
Amazon CloudWatch Events

Guía del usuario



Amazon CloudWatch Events: Guía del usuario

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon CloudWatch Events?	1
Concepts	1
Servicios de AWS relacionados	2
Configuración	4
Inscribirse en Amazon Web Services (AWS)	4
Inicie sesión en la consola de Amazon CloudWatch	4
Credenciales de la cuenta	4
Configurar la interfaz de línea de comandos	5
Puntos de enlace regionales	5
Introducción	6
Creación de una regla de que se dispara en función de un evento	7
Creación de una regla de que se dispare en función de unaAWSAPI llamada a través de CloudTrail	8
Creación de una regla de que se dispara en función de una programación	9
Eliminación o desactivación de una regla de	10
Tutoriales	11
Tutorial: Retransmitir eventos a Systems Manager Run Command	11
Tutorial: Registrar estados de instancia EC2	13
Paso 1: Creación de unAWS LambdaFunción	13
Paso 2: Crear una regla	14
Paso 3: Comprobación de la regla de	15
Tutorial: Estados del grupo de Auto Scaling	16
Paso 1: Creación de unAWS LambdaFunción	16
Paso 2: Crear una regla	17
Paso 3: Comprobación de la regla de	17
Tutorial: Registro de operaciones de nivel de objeto de S3	18
Paso 1: Configurar elAWS CloudTrailRegistro de seguimiento de	18
Paso 2: Creación de unAWS LambdaFunción	19
Paso 3: Crear una regla	20
Paso 4: Comprobación de la regla de	20
Tutorial: Utilizar el transformador de entrada para personalizar qué se transfiere al destino de eventos	20
Crear una regla	21
Tutorial: RegistroAWSAPI Calls (Llamadas a la API)	22
Prerequisite	22
Paso 1: Creación de unAWS LambdaFunción	22
Paso 2: Crear una regla	23
Paso 3: Comprobación de la regla de	23
Tutorial: Programar instantáneas de EBS automatizadas	24
Paso 1: Crear una regla	24
Paso 2: Comprobación de la regla de	25
Tutorial: Programar funciones de Lambda	25
Paso 1: Creación de unAWS LambdaFunción	26
Paso 2: Crear una regla	26
Paso 3: Comprobación de la regla	28
Tutorial: Configuración de Systems Manager Automation como un objetivo de	28
Tutorial: Retransmitir eventos a un flujo de Kinesis	29
Prerequisite	29
Paso 1: Crear una transmisión de Amazon Kinesis	29
Paso 2: Crear una regla	30
Paso 3: Comprobación de la regla de	30
Paso 4: Comprobación de que el evento se ha retransmitido	30
Tutorial: Ejecutar una tarea de Amazon ECS cuando se carga un archivo a un bucket de Amazon S3	31
Tutorial: Programar compilaciones automatizadas con CodeBuild	32
Tutorial: Cambios de estado de registro de instancias de Amazon EC2	33
Programar expresiones para reglas	35

Expresiones Cron	35
Expresiones de frecuencia	38
Patrones de eventos	39
Patrones de eventos	40
Coincidencia de valores nulos y cadenas vacías en patrones de eventos	41
Matrices en patrones de eventos	42
Eventos de servicios admitidos	44
Eventos de inteligencia artificial aumentada de Amazon	45
Eventos Application Auto Scaling	45
AWS Batch Events	45
Eventos programados de Amazon CloudWatch Events	45
Eventos de Amazon Chime	46
Eventos de CloudWatch	46
Eventos de CodeBuild	46
Eventos de CodeCommit	46
AWS CodeDeploy Events	46
Eventos de CodePipeline	47
AWS Config Events	48
Eventos de Amazon EBS	49
Eventos de Auto Scaling de Amazon EC2	49
Eventos de recomendación de reequilibrio de instancias de Amazon EC2	49
Eventos de interrupción de instancias de spot de Amazon EC2	49
Eventos de cambio de estado de Amazon EC2	49
Eventos de Amazon ECR	50
Eventos de Amazon ECS	50
Eventos de AWS Elemental MediaConvert	50
Eventos de AWS Elemental MediaPackage	50
Eventos de AWS Elemental MediaStore	50
Eventos de Amazon EMR	50
Evento de Amazon GameLift	52
AWS Glue Events	59
AWS Ground Station Events	64
Eventos de Amazon GuardDuty	64
AWS Health Events	64
AWS KMS Events	66
Eventos de Amazon Macie	67
Eventos de Amazon Macie	72
Eventos de inicio de sesión de AWS Management Console	72
Eventos de AWS OpsWorks Stacks	72
Eventos de SageMaker	75
AWS Security Hub Events	75
AWS Server Migration Service Events	75
AWS Systems Manager Events	76
AWS Systems ManagerEventos de Automatización	76
AWS Systems ManagerEventos de cambio	77
AWS Systems ManagerEventos de conformidad	78
Eventos de períodos de mantenimiento de AWS Systems Manager	80
Eventos de Parameter Store de AWS Systems Manager	82
AWS Systems ManagerEventos de comando	83
AWS Systems ManagerEventos de State Manager	84
AWS Step Functions Events	85
Eventos de cambio de etiquetasAWSRecursos	85
AWS Trusted Advisor Events	85
Eventos de WorkSpaces	87
Eventos enviados a través de CloudTrail	87
Envío y recepción de eventos entre cuentas de AWS	89
Activación de su cuenta de AWS para recibir eventos de otras cuentas de AWS	90

Envío de eventos a otra cuenta de AWS	91
Escritura de reglas que coincidan con eventos de otra cuenta de AWS	93
Migrar una relación remitente-receptor para usar AWS Organizations	94
Agregar eventos con PutEvents	96
Gestión de errores al utilizar PutEvents	96
Envío de eventos con AWS CLI	98
Cálculo de tamaños de entrada de evento PutEvents	98
Uso de CloudWatch Events con los puntos de enlace de la VPC	100
Availability	100
Creación de un punto de enlace de la VPC para eventos de CloudWatch	101
Control del acceso al punto de enlace de la VPC de CloudWatch Events	101
Monitorización del uso con métricas de CloudWatch	103
Métricas de CloudWatch Events	103
Dimensiones de las métricas de eventos de CloudWatch	103
Reglas administradas	105
Seguridad	106
Etiquetado de sus recursos de eventos de CloudWatch	107
Recursos admitidos en eventos de CloudWatch	107
Administración de etiquetas	107
Convenciones de nomenclatura y uso de las etiquetas	108
Registro de llamadas a API	109
Información de eventos de CloudWatch en CloudTrail	109
Ejemplo: Entradas de archivos de registro de CloudWatch	110
Service Quotas	112
Solución de problemas	113
Mi regla se ha activado pero no se ha invocado mi función de Lambda	113
Acabo de crear o modificar una regla, pero no coincidía con un evento de prueba	114
Mi regla no se activa automáticamente en el momento especificado en ScheduleExpression	115
Mi regla no se activó a la hora esperada	115
Mi regla coincide con las llamadas al API de IAM pero no se ha activado	115
Mi regla no funciona, ya que el rol de IAM asociado a la regla no se tiene en cuenta cuando se activa la regla	116
He creado una regla con un EventPattern que se supone que coincide con un recurso, pero no veo ningún evento que coincida con la regla	116
La entrega de mi evento al destino ha sufrido un retraso	116
Algunos eventos no se entregaron en mi destino	116
Mi regla se activó más de una vez en respuesta a un único evento. ¿Qué garantía ofrece CloudWatch Events para activar reglas o enviar eventos a los destinos?	117
Cómo evitar bucles infinitos	117
Mis eventos no se entregan en la cola de de Amazon SQS de destino	117
Mi regla se activa pero no veo ningún mensaje publicado en mi tema de Amazon SNS	118
Mi tema de Amazon SNS sigue teniendo permisos para eventos de CloudWatch incluso después de haber eliminado la regla asociada al tema de Amazon SNS	119
Qué claves de condición de IAM puedo utilizar con CloudWatch Events	119
Cómo puedo saber si las reglas de CloudWatch Events están rotas	119
Historial de revisión	121
AWSGlosario	124
.....	cxxv

¿Qué es Amazon CloudWatch Events?

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge proporciona más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Amazon CloudWatch Events proporciona una secuencia de eventos de sistema casi en tiempo real que describen cambios en Amazon Web Services (AWS). Mediante reglas sencillas que puede configurar rápidamente, puede asignar los eventos y dirigirlos a uno o más flujos o funciones de destino. CloudWatch Events conoce los cambios operativos a medida que se producen. CloudWatch Events responde a estos cambios operativos y toma medidas correctoras según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado.

También puede utilizar CloudWatch Events para programar acciones automatizadas que se activen automáticamente en determinados momentos a través de expresiones cron o rate. Para obtener más información, consulte [Programar expresiones para reglas \(p. 35\)](#).

Puede configurar la siguiente opción: AWS como destinos para CloudWatch Events:

- Instancias Amazon EC2
- Funciones de AWS Lambda
- Transmisiones de datos Amazon Kinesis Data Streams
- Transmisiones de entrega en Amazon Kinesis Data Firehose
- Registrar grupos en Amazon CloudWatch Logs
- Tareas de Amazon ECS
- Command Ejecutar Systems Manager
- Automatización de Systems Manager
- Trabajos de AWS Batch
- Máquinas de estado Step Functions
- Pipeline en CodePipeline
- Proyectos de CodeBuild
- Plantillas de evaluación de Amazon
- Temas de Amazon SNS
- Colas de Amazon SQS
- Destinos integrados: EC2 `CreateSnapshot` API call, EC2 `RebootInstances` API call, EC2 `StopInstances` API call y EC2 `TerminateInstances` API call.
- El bus de eventos predeterminado de otra cuenta de AWS

Concepts

Antes de comenzar a utilizar CloudWatch Events, debe comprender los siguientes conceptos:

- **Eventos**— Un evento indica un cambio en el entorno de AWS. Los recursos de AWS pueden generar eventos cuando cambia su estado. Por ejemplo, Amazon EC2 genera un evento cuando el estado de una instancia EC2 cambia de pendiente a en ejecución y Amazon EC2 Auto Scaling genera eventos cuando lanza o termina instancias. AWS CloudTrail publica eventos cuando realiza llamadas al API. Puede generar eventos personalizados en el nivel de aplicación y publicarlos en CloudWatch Events. También puede configurar eventos programados que se generan de forma periódica. Para obtener una lista de servicios que generan eventos y eventos de ejemplo de cada servicio, consulte [Ejemplos de eventos de CloudWatch Events de servicios admitidos](#) (p. 44).
- **Reglas**: una regla hace coincidir eventos de entrada y los dirige a destinos para procesamiento. Una regla única puede dirigir a varios destinos, todos los cuales se procesan en paralelo. Las reglas no se procesan en un orden concreto. Esto permite a las distintas partes de una organización buscar y procesar los eventos que les interesan. Una regla puede personalizar el JSON enviado al destino, transmitiendo solo algunas partes o sobrescribiéndolo con una constante.
- **implementación**— Un destino procesa eventos. Los destinos pueden incluir instancias Amazon EC2, AWS Lambda, Amazon ElastiCache, tareas de Amazon ECS, máquinas de estado de Step Functions, temas de Amazon SNS, colas de Amazon SQS y destinos integrados. Un destino recibe eventos en formato JSON.

Los destinos de una regla deben estar en la misma región que la regla.

Servicios de AWS relacionados

Los siguientes servicios se utilizan conjuntamente con CloudWatch Events:

- **AWS CloudTrail** permite monitorizar las llamadas a la API CloudWatch Events para su cuenta, incluidas las llamadas realizadas por la AWS Management Console, el AWS CLI y otros servicios. Cuando el registro de CloudTrail está activado, CloudWatch Events escribe archivos de registro en un bucket de S3. Cada archivo de registro contiene uno o varios registros, en función de la cantidad de acciones que se realizan para satisfacer una solicitud. Para obtener más información, consulte [Registro de llamadas al API de Amazon CloudWatch Events con AWS CloudTrail](#) (p. 109).
- **AWS CloudFormation** le permite modelar y configurar sus recursos de AWS. Puede crear una plantilla que describa los recursos de AWS que desea y AWS CloudFormation se encargará del aprovisionamiento y la configuración de dichos recursos. Puede usar las reglas CloudWatch Events en sus AWS CloudFormation Plantillas. Para obtener más información, consulte [AWS Events# Rule](#) en la AWS CloudFormation Guía del usuario de .
- **AWS Config** le permite registrar los cambios de configuración de los recursos de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se configuraron en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo. También puede crear reglas de AWS Config para comprobar si los recursos son conformes o no de acuerdo con las políticas de su organización. Para obtener más información, consulte [AWS Config Developer Guide](#).
- **AWS Identity and Access Management (IAM)** le ayuda a controlar de forma segura el acceso a los recursos de AWS para sus usuarios. Utilice IAM para controlar quién puede usar su AWS (autenticación), los recursos que pueden usar y cómo pueden usarlos (autorización). Para obtener más información.
- **Amazon Kinesis Data Streams** permite introducir y agregar datos de forma rápida y casi continuada. El tipo de datos utilizado incluye los datos de registros de infraestructura de TI, registros de aplicaciones, redes sociales, fuentes de datos de mercado y datos de secuencias de clics en sitios web. Dado el tiempo de respuesta necesario para la entrada y el procesamiento de datos se realiza en tiempo real, el procesamiento suele ser ligero. Para obtener más información, consulte la [Guía para desarrolladores de Amazon Kinesis Data Streams](#).
- **AWS Lambda** le permite crear aplicaciones que responden rápidamente a nueva información. Cargar el código de aplicación como funciones de Lambda y Lambda ejecuta el código en una infraestructura informática de alta disponibilidad. Lambda ejecuta la administración integral de los recursos informáticos, incluido el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad, el

escalado automático, la implementación de parches de seguridad y la monitorización de código y el registro. Para obtener más información, consulte [AWS Lambda Developer Guide](#).

Configuración de Amazon CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Para utilizar los Amazon CloudWatch Events, necesita un AWS account. Su AWS cuenta de, le permite utilizar servicios (por ejemplo, Amazon EC2) para generar eventos que se pueden visualizar en la consola de CloudWatch, una interfaz basada en web. Además, puede instalar y configurar la AWS Command Line Interface (AWS CLI) para utilizar una interfaz de línea de comandos.

Inscribirse en Amazon Web Services (AWS)

Al crear un AWS Inscríbimos automáticamente en todos los AWS Servicios de . Solo pagará por los servicios que utilice.

Si tiene un AWS Ya, vaya directamente al siguiente paso. Si no dispone de una cuenta de AWS, utilice el siguiente procedimiento para crear una.

Para inscribirse en una cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones en línea.

Parte del procedimiento de inscripción consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Inicie sesión en la consola de Amazon CloudWatch

Inicie sesión en la consola de Amazon CloudWatch

1. Inicie sesión en AWS Management Console y abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. Si es necesario, cambie la región. En la barra de navegación, seleccione la región donde tiene su AWS de AWS.
3. En el panel de navegación, seleccione Events.

Credenciales de la cuenta

Aunque puede utilizar las credenciales del usuario raíz para obtener acceso a CloudWatch Events, le recomendamos que utilice un AWS Identity and Access Management (IAM). Si está utilizando una cuenta de IAM para obtener acceso a CloudWatch, debe contar con los siguientes permisos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "events:*",
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Configurar la interfaz de línea de comandos

Puede utilizar la AWS CLI para realizar operaciones de CloudWatch Events.

Para obtener información acerca de cómo instalar y configurar la AWS CLI, consulte [Configuración inicial de la AWS Command Line Interface](#) en la [AWS Command Line Interface Guía del usuario](#).

Puntos de enlace regionales

Debe habilitar los puntos de enlace regionales (el valor predeterminado) para utilizar CloudWatch Events. Para obtener más información, consulte [Activación y desactivación de AWS STS en una región](#) en la [Guía del usuario de IAM](#).

Introducción a Amazon CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Siga los procedimientos de esta sección para crear y eliminar reglas de CloudWatch Events. Estos son los procedimientos generales que pueden utilizarse con cualquier origen o destino de eventos. Si desea consultar tutoriales sobre casos y destinos específicos, visite [Tutoriales](#).

Cada regla

Contenido

- [Creación de una regla de CloudWatch Events que se activa en función de un evento \(p. 7\)](#)
- [Creación de una regla de CloudWatch Events que se activa en función de unaAWSAPI Llamada a la APIAWS CloudTrail \(p. 8\)](#)
- [Creación de una regla de CloudWatch Events que se activa en función de una programación \(p. 9\)](#)
- [Eliminación o desactivación de una regla de CloudWatch Events \(p. 10\)](#)

