó en el parámetro `GroupId`.

AWSSupport-SetupIPMonitoringFromVPC

Descripción

`AWSSupport-SetupIPMonitoringFromVPC` crea una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la subred especificada y monitorea las IP de destino seleccionadas (IPv4 o IPv6) mediante la ejecución continua de pruebas de ping, MTR, traceroute y tracetcp. Los resultados

se almacenan en los CloudWatch registros de Amazon Logs y se aplican filtros de métricas para visualizar rápidamente las estadísticas de latencia y pérdida de paquetes en un CloudWatch panel de control.

Información adicional

CloudWatch Los datos de los registros se pueden utilizar para solucionar problemas de red y analizar patrones o tendencias. Además, puede configurar CloudWatch alarmas con notificaciones de Amazon SNS cuando la pérdida de paquetes o la latencia alcancen un umbral. Los datos también se pueden utilizar al abrir un caso AWS Support, para ayudar a aislar un problema rápidamente y reducir el tiempo de resolución al investigar un problema de red.

> **Note**
>
> Para limpiar los recursos creados por `AWSSupport-SetupIPMonitoringFromVPC`, puede utilizar el manual de procedimientos `AWSSupport-TerminateIPMonitoringFromVPC`. Para obtener más información, consulte `AWSSupport-TerminateIPMonitoringFromVPC`.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CloudWatchLogGroupNamePrefix

  Tipo: cadena

  Valor predeterminado: / `AWSSupport-SetupIPMonitoringFromVPC`

  Descripción: Prefijo (opcional) utilizado para cada grupo de CloudWatch registros creado para los resultados de las pruebas.

- CloudWatchLogGroupRetentionInDías

  Tipo: cadena

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  Valor predeterminado: 7

  Descripción: (opcional) número de días para los que desea conservar los resultados de monitorización de red.

- InstanceType

  Tipo: cadena

  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

  Valor predeterminado: t2.micro

  Descripción: (opcional) tipo de instancia EC2 para la instancia EC2Rescue. Tamaño recomendado: t2.micro.

- SubnetId

  Tipo: cadena

  Descripción: (opcional) ID de subred para la instancia de monitor. Tenga en cuenta que si especifica una subred privada, debe asegurarse de que haya acceso a Internet para permitir que la instancia del monitor configure la prueba (es decir, instale el agente CloudWatch Logs, interactúe con Systems Manager y CloudWatch).

- TargetIPs

Tipo: cadena

Descripción: (obligatorio) lista separada por comas de IPv4s y/o IPv6s que monitorizar. No se permiten espacios. El tamaño máximo es de 255 caracteres. Tenga en cuenta que si proporciona una IP no válida, la Automation producirá un error y restaurará la configuración de prueba.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que el usuario que ejecuta la automatización tenga adjunta la política gestionada de AutomationRole IAM de AmazonSSM. Además, el usuario debe tener la siguiente política asociada a su cuenta de usuario, grupo o rol:

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

Pasos de documentos

1. **aws:executeAwsApi**: describe la subred proporcionada.
2. **aws:branch**: evalúa la entrada TargetIPs.

   (IPv6) Si TargetIPs contiene una dirección IPv6:

   aws:assertAwsResourceProperty: comprueba que la subred proporcionada tiene un grupo de IPv6 asociado.
3. **aws:executeScript**: obtiene la arquitectura del tipo de instancia y la ruta de parámetros públicos de la versión más reciente de Amazon Linux 2 AMI.
4. **aws:executeAwsApi**: obtiene la versión más reciente de Amazon Linux 2 AMI en Parameter Store.
5. **aws:executeAwsApi**: crea un grupo de seguridad para la prueba en la VPC de subred.

   (Limpieza) Si la creación del grupo de seguridad falla:

   aws:executeAwsApi: elimina el grupo de seguridad creado por la automatización, en caso de que exista.
6. **aws:executeAwsApi**: permite todo el tráfico saliente en el grupo de seguridad de la prueba.

   (Limpieza) Si la creación de la regla de salida del grupo de seguridad falla:

aws:executeAwsApi: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

7. **aws:executeAwsApi**: crea un rol de IAM para la instancia EC2 de prueba.