Restrictions

- Los destinos que asocia a una regla deben estar en la misma región que la regla.
- Algunos tipos de destinos podrían no estar disponibles en todas las regiones. Para obtener más información, consulte [Regiones y puntos de enlace](#) en la Referencia general de Amazon Web Services.
- Creación de reglas con objetivos integrados solo compatibles en la AWS Management Console.
- Si crea una regla con una cola de Amazon SQS cifrada como destino, debe tener incluida la siguiente sección en su política de claves de KMS. Permite que el evento se entregue correctamente a la cola cifrada.

```
{
    "Sid": "Allow CWE to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "events.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

Creación de una regla de CloudWatch Events que se activa en función de un evento

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Siga los pasos que se describen a continuación para crear una regla de CloudWatch Events que se active en función de un evento emitido por una regla de AWS Servicio

Para crear una regla que se active en función de un evento:

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Elija Event Pattern, Build event pattern to match events by service.
 - b. En Service Name, seleccione el servicio que emite el evento para activar la regla.
 - c. En Event Type, seleccione el evento concreto que va a activar la regla. Si la única opción es AWSAPI llamada a través de CloudTrail, el servicio seleccionado no emite eventos y solo puede basar reglas en las llamadas a la API realizadas a este servicio. Para obtener más información acerca de cómo crear este tipo de regla, consulte [Creación de una regla de CloudWatch Events que se activa en función de una AWSAPI Llamada a la API AWS CloudTrail](#) (p. 8).
 - d. En función del servicio que emite el evento, aparecerán opciones para Any... y Specific.... Seleccione Any... para que el disparador esté en cualquier tipo de evento seleccionado o Specific... para elegir uno o varios tipos de evento específicos.
4. En Targets (Destinos), seleccione Add Target (Agregar destino) y elija el servicio de AWS que va a actuar cuando se detecte un evento del tipo seleccionado.
5. En el resto de los campos de esta sección, especifique los datos concretos de este tipo de destino, si es necesario.
6. Si hay muchos tipos de destino, Eventos de CloudWatch necesita permisos para enviar eventos al destino. En estos casos, Eventos de CloudWatch puede crear el rol de IAM necesario para que se ejecute el evento:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
7. Si lo desea, puede repetir los pasos 4 a 6 para agregar otro destino en esta regla.
8. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.

El nombre de la regla debe ser exclusivo dentro de esta región.
9. Elija Create rule.

Creación de una regla de CloudWatch Events que se activa en función de unaAWSAPI Llamada a la APIAWS CloudTrail

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Para crear una regla que se active en función de una acción a través de un servicio de AWS que no emite eventos, puede basar la reglas en llamadas a la API realizadas por dicho servicio. Las llamadas a la API las registra AWS CloudTrail. Para obtener más información sobre las llamadas a la API que puede utilizar como disparadores de reglas, consulte [Servicios compatibles con el historial de eventos de CloudTrail](#).

Las reglas de CloudWatch Events funcionan únicamente en la región en que se han creado. Si configura CloudTrail para realizar un seguimiento de las llamadas a la API en varias regiones, y desea que una regla basada en CloudTrail se active en cada una de esas regiones, debe crear una regla independiente en cada región en la que desea realizar un seguimiento.

Todos los eventos que se entregan a través de CloudTrail tienenAWS API Call via CloudTrailComo el valor de detail-type.

Note

En CloudWatch Events es posible crear reglas que producen bucles infinitos, en los que una regla se activa repetidamente. Por ejemplo, una regla puede detectar que las ACL han cambiado en un bucket de S3 y activar software para cambiarlas al estado deseado. Si la regla no se ha escrito minuciosamente, un nuevo cambio de las ACL vuelve a activar la regla, lo que crea un bucle infinito.

Para evitarlo, escriba las reglas de modo que las acciones ya desencadenadas no vuelvan a activar una misma regla. Por ejemplo, la regla puede activarse solo si las ACL tienen un estado incorrecto, en lugar de después de cualquier cambio.

Un bucle infinito puede generar cargos superiores a los esperados rápidamente. Le recomendamos que utilice la función de presupuestos, que le avisa cuando los cargos superan el límite especificado. Para obtener más información, consulte [Gestión de costos con presupuestos](#).

Para crear una regla de que se dispare en función de una llamada a la API a través de CloudTrail:

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Elija Event Pattern, Build event pattern to match events by service.
 - b. En Service Name, seleccione el servicio que utiliza las operaciones API que van a actuar como disparador.
 - c. Para Tipo de evento, elijaAWSAPI llamada a través de CloudTrail.
 - d. Para activar la regla cuando se invoque la operación API de este servicio, seleccione Any operation. Para activar la regla únicamente cuando se invoquen ciertas operaciones API, seleccione Specific operation(s), escriba el nombre de una operación en el cuadro siguiente y, a continuación, presione INTRO. Para agregar más operaciones, seleccione +.

4. En Targets (Destinos), seleccione Add Target (Agregar destino) y elija el servicio de AWS que va a actuar cuando se detecte un evento del tipo seleccionado.
5. En el resto de los campos de esta sección, especifique los datos concretos de este tipo de destino, si es necesario.
6. Si hay muchos tipos de destino, Eventos de CloudWatch necesita permisos para enviar eventos al destino. En estos casos, Eventos de CloudWatch puede crear el rol de IAM necesario para que se ejecute el evento:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
7. Si lo desea, puede repetir los pasos 4 a 6 para agregar otro destino en esta regla.
8. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.
El nombre de la regla debe ser exclusivo dentro de esta región.
9. Elija Create rule.

Creación de una regla de CloudWatch Events que se activa en función de una programación

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Siga los pasos que se describen a continuación para crear una regla de CloudWatch Events que se active en función de una programación periódica:

Para crear una regla que se active en función de una programación periódica

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, seleccione Schedule.
4. Seleccione Fixed rate of y especifique la frecuencia con la que se va a ejecutar la tarea o seleccione Cron expression y especifique una expresión Cron que determine cuándo debe activarse la tarea. Para obtener más información acerca de la sintaxis de la expresión Cron, consulte [Programar expresiones para reglas \(p. 35\)](#).
5. En Targets (Destinos), seleccione Add Target (Agregar destino) y elija el servicio de AWS que va a actuar cuando se detecte un evento del tipo seleccionado.
6. En el resto de los campos de esta sección, especifique los datos concretos de este tipo de destino, si es necesario.
7. Si hay muchos tipos de destino, Eventos de CloudWatch necesita permisos para enviar eventos al destino. En estos casos, Eventos de CloudWatch puede crear el rol de IAM necesario para que se ejecute el evento:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).

- Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
8. Si lo desea, puede repetir los pasos 5 a 7 para agregar otro destino en esta regla.
 9. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.

El nombre de la regla debe ser exclusivo dentro de esta región.
 10. Elija Create rule.

Eliminación o desactivación de una regla de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Siga los pasos que se describen a continuación para eliminar o deshabilitar una regla de CloudWatch Events.

Para eliminar o desactivar una regla

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Rules (Reglas).

Las reglas administradas tienen un icono de cubo junto a sus nombres. Para obtener más información, consulte [Reglas administradas por Amazon CloudWatch Events \(p. 105\)](#).

3. Aplique alguna de las siguientes acciones:
 - a. Para eliminar una regla, seleccione el botón que aparece junto a la regla y elija Actions, Delete, Delete.

Si la regla es una regla administrada, debe escribir el nombre de la regla para confirmar que se trata de una regla administrada y que la eliminación puede detener la funcionalidad en el servicio que ha creado la regla. Para continuar, escriba el nombre de la regla y elija Force delete (Forzar eliminación).
 - b. Para desactivar temporalmente una regla, seleccione el botón que aparece junto a la regla y elija Actions, Disable, Disable.

No puede habilitar una regla administrada.

Tutoriales de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

En los siguientes tutoriales, se explica cómo crear reglas de CloudWatch Events para determinadas tareas y objetivos.

Tutoriales:

- [Tutorial: Utilice eventos de CloudWatch para retransmitir eventos aAWS Systems ManagerRun Command \(p. 11\)](#)
- [Tutorial: Registrar el estado de una instancia Amazon EC2 con eventos de CloudWatch Events \(p. 13\)](#)
- [Tutorial: Registrar el estado de un grupo de Auto Scaling con Eventos de CloudWatch Events \(p. 16\)](#)
- [Tutorial: Registro de operaciones de nivel de objetos de Amazon S3 con eventos de CloudWatch Events \(p. 18\)](#)
- [Tutorial: Utilizar el transformador de entrada para personalizar qué se transfiere al destino de eventos \(p. 20\)](#)
- [Tutorial: RegistroAWSLlamadas a API mediante eventos de CloudWatch \(p. 22\)](#)
- [Tutorial: Programar instantáneas automatizadas de Amazon EBS mediante eventos de CloudWatch \(p. 24\)](#)
- [Tutorial: ScheduleAWS LambdaFunciones con eventos de CloudWatch \(p. 25\)](#)
- [Tutorial: EstablezcaAWS Systems ManagerObtención de eventos de CloudWatch Events \(p. 28\)](#)
- [Tutorial: Retransmitir eventos a un flujo de Amazon Kinesis con eventos de CloudWatch Events \(p. 29\)](#)
- [Tutorial: Ejecutar una tarea de Amazon ECS cuando se carga un archivo a un bucket de Amazon S3 \(p. 31\)](#)
- [Tutorial: Programar compilaciones automatizadas con CodeBuild \(p. 32\)](#)
- [Tutorial: Cambios de estado de registro de instancias de Amazon EC2 \(p. 33\)](#)

Tutorial: Utilice eventos de CloudWatch para retransmitir eventos aAWS Systems ManagerRun Command

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede utilizar eventos de Amazon CloudWatch Events para invocarAWS Systems ManagerEjecutar Command y realizar acciones en instancias de Amazon EC2 cuando se producen determinados eventos. En este tutorial, configure Ejecutar comando para ejecutar comandos de shell y configurar cada nueva instancia que se lance en un grupo de Amazon EC2 Auto Scaling. En este tutorial se supone que ya ha asignado una etiqueta al grupo de Amazon EC2 Auto Scaling, con `environment` como la clave y `production` como el valor.

Para crear la regla Eventos de CloudWatch

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Elija Event Pattern, Build event pattern to match events by service.
 - b. En Service Name, elija Auto Scaling. En Event Type, seleccione Instance Launch and Terminate.
 - c. Elija Specific instance event(s), EC2 Instance-launch Lifecycle Action.
 - d. De forma predeterminada, la regla coincide con cualquier grupo de Amazon EC2 Auto Scaling de la región. Para que la regla coincida con un grupo específico, elija Specific group name(s) y, a continuación, seleccione uno o varios grupos.

The screenshot shows the 'Event Source' configuration interface in the AWS console. It includes a title 'Event Source' and a subtitle 'Build or customize an Event Pattern or set a Schedule to invoke Targets.' There are two radio buttons: 'Event Pattern' (selected) and 'Schedule'. Below this is a dropdown menu for 'Build event pattern to match events by service'. The configuration fields are: 'Service Name' (Auto Scaling), 'Event Type' (Instance Launch and Terminate), 'Any instance event' (unselected) and 'Specific instance event(s)' (selected) with a dropdown showing 'EC2 Instance-launch Lifecycle Action', and 'Any group name' (selected) and 'Specific group name(s)' (unselected) with an empty dropdown.

4. En Targets, elija Add Target, SSM Run Command.
5. Para Documento, elija AWS-RunShellScript (Linux). Hay muchas otras opciones de Documento (Documento) que cubren tanto las instancias de Linux como de Windows. En Target key (Clave de destino), escriba `tag:environment`. En Target value(s) (Valores de destino), escriba `production` y seleccione Add (Agregar).
6. En Configure parameter(s), elija Constant.
7. En Commands, escriba un comando de shell y elija Add. Repita este paso para todos los comandos que ejecutar cuando se lanza una instancia.
8. Si es necesario, escriba la información pertinente en WorkingDirectory y ExecutionTimeout.
9. CloudWatch pueden crear el rol de IAM necesario para que se ejecute su evento:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).

The screenshot shows the 'Targets' configuration page in the AWS CloudWatch console. At the top, it says 'Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.' Below this, a dropdown menu is set to 'SSM Run Command'. The configuration fields are as follows:

- Document***: AWS-RunShellScript (Linux)
- Target key***: tag:environment
- Target value(s)***: production

Below these fields, there is a note: 'A Run Command Target provides a way to specify which EC2 Instances to invoke SSM Run Command on. [Learn more](#)'. Under the heading 'Configure parameter(s)', the 'Constant' radio button is selected. At the bottom, there are three empty dropdown menus for 'Commands', 'WorkingDirectory', and 'ExecutionTimeout'.

10. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.
11. Elija Create rule.

Tutorial: Registrar el estado de una instancia Amazon EC2 con eventos de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede crear unAWS LambdaFunción que registre los cambios de estado de una instancia Amazon EC2. Tiene la opción de crear una regla que ejecute la función cuando haya una transición de estado o una transición a uno o varios estados de interés. En este tutorial, puede registrar el lanzamiento de una nueva instancia.

Paso 1: Creación de unAWS LambdaFunción

Cree una función Lambda para registrar los eventos de cambio de estado. Especifique esta función cuando cree la regla.

Para crear una función de Lambda

1. Abra el iconoAWS Lambdaen<https://console.aws.amazon.com/lambda/>.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Get Started Now. De lo contrario, elija Create a Lambda function (Crear una función Lambda).

3. En la página Select blueprint (Seleccionar proyecto), escriba `hello` para el filtro y seleccione el proyecto `hello-world`.
4. En la página Configure triggers, elija Next.
5. En la página Configure function, haga lo siguiente:
 - a. Escriba un nombre y la descripción de Lambda function. Por ejemplo, nombre la función "LogEC2InstanceStateChange".
 - b. Edite el código de muestra de la función Lambda. Por ejemplo:

```
'use strict';

exports.handler = (event, context, callback) => {
  console.log('LogEC2InstanceStateChange');
  console.log('Received event:', JSON.stringify(event, null, 2));
  callback(null, 'Finished');
};
```

- c. En Role (Rol), elija Choose an existing role (Elegir un rol existente). En Existing role (Rol existente), seleccione su rol de ejecución básico. De lo contrario, cree un nuevo rol de ejecución básico.
 - d. Seleccione Next (Siguiente).
6. En la página Review, seleccione Create function.

Paso 2: Crear una regla

Cree una regla para ejecutar su función Lambda siempre que lance una instancia de Amazon EC2.

Para crear una regla de CloudWatch Events

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione EC2, elija EC2 Instance State-change Notification (Notificación de cambio de estado de instancia EC2).
 - d. Seleccione Specific state(s) (Estados específicos), Running (En ejecución).
 - e. De forma predeterminada, la regla coincide con cualquier instancia en la región. Para que la regla coincida con una instancia específica, seleccione Specific instance(s) (Instancias específicas) y, a continuación, seleccione una o varias instancias.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern Schedule

Build event pattern to match events by service

Service Name: EC2

Event Type: EC2 Instance State-change Notification

Any state Specific state(s)

running

Any instance Specific instance(s)

4. Para implementación, elija Agregar destino, Lambda función.
5. En Function (Función), seleccione la función Lambda que ha creado.
6. Seleccione Configure details.
7. En Rule definition, escriba un nombre y la descripción de la regla.
8. Elija Create rule.

Paso 3: Comprobación de la regla de

Para probar la regla, lance una instancia Amazon EC2. Después de esperar unos minutos a que la instancia se lance e inicialice, puede comprobar que la función de Lambda se ha invocado.

Para probar la regla lanzando una instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Lance una instancia. Para obtener más información, consulte [Lanzar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
4. En el panel de navegación, seleccione Events, Rules, el nombre de la regla que ha creado y Show metrics for the rule.
5. Para ver la salida de la función Lambda, haga lo siguiente:
 - a. En el panel de navegación, elija Logs.
 - b. Seleccione el nombre del grupo de registros de la función Lambda (/aws/lambda/-name).
 - c. Elija el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha lanzado.
6. (Opcional) Cuando haya terminado, puede abrir la consola de Amazon EC2 y detener o terminar la instancia que ha lanzado. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Tutorial: Registrar el estado de un grupo de Auto Scaling con Eventos de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede ejecutar un AWS Lambda Función que registre un evento siempre que un grupo de Auto Scaling lance o termine una instancia de Amazon EC2 y si el evento lanzar o terminar se ha realizado correctamente.

Para obtener información sobre escenarios adicionales de CloudWatch Events con eventos de Auto Scaling de Amazon EC2, consulte [Obtención de eventos de CloudWatch cuando su grupo Auto Scaling se escala](#) en la Guía del usuario de Auto Scaling de Amazon EC2.

Paso 1: Creación de un AWS Lambda Función

Cree una función Lambda para registrar los eventos de escalado ascendente y descendente para su grupo de Auto Scaling. Especifique esta función cuando cree la regla.

Para crear una función de Lambda

1. Abra el icono AWS Lambda en <https://console.aws.amazon.com/lambda/>.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Get Started Now. De lo contrario, elija Create a Lambda function (Crear una función Lambda).
3. En la página Select blueprint (Seleccionar proyecto), escriba hello para el filtro y seleccione el proyecto hello-world.
4. En la página Configure triggers, elija Next.
5. En la página Configure function, haga lo siguiente:
 - a. Escriba un nombre y la descripción de Lambda function. Por ejemplo, asigne a la función el nombre "LogAutoScalingEvent".
 - b. Edite el código de muestra de la función Lambda. Por ejemplo:

```
'use strict';

exports.handler = (event, context, callback) => {
  console.log('LogAutoScalingEvent');
  console.log('Received event:', JSON.stringify(event, null, 2));
  callback(null, 'Finished');
};
```

- c. En Role (Rol), elija Choose an existing role (Elegir un rol existente). En Existing role (Rol existente), seleccione su rol de ejecución básico. De lo contrario, cree un nuevo rol de ejecución básico.
 - d. Seleccione Next (Siguiente).
6. Elija Create function (Crear función).

Paso 2: Crear una regla

Cree una regla para ejecutar su función de Lambda siempre que su grupo de Auto Scaling lance o termine una instancia.

Para crear una regla de

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione Auto Scaling, Lanzamiento y terminación de instancias.
 - d. Para capturar todos los eventos de lanzamiento y terminación de instancia que se hayan realizado correctamente o que no lo hayan hecho, elija Any instance event (Cualquier evento de instancia).

The screenshot shows the 'Event Source' configuration interface in the AWS CloudWatch console. It is titled 'Event Source' and has a subtitle 'Build or customize an Event Pattern or set a Schedule to invoke Targets.' There are two radio buttons at the top: 'Event Pattern' (selected) and 'Schedule'. Below this is a dropdown menu labeled 'Build event pattern to match events by service'. Underneath, there are two dropdown menus: 'Service Name' (set to 'Auto Scaling') and 'Event Type' (set to 'Instance Launch and Terminate'). Below these are two sections, each with a radio button and a dropdown menu. The first section has 'Any instance event' selected and an empty dropdown. The second section has 'Any group name' selected and an empty dropdown.

4. De forma predeterminada, la regla coincide con cualquier grupo de Auto Scaling en la región. Para que la regla coincida con un grupo de Auto Scaling específico, elija Nombre de grupo específico Y, a continuación, seleccione uno o varios grupos de Auto Scaling.
5. Para implementación, elija Agregar destino, Lambda function.
6. En Function (Función), seleccione la función Lambda que ha creado.
7. Seleccione Configure details.
8. En Rule definition, escriba un nombre y la descripción de la regla. (Por ejemplo, describa la regla como «Registrar cada vez que un grupo Auto Scaling ascendente o descendente»).
9. Elija Create rule.

Paso 3: Comprobación de la regla de

Puede probar la regla manualmente escalando un grupo de Auto Scaling para que lance una instancia. Después de esperar unos minutos a que se produzca el evento de escalado horizontal, verifique que la función de Lambda se ha invocado.

Para probar la regla con un grupo de Auto Scaling

1. Para aumentar el tamaño del grupo de Auto Scaling (Auto Scaling), haga lo siguiente:
 - a. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
 - b. En el panel de navegación, seleccione Auto Scaling, Auto Scaling Groups.
 - c. Seleccione la casilla del grupo de Auto Scaling.
 - d. En la pestaña Details, seleccione Edit. En Desired, aumente la capacidad deseada en 1. Por ejemplo, si el valor actual es 2, escriba 3. La capacidad deseada debe ser menor o igual que el tamaño máximo del grupo. Si el nuevo valor de Desired es mayor que Max, debe actualizar Max. Cuando termine de actualizar las etiquetas, elija Save.
2. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
3. En el panel de navegación, seleccione Events, Rules, el nombre de la regla que ha creado y Show metrics for the rule.
4. Para ver la salida de la función Lambda, haga lo siguiente:
 - a. En el panel de navegación, elija Logs.
 - b. Seleccione el nombre del grupo de registros de la función Lambda (/aws/lambda/-name).
 - c. Seleccione el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha lanzado.
5. (Opcional) Cuando haya terminado, puede reducir la capacidad deseada en uno para que el grupo de Auto Scaling vuelva a su tamaño anterior.

Tutorial: Registro de operaciones de nivel de objetos de Amazon S3 con eventos de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede registrar las operaciones de API de nivel de objeto que tienen lugar en los buckets de S3. Antes de que Amazon CloudWatch Events pueda asignar estos eventos, debe utilizar AWS CloudTrail para configurar un registro de seguimiento configurado para recibir estos eventos.

Paso 1: Configurar el AWS CloudTrail Registro de seguimiento de

Para registrar eventos de datos para un bucket de S3 en AWS CloudTrail y CloudWatch Events, cree una pista. Un registro de seguimiento captura las llamadas a la API y los eventos relacionados de la cuenta y entrega los archivos de registro en un bucket de S3 especificado. Puede actualizar un registro de seguimiento existente o crear uno nuevo.

Para crear un registro de seguimiento

1. Abra la consola de CloudTrail en<https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, seleccione Trails (Registros de seguimiento), Create trail (Crear registro de seguimiento).
3. En Trail name, escriba un nombre para el registro de seguimiento.
4. En Data events, escriba el nombre del bucket y el prefijo (opcional). Puede añadir hasta 250 objetos de Amazon S3 a cada registro de seguimiento.
 - Para registrar eventos de datos de todos los objetos de Amazon S3 en un bucket, especifique un bucket de S3 y un prefijo vacío. Cuando un evento se produce en un objeto de dicho bucket de , el registro de seguimiento procesa y registra el evento.
 - Para registrar eventos de datos de objetos de Amazon S3 concretos, elijaAñadir bucket de S3Y, a continuación, especifique un bucket de S3 y, de forma opcional, el prefijo del objeto. Cuando un evento se produce en un objeto en dicho bucket de y el objeto comienza por el prefijo indicado, el registro de seguimiento procesa y registra el evento.
5. En cada recurso, especifique si desea registrar los eventos de tipo Read (Lectura), Write (Escritura) o ambos.
6. En Storage location, cree o seleccione un bucket de S3 existente para designarlo como almacenamiento del archivo de registro.
7. Seleccione Create.

Para obtener más información, consulte[Eventos de datos](#) en laAWS CloudTrailGuía del usuario de .

Paso 2: Creación de unAWS LambdaFunción

Cree una función Lambda para registrar eventos de datos para sus buckets de S3. Especifique esta función cuando cree la regla.

Para crear una función de Lambda

1. Abra el iconoAWS Lambdaen<https://console.aws.amazon.com/lambda/>.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Create a function (Crear una función). De lo contrario, seleccione Create function (Crear función).
3. Elija Author from scratch.
4. En Author from scratch (Crear desde cero), haga lo siguiente:
 - a. Escriba un nombre para la función de Lambda. Por ejemplo, nombre la función "LogS3DataEvents".
 - b. En Role, seleccione Create a custom role.

Se abrirá una nueva ventana. Cambie el Role name (Nombre del rol) si fuera necesario y elija Allow (Permitir).
 - c. En la consola de Lambda, elijaCreate function.
5. Edite el código de la función de Lambda según se indica a continuación y elija Save (Guardar).