   (Limpieza) Si la creación del rol falla:

   a. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización, en caso de que exista.

   b. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

8. **aws:executeAwsApi**- adjunte la política administrada de AmazonSSM ManagedInstanceCore

   (Limpieza) Si la asociación de políticas falla:

   a. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada de AmazonSSM de la función creada por la automatización, si está asociada.

   b. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

   c. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

9. **aws:executeAwsApi**- adjunte una política en línea que permita configurar las retenciones de los grupos de CloudWatch registros y crear un panel de control CloudWatch

   (Limpieza) Si la asociación de políticas insertadas falla:

   a. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización, si se creó.

   b. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM del rol creado por la automatización.

   c. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

   d. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

10. **aws:executeAwsApi**: crea un perfil de instancia de IAM.

    (Limpieza) Si la creación del perfil de instancia falla:

    a. **aws:executeAwsApi**: elimina el perfil de instancia de creado por la automatización, en caso de que exista.

b. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

c. **aws:executeAwsApi**- elimine la política ManagedInstanceCore gestionada por AmazonSSM del rol creado por la automatización.

d. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

e. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

11 **aws:executeAwsApi**: adjunta el rol de IAM al perfil de instancias.

(Limpieza) Si la asociación del perfil de instancia con el rol falla:

a. **aws:executeAwsApi**: quita el perfil de instancia de del rol, si están asociados.

b. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

c. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

d. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

e. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

f. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

12 **aws:sleep**: espera a que el perfil de instancia vuelva a estar disponible.

13 **aws:runInstances**: permite crear la instancia de prueba en la subred especificada y con el perfil de instancia que creó anteriormente asociado.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

14 **aws:branch**: evalúa la entrada TargetIPs.

(IPv6) Si TargetIPs contiene una dirección IPv6:

aws:executeAwsApi: asigna un IPv6 a la instancia de prueba.

15 **aws:waitForAwsResourceProperty**: espera a que la instancia de prueba se convierta en una instancia gestionada.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

16 **aws:runCommand**: instala los requisitos previos de la prueba:

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

17. **aws:runCommand**: comprueba que las IP proporcionadas son direcciones IPv4 y/o IPv6 correctas desde el punto de vista sintáctico.

    (Limpieza) Si el paso falla:

    a. **aws:changeInstanceState**: termina la instancia de prueba.

    b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

    c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

    d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

    e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

    f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

    g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

18. **aws:runCommand**: define la prueba de MTR para cada una de las IP proporcionadas.

    (Limpieza) Si el paso falla:

    a. **aws:changeInstanceState**: termina la instancia de prueba.

    b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

    c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

    d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

    e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

    f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

    g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

19. **aws:runCommand**: define la primera prueba de ping para cada una de las IP proporcionadas.

    (Limpieza) Si el paso falla:

    a. **aws:changeInstanceState**: termina la instancia de prueba.

    b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

    c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

20 **aws:runCommand**: define la segunda prueba de ping para cada una de las IP proporcionadas.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

21 **aws:runCommand**: define la prueba de tracepath para cada una de las IP proporcionadas.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

22 **aws:runCommand**: define la prueba de traceroute para cada una de las IP proporcionadas.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

23 **aws:runCommand**- configurar los registros. CloudWatch

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

24 **aws:runCommand**: programa trabajos cron para ejecutar cada prueba cada minuto.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

25 **aws:sleep**: espera a que las pruebas generen algunos datos.

26 **aws:runCommand**- establezca las retenciones de grupos de CloudWatch registros deseadas.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

27 **aws:runCommand**- defina los filtros de métricas de los grupos de CloudWatch registros.

(Limpieza) Si el paso falla:

a. **aws:changeInstanceState**: termina la instancia de prueba.

b. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

c. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

d. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

e. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

f. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

g. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

28 **aws:runCommand**- crear el panel de control. CloudWatch

(Limpieza) Si el paso falla:

a. **aws:executeAwsApi**- eliminar el CloudWatch panel de control, si existe.

b. **aws:changeInstanceState**: termina la instancia de prueba.

c. **aws:executeAwsApi**: quita el perfil de instancia de IAM del rol.

d. **aws:executeAwsApi**: elimina el perfil de instancia de IAM creado por la automatización.

e. **aws:executeAwsApi**- elimine la política CloudWatch en línea del rol creado por la automatización.

f. **aws:executeAwsApi**- separe la política ManagedInstanceCore gestionada por AmazonSSM de la función creada por la automatización.

g. **aws:executeAwsApi**: elimina el rol de IAM creado por la automatización.

h. **aws:executeAwsApi**: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

Salidas

create CloudWatch Dashboards.Output: la URL del panel de control. CloudWatch

ManagedInstancecrear. InstanceIds - el ID de la instancia de prueba.

AWSSupport-TerminateIPMonitoringFromVPC

Descripción

`AWSSupport-TerminateIPMonitoringFromVPC` finaliza una prueba de supervisión de IP iniciada previamente por `AWSSupport-SetupIPMonitoringFromVPC`. Se eliminarán los datos relacionados con el ID de prueba especificado.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- AutomationExecution- ID

  Tipo: cadena

  Descripción: (obligatorio) el ID de ejecución de la automatización de cuando ejecutó anteriormente el manual de procedimientos `AWSSupport-SetupIPMonitoringFromVPC`. Se eliminan todos los recursos asociados a este ID de ejecución.
- InstanceId

  Tipo: cadena

  Descripción: (opcional) ID de instancia para la instancia de monitor.
- SubnetId

  Tipo: cadena

  Descripción: (opcional) ID de subred para la instancia de monitor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que el usuario que ejecuta la automatización tenga adjunta la política gestionada de AutomationRole IAM de AmazonSSM. Además, el usuario debe tener la siguiente política asociada a su usuario, grupo o rol:

```
{
"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"
    ]
}
```

Pasos de documentos

1. `aws:assertAwsResourceProperty`- comprueban AutomationExecutionId y InstanceId están relacionados con la misma prueba.
2. `aws:assertAwsResourceProperty`- comprueban SubnetId y InstanceId están relacionados con la misma prueba.
3. `aws:executeAwsApi`: recupera el grupo de seguridad de prueba.
4. `aws:executeAwsApi`- eliminar el CloudWatch panel de control.
5. `aws:changeInstanceState`: termina la instancia de prueba.
6. `aws:executeAwsApi`: quita el perfil de instancia de IAM del rol.
7. `aws:executeAwsApi`: elimina el perfil de instancia de IAM creado por la automatización.
8. `aws:executeAwsApi`- elimine la política CloudWatch en línea del rol creado por la automatización.
9. `aws:executeAwsApi`- separe la política gestionada por AmazonSSM ManagedInstance Core del rol creado por la automatización.
10. `aws:executeAwsApi`: elimina el rol de IAM creado por la automatización.
11. `aws:executeAwsApi`: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

Salidas

Ninguna

AWS WAF

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS WAF Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Descripción

El `AWS-AddWAFRegionalRuleToRuleGroup` manual agrega una regla AWS WAF regional existente a un grupo de reglas AWS WAF regionales. Solo se admiten los grupos de reglas regionales AWS WAF clásicos. AWS WAF Los grupos de reglas regionales clásicos pueden tener un máximo de 10 reglas.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- RuleGroupID

  Tipo: cadena

  Descripción: (obligatorio) El ID del grupo de reglas que quieres actualizar.

- RulePriority

  Tipo: entero

  Descripción: (Obligatorio) La prioridad de la nueva regla. La prioridad de las reglas determina el orden en que se evalúan las reglas de un grupo regional. Las reglas con un valor más bajo tienen mayor prioridad que las reglas con un valor más alto. El valor debe ser un número entero. Si agrega varias reglas a un grupo de reglas regional, los valores no tienen que ser consecutivos.

- RuleId

  Tipo: cadena

  Descripción: (obligatorio) El identificador de la regla que desea agregar a su grupo de reglas regional.