```
'use strict';

exports.handler = (event, context, callback) => {
  console.log('LogS3DataEvents');
  console.log('Received event:', JSON.stringify(event, null, 2));
  callback(null, 'Finished');
};
```


Paso 3: Crear una regla

Cree una regla para ejecutar su función Lambda en respuesta a un evento de datos de Amazon S3.

Para crear una regla de

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Rules (Reglas), Create rule (Crear regla).
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione Simple Storage Service (S3), Object Level Operations (Operaciones de nivel de objeto).
 - d. Seleccione Specific operation(s) (Operaciones específicas), PutObject.
 - e. De forma predeterminada, la regla coincide con los eventos de datos de todos los buckets de la región. Para asignar eventos de datos a buckets específicos, elija Specify bucket(s) by name y, a continuación, especifique uno o varios buckets.
4. Para implementación, elija Agregar destino, Lambda function.
5. En Function (Función), seleccione la función Lambda que ha creado.
6. Seleccione Configure details.
7. En Rule definition, escriba un nombre y la descripción de la regla.
8. Elija Create rule.

Paso 4: Comprobación de la regla de

Para probar la regla, coloque un objeto en su bucket de S3. Puede verificar que su función Lambda fue invocada.

Para ver los registros para la función Lambda

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Logs.
3. Seleccione el nombre del grupo de registros de la función Lambda (/aws/lambda/-name).
4. Seleccione el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha lanzado.

También puede comprobar el contenido de los registros de CloudTrail en el bucket de S3 especificado para su registro de seguimiento. Para obtener más información, consulte [Obtención y visualización de archivos de registro de CloudTrail](#) en la AWS CloudTrail Guía del usuario.

Tutorial: Utilizar el transformador de entrada para personalizar qué se transfiere al destino de eventos

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge

ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede utilizar la característica de transformador de entrada de CloudWatch Events para personalizar el texto que se toma de un evento antes introducirlo en el destino de una regla.

Puede definir varias rutas de JSON a partir del evento y asignar sus salidas a distintas variables. A continuación, puede utilizar estas variables en la plantilla de entrada como `<nombre-variable>`. Los caracteres `<` y `>` no pueden utilizar un carácter de escape.

Si especifica una variable que coincida con una ruta JSON que no existe en el evento, dicha variable no se crea y no aparece en la salida.

En este tutorial, extraemos el ID de instancia y el estado de una instancia de Amazon EC2 desde el evento de cambio de estado de instancia. Utilizamos el transformador de entrada para colocar dichos datos en un mensaje fácil de leer que se envía a un tema de Amazon SNS. La regla se activa cuando alguna instancia cambia a cualquier estado. Por ejemplo, con esta regla, el siguiente evento de notificación de cambio de estado de instancia Amazon EC2 produce el mensaje de Amazon SNS La instancia de EC2 i-1234567890abcdef0 ha cambiado de estado a pararse.

```
{
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2015-11-11T21:29:54Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/ i-1234567890abcdef0"
  ],
  "detail": {
    "instance-id": " i-1234567890abcdef0",
    "state": "stopped"
  }
}
```

Esto se consigue asignando la variable `instancia` a la ruta de JSON `$.detail.instance-id` desde el evento y la variable `estado` a la ruta de JSON `$.detail.state`. A continuación, establecemos la plantilla de entrada como "The EC2 instance `<instance>` has changed state to `<state>`".

Crear una regla

Para personalizar la información de cambio de estado de instancia enviada a un destino utilizando el transformador de entrada

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione EC2, elija EC2 Instance State-change Notification (Notificación de cambio de estado de instancia EC2).
 - d. Elija Any state (Cualquier estado), Any instance (Cualquier instancia).
4. En Targets (Destinos), elija Add target (Agregar destino), SNS topic (Tema de SNS).

5. Para Tema, seleccione el tema de Amazon SNS para el que desea que se le notifique cuando las instancias de Amazon EC2 cambian de estado.
6. Elija Configure input, Input Transformer.
7. En el cuadro siguiente, escriba {"state" : "\$.detail.state", "instance" : "\$.detail.instance-id"}
8. En el cuadro siguiente, escriba The EC2 instance <instance> has changed state to <state>."
9. Seleccione Configure details.
10. Escriba un nombre y una descripción de la regla y seleccione Create rule.

Tutorial: RegistroAWSLlamadas a API mediante eventos de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede utilizar una función de AWS Lambda que registre cada llamada a la API de AWS. Por ejemplo, puede crear una regla para registrar cualquier operación dentro de Amazon EC2 o puede limitar esta regla para registrar solo una llamada a la API específica. En este tutorial, registra cada vez que se detiene una instancia Amazon EC2.

Prerequisite

Antes de poder asignar estos eventos, debe utilizar AWS CloudTrail para configurar un registro de seguimiento. Si no dispone de un registro de seguimiento, complete el siguiente procedimiento.

Para crear un registro de seguimiento

1. Abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Trails (Registros de seguimiento), Create trail (Crear un registro de seguimiento).
3. En Trail name, escriba un nombre para el registro de seguimiento.
4. Para Ubicación del almacenamiento, en Cree un nuevo bucket de S3 Escriba el nombre del nuevo bucket al que CloudTrail debe entregar los registros.
5. Seleccione Create.

Paso 1: Creación de unAWS LambdaFunción

Cree una función Lambda para registrar los eventos de llamada al API. Especifique esta función cuando cree la regla.

Para crear una función de Lambda

1. Abra el iconoAWS Lambda en <https://console.aws.amazon.com/lambda/>.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Get Started Now. De lo contrario, elija Create a Lambda function (Crear una función Lambda).

3. En la página Select blueprint (Seleccionar proyecto), escriba `hello` para el filtro y seleccione el proyecto `hello-world`.
4. En la página Configure triggers, elija Next.
5. En la página Configure function, haga lo siguiente:

- a. Escriba un nombre y la descripción de Lambda function. Por ejemplo, nombre la función "LogEC2StopInstance".
- b. Edite el código de muestra de la función Lambda. Por ejemplo:

```
'use strict';

exports.handler = (event, context, callback) => {
  console.log('LogEC2StopInstance');
  console.log('Received event:', JSON.stringify(event, null, 2));
  callback(null, 'Finished');
};
```

- c. En Role (Rol), elija Choose an existing role (Elegir un rol existente). En Existing role (Rol existente), seleccione su rol de ejecución básico. De lo contrario, cree un nuevo rol de ejecución básico.
 - d. Seleccione Next (Siguiente).
6. En la página Review, seleccione Create function.

Paso 2: Crear una regla

Cree una regla para ejecutar su función Lambda siempre que pare una instancia de Amazon EC2.

Para crear una regla de

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione EC2, AWSAPI llamada a través de CloudTrail.
 - d. Elija Specific operation(s) y, a continuación, escriba `StopInstances` en la casilla siguiente.
4. Para implementación, elija Agregar destino, Lambda function.
5. En Function (Función), seleccione la función Lambda que ha creado.
6. Seleccione Configure details.
7. En Rule definition, escriba un nombre y la descripción de la regla.
8. Elija Create rule.

Paso 3: Comprobación de la regla de

Puede probar la regla parando una instancia de Amazon EC2 mediante la consola de Amazon EC2. Después de esperar unos minutos a que la instancia se pare, compruebe la AWS Lambda. En la consola de CloudWatch para comprobar que la función se invocó.

Para probar la regla parando una instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.

2. Lance una instancia. Para obtener más información, consulte [Lanzar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Detenga la instancia. Para obtener más información, consulte [Detener e iniciar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
4. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
5. En el panel de navegación, seleccione Events, el nombre de la regla que ha creado y Show metrics for the rule.
6. Para ver la salida de la función Lambda, haga lo siguiente:
 - a. En el panel de navegación, elija Logs.
 - b. Seleccione el nombre del grupo de registros de la función Lambda (/aws/lambda/-name).
 - c. Seleccione el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha detenido.
7. (Opcional) Cuando haya terminado, puede terminar la instancia parada. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Tutorial: Programar instantáneas automatizadas de Amazon EBS mediante eventos de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede ejecutar reglas de eventos de CloudWatch Events de acuerdo con una programación. En este tutorial, debe crear una instantánea automatizada de un volumen de Amazon Elastic Block Store (Amazon EBS) existente en un programa. Puede seleccionar una frecuencia fija para que se cree una instantánea cada pocos minutos o utilizar una expresión Cron para indicar que la instantánea debe crearse a una hora concreta del día.

Important

Creación de reglas con objetivos integrados solo compatibles en la AWS Management Console.

Paso 1: Crear una regla

Cree una regla que realice instantáneas de manera programada. Puede utilizar una expresión de frecuencia o una expresión Cron para especificar la programación. Para obtener más información, consulte [Programar expresiones para reglas](#) (p. 35).

Para crear una regla de

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event Source, haga lo siguiente:

- a. Elija Schedule.
- b. Elija Fixed rate of y especifique el intervalo de programación (por ejemplo, 5 minutos). También puede seleccionar Cron expression y especificar una expresión Cron (por ejemplo, cada 15 minutos de lunes a viernes, a partir de la hora actual).
4. En Targets (Destinos), elija Add target (Añadir destino) y, a continuación, seleccione EC2 CreateSnapshot API call (Llamada al API CreateSnapshot de EC2). Es posible que tenga que desplazarse hacia arriba por la lista de destinos posibles para encontrar la opción EC2 CreateSnapshot API call (Llamada a la API CreateSnapshot de EC2).
5. ParaID de volumen de, escriba el ID de volumen del volumen de Amazon EBS de destino.
6. Elija Create a new role for this specific resource. El nuevo rol concede al destino permisos para obtener acceso a los recursos en su nombre.
7. Seleccione Configure details.
8. En Rule definition, escriba un nombre y la descripción de la regla.
9. Elija Create rule.

Paso 2: Comprobación de la regla de

Puede verificar la regla consultando la primera instantánea después de tomarla.

Para probar la regla

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Elastic Block Store, Snapshots (Instantáneas).
3. Compruebe que la primera instantánea aparezca en la lista.
4. (Opcional) Cuando haya terminado, puede deshabilitar la regla para evitar que se tomen instantáneas adicionales.
 - a. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
 - b. En el panel de navegación, elija Events (Eventos), Rules (Reglas).
 - c. Seleccione la regla y elija Actions (Acciones), Disable (Desactivar).
 - d. Cuando se le indique que confirme, elija Disable , (Desactivar) .

Tutorial: ScheduleAWS LambdaFunciones con eventos de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede configurar una regla para ejecutar una función AWS Lambda de manera programada. Este tutorial muestra cómo utilizar la AWS Management Console o la AWS CLI para crear la regla. Si desea utilizar elAWS CLIpero no la han instalado, consulte la [AWS Command Line InterfaceGuía del usuario](#).

CloudWatch no proporciona precisión de segundo nivel en expresiones de programación. La mejor resolución al utilizar una expresión Cron es un minuto. Debido a la naturaleza distribuida de los eventos de CloudWatch y los servicios de destino, el retraso entre el momento en que la regla programada se activa y el momento en que el servicio de destino realiza la ejecución del recurso de destino puede ser de varios segundos. La regla programada se activa dentro de ese minuto, pero no específicamente en el segundo 0.

Paso 1: Creación de unAWS LambdaFunción

Cree una función Lambda para registrar los eventos programados. Especifique esta función cuando cree la regla.

Para crear una función de Lambda

1. Abra el iconoAWS Lambdaen<https://console.aws.amazon.com/lambda/>.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Get Started Now. De lo contrario, elija Create a Lambda function (Crear una función Lambda).
3. En la página Select blueprint (Seleccionar proyecto), escriba hello para el filtro y seleccione el proyecto hello-world.
4. En la página Configure triggers, elija Next.
5. En la página Configure function, haga lo siguiente:
 - a. Escriba un nombre y la descripción de Lambda function. Por ejemplo, nombre la función "LogScheduledEvent".
 - b. Edite el código de muestra de la función Lambda. Por ejemplo:

```
'use strict';

exports.handler = (event, context, callback) => {
  console.log('LogScheduledEvent');
  console.log('Received event:', JSON.stringify(event, null, 2));
  callback(null, 'Finished');
};
```

- c. En Role (Rol), elija Choose an existing role (Elegir un rol existente). En Existing role (Rol existente), seleccione su rol de ejecución básico. De lo contrario, cree un nuevo rol de ejecución básico.
 - d. Seleccione Next (Siguiente).
6. En la página Review, seleccione Create function.

Paso 2: Crear una regla

Cree una regla para ejecutar su función Lambda de manera programada.

Para crear una regla con la consola

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event Source, haga lo siguiente:
 - a. Elija Schedule.
 - b. Elija Fixed rate of y especifique el intervalo de programación (por ejemplo, 5 minutos).
4. Paraimplementación, elijaAgregar destino,Lambda function.

5. En Function (Función), seleccione la función Lambda que ha creado.
6. Seleccione Configure details.
7. En Rule definition, escriba un nombre y la descripción de la regla.
8. Elija Create rule.

Si lo prefiere, puede crear la regla utilizando la AWS CLI. En primer lugar, debe conceder permiso a la regla para invocar su función Lambda. A continuación, puede crear la regla y añadir la función Lambda como destino.

Para crear una regla mediante la AWS CLI

1. Utilice el siguiente comando `put-rule` para crear una regla que se activa de forma programada:

```
aws events put-rule \  
--name my-scheduled-rule \  
--schedule-expression 'rate(5 minutes)'
```

Cuando esta regla se activa, genera un evento que sirve como entrada a los destinos de esta regla. El siguiente es un evento de ejemplo:

```
{  
  "version": "0",  
  "id": "53dc4d37-cffa-4f76-80c9-8b7d4a4d2eaa",  
  "detail-type": "Scheduled Event",  
  "source": "aws.events",  
  "account": "123456789012",  
  "time": "2015-10-08T16:53:06Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:events:us-east-1:123456789012:rule/my-scheduled-rule"  
  ],  
  "detail": {}  
}
```

2. Utilice el siguiente [permiso de complemento](#) Para confiar el principal de servicio de CloudWatch Events (`events.amazonaws.com`) y los permisos de ámbito a la regla con el nombre de recurso de Amazon (ARN) especificado:

```
aws lambda add-permission \  
--function-name LogScheduledEvent \  
--statement-id my-scheduled-event \  
--action 'lambda:InvokeFunction' \  
--principal events.amazonaws.com \  
--source-arn arn:aws:events:us-east-1:123456789012:rule/my-scheduled-rule
```

3. Utilice el siguiente [destinos de put](#) Para agregar la función Lambda que ha creado a esta regla para que se ejecute cada 5 minutos:

```
aws events put-targets --rule my-scheduled-rule --targets file://targets.json
```

Crear el archivo `targets.json` con el siguiente contenido:

```
[  
  {  
    "Id": "1",  
    "Arn": "arn:aws:lambda:us-east-1:123456789012:function:LogScheduledEvent"  
  }  
]
```


]

Paso 3: Comprobación de la regla

Al menos cinco minutos después de completar el paso 2, puede comprobar que se invocó la función de Lambda.

Para probar la regla

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Events, Rules, el nombre de la regla que ha creado y Show metrics for the rule.
3. Para ver la salida de la función Lambda, haga lo siguiente:
 - a. En el panel de navegación, elija Logs.
 - b. Seleccione el nombre del grupo de registros de la función Lambda (/aws/lambda/-name).
 - c. Seleccione el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha lanzado.
4. (Opcional) Cuando haya terminado, puede deshabilitar la regla.
 - a. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
 - b. En el panel de navegación, elija Events (Eventos), Rules (Reglas).
 - c. Seleccione la regla y elija Actions (Acciones), Disable (Desactivar).
 - d. Cuando se le indique que confirme, elija Disable , (Desactivar) .

Tutorial: Establezca AWS Systems Manager Obtención de eventos de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede usar CloudWatch Events para invocar AWS Systems Manager La automatización de periódicamente o cuando se detecten eventos específicos. En este tutorial se presupone que está invocando la automatización de Systems Manager según determinados eventos.

Para crear la regla Eventos de CloudWatch

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Elija Event Pattern y Build event pattern to match events by service.

- b. En Service Name y Event Type, elija el servicio y el tipo de evento que desea utilizar como disparador.

En función del servicio y tipo de evento que elija, es posible que deba especificar opciones adicionales en Event Source.

4. En Targets, elija Add Target, SSM Automation.
5. Para Documento, elija el documento de Systems Manager que se va a ejecutar cuando se active el destino de.
6. (Opcional) Para especificar una versión concreta del documento, seleccione Configure document version.
7. En Configure parameter(s), seleccione No Parameter(s) o Constant.

Si selecciona Constant, especifique las constantes que se van a pasar a la ejecución del documento.

8. CloudWatch pueden crear el rol de IAM necesario para que se ejecute su evento:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
9. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.
10. Elija Create rule.

Tutorial: Retransmitir eventos a un flujo de Amazon Kinesis con eventos de CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede retransmitir AWS Los eventos de llamadas de API en CloudWatch Events a un flujo de Amazon Kinesis.

Prerequisite

Instale la AWS CLI. Para obtener más información, consulte la [Guía del usuario de AWS Command Line Interface](#).

Paso 1: Crear una transmisión de Amazon Kinesis

Utilice el siguiente comando `create-stream` para crear un flujo.

```
aws kinesis create-stream --stream-name test --shard-count 1
```

Cuando el estado del flujo sea `ACTIVE`, el flujo está listo. Utilice el siguiente comando `describe-stream` para comprobar el estado del flujo:

```
aws kinesis describe-stream --stream-name test
```

Paso 2: Crear una regla

Por ejemplo, cree una regla para enviar eventos a su flujo cuando se para una instancia Amazon EC2.

Para crear una regla de

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. Seleccione EC2, elija Instance State-change Notification (Notificación de cambio de estado de instancia).
 - d. Seleccione Specific state(s) (Estados específicos), Running (En ejecución).
4. En Targets (Destinos), seleccione Add target (Agregar destino), Kinesis stream (Flujo de Kinesis).
5. En Stream, seleccione el flujo que ha creado.
6. Elija Create a new role for this specific resource.
7. Seleccione Configure details.
8. En Rule definition, escriba un nombre y la descripción de la regla.
9. Elija Create rule.

Paso 3: Comprobación de la regla de

Para probar la regla, pare una instancia Amazon EC2. Después de esperar unos minutos a que la instancia se pare, compruebe las métricas de CloudWatch para comprobar que la función se invocó.

Para probar la regla parando una instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Lance una instancia. Para obtener más información, consulte [Lanzar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
4. En el panel de navegación, seleccione Events, Rules, el nombre de la regla que ha creado y Show metrics for the rule.
5. (Opcional) Cuando haya terminado, puede terminar la instancia. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Paso 4: Comprobación de que el evento se ha retransmitido

Puede obtener el registro del flujo para verificar que el evento se ha transmitido.

Para obtener el registro

1. Utilice el siguiente [get-shard-iterator](#) para comenzar a leer desde su flujo de Kinesis:

```
aws kinesis get-shard-iterator --shard-id shardId-000000000000 --shard-iterator-type  
TRIM_HORIZON --stream-name test
```

A continuación, se muestra un ejemplo del resultado:

```
{  
  "ShardIterator": "AAAAAAAAAAHSywljv0zEgPX4NyKdZ5wryMzP9yALs8NeKbUjp1IxtZs1Sp  
+KEd9I6AJ9ZG4LNR1EMi+9Md/nHvtLyxpfhEzYvkTZ4D9DQVz/mBYWRO6OTZRKnW9gd  
+efGN2aHFdkH1rJl4BL9Wyrk+ghYG22D2T1Da2EyNSH1+LAbK33gQweTJADBdyMwlo5r6PqcP2dzhg="
```

2. Utilice el siguiente comando `get-records` para obtener el registro. El iterador de fragmentos es el que obtuvo en el paso anterior:

```
aws kinesis get-records --shard-  
iterator AAAAAAAAAAHSywljv0zEgPX4NyKdZ5wryMzP9yALs8NeKbUjp1IxtZs1Sp+KEd9I6AJ9ZG4LNR1EMi  
+9Md/nHvtLyxpfhEzYvkTZ4D9DQVz/mBYWRO6OTZRKnW9gd+efGN2aHFdkH1rJl4BL9Wyrk  
+ghYG22D2T1Da2EyNSH1+LAbK33gQweTJADBdyMwlo5r6PqcP2dzhg=
```

Si el comando se realiza correctamente, solicita registros del flujo para el fragmento especificado. Puede recibir cero o más registros. Los registros devueltos podrían no representar todos los registros del flujo. Si no recibe los datos que espera, siga llamando a `get-records`.

Los registros de Kinesis están codificados en Base64. Sin embargo, el soporte de flujos en la AWS CLI no proporciona descodificación base64. Si utiliza un descodificador base64 para descodificar manualmente los datos, verá que el evento se retransmite al flujo en formato JSON.

Tutorial: Ejecutar una tarea de Amazon ECS cuando se carga un archivo a un bucket de Amazon S3

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede utilizar CloudWatch Events para ejecutar tareas de Amazon ECS cuando determinados AWS se producen eventos. En este tutorial, configurará una regla de eventos de CloudWatch que ejecuta una tarea de Amazon ECS siempre que se cargue un archivo en un determinado bucket de Amazon S3 mediante la operación PUT de Amazon S3.

En este tutorial se presupone que ya ha creado la definición de la tarea en Amazon ECS.

Para ejecutar una tarea de Amazon ECS siempre que se cargue un archivo en un bucket de S3 mediante la operación PUT

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.

2. En el panel de navegación, elija Events, Create rule.
3. En Event source, haga lo siguiente:
 - a. Seleccione Event Pattern.
 - b. Seleccione Build event pattern to match events by service.
 - c. En Service Name (Nombre de servicio), seleccione Simple Storage Service (S3).
 - d. En Event Type (Tipo de evento), elija Object Level Operations (Operaciones de nivel de objeto).
 - e. Seleccione Specific operation(s) (Operaciones específicas), Put Object (Poner objeto).
 - f. Elija Specific bucket(s) by name (Buckets específicos por nombre) y escriba el nombre del bucket.
4. En Targets (Destinos), haga lo siguiente:
 - a. Elija Add target (Agregar destino), ECS task (Tarea de ECS).
 - b. En Cluster (Clúster) y Task Definition (Definición de tarea), seleccione los recursos que ha creado.
 - c. Para Tipo de lanzamiento, elija `FARGATE` o `EC2.FARGATE` se muestra únicamente en las regiones en las que `AWS Fargate` es compatible con .
 - d. (Opcional) Especifique un valor para Task Group (Grupo de tareas). Si Launch Type (Tipo de lanzamiento) es `FARGATE`, puede especificar un valor para Platform Version (Versión de plataforma). Especifique solo la parte numérica de la versión de la plataforma, como 1.1.0.
 - e. (Opcional) Especifique una revisión de definición de tarea y un recuento de tareas. Si no especifica una revisión de definición de tarea, se utiliza la última.
 - f. Si la definición de la tarea utiliza el modo de red `awsvpc`, debe especificar las subredes y los grupos de seguridad. Todas las subredes y los grupos de seguridad deben estar en la misma VPC.

Si especifica más de un grupo o subred de seguridad, sepárelos con comas pero no con espacios.

En Subnets (Subredes), especifique el valor de `subnet-id` completo para cada subred, como en el siguiente ejemplo:

```
subnet-123abcd, subnet-789abcd
```
 - g. Elija si desea permitir la asignación automática de la dirección IP pública.
 - h. CloudWatch pueden crear el rol de IAM necesario para que se ejecute su tarea:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente). Debe ser un rol que ya tenga permisos suficientes para invocar la compilación. CloudWatch no concede permisos adicionales para el rol que seleccione.
5. Seleccione Configure details.
6. En Rule definition, escriba un nombre y la descripción de la regla.
7. Elija Create rule.

Tutorial: Programar compilaciones automatizadas con CodeBuild

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge

ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

En el ejemplo de este tutorial, programará CodeBuild para que ejecute una compilación cada noche a las 20:00 GMT. También puede pasar una constante a CodeBuild para usarla en esta compilación programada.

Para crear una regla que programe una compilación de proyecto de CodeBuild por la noche a las 20:00

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create rule.
3. En Event Source, haga lo siguiente:
 - a. Elija Schedule.
 - b. SeleccionarExpresiones crony especifique lo siguiente como la expresión: `20? * LUN-VIE *`. Para obtener más información acerca de las expresiones de cron, consulte [Programar expresiones para reglas \(p. 35\)](#).
4. En Targets (Destinos), seleccione Add target (Agregar destino), CodeBuild project (Proyecto de CodeBuild).
5. En Project ARN, escriba el ARN del proyecto de compilación.
6. En este tutorial, añadimos el paso opcional de pasar un parámetro a CodeBuild, para omitir el valor predeterminado. Esto no es obligatorio cuando se configura CodeBuild como objetivo. Para pasar el parámetro, elija Configure input, Constant (JSON text).

En el cuadro bajoConstante (texto JSON), escriba lo siguiente para configurar la anulación de tiempo de espera a 30 minutos para estas compilaciones programadas: `{«timeoutInMinutesOverride»: 30}`

Para obtener más información acerca de los parámetros que puede pasar, consulte [StartBuild](#). No puede pasar el parámetro `projectName` en este campo. En su lugar, debe especificar el proyecto mediante el ARN en Project ARN.

7. CloudWatch pueden crear el rol de IAM necesario para que se ejecute su proyecto de compilación:
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente). Debe ser un rol que ya tenga permisos suficientes para invocar la compilación. CloudWatch no concede permisos adicionales para el rol que seleccione.
8. Seleccione Configure details
9. En Rule definition, escriba un nombre y la descripción de la regla.
10. Elija Create rule.

Tutorial: Cambios de estado de registro de instancias de Amazon EC2

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge

ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

En el ejemplo de este tutorial, vamos a crear una regla que hace que las notificaciones de cambios en estado en Amazon EC2 se registren en CloudWatch Logs.

Para crear una regla para registrar notificaciones de cambios de estado de Amazon EC2 en CloudWatch Logs

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija **Eventos** y luego **Crear regla**.
3. En **Event Source**, haga lo siguiente:
 - a. Seleccione **Event Pattern**.
 - b. En **Service Name** (Nombre de servicio), elija **EC2**.
 - c. En **Event Type** (Tipo de evento), elija **EC2 Instance State-change Notification** (Notificación de cambio de estado de instancia).
4. En **Targets**, seleccione **Add target**. En la lista de servicios, elija **CloudWatch log group** (Grupo de registros de CloudWatch).
5. Para **Grupo de logs**, escriba un nombre para el grupo de registros de recibir las notificaciones de cambio de estado.
6. Seleccione **Configure details**.
7. Para **Definición de regla**, escriba un nombre y la descripción de la regla.
8. Elija **Create rule**.

Programar expresiones para reglas

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede crear reglas que se activen automáticamente con arreglo a una programación automatizada en Eventos de CloudWatch mediante expresiones cron o de frecuencia. Todos los eventos programados utilizan la zona horaria UTC y la precisión mínima para programas es de 1 minuto.

CloudWatch Events admite expresiones cron y expresiones rate. Las expresiones rate son más fáciles de definir, pero no ofrecen el control preciso que proporcionan las expresiones cron. Por ejemplo, con una expresión cron, puede definir una regla que se active a una hora especificada de un determinado día de cada semana o mes. Por el contrario, las expresiones rate activan una regla a un ritmo regular, como una vez cada hora o una vez cada día.

Note

CloudWatch Events no proporciona precisión de segundo nivel en expresiones de programación. La mejor resolución al utilizar una expresión Cron es un minuto. Debido a la naturaleza distribuida de los eventos de destino y del CloudWatch, el retraso entre el momento en que la regla programada se activa y el momento en que el servicio de destino realiza la ejecución del recurso de destino puede ser de varios segundos. La regla programada se activa dentro de ese minuto, pero no en el segundo 0 preciso.

Formatos

- [Expresiones Cron \(p. 35\)](#)
- [Expresiones de frecuencia \(p. 38\)](#)

Expresiones Cron

Las expresiones Cron tienen seis campos obligatorios, que están separados por un espacio en blanco.

Sintaxis

```
cron(fields)
```

Campo	Valores	Caracteres comodín
Minutes	0-59	, - * /
Hours	0-23	, - * /

Campo	Valores	Caracteres comodín
Day-of-month	1-31	, - * ? / L W
Month	1-12 o JAN-DEC	, - * /
Day-of-week	1-7 o SUN-SAT	, - * ? L
Year	1970-2199	, - * /

Wildcards

- El carácter comodín , (coma) incluye valores adicionales. En el campo Month, JAN, FEB, MAR incluiría enero, febrero y marzo.
- El - (guion) especifica intervalos. En el campo Day, 1-15 incluiría los días del 1 al 15 del mes especificado.
- El * (asterisco) incluye todos los valores del campo. En el campo Hours, * incluiría cada hora. No puede utilizar * en los campos Day-of-month (Día del mes) y Day-of-week (Día de la semana). Si lo utiliza en uno, debe utilizar ? en el otro.
- El comodín / (barra inclinada) especifica incrementos. En el campo Minutes, puede escribir 1/10 para especificar cada décimo minuto, empezando desde el primer minuto de la hora (por ejemplo, los minutos 11, 21 y 31, etc.).
- El comodín ? (signo de interrogación) especifica uno u otro. En el campo Day-of-month puede escribir 7 y si no se preocupó de qué día de la semana era el 7º, podría escribir ? en el campo Day-of-week.
- El comodín L en los campos Day-of-month o Day-of-week especifica el último día del mes o de la semana.
- El comodín w en el campo Day-of-month especifica un día de la semana. En el campo Day-of-month (Día del mes), 3w especifica el día de la semana más cercano al tercer día del mes.
- El comodín # en el campo Day-of-week especifica una instancia concreta del día de la semana de un mes. Por ejemplo, 3#2 sería el segundo martes del mes: el número 3 hace referencia al martes, ya que es el tercer día de la semana en el calendario anglosajón, mientras que 2 hace referencia al segundo día de ese tipo dentro de un mes.

Note

Si utiliza un carácter '#', sólo puede definir una expresión en el campo día de la semana. Por ejemplo, "3#1, 6#3" no es válido porque se interpreta como dos expresiones.

Restrictions

- No se pueden especificar los campos Day-of-month y Day-of-week en la misma expresión Cron. Si especifica un valor (o un *) en uno de los campos, debe utilizar un ? (signo de interrogación) en el otro.
- No se admiten las expresiones Cron que conducen a frecuencias superiores a 1 minuto.

Examples

Puede utilizar las siguientes cadenas cron de ejemplo al crear una regla con programa.

Minutos	Hours	Día del mes	Month	Día de la semana	Year	Significado
0	10	*	*	?	*	Ejecutar a las 10:00 h

Minutos	Hours	Día del mes	Month	Día de la semana	Year	Significado
						(UTC) todos los días
15	12	*	*	?	*	Ejecutar a las 12.15 h (UTC) todos los días
0	18	?	*	MON-FRI	*	Ejecutar a las 18.00 h (UTC) de lunes a viernes
0	8	1	*	?	*	Ejecutar a las 8.00 horas (UTC) cada primer día del mes
0/15	*	*	*	?	*	Ejecutar cada 15 minutos
0/10	*	?	*	MON-FRI	*	Ejecutar cada 10 minutos de lunes a viernes
0/5	8-17	?	*	MON-FRI	*	Ejecutar cada 5 minutos de lunes a viernes entre las 8.00 y las 17.55 h (UTC)

Los siguientes ejemplos muestran cómo utilizar expresiones Cron con el comando AWS CLI `put-rule` de la . El primer ejemplo crea una regla que se activa cada día a las 12.00 UTC.

```
aws events put-rule --schedule-expression "cron(0 12 * * ? *)" --name MyRule1
```

El siguiente ejemplo crea una regla que se activa cada día, a los 5 y 35 minutos después de las 14:00 UTC.

```
aws events put-rule --schedule-expression "cron(5,35 14 * * ? *)" --name MyRule2
```

El siguiente ejemplo crea una regla que se activa a las 10.15 UTC, el último viernes de cada mes, entre los años 2002 y 2005.

```
aws events put-rule --schedule-expression "cron(15 10 ? * 6L 2002-2005)" --name MyRule3
```

Expresiones de frecuencia

Una expresión de frecuencia comienza cuando se crea una regla de evento programado y, a continuación, se ejecuta en su programa definido.

Las expresiones de frecuencia tienen dos campos obligatorios. Los campos están separados por un espacio en blanco.

Sintaxis

```
rate(value unit)
```

value

Un número positivo.

unidad

La unidad de tiempo. Se requieren diferentes unidades para valores de 1, como `minute`, y valores superiores a 1, como `minutes`.

Valores válidos: minuto | minutos | hora | horas | día | días

Restrictions

Si el valor es igual a 1, entonces la unidad debe ser singular. Del mismo modo, para valores mayores que 1, la unidad debe ser plural. Por ejemplo, las frecuencias `rate(1 hours)` y `rate(5 hour)` no son válidas, pero `rate(1 hour)` y `rate(5 hours)` son válidas.

Examples

Los siguientes ejemplos muestran cómo utilizar expresiones de frecuencia con el comando `AWS CLI` `put-rule` de la [línea de comandos](#). El primer ejemplo activa la regla cada minuto, el segundo ejemplo la activa cada 5 minutos, el tercero la activa una vez cada hora y el último la activa una vez al día.

```
aws events put-rule --schedule-expression "rate(1 minute)" --name MyRule2
```

```
aws events put-rule --schedule-expression "rate(5 minutes)" --name MyRule3
```

```
aws events put-rule --schedule-expression "rate(1 hour)" --name MyRule4
```

```
aws events put-rule --schedule-expression "rate(1 day)" --name MyRule5
```

Patrones de eventos de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Los eventos en Amazon CloudWatch Events se representan como objetos JSON. Para obtener más información acerca de los objetos JSON, consulte [RFC 7159](#). El siguiente es un evento de ejemplo:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ec2:us-west-1:123456789012:instance/ i-1234567890abcdef0"
  ],
  "detail": {
    "instance-id": " i-1234567890abcdef0",
    "state": "terminated"
  }
}
```

Es importante recordar los detalles siguientes acerca de un evento:

- Todos tienen los mismos campos de nivel superior (los que aparecen en el ejemplo anterior) que nunca faltan.
- El contenido del campo de nivel superior detail será diferente en función del servicio que haya generado el evento y de cuál sea el evento. La combinación de los campos source y detail-type sirve para identificar los campos y los valores encontrados en detail. Para ver ejemplos de eventos generados por los servicios de AWS, consulte [Tipos de evento para CloudWatch Events](#).

Cada campo de evento se describe a continuación.

version

De forma predeterminada, está definido en 0 (cero) en todos los eventos.

id

Se genera un valor único para cada evento. Esto puede resultar útil a la hora de realizar un seguimiento de los eventos mientras se desplazan a destinos a través de reglas y se procesan.

detail-type

Identifica, en combinación con source, los campos y los valores que aparecen en detail.

Todos los eventos que se entregan a través de CloudTrail tienen `AWS API Call via CloudTrail` como el valor de `detail-type`. Para obtener más información, consulte [Eventos enviados a través de CloudTrail \(p. 87\)](#).

origen

Identifica el servicio del que se obtuvo el evento. Todos los eventos provienen deAWSempezar por»AWS.» Los eventos generados por el cliente pueden tener cualquier valor aquí, salvo que no pueden empezar por»AWS.» Le recomendamos que utilice cadenas de nombres de dominio inversas que utilicen el estilo de nombres de paquetes de Java.