- RuleAction

  Tipo: cadena

  Descripción: (Obligatorio) Especifica la acción que AWS WAF se lleva a cabo cuando una solicitud web cumple las condiciones de la regla.

  Valores válidos: ALLOW | BLOCK | COUNT

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Pasos de documentos

- getWAF ChangeToken (aws:executeAwsApi): recupera un token de AWS WAF cambio para garantizar que el runbook no envíe solicitudes contradictorias al servicio.
- addWAF RuleTo WAF RegionalRuleGroup (aws:Executescript): añade la regla especificada al grupo de reglas regional. AWS WAF
- VerifyChangeTokenPropagating (aws:wait ForAwsResourceProperty) - Verifica que el estado del token de cambio sea o. `PENDING` `INSYNC`
- VerifyRuleAddedToRuleGroup (AWS:Executescript) - Verifica que la AWS WAF regla especificada se haya agregado al grupo de reglas regional de destino.

Salidas

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Resultado del paso que verifica que la nueva regla se agregó al grupo de reglas regional.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Resultado de la operación de la `ListActivatedRulesInRuleGroup` API.

AWS-AddWAFRegionalRuleToWebAcl

Descripción

El `AWS-AddWAFRegionalRuleToWebAcl` manual agrega una regla AWS WAF regional, un grupo de reglas o una regla basada en tasas existentes a una lista de control de acceso web (ACL) regional AWS WAF clásica. Este manual no actualiza las ACL web regionales AWS WAF clásicas existentes administradas por. AWS Firewall Manager

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- WebACLId

  Tipo: cadena

  Descripción: (obligatorio) El ID de la ACL web que desea actualizar.
- ActivatedRulePrioridad

  Tipo: entero

  Descripción: (Obligatoria) La prioridad de la nueva regla. La prioridad de las reglas determina el orden en que se evalúan las reglas de una ACL web. Las reglas con un valor más bajo tienen mayor prioridad que las reglas con un valor más alto. El valor debe ser un número entero. Si agrega varias reglas a una ACL web regional, los valores no tienen que ser consecutivos.
- ActivatedRuleRuleId

  Tipo: cadena

  Descripción: (Obligatorio) El ID de la regla normal, la regla basada en tasas o el grupo que desea agregar a la ACL web.

- ActivatedRuleAcción

  Tipo: cadena

  Valores válidos: ALLOW | BLOCK | COUNT

  Descripción: (opcional) Especifica la acción que AWS WAF se realiza cuando una solicitud web cumple las condiciones de la regla.

- ActivatedRuleTipo

  Tipo: cadena

  Valores válidos: REGULAR | RATE_BASED | GROUP

  Predeterminado: REGULAR

  Descripción: (opcional) El tipo de regla que va a agregar a la ACL web. Aunque este campo es opcional, tenga en cuenta que si intenta agregar una `RATE_BASED` regla a una ACL web sin establecer el tipo, la solicitud fallará porque la solicitud utiliza una `REGULAR` regla de forma predeterminada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Pasos de documentos

- DetermineWebACL NotIn FMS AndRulePriority (AWS:ExecuteScript): verifica si la ACL AWS WAF web se encuentra en una política de seguridad de Firewall Manager y verifica que el ID de prioridad no entre en conflicto con una ACL existente.

- AddRuleOrRuleGroupToWebACL (aws:ExecuteScript): agrega la regla especificada a la ACL web. AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (AWS:ExecuteScript): verifica que la regla especificada se haya agregado a la ACL web de destino. AWS WAF

Salidas

- DetermineWebNotInPrioridad AndRule ACL FMS. PrereqResponse: Resultado del `DetermineWebACLNotInFMSAndRulePriority` paso.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Resultado del `AddRuleOrRuleGroupToWebACL` paso.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Resultado del `VerifyRuleOrRuleGroupAddedToWebAcl` paso.

AWSConfigRemediation-EnableWAFClassicLogging

Descripción

El `AWSConfigRemediation-EnableWAFClassicLogging` runbook permite iniciar sesión en Amazon Data Firehose (Firehose) para obtener AWS WAF la lista de control de acceso web (ACL web) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DeliveryStreamNombre

  Tipo: cadena

  Descripción: (Obligatorio) El nombre de la transmisión de entrega de Firehose a la que desea enviar los registros.