Para encontrar el valor correcto de `source` para unAWSPara ello, consulte la tabla en [AWS Espacios de nombres de servicios de](#). Por ejemplo, el `source` El valor de Amazon CloudFront es `aws.cloudfront`.

cuenta

El número de 12 dígitos que identifica unAWSaccount.

tiempo

La marca temporal del evento, que puede especificar el servicio que origina el evento. Si el evento abarca un intervalo de tiempo, el servicio podría elegir notificar la hora de inicio, por lo que este valor puede ser muy anterior al momento en que se recibe el evento en realidad.

region

Identifica elAWSEn la que se originó el evento.

recursos

Esta matriz JSON contiene ARN que identifican recursos que participan en el evento. La inclusión de estos ARN es decisión del servicio. Por ejemplo, los cambios de estado de instancia de Amazon EC2 incluyen los ARN de instancia de Amazon EC2, los eventos de Auto Scaling incluyen los ARN tanto para instancias como para grupos de Auto Scaling, pero las llamadas al API conAWS CloudTrailno incluyen ARN de recursos.

detail

Un objeto JSON, cuyo contenido es decisión del servicio que origina el evento. El contenido de detalle en el ejemplo anterior es muy sencillo, tan solo dos campos.AWS Los eventos de llamadas al API tienen objetos de detalle con unos 50 campos anidados en varios niveles de profundidad.

Patrones de eventos

Las reglas utilizan patrones de eventos para seleccionar eventos y dirigirlos a los destinos. Un patrón coincide con un evento o bien no coincide. Los patrones de eventos se representan como objetos JSON con una estructura similar a la de eventos, por ejemplo:

```
{
  "source": [ "aws.ec2" ],
  "detail-type": [ "EC2 Instance State-change Notification" ],
  "detail": {
    "state": [ "running" ]
  }
}
```

Es importante recordar lo siguiente acerca de la coincidencia de patrones de eventos:

- Para que un patrón coincida con un evento, el evento debe contener todos los nombres de campos enumerados en el patrón. Los nombres de los campos deben aparecer en el evento con la misma estructura de anidación.
- Otros campos del evento no mencionados en el patrón se ignoran; efectivamente, existe un comodín `**.*.*` para los campos no mencionados.
- La coincidencia exacta (carácter a carácter), sin necesidad de cambio de mayúsculas/minúsculas o cualquier otra normalización de cadenas.

- Los valores que se coincidan siguen las reglas JSON: Cadenas entre comillas, números y palabras clave sin comilla `true`, `false`, y `null`.
- La coincidencia de números está a nivel de representación de cadena. Por ejemplo, 300, 300.0 y 3.0e2 no se consideran iguales.

Al escribir patrones para buscar eventos coincidentes, puede utilizar la API `TestEventPattern` o el comando de la CLI `test-event-pattern` para asegurarse de que su patrón buscará eventos coincidentes con los deseados. Para obtener más información, consulte [TestEventPattern](#) o [test-event-pattern](#).

Los siguientes patrones de eventos coincidirían con el evento en la parte superior de esta página. El primer patrón coincide porque uno de los valores de instancia especificados en el patrón coincide con el evento (y el patrón no especifica ningún campo adicional no incluido en el evento). El segundo coincide porque el evento contiene el estado "terminado".

```
{
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-12345678",
    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcdefgh"
  ]
}
```

```
{
  "detail": {
    "state": [ "terminated" ]
  }
}
```

Estos patrones de evento no coinciden con el evento en la parte superior de esta página. El primer patrón no coincide porque el patrón especifica un valor "pendiente" para el estado y este valor no aparece en el evento. El segundo patrón no coincide ya que el valor de recurso especificado en el patrón no aparece en el evento.

```
{
  "source": [ "aws.ec2" ],
  "detail-type": [ "EC2 Instance State-change Notification" ],
  "detail": {
    "state": [ "pending" ]
  }
}
```

```
{
  "source": [ "aws.ec2" ],
  "detail-type": [ "EC2 Instance State-change Notification" ],
  "resources": [ "arn:aws:ec2:us-east-1::image/ami-12345678" ]
}
```

Coincidencia de valores nulos y cadenas vacías en patrones de eventos

Puede crear un patrón que coincida con un campo de evento que tenga un valor nulo o una cadena vacía. Para ver cómo funciona, tenga en cuenta el siguiente evento de ejemplo:

```
{
  "version": "0",
  "id": "3e3c153a-8339-4e30-8c35-687ebef853fe",
  "detail-type": "EC2 Instance Launch Successful",
  "source": "aws.autoscaling",
  "account": "123456789012",
  "time": "2015-11-11T21:31:47Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "eventVersion": "",
    "responseElements": null
  }
}
```

Para hacer coincidir eventos donde el valor de `eventVersion` es una cadena vacía, utilice el siguiente patrón, que coincidiría con el ejemplo de evento.

```
{
  "detail": {
    "eventVersion": [""]
  }
}
```

Para hacer coincidir eventos donde el valor de `responseElements` es nulo, utilice el siguiente patrón, que coincidiría con el ejemplo de evento.

```
{
  "detail": {
    "responseElements": [null]
  }
}
```

Los valores nulos y las cadenas vacías no son intercambiables en coincidencia de patrones. Un patrón que se escribe para detectar cadenas vacías no capturarán valores de `null`.

Matrices en patrones de eventos de CloudWatch

El valor de cada campo en un patrón es una matriz que contiene uno o varios valores, y el patrón coincide si alguno de los valores de la matriz coincide con el valor en el evento. Si el valor en el evento es una matriz, entonces el patrón coincide si la intersección de la matriz del patrón y la matriz de eventos no está vacía.

Por ejemplo, supongamos que un patrón de eventos incluye el texto siguiente:

```
"resources": [
  "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f",
  "arn:aws:ec2:us-east-1:111122223333:instance/i-b188560f",
  "arn:aws:ec2:us-east-1:444455556666:instance/i-b188560f",
]
```

El patrón del ejemplo coincidiría con un evento que tuviera el siguiente texto, ya que el primer elemento de la matriz del patrón coincide con el segundo elemento de la matriz de eventos.

```
"resources": [  
  "arn:aws:autoscaling:us-east-1:123456789012:autoScalingGroup:eb56d16b-bbf0-401d-b893-  
d5978ed4a025:autoScalingGroupName/ASGTerminate",  
  "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f"  
]
```


Ejemplos de eventos de CloudWatch Events de servicios admitidos

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

La AWS en la lista siguiente, emiten eventos que puede detectar CloudWatch Events.

Además, también puede utilizar CloudWatch Events con servicios que no emiten eventos y que, por tanto, no figuran en esta página, observando los eventos enviados a través de CloudTrail. Para obtener más información, consulte [Eventos enviados a través de CloudTrail \(p. 87\)](#).

Tipos de eventos

- [Eventos de inteligencia artificial aumentada de Amazon \(p. 45\)](#)
- [Eventos Application Auto Scaling \(p. 45\)](#)
- [AWS Batch Events \(p. 45\)](#)
- [Eventos programados de Amazon CloudWatch Events \(p. 45\)](#)
- [Eventos de Amazon Chime \(p. 46\)](#)
- [Eventos de CloudWatch \(p. 46\)](#)
- [Eventos de CodeBuild \(p. 46\)](#)
- [Eventos de CodeCommit \(p. 46\)](#)
- [AWS CodeDeploy Events \(p. 46\)](#)
- [Eventos de CodePipeline \(p. 47\)](#)
- [AWS Config Events \(p. 48\)](#)
- [Eventos de Amazon EBS \(p. 49\)](#)
- [Eventos de Auto Scaling de Amazon EC2 \(p. 49\)](#)
- [Eventos de recomendación de reequilibrio de instancias de Amazon EC2 \(p. 49\)](#)
- [Eventos de interrupción de instancias de spot de Amazon EC2 \(p. 49\)](#)
- [Eventos de cambio de estado de Amazon EC2 \(p. 49\)](#)
- [Amazon Elastic Container Registry \(p. 50\)](#)
- [Eventos de Amazon Elastic Container Service \(p. 50\)](#)
- [Eventos de AWS Elemental MediaConvert \(p. 50\)](#)
- [Eventos de AWS Elemental MediaPackage \(p. 50\)](#)
- [Eventos de AWS Elemental MediaStore \(p. 50\)](#)
- [Eventos de Amazon EMR \(p. 50\)](#)
- [Evento de Amazon GameLift \(p. 52\)](#)
- [AWS Glue Events \(p. 59\)](#)
- [AWS Ground Station Events \(p. 64\)](#)
- [Eventos de Amazon GuardDuty \(p. 64\)](#)

- [AWS Health Events](#) (p. 64)
- [AWS KMS Events](#) (p. 66)
- [Eventos de Amazon Macie](#) (p. 67)
- [Eventos de Amazon Macie](#) (p. 72)
- [Eventos de inicio de sesión de AWS Management Console](#) (p. 72)
- [Eventos de AWS OpsWorks Stacks](#) (p. 72)
- [Eventos de SageMaker](#) (p. 75)
- [AWS Security Hub Events](#) (p. 75)
- [AWS Server Migration Service Events](#) (p. 75)
- [AWS Systems Manager Events](#) (p. 76)
- [AWS Step Functions Events](#) (p. 85)
- [Eventos de cambio de etiquetasAWSRecursos](#) (p. 85)
- [AWS Trusted Advisor Events](#) (p. 85)
- [Eventos de WorkSpaces](#) (p. 87)
- [Eventos enviados a través de CloudTrail](#) (p. 87)

Eventos de inteligencia artificial aumentada de Amazon

Para ver ejemplos de eventos generados por la inteligencia artificial aumentada de Amazon, consulte [Uso de eventos en la inteligencia artificial aumentada de Amazon](#).

Eventos Application Auto Scaling

Para consultar ejemplos de eventos generados por Application Auto Scaling, consulte [Eventos de Auto Scaling de aplicaciones y EventBridge](#).

AWS Batch Events

Para ver ejemplos de eventos generados por AWS Batch, consulte [Eventos de AWS Batch](#).

Eventos programados de Amazon CloudWatch Events

A continuación se muestra un ejemplo de un evento programado:

```
{
  "id": "53dc4d37-cffa-4f76-80c9-8b7d4a4d2eaa",
  "detail-type": "Scheduled Event",
  "source": "aws.events",
  "account": "123456789012",
  "time": "2019-10-08T16:53:06Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:events:us-east-1:123456789012:rule/MyScheduledRule" ],
  "detail": {}
}
```

```
}
```

Eventos de Amazon Chime

Para consultar ejemplos de eventos generados por Amazon Chime, consulte [Automatización de Amazon Chime con EventBridge](#).

Eventos de CloudWatch

Para ver eventos de ejemplo de CloudWatch, consulte [Eventos de alarma y EventBridge en la AWS CodeBuild Guía del usuario](#) de.

Eventos de CodeBuild

Para ver eventos de ejemplo de CodeBuild, consulte [Referencia del formato de entrada de las notificaciones de compilación](#) en la AWS CodeBuild Guía del usuario de.

Eventos de CodeCommit

Para ver eventos de ejemplo de CodeCommit, consulte [Supervisión de eventos de CodeCommit en eventos EventBridge y CloudWatch](#) en la AWS CodeCommit Guía del usuario de.

AWS CodeDeploy Events

A continuación, se muestran ejemplos de los eventos de CodeDeploy. Para obtener más información, consulte [Monitorizar implementaciones con eventos de CloudWatch](#) en la AWS CodeDeploy Guía del usuario de.

Notificación de cambio de estado de implementación de CodeDeploy

Se ha producido un cambio en el estado de una implementación.

```
{
  "account": "123456789012",
  "region": "us-east-1",
  "detail-type": "CodeDeploy Deployment State-change Notification",
  "source": "aws.codedeploy",
  "version": "0",
  "time": "2016-06-30T22:06:31Z",
  "id": "c071bfbf-83c4-49ca-a6ff-3df053957145",
  "resources": [
    "arn:aws:codedeploy:us-east-1:123456789012:application:myApplication",
    "arn:aws:codedeploy:us-east-1:123456789012:deploymentgroup:myApplication/myDeploymentGroup"
  ],
  "detail": {
    "instanceGroupId": "9fd2fbef-2157-40d8-91e7-6845af69e2d2",
    "region": "us-east-1",
    "application": "myApplication",
    "deploymentId": "d-123456789",
  }
}
```

```
"state": "SUCCESS",  
  "deploymentGroup": "myDeploymentGroup"  
}
```

Notificación de cambio de estado de instancia CodeDeploy

Se ha producido un cambio en el estado de una instancia que pertenece a un grupo de implementaciones.

```
{  
  "account": "123456789012",  
  "region": "us-east-1",  
  "detail-type": "CodeDeploy Instance State-change Notification",  
  "source": "aws.codedeploy",  
  "version": "0",  
  "time": "2016-06-30T23:18:50Z",  
  "id": "fb1d3015-c091-4bf9-95e2-d98521ab2ecb",  
  "resources": [  
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaa",  
    "arn:aws:codedeploy:us-east-1:123456789012:deploymentgroup:myApplication/  
myDeploymentGroup",  
    "arn:aws:codedeploy:us-east-1:123456789012:application:myApplication"  
  ],  
  "detail": {  
    "instanceId": "i-0000000aaaaaaaa",  
    "region": "us-east-1",  
    "state": "SUCCESS",  
    "application": "myApplication",  
    "deploymentId": "d-123456789",  
    "instanceGroupId": "8cd3bfa8-9e72-4cbe-a1e5-da4efc7efd49",  
    "deploymentGroup": "myDeploymentGroup"  
  }  
}
```

Eventos de CodePipeline

A continuación, se muestran ejemplos de eventos para CodePipeline.

Cambio de estado de ejecución de la canalización

```
{  
  "version": "0",  
  "id": "CWE-event-id",  
  "detail-type": "CodePipeline Pipeline Execution State Change",  
  "source": "aws.codepipeline",  
  "account": "123456789012",  
  "time": "2017-04-22T03:31:47Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:codepipeline:us-east-1:123456789012:pipeline:myPipeline"  
  ],  
  "detail": {  
    "pipeline": "myPipeline",  
    "version": "1",  
    "state": "STARTED",  
    "execution-id": "01234567-0123-0123-0123-012345678901"  
  }  
}
```

Cambio de estado de ejecución de la etapa

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "CodePipeline Stage Execution State Change",
  "source": "aws.codepipeline",
  "account": "123456789012",
  "time": "2017-04-22T03:31:47Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:codepipeline:us-east-1:123456789012:pipeline:myPipeline"
  ],
  "detail": {
    "pipeline": "myPipeline",
    "version": "1",
    "execution-id": "01234567-0123-0123-0123-012345678901",
    "stage": "Prod",
    "state": "STARTED"
  }
}
```

Cambio de estado de ejecución de la acción

En este ejemplo, hay dos campos `region`. El que aparece en la parte superior es el nombre de la región de AWS donde se ejecuta la acción de la canalización de destino. En este ejemplo, es `us-east-1`. El campo `region` de la sección `detail` es la región de AWS en la que se creó el evento. Coincide con la región donde se creó la canalización. En este ejemplo, es `us-west-2`.

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "CodePipeline Action Execution State Change",
  "source": "aws.codepipeline",
  "account": "123456789012",
  "time": "2017-04-22T03:31:47Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:codepipeline:us-east-1:123456789012:pipeline:myPipeline"
  ],
  "detail": {
    "pipeline": "myPipeline",
    "version": 1,
    "execution-id": "01234567-0123-0123-0123-012345678901",
    "stage": "Prod",
    "action": "myAction",
    "state": "STARTED",
    "region": "us-west-2",
    "type": {
      "owner": "AWS",
      "category": "Deploy",
      "provider": "CodeDeploy",
      "version": 1
    }
  }
}
```

AWS Config Events

Para obtener más información sobre laAWS ConfigPara ver eventos, consulte[MonitoreoAWS Config](#)en la [AWS Config Guía para desarrolladores](#).

Eventos de Amazon EBS

Para obtener más información acerca de los eventos de Amazon EBS, consulte [Amazon CloudWatch Events para Amazon EBS](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Eventos de Auto Scaling de Amazon EC2

Para obtener información acerca de los eventos de Auto Scaling, consulte [Obtención de eventos de CloudWatch cuando su grupo Auto Scaling se escala](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Eventos de recomendación de reequilibrio de instancias de Amazon EC2

Para obtener más información acerca de los eventos de recomendaciones de reequilibrio de instancias de EC2, consulte [Monitorizar señales de recomendación de reequilibrio](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Eventos de interrupción de instancias de spot de Amazon EC2

Para obtener información acerca de los eventos de interrupción de instancias de spot, consulte [Avisos de interrupción de instancias de spot](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Eventos de cambio de estado de Amazon EC2

A continuación, se muestra un ejemplo de los eventos de instancias de Amazon EC2 cuando cambia el estado de la instancia.

EC2 Instance State-change Notification

Este ejemplo es para una instancia con el estado `pending`. Los demás valores posibles para `state` incluyen `running`, `shutting-down`, `stopped`, `stopping` y `terminated`.

```
{
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-11-11T21:29:54Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
  ],
  "detail": {
    "instance-id": "i-abcd1111",
    "state": "pending"
  }
}
```

Amazon Elastic Container Registry

Amazon ECR envía eventos de acciones de imagen a EventBridge. Los eventos se envían cuando las imágenes se insertan, escanean o eliminan.

Para ver eventos de ejemplo de Amazon ECS, consulte [Eventos de Amazon ECR](#) en la Amazon Elastic Container Registry.

Eventos de Amazon Elastic Container Service

Amazon ECS envía dos tipos de eventos a EventBridge: eventos de instancia de contenedor y eventos de tarea. Los eventos de instancia de contenedor se envían únicamente si se utiliza el tipo de lanzamiento EC2 para las tareas. Para las tareas que usan el tipo de lanzamiento Fargate, solamente se reciben eventos de estado de tareas. Amazon ECS realiza el seguimiento de las instancias y de las tareas de contenedor. Si alguno de estos recursos cambia, se activa un evento. Estos eventos se clasifican como eventos de cambio de estado de instancia de contenedor o eventos de cambio de estado de tarea.

Para ver eventos de ejemplo de Amazon ECS, consulte [Eventos de Amazon ECS](#) en la Amazon Elastic Container Service.

Eventos de AWS Elemental MediaConvert

Para ver eventos de ejemplo de MediaConvert, consulte [Uso de eventos de CloudWatch para supervisar trabajos de AWS Elemental MediaConvert](#) en la Guía del usuario AWS Elemental MediaConvert.

Eventos de AWS Elemental MediaPackage

Para ver eventos de ejemplo de MediaPackage, consulte [Monitorización de AWS Elemental MediaPackage con Amazon CloudWatch Events](#) en la Guía del usuario AWS Elemental MediaPackage.

Eventos de AWS Elemental MediaStore

Para ver eventos de ejemplo de MediaStore, consulte [Automatización de AWS Elemental MediaStore con eventos de CloudWatch](#) en la Guía del usuario AWS Elemental MediaStore.

Eventos de Amazon EMR

Los eventos notificados por Amazon EMR han `aws.emr` como el valor de `source`, mientras que los eventos de API de Amazon EMR notificados a través de CloudTrail `aws.elasticmapreduce` como el valor de `source`.

A continuación, se muestran ejemplos de eventos notificados por Amazon EMR.