- WebACLId

  Tipo: cadena

  Descripción: (obligatorio) El ID de la ACL AWS WAF web en la que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Pasos de documentos

- `aws:executeAwsApi`: confirma que existe el flujo de entrega que especifique en `DeliveryStreamName`.
- `aws:executeAwsApi`- Recopila el ARN de la ACL web especificada en AWS WAF `WebACLId` el parámetro.

- `aws:executeAwsApi`: permite el registro para la web ACL.
- `aws:assertAwsResourceProperty`- Verifica que el registro esté habilitado en la AWS WAF ACL web.

`AWSConfigRemediation-EnableWAFClassicRegionalLogging`

Descripción

El `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook permite iniciar sesión en Amazon Data Firehose (Firehose) para AWS WAF la lista de control de acceso web (ACL) que especifique.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.
- LogDestinationConfiguraciones

  Tipo: cadena

  Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la transmisión de entrega de Firehose a la que desea enviar los registros.

- WebACLId

  Tipo: cadena

  Descripción: (obligatorio) El ID de la ACL AWS WAF web en la que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Pasos de documentos

- `aws:executeAwsApi`- Recopila el ARN de la ACL web especificada en AWS WAF `WebACLId` el parámetro.
- `aws:executeAwsApi`: permite el registro para la web ACL.
- `aws:assertAwsResourceProperty`- Verifica que el registro esté habilitado en la AWS WAF ACL web.

AWSConfigRemediation-EnableWAFV2Logging

Descripción

El `AWSConfigRemediation-EnableWAFV2Logging` runbook permite registrar una lista de control de acceso web AWS WAF (ACL web) (AWS WAF V2) con el flujo de entrega de Amazon Data Firehose (Firehose) especificado.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRol

  Tipo: cadena

  Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LogDestinationConfiguraciones

  Tipo: cadena

  Descripción: (Obligatorio) El ARN del flujo de entrega de Firehose que desea asociar a la ACL web.

  > **Note**
  >
  > El ARN de la transmisión de entrega de Firehose debe empezar por el prefijo. `aws-waf-logs-` Por ejemplo, `aws-waf-logs-us-east-2-analytics`. Para obtener más información, consulte Amazon Data Firehose.

- WebAclArn

  Tipo: cadena

  Descripción: (obligatorio) el ARN de la web ACL para la que se habilitará el registro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Pasos de documentos

- `aws:executeScript`- Habilita el registro para la AWS WAF ACL web de la versión 2 y verifica que el registro tenga la configuración especificada.

Amazon WorkSpaces

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon WorkSpaces. Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

`AWS-CreateWorkSpace`

Descripción

El `AWS-CreateWorkSpace` runbook crea un nuevo escritorio WorkSpaces virtual de Amazon, conocido como a WorkSpace, en función de los valores que especifique para los parámetros de entrada. Para obtener más información WorkSpaces, consulta ¿Qué es Amazon WorkSpaces? en la Guía de WorkSpaces administración de Amazon.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

  Tipo: cadena

  Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
- BundleId

  Tipo: cadena

  Descripción: (Obligatorio) El identificador del paquete que se utilizará en WorkSpace.
- ComputeTypeNombre

  Tipo: cadena

  Valores válidos: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  Descripción: (opcional) El tipo de cálculo de su WorkSpace.
- DirectoryId

  Tipo: cadena

  Descripción: (obligatorio) El ID del directorio al que quieres WorkSpace añadirlo.

- RootVolumeEncryptionEnabled

  Tipo: Booleano

  Valores válidos: true | false

  Predeterminado: false

  Descripción: (opcional) Determina si el volumen raíz del WorkSpace está cifrado.

- RootVolumeSizeGib

  Tipo: entero

  Descripción: (obligatorio) El tamaño del volumen raíz del WorkSpace.

- RunningMode

  Tipo: cadena

  Valores válidos: ALWAYS_ON | AUTO_STOP

  Descripción: (Obligatorio) El modo de ejecución del WorkSpace.

- RunningModeAutoStopTimeoutInMinutos

  Tipo: entero

  Descripción: (opcional) El tiempo transcurrido desde que un usuario cierra sesión y se WorkSpaces detiene. Especifique un valor en intervalos de 60 minutos.

- Etiquetas

  Tipo: cadena

  Descripción: (opcional) Etiquetas que desea aplicar a WorkSpace.

- UserName

  Tipo: cadena

  Descripción: (obligatorio) El nombre de usuario que se va a asociar a WorkSpace.

- UserVolumeEncryptionEnabled

  Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) Determina si el volumen de usuarios del WorkSpace está cifrado.

- UserVolumeSizeGib

  Tipo: entero

  Descripción: (obligatorio) El tamaño del volumen de usuarios del WorkSpace.

- VolumeEncryptionClave

  Tipo: cadena

  Descripción: (opcional) La AWS Key Management Service clave simétrica que desea utilizar para cifrar los datos almacenados en su. WorkSpace

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Pasos de documentos

- `aws:executeScript`- Crea una WorkSpace basada en los valores que especifique para los parámetros de entrada.
- `aws:waitForAwsResourceProperty`- Verifica el estado del WorkSpace es`AVAILABLE`.

Salidas

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

Descripción

El `AWSSupport-RecoverWorkSpace` runbook lleva a cabo los pasos de recuperación en el escritorio WorkSpaces virtual de Amazon, conocido como a WorkSpace, que usted especifique. El runbook lo reinicia y WorkSpace, si el estado se mantiene`UNHEALTHY`, lo restaura o reconstruye en WorkSpace función de los valores que especifique para los parámetros de entrada. Antes de utilizar este manual, te recomendamos que consultes la sección Solución de WorkSpaces problemas en la Guía de WorkSpaces administración de Amazon.

> **Important**
>
> Restaurar o reconstruir un WorkSpace es una acción potencialmente destructiva que puede provocar la pérdida de datos. Esto se debe a que WorkSpace se restaura a partir de la última instantánea disponible y los datos recuperados de las instantáneas pueden tener una antigüedad de hasta 12 horas.
>
> La opción de restauración recrea tanto el volumen raíz como el volumen de usuarios en función de las instantáneas más recientes. La opción de reconstrucción recrea el volumen de usuario a partir de la instantánea más reciente y recrea el volumen de usuario a WorkSpace partir de la imagen asociada al paquete desde el que WorkSpace se creó. Se pierden las aplicaciones que se instalaron o la configuración del sistema que se modificó después de WorkSpace su creación. Para obtener más información sobre la restauración y la reconstrucción WorkSpaces, consulte Restore a WorkSpace and Rebuild a WorkSpace en la Amazon WorkSpaces Administration Guide.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Acknowledge

  Tipo: cadena

  Valores válidos: Yes

  Descripción: (Obligatorio) Si introduce sí, entiende que las acciones de restauración y reconstrucción intentarán recuperar la WorkSpace instantánea más reciente y que los datos restaurados a partir de estas instantáneas pueden tener una antigüedad de hasta 12 horas.

- Reboot

  Tipo: cadena

  Valores válidos: Yes | No

  Valor predeterminado: Yes

  Descripción: (Obligatorio) Determina si WorkSpace se reinicia.

- Reconstruir

  Tipo: cadena

  Valores válidos: Yes | No

  Valor predeterminado: No

  Descripción: (Obligatoria) Determina si WorkSpace se reconstruye.

- Restaurar

  Tipo: cadena

  Valores válidos: Yes | No

  Valor predeterminado: No

Descripción: (Obligatoria) Determina si WorkSpace se restaura.