Cambio de estado de política de Auto Scaling de Amazon EMR

```
{
  "version": "0",
  "id": "2f8147ab-8c48-47c6-b0b6-3ee23ec8d300",
  "detail-type": "EMR Auto Scaling Policy State Change",
```

```
"source": "aws.emr",
"account": "123456789012",
"time": "2016-12-16T20:42:44Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "resourceId": "ig-X2LBMHTGPCBU",
  "clusterId": "j-1YONHTCP3YZKC",
  "state": "PENDING",
  "message": "AutoScaling policy modified by user request",
  "scalingResourceType": "INSTANCE_GROUP"
}
}
```

Cambio de estado de clúster de Amazon EMR: Starting

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "EMR Cluster State Change",
  "source": "aws.emr",
  "account": "123456789012",
  "time": "2016-12-16T20:43:05Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "severity": "INFO",
    "stateChangeReason": "{\"code\":\"\"}",
    "name": "Development Cluster",
    "clusterId": "j-123456789ABCD",
    "state": "STARTING",
    "message": "Amazon EMR cluster j-123456789ABCD (Development Cluster) was requested at 2016-12-16 20:42 UTC and is being created."
  }
}
```

Cambio de estado de clúster de Amazon EMR: Terminated

```
{
  "version": "0",
  "id": "1234abb0-f87e-1234-b7b6-000000123456",
  "detail-type": "EMR Cluster State Change",
  "source": "aws.emr",
  "account": "123456789012",
  "time": "2016-12-16T21:00:23Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "severity": "INFO",
    "stateChangeReason": "{\"code\":\"USER_REQUEST\",\"message\":\"Terminated by user request\"}",
    "name": "Development Cluster",
    "clusterId": "j-123456789ABCD",
    "state": "TERMINATED",
    "message": "Amazon EMR Cluster jj-123456789ABCD (Development Cluster) has terminated at 2016-12-16 21:00 UTC with a reason of USER_REQUEST."
  }
}
```

Cambio de estado de grupo de instancias de Amazon EMR

```
{
```



```
"version": "0",
"id": "999cccaa-eaaa-0000-1111-123456789012",
"detail-type": "EMR Instance Group State Change",
"source": "aws.emr",
"account": "123456789012",
"time": "2016-12-16T20:57:47Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "market": "ON_DEMAND",
  "severity": "INFO",
  "requestedInstanceCount": "2",
  "instanceType": "m3.xlarge",
  "instanceGroupType": "CORE",
  "instanceGroupId": "ig-ABCDEFGHIJKL",
  "clusterId": "j-123456789ABCD",
  "runningInstanceCount": "2",
  "state": "RUNNING",
  "message": "The resizing operation for instance group ig-ABCDEFGHIJKL in Amazon EMR cluster j-123456789ABCD (Development Cluster) is complete. It now has an instance count of 2. The resize started at 2016-12-16 20:57 UTC and took 0 minutes to complete."
}
```

Cambio de estado de paso de Amazon EMR

```
{
  "version": "0",
  "id": "999cccaa-eaaa-0000-1111-123456789012",
  "detail-type": "EMR Step Status Change",
  "source": "aws.emr",
  "account": "123456789012",
  "time": "2016-12-16T20:53:09Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "severity": "ERROR",
    "actionOnFailure": "CONTINUE",
    "stepId": "s-ZYXWVUTSRQPON",
    "name": "CustomJAR",
    "clusterId": "j-123456789ABCD",
    "state": "FAILED",
    "message": "Step s-ZYXWVUTSRQPON (CustomJAR) in Amazon EMR cluster j-123456789ABCD (Development Cluster) failed at 2016-12-16 20:53 UTC."
  }
}
```

Evento de Amazon GameLift

A continuación, se muestran ejemplos de eventos de Amazon GameLift. Para obtener más información, consulte [Referencia de eventos de FlexMatch](#) en la Guía para desarrolladores de Amazon GameLift.

Búsqueda de emparejamiento

```
{
  "version": "0",
  "id": "cc3d3ebe-1d90-48f8-b268-c96655b8f013",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
```

```
"time": "2017-08-08T21:15:36.421Z",
"region": "us-west-2",
"resources": [
  "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
],
"detail": {
  "tickets": [
    {
      "ticketId": "ticket-1",
      "startTime": "2017-08-08T21:15:35.676Z",
      "players": [
        {
          "playerId": "player-1"
        }
      ]
    }
  ],
  "estimatedWaitMillis": "NOT_AVAILABLE",
  "type": "MatchmakingSearching",
  "gameSessionInfo": {
    "players": [
      {
        "playerId": "player-1"
      }
    ]
  }
}
}
```

Posible emparejamiento creado

```
{
  "version": "0",
  "id": "fce8633f-aea3-45bc-aebe-99d639cad2d4",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-08T21:17:41.178Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-08T21:15:35.676Z",
        "players": [
          {
            "playerId": "player-1",
            "team": "red"
          }
        ]
      },
      {
        "ticketId": "ticket-2",
        "startTime": "2017-08-08T21:17:40.657Z",
        "players": [
          {
            "playerId": "player-2",
            "team": "blue"
          }
        ]
      }
    ]
  }
}
```

```
"acceptanceTimeout": 600,
"ruleEvaluationMetrics": [
  {
    "ruleName": "EvenSkill",
    "passedCount": 3,
    "failedCount": 0
  },
  {
    "ruleName": "EvenTeams",
    "passedCount": 3,
    "failedCount": 0
  },
  {
    "ruleName": "FastConnection",
    "passedCount": 3,
    "failedCount": 0
  },
  {
    "ruleName": "NoobSegregation",
    "passedCount": 3,
    "failedCount": 0
  }
],
"acceptanceRequired": true,
"type": "PotentialMatchCreated",
"gameSessionInfo": {
  "players": [
    {
      "playerId": "player-1",
      "team": "red"
    },
    {
      "playerId": "player-2",
      "team": "blue"
    }
  ]
},
"matchId": "3faf26ac-f06e-43e5-8d86-08feff26f692"
}
```

Aceptación de emparejamiento

```
{
  "version": "0",
  "id": "b3f76d66-c8e5-416a-aa4c-aa1278153edc",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-09T20:04:42.660Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-09T20:01:35.305Z",
        "players": [
          {
            "playerId": "player-1",
            "team": "red"
          }
        ]
      }
    ]
  }
}
```

```
    },
    {
      "ticketId": "ticket-2",
      "startTime": "2017-08-09T20:04:16.637Z",
      "players": [
        {
          "playerId": "player-2",
          "team": "blue",
          "accepted": false
        }
      ]
    }
  ],
  "type": "AcceptMatch",
  "gameSessionInfo": {
    "players": [
      {
        "playerId": "player-1",
        "team": "red"
      },
      {
        "playerId": "player-2",
        "team": "blue",
        "accepted": false
      }
    ]
  },
  "matchId": "848b5f1f-0460-488e-8631-2960934d13e5"
}
```

Aceptación de emparejamiento completado

```
{
  "version": "0",
  "id": "b1990d3d-f737-4d6c-b150-af5ace8c35d3",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-08T20:43:14.621Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-08T20:30:40.972Z",
        "players": [
          {
            "playerId": "player-1",
            "team": "red"
          }
        ]
      },
      {
        "ticketId": "ticket-2",
        "startTime": "2017-08-08T20:33:14.111Z",
        "players": [
          {
            "playerId": "player-2",
            "team": "blue"
          }
        ]
      }
    ]
  }
}
```

```
    }  
  ],  
  "acceptance": "TimedOut",  
  "type": "AcceptMatchCompleted",  
  "gameSessionInfo": {  
    "players": [  
      {  
        "playerId": "player-1",  
        "team": "red"  
      },  
      {  
        "playerId": "player-2",  
        "team": "blue"  
      }  
    ]  
  },  
  "matchId": "a0d9bd24-4695-4f12-876f-ea6386dd6dce"  
}
```

El emparejamiento se realizó correctamente

```
{  
  "version": "0",  
  "id": "5ccb6523-0566-412d-b63c-1569e00d023d",  
  "detail-type": "GameLift Matchmaking Event",  
  "source": "aws.gamelift",  
  "account": "123456789012",  
  "time": "2017-08-09T19:59:09.159Z",  
  "region": "us-west-2",  
  "resources": [  
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"  
  ],  
  "detail": {  
    "tickets": [  
      {  
        "ticketId": "ticket-1",  
        "startTime": "2017-08-09T19:58:59.277Z",  
        "players": [  
          {  
            "playerId": "player-1",  
            "playerSessionId": "psess-6e7c13cf-10d6-4756-a53f-db7de782ed67",  
            "team": "red"  
          }  
        ]  
      },  
      {  
        "ticketId": "ticket-2",  
        "startTime": "2017-08-09T19:59:08.663Z",  
        "players": [  
          {  
            "playerId": "player-2",  
            "playerSessionId": "psess-786b342f-9c94-44eb-bb9e-c1de46c472ce",  
            "team": "blue"  
          }  
        ]  
      }  
    ]  
  }  
},  
  "type": "MatchmakingSucceeded",  
  "gameSessionInfo": {  
    "gameSessionArn": "arn:aws:gamelift:us-west-2:123456789012:gamesession/836cf48d-  
bcb0-4a2c-bec1-9c456541352a",  
    "ipAddress": "192.168.1.1",  
    "port": 10777,  
    "players": [  
      {  
        "playerId": "player-1",  
        "playerSessionId": "psess-6e7c13cf-10d6-4756-a53f-db7de782ed67",  
        "team": "red"  
      },  
      {  
        "playerId": "player-2",  
        "playerSessionId": "psess-786b342f-9c94-44eb-bb9e-c1de46c472ce",  
        "team": "blue"  
      }  
    ]  
  }  
}
```

```
{
  {
    "playerId": "player-1",
    "playerSessionId": "psess-6e7c13cf-10d6-4756-a53f-db7de782ed67",
    "team": "red"
  },
  {
    "playerId": "player-2",
    "playerSessionId": "psess-786b342f-9c94-44eb-bb9e-clde46c472ce",
    "team": "blue"
  }
]
},
"matchId": "c0ec1a54-7fec-4b55-8583-76d67adb7754"
}
}
```

Tiempo de espera del emparejamiento agotado

```
{
  "version": "0",
  "id": "fe528a7d-46ad-4bdc-96cb-b094b5f6bf56",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-09T20:11:35.598Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "reason": "TimedOut",
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-09T20:01:35.305Z",
        "players": [
          {
            "playerId": "player-1",
            "team": "red"
          }
        ]
      }
    ]
  },
  "ruleEvaluationMetrics": [
    {
      "ruleName": "EvenSkill",
      "passedCount": 3,
      "failedCount": 0
    },
    {
      "ruleName": "EvenTeams",
      "passedCount": 3,
      "failedCount": 0
    },
    {
      "ruleName": "FastConnection",
      "passedCount": 3,
      "failedCount": 0
    },
    {
      "ruleName": "NoobSegregation",
      "passedCount": 3,
      "failedCount": 0
    }
  ],
}
```

```
"type": "MatchmakingTimedOut",
"message": "Removed from matchmaking due to timing out.",
"gameSessionInfo": {
  "players": [
    {
      "playerId": "player-1",
      "team": "red"
    }
  ]
}
}
```

Emparejamiento cancelado

```
{
  "version": "0",
  "id": "8d6f84da-5e15-4741-8d5c-5ac99091c27f",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-09T20:00:07.843Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "reason": "Cancelled",
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-09T19:59:26.118Z",
        "players": [
          {
            "playerId": "player-1"
          }
        ]
      }
    ]
  },
  "ruleEvaluationMetrics": [
    {
      "ruleName": "EvenSkill",
      "passedCount": 0,
      "failedCount": 0
    },
    {
      "ruleName": "EvenTeams",
      "passedCount": 0,
      "failedCount": 0
    },
    {
      "ruleName": "FastConnection",
      "passedCount": 0,
      "failedCount": 0
    },
    {
      "ruleName": "NoobSegregation",
      "passedCount": 0,
      "failedCount": 0
    }
  ],
  "type": "MatchmakingCancelled",
  "message": "Cancelled by request.",
  "gameSessionInfo": {
    "players": [
```

```
    {
      "playerId": "player-1"
    }
  ]
}
}
```

Error de emparejamiento

```
{
  "version": "0",
  "id": "025b55a4-41ac-4cf4-89d1-f2b3c6fd8f9d",
  "detail-type": "GameLift Matchmaking Event",
  "source": "aws.gamelift",
  "account": "123456789012",
  "time": "2017-08-16T18:41:09.970Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:gamelift:us-west-2:123456789012:matchmakingconfiguration/SampleConfiguration"
  ],
  "detail": {
    "tickets": [
      {
        "ticketId": "ticket-1",
        "startTime": "2017-08-16T18:41:02.631Z",
        "players": [
          {
            "playerId": "player-1",
            "team": "red"
          }
        ]
      }
    ]
  },
  "customEventData": "foo",
  "type": "MatchmakingFailed",
  "reason": "UNEXPECTED_ERROR",
  "message": "An unexpected error was encountered during match placing.",
  "gameSessionInfo": {
    "players": [
      {
        "playerId": "player-1",
        "team": "red"
      }
    ]
  },
  "matchId": "3ea83c13-218b-43a3-936e-135cc570cba7"
}
```

AWS Glue Events

El formato es el de AWS Glue rápidamente.

Ejecución de trabajo correcta

```
{
  "version": "0",
  "id": "abcdef00-1234-5678-9abc-def012345678",
  "detail-type": "Glue Job State Change",
  "source": "aws.glue",
}
```



```
"account": "123456789012",
"time": "2017-09-07T18:57:21Z",
"region": "us-west-2",
"resources": [],
"detail": {
  "jobName": "MyJob",
  "severity": "INFO",
  "state": "SUCCEEDED",
  "jobRunId": "jr_abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789",
  "message": "Job run succeeded"
}
}
```

Ejecución de trabajo con error

```
{
  "version": "0",
  "id": "abcdef01-1234-5678-9abc-def012345678",
  "detail-type": "Glue Job State Change",
  "source": "aws.glue",
  "account": "123456789012",
  "time": "2017-09-07T06:02:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "jobName": "MyJob",
    "severity": "ERROR",
    "state": "FAILED",
    "jobRunId": "jr_0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef",
    "message": "JobName:MyJob and
JobRunId:jr_0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef failed to
execute with exception Role arn:aws:iam:123456789012:role/Glue_Role should be given
assume role permissions for Glue Service."
  }
}
```

Tiempo de espera

```
{
  "version": "0",
  "id": "abcdef00-1234-5678-9abc-def012345678",
  "detail-type": "Glue Job State Change",
  "source": "aws.glue",
  "account": "123456789012",
  "time": "2017-11-20T20:22:06Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "jobName": "MyJob",
    "severity": "WARN",
    "state": "TIMEOUT",
    "jobRunId": "jr_abc0123456789abcdef0123456789abcdef0123456789abcdef0123456789def",
    "message": "Job run timed out"
  }
}
```

Ejecución de tarea detenida

```
{
  "version": "0",
  "id": "abcdef00-1234-5678-9abc-def012345678",
  "detail-type": "Glue Job State Change",
```

```
"source": "aws.glue",
"account": "123456789012",
"time": "2017-11-20T20:22:06Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "jobName": "MyJob",
  "severity": "INFO",
  "state": "STOPPED",
  "jobRunId": "jr_abc0123456789abcdef0123456789abcdef0123456789abcdef0123456789def",
  "message": "Job run stopped"
}
}
```

Rastreador iniciado

```
{
  "version": "0",
  "id": "05efe8a2-c309-6884-a41b-3508bc9695",
  "detail-type": "Glue Crawler State Change",
  "source": "aws.glue",
  "account": "561226563745",
  "time": "2017-11-11T01:09:46Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "accountId": "561226563745",
    "crawlerName": "S3toS3AcceptanceTestCrawlera470bd94-9e00-4518-8942-e80c8431c322",
    "startTime": "2017-11-11T01:09:46Z",
    "state": "Started",
    "message": "Crawler Started"
  }
}
```

Rastreador correcto

```
{
  "version": "0",
  "id": "3d675db5-59b9-6388-b8e8-e0a9b6d567a9",
  "detail-type": "Glue Crawler State Change",
  "source": "aws.glue",
  "account": "561226563745",
  "time": "2017-11-11T01:25:00Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "tablesCreated": "0",
    "warningMessage": "N/A",
    "partitionsUpdated": "0",
    "tablesUpdated": "0",
    "message": "Crawler Succeeded",
    "partitionsDeleted": "0",
    "accountId": "561226563745",
    "runningTime (sec)": "7",
    "tablesDeleted": "0",
    "crawlerName": "SchedulerTestCrawler51fb3a8b-1015-49f0-a969-ca126680b94b",
    "completionDate": "2017-11-11T01:25:00Z",
    "state": "Succeeded",
    "partitionsCreated": "0",
  }
}
```

```
    "cloudWatchLogLink": "https://console.aws.amazon.com/  
cloudwatch/home?region=us-east-1#logEventViewer:group=/aws-glue/  
crawlers;stream=SchedulerTestCrawler51fb3a8b-1015-49f0-a969-ca126680b94b"  
  }  
}
```

Rastreador con error

```
{  
  "version": "0",  
  "id": "f7965b59-470f-2e06-bb89-a8cebaabefac",  
  "detail-type": "Glue Crawler State Change",  
  "source": "aws.glue",  
  "account": "782104008917",  
  "time": "2017-10-20T05:10:08Z",  
  "region": "us-east-1",  
  "resources": [  
  ],  
  "detail": {  
    "crawlerName": "test-crawler-notification",  
    "errorMessage": "Internal Service Exception",  
    "accountId": "1234",  
    "cloudWatchLogLink": "https://console.aws.amazon.com/cloudwatch/home?region=us-  
east-1#logEventViewer:group=/aws-glue/crawlers;stream=test-crawler-notification",  
    "state": "Failed",  
    "message": "Crawler Failed"  
  }  
}
```

La ejecución de trabajo está en estado inicial

```
{  
  "version": "0",  
  "id": "66fbc5e1-aac3-5e85-63d0-856ec669a050",  
  "detail-type": "Glue Job Run Status",  
  "source": "aws.glue",  
  "account": "123456789012",  
  "time": "2018-04-24T20:57:34Z",  
  "region": "us-east-1",  
  "resources": [],  
  "detail": {  
    "jobName": "MyJob",  
    "severity": "INFO",  
    "notificationCondition": {  
      "NotifyDelayAfter": 1.0  
    },  
    "state": "STARTING",  
    "jobRunId": "jr_6aa58e7a3aa44e2e4c7db2c50e2f7396cb57901729e4b702dcb2cfbb3f7a86",  
    "message": "Job is in STARTING state",  
    "startedOn": "2018-04-24T20:55:47.941Z"  
  }  
}
```

La ejecución de trabajo está en estado en ejecución

```
{  
  "version": "0",  
  "id": "66fbc5e1-aac3-5e85-63d0-856ec669a050",  
  "detail-type": "Glue Job Run Status",  
  "source": "aws.glue",  
  "account": "123456789012",
```

```
"time": "2018-04-24T20:57:34Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "jobName": "MyJob",
  "severity": "INFO",
  "notificationCondition": {
    "NotifyDelayAfter": 1.0
  },
  "state": "RUNNING",
  "jobRunId": "jr_6aa58e7a3aa44e2e4c7db2c50e2f7396cb57901729e4b702dcb2cfbb3f7a86",
  "message": "Job is in RUNNING state",
  "startedOn": "2018-04-24T20:55:47.941Z"
}
}
```

La ejecución de trabajo está en estado "deteniendo"

```
{
  "version": "0",
  "id": "66fbc5e1-aac3-5e85-63d0-856ec669a050",
  "detail-type": "Glue Job Run Status",
  "source": "aws.glue",
  "account": "123456789012",
  "time": "2018-04-24T20:57:34Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "jobName": "MyJob",
    "severity": "INFO",
    "notificationCondition": {
      "NotifyDelayAfter": 1.0
    },
    "state": "STOPPING",
    "jobRunId": "jr_6aa58e7a3aa44e2e4c7db2c50e2f7396cb57901729e4b702dcb2cfbb3f7a86",
    "message": "Job is in STOPPING state",
    "startedOn": "2018-04-24T20:55:47.941Z"
  }
}
```

AWS Glue Cambio del estado de la tabla del catálogo de datos de

```
{
  "version": "0",
  "id": "2617428d-715f-edef-70b8-d210da0317a0",
  "detail-type": "Glue Data Catalog Table State Change",
  "source": "aws.glue",
  "account": "123456789012",
  "time": "2019-01-16T18:16:01Z",
  "region": "eu-west-1",
  "resources": [
    "arn:aws:glue:eu-west-1:123456789012:table/d1/t1"
  ],
  "detail": {
    "databaseName": "d1",
    "changedPartitions": [
      "[C.pdf, dir3]",
      "[D.doc, dir4]"
    ],
    "typeOfChange": "BatchCreatePartition",
    "tableName": "t1"
  }
}
```

AWS Glue Cambio del estado de la base de datos del catálogo de datos de

En el siguiente ejemplo, `typeOfChange` es `CreateTable`. Otros valores posibles para este campo son `CreateDatabase` y `UpdateTable`.