- WorkspaceId

  Tipo: cadena

  Descripción: (obligatorio) El identificador del WorkSpace objeto que desea recuperar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Pasos de documentos

- `aws:executeAwsApi`- Recopila el estado del WorkSpace que especifique en el `WorkspaceId` parámetro.
- `aws:assertAwsResourceProperty`- Verifica el estado de WorkSpace is`AVAILABLE`,, `ERROR` `IMPAIREDSTOPPED`, o. `UNHEALTHY`
- `aws:branch`- Sucursales en función del estado del WorkSpace.
- `aws:executeAwsApi`- Inicia el WorkSpace.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Action`.
- `aws:waitForAwsResourceProperty`- Espera el WorkSpace estado una vez iniciado.
- `aws:waitForAwsResourceProperty`- Espera a que el WorkSpace estado cambie a`AVAILABLE`, `ERRORIMPAIRED`, o `UNHEALTHY` después de su inicio.

- `aws:executeAwsApi`- Recopila el estado de una WorkSpace vez iniciado.
- `aws:branch`- Las ramas se basan en el estado en el que se encuentran WorkSpace después de su puesta en marcha.
- `aws:executeAwsApi`- Reúne las instantáneas disponibles para restaurarlas o reconstruirlas. WorkSpace
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Reboot`.
- `aws:executeAwsApi`- Reinicia el. WorkSpace
- `aws:executeAwsApi`- Recopila el estado de una WorkSpace vez iniciado.
- `aws:waitForAwsResourceProperty`- Espera a que cambie el WorkSpace estado de. `REBOOTING`
- `aws:waitForAwsResourceProperty`- Espera a que el WorkSpace estado cambie a `AVAILABLE` o `UNHEALTHY` después `ERROR` de reiniciarse.
- `aws:executeAwsApi`- Recopila el estado de después de reiniciarse. WorkSpace
- `aws:branch`- Las ramas se basan en el estado en el que se encuentren tras el reinicio WorkSpace .
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Restore`.
- `aws:executeAwsApi`- Restaura el. WorkSpace Si se produce un error en la restauración, el runbook intentará reconstruirlo. WorkSpace
- `aws:waitForAwsResourceProperty`- Espera a que cambie el WorkSpace estado de. `RESTORING`
- `aws:waitForAwsResourceProperty`- Espera a que el WorkSpace estado cambie a `AVAILABLEERROR`, o `UNHEALTHY` después de ser restaurado.
- `aws:executeAwsApi`- Recopila el estado del WorkSpace tras su restauración.
- `aws:branch`- Las ramas se basan en el estado de la restauración WorkSpace posterior.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Rebuild`.
- `aws:executeAwsApi`- Reconstruye el WorkSpace.
- `aws:waitForAwsResourceProperty`- Espera a que cambie el WorkSpace estado de. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Espera a que el WorkSpace estado cambie a o `UNHEALTHY` después `AVAILABLE` de `ERROR` ser reconstruido.
- `aws:executeAwsApi`- Recopila el estado del WorkSpace tras su reconstrucción.

- `aws:assertAwsResourceProperty`- Confirma el estado del sistema WorkSpace . `AVAILABLE`

X-Ray

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS X-Ray Para obtener información acerca de los manuales de procedimientos, consulte Trabajar con manuales de procedimientos. Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte Cómo ver contenido del manual de procedimientos.

Temas

- AWSConfigRemediation-UpdateXRayKMSKey

`AWSConfigRemediation-UpdateXRayKMSKey`

Descripción

El `AWSConfigRemediation-UpdateXRayKMSKey` manual permite el cifrado de sus AWS X-Ray datos mediante una clave AWS Key Management Service (AWS KMS). Este manual solo debe usarse como referencia para garantizar que sus AWS X-Ray datos estén cifrados de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varios conjuntos de datos con diferentes claves de KMS.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeFunción

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KeyId

  Tipo: cadena

  Descripción: (obligatorio) El nombre del recurso de Amazon (ARN), el ID de clave o el alias de clave de la clave de KMS que desea utilizar AWS X-Ray para cifrar los datos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Pasos de documentos

- `aws:executeAwsApi`: permite el cifrado de sus datos X-Ray mediante la clave de KMS que especifique en el parámetro `KeyId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado de la configuración de cifrado de su X-Ray sea `ACTIVE`.
- `aws:executeAwsApi`: recopila el ARN de la clave que especifique en el parámetro `KeyId`.
- `aws:assertAwsResourceProperty`: verifica que el cifrado esté habilitado en su X-Ray.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.