```
{
  "version": "0",
  "id": "60e7ddc2-a588-5328-220a-21c060f6c3f4",
  "detail-type": "Glue Data Catalog Database State Change",
  "source": "aws.glue",
  "account": "123456789012",
  "time": "2019-01-16T18:08:48Z",
  "region": "eu-west-1",
  "resources": [
    "arn:aws:glue:eu-west-1:123456789012:table/d1/t1"
  ],
  "detail": {
    "databaseName": "d1",
    "typeOfChange": "CreateTable",
    "changedTables": [
      "t1"
    ]
  }
}
```

AWS Ground Station Events

Para obtener información sobre el ejemplo AWS Ground Station Para ver eventos, consulte [Automatización de AWS Ground Station Eventos de CloudWatch](#) en la AWS Ground Station Guía del usuario de.

Eventos de Amazon GuardDuty

Para obtener información acerca de ejemplos de eventos de Amazon GuardDuty, consulte [Monitorizar Amazon GuardDuty con Amazon CloudWatch Events](#) en la Guía del usuario de Amazon GuardDuty.

AWS Health Events

A continuación, se muestra el formato de la AWS Personal Health Dashboard (AWS Health) eventos. Para obtener más información, consulte [Administración AWS Health Amazon CloudWatch Events](#) en la AWS Health Guía del usuario de.

AWS Health Formato de eventos

```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2016-06-05T06:27:57Z",
  "region": "region",
  "resources": [],
  "detail": {
    "eventArn": "arn:aws:health:region::event/id",
  }
}
```

```
"service": "service",
"eventTypeCode": "AWS_service_code",
"eventTypeCategory": "category",
"startTime": "Sun, 05 Jun 2016 05:01:10 GMT",
"endTime": "Sun, 05 Jun 2016 05:30:57 GMT",
"eventDescription": [{
  "language": "lang-code",
  "latestDescription": "description"
}]
...
}
}
```

eventTypeCategory

El código de categoría del evento. Los valores posibles son `issue`, `accountNotification` y `scheduledChange`.

eventTypeCode

El identificador único para el tipo de evento. Entre los ejemplos se incluyen `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` y `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED`. Los eventos que incluyen `MAINTENANCE_SCHEDULED` suelen devolverse unas dos semanas antes de `startTime`.

id

El identificador único para el evento.

service

El servicio de AWS afectado por el evento. Por ejemplo, `EC2`, `S3`, `REDSHIFT` o `RDS`.

Problema con API de Elastic Load Balancing

```
{
  "version": "0",
  "id": "121345678-1234-1234-1234-123456789012",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2016-06-05T06:27:57Z",
  "region": "ap-southeast-2",
  "resources": [],
  "detail": {
    "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
    "service": "ELASTICLOADBALANCING",
    "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
    "eventTypeCategory": "issue",
    "startTime": "Sat, 11 Jun 2016 05:01:10 GMT",
    "endTime": "Sat, 11 Jun 2016 05:30:57 GMT",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }]
  }
}
```

Rendimiento de la unidad de almacén de instancias de Amazon EC2 degradado

```
{
  "version": "0",
  "id": "121345678-1234-1234-1234-123456789012",
```

```
"detail-type": "AWS Health Event",
"source": "aws.health",
"account": "123456789012",
"time": "2016-06-05T06:27:57Z",
"region": "us-west-2",
"resources": [
  "i-abcd1111"
],
"detail": {
  "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
  "service": "EC2",
  "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
  "eventTypeCategory": "issue",
  "startTime": "Sat, 05 Jun 2016 15:10:09 GMT",
  "eventDescription": [{
    "language": "en_US",
    "latestDescription": "A description of the event will be provided here"
  }],
  "affectedEntities": [{
    "entityValue": "i-abcd1111",
    "tags": {
      "stage": "prod",
      "app": "my-app"
    }
  }
}
```

AWS KMS Events

Los siguientes ejemplos corresponden a eventos de AWS Key Management Service (AWS KMS). Para obtener más información, consulte [AWS KMS Eventos](#) en la [AWS Key Management Service Guía para desarrolladores](#).

Rotación de CMK de KMS

AWS KMS cambió automáticamente un material relacionado con claves de CMK.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "KMS CMK Rotation",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2016-08-25T21:05:33Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Vencimiento del material de claves importado de KMS

AWS KMS eliminó un material relacionado con claves de CMK caducado.

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
```

```
"detail-type": "KMS Imported Key Material Expiration",
"source": "aws.kms",
"account": "111122223333",
"time": "2016-08-22T20:12:19Z",
"region": "us-west-2",
"resources": [
  "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
],
"detail": {
  "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
}
```

Eliminación de CMK de KMS

AWS KMS completó una eliminación de CMK programada.

```
{
  "version": "0",
  "id": "e9ce3425-7d22-412a-a699-e7a5fc3fbc9a",
  "detail-type": "KMS CMK Deletion",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2016-08-19T03:23:45Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Eventos de Amazon Macie

A continuación, se muestran ejemplos de eventos de Amazon Macie Classic.

Alerta creada

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2017-04-24T22:28:49Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id"
  ],
  "detail": {
    "notification-type": "ALERT_CREATED",
    "name": "Scanning bucket policies",
    "tags": [
      "Custom_Alert",
      "Insider"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
  }
}
```



```
"risk-score": 80,
"trigger": {
  "rule-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id",
  "alert-type": "basic",
  "created-at": "2017-01-02 19:54:00.644000",
  "description": "Alerting on failed enumeration of large number of bucket policies",
  "risk": 8
},
"created-at": "2017-04-18T00:21:12.059000",
"actor": "555566667777:assumed-role:superawesome:aroaidpldc7nsesfnheji",
"summary": {
  "Description": "Alerting on failed enumeration of large number of bucket policies",
  "IP": {
    "34.199.185.34": 121,
    "34.205.153.2": 2,
    "72.21.196.70": 2
  },
  "Time Range": [
    {
      "count": 125,
      "start": "2017-04-24T20:23:49Z",
      "end": "2017-04-24T20:25:54Z"
    }
  ],
  "Source ARN": "arn:aws:sts::123456789012:assumed-role/RoleName",
  "Record Count": 1,
  "Location": {
    "us-east-1": 125
  },
  "Event Count": 125,
  "Events": {
    "GetBucketLocation": {
      "count": 48,
      "ISP": {
        "Amazon": 48
      }
    },
    "ListRoles": {
      "count": 2,
      "ISP": {
        "Amazon": 2
      }
    },
    "GetBucketPolicy": {
      "count": 37,
      "ISP": {
        "Amazon": 37
      },
      "Error Code": {
        "NoSuchBucketPolicy": 22
      }
    },
    "GetBucketAcl": {
      "count": 37,
      "ISP": {
        "Amazon": 37
      }
    },
    "ListBuckets": {
      "count": 1,
      "ISP": {
        "Amazon": 1
      }
    }
  },
  "recipientAccountId": {
```

```
    "123456789012": 125
  }
}
}
```

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2017-04-18T18:15:41Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id"
  ],
  "detail": {
    "notification-type": "ALERT_CREATED",
    "name": "Bucket is writable by all authenticated users",
    "tags": [
      "Custom_Alert",
      "Audit"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
    "risk-score": 70,
    "trigger": {
      "rule-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id",
      "alert-type": "basic",
      "created-at": "2017-04-08 00:21:30.749000",
      "description": "Bucket is writable by all authenticated users",
      "risk": 7
    },
    "created-at": "2017-04-18T18:16:17.046454",
    "actor": "444455556666",
    "summary": {
      "Description": "Bucket is writable by all authenticated users",
      "Bucket": {
        "secret-bucket-name": 1
      },
      "Record Count": 1,
      "ACL": {
        "secret-bucket-name": [
          {
            "Owner": {
              "DisplayName": "bucket_owner",
              "ID": "089d2842f4b392f5c5c61f073bd2e4a37b3bb2e62659318c6960e8981648a17e"
            },
            "Grants": [
              {
                "Grantee": {
                  "Type": "Group",
                  "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
                },
                "Permission": "WRITE"
              }
            ]
          }
        ]
      }
    },
    "Event Count": 1,
    "Timestamps": {
```

```
    "2017-01-10T22:48:06.784937": 1
  }
}
}
```

Alerta actualizada

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2017-04-18T17:47:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
    "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id"
  ],
  "detail": {
    "notification-type": "ALERT_UPDATED",
    "name": "Public bucket contains high risk object",
    "tags": [
      "Custom_Alert",
      "Audit"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id/alert/alert_id",
    "risk-score": 100,
    "trigger": {
      "rule-arn": "arn:aws:macie:us-east-1:123456789012:trigger/trigger_id",
      "alert-type": "basic",
      "created-at": "2017-04-08 00:23:39.138000",
      "description": "Public bucket contains high risk object",
      "risk": 10
    },
    "created-at": "2017-04-08T00:36:26.270000",
    "actor": "public_bucket",
    "summary": {
      "Description": "Public bucket contains high risk object",
      "Object": {
        "public_bucket/secret_key.txt": 1,
        "public_bucket/financial_summary.txt": 1
      },
      "Record Count": 2,
      "Themes": {
        "Secret Markings": 1,
        "Corporate Proposals": 1,
        "Confidential Markings": 1
      },
      "Event Count": 2,
      "DLP risk": {
        "7": 2
      },
      "Owner": {
        "bucket_owner": 2
      },
      "Timestamps": {
        "2017-04-03T16:12:53+00:00": 2
      }
    }
  }
}
```

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2017-04-22T03:31:47Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:123456789012:trigger/macie/alert/alert_id",
    "arn:aws:macie:us-east-1:123456789012:trigger/macie"
  ],
  "detail": {
    "notification-type": "ALERT_UPDATED",
    "name": "Lists the instance profiles that have the specified associated IAM role, Lists the names of the inline policies that are embedded in the specified IAM role",
    "tags": [
      "Predictive",
      "Behavioral_Anomaly"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:123456789012:trigger/macie/alert/alert_id",
    "risk-score": 20,
    "created-at": "2017-04-22T03:08:35.256000",
    "actor": "123456789012:assumed-role:rolename",
    "trigger": {
      "alert-type": "predictive",
      "features": {
        "distinctEventName": {
          "name": "distinctEventName",
          "description": "Event Names executed during a user session",
          "narrative": "A sudden increase in event names utilized by a user can be an indicator of a change in user behavior or account risk",
          "risk": 3
        },
        "ListInstanceProfilesForRole": {
          "name": "ListInstanceProfilesForRole",
          "description": "Lists the instance profiles that have the specified associated IAM role",
          "narrative": "Information collection activity suggesting the start of a reconnaissance or exfiltration campaign",
          "anomalous": true,
          "multiplier": 8.420560747663552,
          "excession_times": [
            "2017-04-21T18:00:00Z"
          ],
          "risk": 1
        },
        "ListRolePolicies": {
          "name": "ListRolePolicies",
          "description": "Lists the names of the inline policies that are embedded in the specified IAM role",
          "narrative": "Information collection activity suggesting the start of a reconnaissance or exfiltration campaign",
          "anomalous": true,
          "multiplier": 12.017441860465116,
          "excession_times": [
            "2017-04-21T18:00:00Z"
          ],
          "risk": 2
        }
      }
    }
  }
}
```

```
}
```

Eventos de Amazon Macie

Para consultar ejemplos de eventos generados por Amazon Macie, consulte [Esquema de eventos para los resultados de Amazon Macie](#).

Eventos de inicio de sesión de AWS Management Console

AWS Management Console Los eventos de CloudWatch solo pueden detectar en la región EE.UU. Este (Norte de Virginia).

A continuación, se muestra un ejemplo de un evento de inicio de sesión de la consola:

```
{
  "id": "6f87d04b-9f74-4f04-a780-7acf4b0a9b38",
  "detail-type": "AWS Console Sign In via CloudTrail",
  "source": "aws.signin",
  "account": "123456789012",
  "time": "2016-01-05T18:21:27Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "Root",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::123456789012:root",
      "accountId": "123456789012"
    },
    "eventTime": "2016-01-05T18:21:27Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "0.0.0.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
      "ConsoleLogin": "Success"
    },
    "additionalEventData": {
      "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true",
      "MobileVersion": "No",
      "MFAUsed": "No" },
    "eventID": "324731c0-64b3-4421-b552-dfc3c27df4f6",
    "eventType": "AwsConsoleSignIn"
  }
}
```

Eventos de AWS OpsWorks Stacks

Los siguientes ejemplos corresponden a eventos de AWS OpsWorks Stacks.

AWS OpsWorks Cambio de estado de instancia de Stacks

Indica un cambio en el estado de una instancia AWS OpsWorks Stacks. A continuación se indican los estados de instancia.

- booting
- connection_lost
- online
- pending
- rebooting
- requested
- running_setup
- setup_failed
- shutting_down
- start_failed
- stopping
- stop_failed
- stopped
- terminating
- terminated

```
{
  "version": "0",
  "id": "dc5fa8df-48f1-2108-b1b9-1fe5ebcf2296",
  "detail-type": "OpsWorks Instance State Change",
  "source": "aws.opsworks",
  "account": "123456789012",
  "time": "2018-01-25T11:12:23Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:opsworks:us-east-1:123456789012:instance/a648d98f-fdd8-4323-952a-a50z3e4z500z"
  ],
  "detail": {
    "initiated_by": "user",
    "hostname": "testing1",
    "stack-id": "acd3df16-e859-4598-8414-377b12a902da",
    "layer-ids": [
      "d1a0cb7f-c7e9-4a63-811c-976f0267b2c8"
    ],
    "instance-id": "a648d98f-fdd8-4323-952a-a50z3e4z500z",
    "ec2-instance-id": "i-08b1c2b67aa292276",
    "status": "requested"
  }
}
```

El campo `initiated_by` solo se rellena cuando la instancia se encuentra en los estados `requested`, `terminating` o `stopping`. El campo `initiated_by` puede contener uno de los siguientes valores.

- `user`: un usuario ha solicitado el cambio de estado de instancia con la API o la AWS Management Console.
- `auto-scaling`: la característica de escalado automático de AWS OpsWorks Stacks ha iniciado el cambio de estado de instancia.
- `auto-healing`: la característica de recuperación automática de AWS OpsWorks Stacks ha iniciado el cambio de estado de instancia.

AWS OpsWorks Cambio de estado de comando de Stacks

Un cambio que se ha producido en el estado de un comando de AWS OpsWorks Stacks. A continuación se indican los estados de comando.

- **expired**: se ha agotado el tiempo de espera de comando.
- **failed**: se ha producido un error de comando general.
- **skipped**: un comando se ha omitido porque la instancia tiene un estado en AWS OpsWorks Stacks que en Amazon EC2.
- **successful**: un comando se ha realizado correctamente.
- **superseded**: un comando se ha omitido porque habría aplicado cambios de configuración que ya se han aplicado.

```
{
  "version": "0",
  "id": "96c778b6-a40e-c8c1-aa5c-c9852a3a7b52",
  "detail-type": "OpsWorks Command State Change",
  "source": "aws.opsworks",
  "account": "123456789012",
  "time": "2018-01-26T08:54:40Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:opsworks:us-east-1:123456789012:instance/a648d98f-fdd8-4323-952a-a50a3e4e500f"
  ],
  "detail": {
    "command-id": "acc9f4f3-a3ec-4fab-b70f-c7d04e71e3ec",
    "instance-id": "a648d98f-fdd8-4323-952a-a50a3e4e500f",
    "type": "setup",
    "status": "successful"
  }
}
```

AWS OpsWorks Cambio de estado de implementación de Stacks

Un cambio que se ha producido en el estado de una implementación de AWS OpsWorks Stacks. A continuación se indican los estados de implementación.

- **running**
- **successful**
- **failed**

```
{
  "version": "0",
  "id": "b8230afa-60c7-f43f-b632-841c1c5b22ff",
  "detail-type": "OpsWorks Deployment State Change",
  "source": "aws.opsworks",
  "account": "123456789012",
  "time": "2018-01-25T11:15:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:opsworks:us-east-1:123456789012:instance/a648d98f-fdd8-4323-952a-a50a3e4e500f"
  ],
  "detail": {
    "duration": 16,
    "stack-id": "acd3df16-e859-4598-8414-377b12a902da",
    "instance-ids": [
      "a648d98f-fdd8-4323-952a-a50a3e4e500f"
    ]
  }
}
```

```
"deployment-id": "606419dc-418e-489c-8531-bff9770fc346",  
"command": "configure",  
"status": "successful"  
}  
}
```

El campo `duration` solo se rellena cuando finaliza una implementación y muestra el tiempo en segundos.

AWS OpsWorks Alerta de Stacks

Se ha generado un error de servicio de AWS OpsWorks Stacks.

```
{  
  "version": "0",  
  "id": "f99faa6f-0e27-e398-95bb-8f190806d275",  
  "detail-type": "OpsWorks Alert",  
  "source": "aws.opsworks",  
  "account": "123456789012",  
  "time": "2018-01-20T16:51:29Z",  
  "region": "us-east-1",  
  "resources": [],  
  "detail": {  
    "stack-id": "2f48f2be-ac7d-4dd5-80bb-88375f94db7b",  
    "instance-id": "986efb74-69e8-4c6d-878e-5b77c054cbb0",  
    "type": "InstanceStop",  
    "message": "The shutdown of the instance timed out. Please try stopping it again."  
  }  
}
```

Eventos de SageMaker

Para obtener información acerca de ejemplos de eventos de SageMaker, consulte [Automatización de SageMaker con Amazon EventBridge](#) en la Guía para desarrolladores de SageMaker

AWS Security Hub Events

Para obtener información acerca de ejemplos de eventos de Security Hub, consulte [Monitoreo AWS Security Hub](#) en la [AWS Security Hub Guía del usuario](#) de [Amazon CloudWatch Events](#).

AWS Server Migration Service Events

Los siguientes ejemplos corresponden a eventos para AWS Server Migration Service.

Notificación de trabajo de replicación eliminada

```
{  
  "version": "0",  
  "id": "5630992d-92cd-439f-f2a8-92c8212aee24",  
  "detail-type": "Server Migration Job State Change",  
  "source": "aws.sms",  
  "account": "123456789012",  
  "time": "2018-02-07T22:30:11Z",  
  "region": "us-west-1",  
}
```



```
"resources": [
  "arn:aws:sms:us-west-1:123456789012:sms-job-21a64348"
],
"detail": {
  "state": "Deleted",
  "replication-run-id": "N/A",
  "replication-job-id": "sms-job-21a64348",
  "version": "1.0"
}
}
```

Notificación de trabajo de replicación completado

```
{
  "version": "0",
  "id": "3f9c59cc-f941-522a-be6d-f08e44ff1715",
  "detail-type": "Server Migration Job State Change",
  "source": "aws.sms",
  "account": "123456789012",
  "time": "2018-02-07T22:54:00Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:sms:us-west-1:123456789012:sms-job-2ea64347",
    "arn:aws:sms:us-west-1:123456789012:sms-job-2ea64347/sms-run-e1a64388"
  ],
  "detail": {
    "state": "Completed",
    "replication-run-id": "sms-run-e1a64388",
    "replication-job-id": "sms-job-2ea64347",
    "ami-id": "ami-746d6314",
    "version": "1.0"
  }
}
```

AWS Systems Manager Events

Los siguientes ejemplos corresponden a eventos para AWS Systems Manager. Para obtener más información, consulte [Supervisión de eventos de Systems Manager con Amazon EventBridge](#) en la [AWS Systems Manager Guía del usuario](#) de.

Tipos de evento de Systems Manager

- [AWS Systems Manager Eventos de Automatización](#) (p. 76)
- [AWS Systems Manager Eventos de cambio](#) (p. 77)
- [AWS Systems Manager Eventos de conformidad](#) (p. 78)
- [Eventos de períodos de mantenimiento de AWS Systems Manager](#) (p. 80)
- [Eventos de Parameter Store de AWS Systems Manager](#) (p. 82)
- [AWS Systems Manager Eventos de comando](#) (p. 83)
- [AWS Systems Manager Eventos de State Manager](#) (p. 84)

AWS Systems Manager Eventos de Automatización

Notificación de cambio de estado de paso de Automation

```
{
```

```
"version": "0",
"id": "eeca120b-a321-433e-9635-dab369006a6b",
"detail-type": "EC2 Automation Step Status-change Notification",
"source": "aws.ssm",
"account": "123456789012",
"time": "2016-11-29T19:43:35Z",
"region": "us-east-1",
"resources": ["arn:aws:ssm:us-east-1:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
"arn:aws:ssm:us-east-1:123456789012:automation-definition/runcommand1:1"],
"detail": {
  "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
  "Definition": "runcommand1",
  "DefinitionVersion": 1.0,
  "Status": "Success",
  "EndTime": "Nov 29, 2016 7:43:25 PM",
  "StartTime": "Nov 29, 2016 7:43:23 PM",
  "Time": 2630.0,
  "StepName": "runFixedCmds",
  "Action": "aws:runCommand"
}
}
```

Notificación de cambio de estado de ejecución de Automation

```
{
  "version": "0",
  "id": "d290ece9-1088-4383-9df6-cd5b4ac42b99",
  "detail-type": "EC2 Automation Execution Status-change Notification",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2016-11-29T19:43:35Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ssm:us-east-1:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
"arn:aws:ssm:us-east-1:123456789012:automation-definition/runcommand1:1"],
  "detail": {
    "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
    "Definition": "runcommand1",
    "DefinitionVersion": 1.0,
    "Status": "Success",
    "StartTime": "Nov 29, 2016 7:43:20 PM",
    "EndTime": "Nov 29, 2016 7:43:26 PM",
    "Time": 5753.0,
    "ExecutedBy": "arn:aws:iam::123456789012:user/userName"
  }
}
```

AWS Systems ManagerEventos de cambio

A continuación, se muestran ejemplos de los eventos paraAWS Systems ManagerCalendario de cambios

Note

Cambios de estado para calendarios compartidos desde otrosAWSLas cuentas no se admiten actualmente.

ABIERTO

```
{
  "version": "0",
```

```
"id": "47a3f03a-f30d-1011-ac9a-du3bdEXAMPLE",
"detail-type": "Calendar State Change",
"source": "aws.ssm",
"account": "111222333444",
"time": "2020-09-19T18:00:07Z",
"region": "us-east-2",
"resources": [
  "arn:aws:ssm:us-east-2:111222333444:document/MyCalendar"
],
"detail": {
  "state": "OPEN",
  "atTime": "2020-09-19T18:00:07Z",
  "nextTransitionTime": "2020-10-11T18:00:07Z"
}
}
```

Calendario CERRADO

```
{
  "version": "0",
  "id": "f30df03a-1011-ac9a-47a3-f761eEXAMPLE",
  "detail-type": "Calendar State Change",
  "source": "aws.ssm",
  "account": "111222333444",
  "time": "2020-09-17T21:40:02Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:111222333444:document/MyCalendar"
  ],
  "detail": {
    "state": "CLOSED",
    "atTime": "2020-08-17T21:40:00Z",
    "nextTransitionTime": "2020-09-19T18:00:07Z"
  }
}
```

AWS Systems ManagerEventos de conformidad

A continuación, se muestran ejemplos de los eventos paraAWS Systems ManagerConformidad

Conformidad con la asociación

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-07-17T19:03:26Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ssm:us-west-1:461348341421:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "last-runtime": "2017-01-01T10:10:10Z",
    "compliance-status": "compliant",
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-type": "Association"
  }
}
```

Sin conformidad con la asociación

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-07-17T19:02:31Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ssm:us-west-1:461348341421:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "last-runtime": "2017-01-01T10:10:10Z",
    "compliance-status": "non_compliant",
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-type": "Association"
  }
}
```

Conformidad con los parches

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-07-17T19:03:26Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ssm:us-west-1:461348341421:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-status": "compliant",
    "compliance-type": "Patch",
    "patch-baseline-id": "PB789",
    "severity": "critical"
  }
}
```

Sin conformidad con los parches

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-07-17T19:02:31Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ssm:us-west-1:461348341421:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-status": "non_compliant",
    "compliance-type": "Patch",
  }
}
```

```
"patch-baseline-id": "PB789",  
"severity": "critical"  
}  
}
```

Eventos de períodos de mantenimiento de AWS Systems Manager

A continuación, se muestran ejemplos de los eventos de períodos de mantenimiento de Systems Manager.

Registrar un destino

El otro valor de estado válido esDEREGISTERED.

```
{  
  "version": "0",  
  "id": "01234567-0123-0123-0123-0123456789ab",  
  "detail-type": "Maintenance Window Target Registration Notification",  
  "source": "aws.ssm",  
  "account": "012345678901",  
  "time": "2016-11-16T00:58:37Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ssm:us-west-2:001312665065:maintenancewindow/mw-0ed7251d3fcf6e0c2",  
    "arn:aws:ssm:us-west-2:001312665065:windowtarget/  
e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6"  
  ],  
  "detail": {  
    "window-target-id": "e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6",  
    "window-id": "mw-0ed7251d3fcf6e0c2",  
    "status": "REGISTERED"  
  }  
}
```

Tipo de ejecución de ventana

Los otros valores de estado válidos sonPENDING,IN_PROGRESS,SUCCESS,FAILED,TIMED_OUT,YSKIPPED_OVERLAPPING.

```
{  
  "version": "0",  
  "id": "01234567-0123-0123-0123-0123456789ab",  
  "detail-type": "Maintenance Window Execution State-change Notification",  
  "source": "aws.ssm",  
  "account": "012345678901",  
  "time": "2016-11-16T01:00:57Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ssm:us-west-2:0123456789ab:maintenancewindow/mw-123456789012345678"  
  ],  
  "detail": {  
    "start-time": "2016-11-16T01:00:56.427Z",  
    "end-time": "2016-11-16T01:00:57.070Z",  
    "window-id": "mw-0ed7251d3fcf6e0c2",  
    "window-execution-id": "b60fb56e-776c-4e5c-84ee-123456789012",  
    "status": "TIMED_OUT"  
  }  
}
```

Tipo de ejecución de tarea

Los otros valores de estado válidos son `IN_PROGRESS`, `SUCCESS`, `FAILED`, y `TIMED_OUT`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "Maintenance Window Task Execution State-change Notification",
  "source": "aws.ssm",
  "account": "012345678901",
  "time": "2016-11-16T01:00:56Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-west-2:0123456789ab:maintenancewindow/mw-123456789012345678"
  ],
  "detail": {
    "start-time": "2016-11-16T01:00:56.759Z",
    "task-execution-id": "6417e808-7f35-4d1a-843f-123456789012",
    "end-time": "2016-11-16T01:00:56.847Z",
    "window-id": "mw-0ed7251d3fcf6e0c2",
    "window-execution-id": "b60fb56e-776c-4e5c-84ee-123456789012",
    "status": "TIMED_OUT"
  }
}
```

Destino de tarea procesado

Los otros valores de estado válidos son `IN_PROGRESS`, `SUCCESS`, `FAILED`, y `TIMED_OUT`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "Maintenance Window Task Target Invocation State-change Notification",
  "source": "aws.ssm",
  "account": "012345678901",
  "time": "2016-11-16T01:00:57Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-west-2:0123456789ab:maintenancewindow/mw-123456789012345678"
  ],
  "detail": {
    "start-time": "2016-11-16T01:00:56.427Z",
    "end-time": "2016-11-16T01:00:57.070Z",
    "window-id": "mw-0ed7251d3fcf6e0c2",
    "window-execution-id": "b60fb56e-776c-4e5c-84ee-123456789012",
    "task-execution-id": "6417e808-7f35-4d1a-843f-123456789012",
    "window-target-id": "e7265f13-3cc5-4f2f-97a9-123456789012",
    "status": "TIMED_OUT",
    "owner-information": "Owner"
  }
}
```

Cambio de estado de ventana

Los valores de estado válidos son `ENABLED` y `DISABLED`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "Maintenance Window State-change Notification",
  "source": "aws.ssm",
  "account": "012345678901",
  "time": "2016-11-16T00:58:37Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ssm:us-west-2:0123456789ab:maintenancewindow/mw-123456789012345678"  
  ],  
  "detail": {  
    "window-id": "mw-123456789012",  
    "status": "DISABLED"  
  }  
}
```

Eventos de Parameter Store de AWS Systems Manager

A continuación, se muestran ejemplos de los eventos de Almacén de parámetros de Systems Manager.

Crear parámetro

```
{  
  "version": "0",  
  "id": "6a7e4feb-b491-4cf7-a9f1-bf3703497718",  
  "detail-type": "Parameter Store Change",  
  "source": "aws.ssm",  
  "account": "123456789012",  
  "time": "2017-05-22T16:43:48Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ssm:us-east-1:123456789012:parameter/foo"  
  ],  
  "detail": {  
    "operation": "Create",  
    "name": "foo",  
    "type": "String",  
    "description": "Sample Parameter"  
  }  
}
```

Actualizar parámetro

```
{  
  "version": "0",  
  "id": "9547ef2d-3b7e-4057-b6cb-5fdf09ee7c8f",  
  "detail-type": "Parameter Store Change",  
  "source": "aws.ssm",  
  "account": "123456789012",  
  "time": "2017-05-22T16:44:48Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ssm:us-east-1:123456789012:parameter/foo"  
  ],  
  "detail": {  
    "operation": "Update",  
    "name": "foo",  
    "type": "String",  
    "description": "Sample Parameter"  
  }  
}
```

Eliminar parámetro

```
{
```

```
"version": "0",
"id": "80e9b391-6a9b-413c-839a-453b528053af",
"detail-type": "Parameter Store Change",
"source": "aws.ssm",
"account": "123456789012",
"time": "2017-05-22T16:45:48Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ssm:us-east-1:123456789012:parameter/foo"
],
"detail": {
  "operation": "Delete",
  "name": "foo",
  "type": "String",
  "description": "Sample Parameter"
}
}
```

AWS Systems ManagerEventos de comando

Notificación de cambio de estado de Run Command

```
{
  "version": "0",
  "id": "51c0891d-0e34-45b1-83d6-95db273d1602",
  "detail-type": "EC2 Command Status-change Notification",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2016-07-10T21:51:32Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"],
  "detail": {
    "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
    "document-name": "AWS-RunPowerShellScript",
    "expire-after": "2016-07-14T22:01:30.049Z",
    "parameters": {
      "executionTimeout": ["3600"],
      "commands": ["date"]
    },
    "requested-date-time": "2016-07-10T21:51:30.049Z",
    "status": "Success"
  }
}
```

Notificación de cambio de estado de invocación de Run Command

```
{
  "version": "0",
  "id": "4780e1b8-f56b-4de5-95f2-95db273d1602",
  "detail-type": "EC2 Command Invocation Status-change Notification",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2016-07-10T21:51:32Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"],
  "detail": {
    "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
    "document-name": "AWS-RunPowerShellScript",
    "instance-id": "i-9bb89e2b",
    "requested-date-time": "2016-07-10T21:51:30.049Z",
    "status": "Success"
  }
}
```



```
}
```

AWS Systems ManagerEventos de State Manager

Cambio de estado de asociación de State Manager

```
{
  "version": "0",
  "id": "db839caf-6f6c-40af-9a48-25b2ae2b7774",
  "detail-type": "EC2 State Manager Association State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-05-16T23:01:10Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ssm:us-west-1::document/AWS-RunPowerShellScript"
  ],
  "detail": {
    "association-id": "6e37940a-23ba-4ab0-9b96-5d0a1a05464f",
    "document-name": "AWS-RunPowerShellScript",
    "association-version": "1",
    "document-version": "Optional.empty",
    "targets": "[{\\"key\\": \"InstanceIds\\\", \"values\\\": [\\\"i-12345678\\\"]}]",
    "creation-date": "2017-02-13T17:22:54.458Z",
    "last-successful-execution-date": "2017-05-16T23:00:01Z",
    "last-execution-date": "2017-05-16T23:00:01Z",
    "last-updated-date": "2017-02-13T17:22:54.458Z",
    "status": "Success",
    "association-status-aggregated-count": "{\\"Success\\": 1}",
    "schedule-expression": "cron(0 */30 * * * ? *)",
    "association-cwe-version": "1.0"
  }
}
```

Cambio de estado de asociación de instancia de State Manager

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "EC2 State Manager Instance Association State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2017-02-23T15:23:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-12345678",
    "arn:aws:ssm:us-east-1:123456789012:document/my-custom-document"
  ],
  "detail": {
    "association-id": "34fcb7e0-9a14-4984-9989-0e04e3f60bd8",
    "instance-id": "i-12345678",
    "document-name": "my-custom-document",
    "document-version": "1",
    "targets": "[{\\"key\\": \"instanceids\\\", \"values\\\": [\\\"i-12345678\\\"]}]",
    "creation-date": "2017-02-23T15:23:48Z",
    "last-successful-execution-date": "2017-02-23T16:23:48Z",
    "last-execution-date": "2017-02-23T16:23:48Z",
    "status": "Success",
    "detailed-status": "",
    "error-code": "testErrorCode",
    "execution-summary": "testExecutionSummary",
    "output-url": "sampleurl",
  }
}
```

```
    "instance-association-cwe-version": "1"  
  }  
}
```

AWS Step Functions Events

Para ver eventos de ejemplo Step Functions, consulte [Ejemplos de Events Functions](#) en la [AWS Step Functions Guía para desarrolladores](#).

Eventos de cambio de etiquetas AWS Recursos

A continuación se muestra un ejemplo de un evento de etiqueta.

```
{  
  "version": "0",  
  "id": "ffd8a6fe-32f8-ef66-c85c-111111111111",  
  "detail-type": "Tag Change on Resource",  
  "source": "aws.tag",  
  "account": "123456789012",  
  "time": "2018-09-18T20:41:06Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaa"  
  ],  
  "detail": {  
    "changed-tag-keys": [  
      "key2",  
      "key3"  
    ],  
    "service": "ec2",  
    "resource-type": "instance",  
    "version": 5,  
    "tags": {  
      "key4": "value4",  
      "key1": "value1",  
      "key2": "value2"  
    }  
  }  
}
```

AWS Trusted Advisor Events

Los siguientes ejemplos corresponden a eventos para AWS Trusted Advisor . Para obtener más información, consulte [Monitoreo Trusted Advisor](#) [Comprobar resultados con Amazon CloudWatch Events](#) en la [AWS Support Guía del usuario](#) de.

Utilización baja de instancias de Amazon EC2

```
{  
  "version": "0",  
  "id": "1234abcd-ab12-123a-123a-1234567890ab",  
  "detail-type": "Trusted Advisor Check Item Refresh Notification",  
  "source": "aws.trustedadvisor",  
  "account": "123456789012",  
  "time": "2018-01-12T20:07:49Z",  
  "region": "us-east-2",  
}
```

```

"resources": [],
"detail": {
  "check-name": "Low Utilization Amazon EC2 Instances",
  "check-item-detail": {
    "Day 1": "0.1% 0.00MB",
    "Day 2": "0.1% 0.00MB",
    "Day 3": "0.1% 0.00MB",
    "Region/AZ": "ca-central-1a",
    "Estimated Monthly Savings": "$9.22",
    "14-Day Average CPU Utilization": "0.1%",
    "Day 14": "0.1% 0.00MB",
    "Day 13": "0.1% 0.00MB",
    "Day 12": "0.1% 0.00MB",
    "Day 11": "0.1% 0.00MB",
    "Day 10": "0.1% 0.00MB",
    "14-Day Average Network I/O": "0.00MB",
    "Number of Days Low Utilization": "14 days",
    "Instance Type": "t2.micro",
    "Instance ID": "i-01234567890abcdef",
    "Day 8": "0.1% 0.00MB",
    "Instance Name": null,
    "Day 9": "0.1% 0.00MB",
    "Day 4": "0.1% 0.00MB",
    "Day 5": "0.1% 0.00MB",
    "Day 6": "0.1% 0.00MB",
    "Day 7": "0.1% 0.00MB"
  },
  "status": "WARN",
  "resource_id": "arn:aws:ec2:ca-central-1:123456789012:instance/i-01234567890abcdef",
  "uuid": "aa12345f-55c7-498e-b7ac-123456789012"
}
}

```

Optimización del balanceador de carga

```

{
  "version": "0",
  "id": "1234abcd-ab12-123a-123a-1234567890ab",
  "detail-type": "Trusted Advisor Check Item Refresh Notification",
  "source": "aws.trustedadvisor",
  "account": "123456789012",
  "time": "2018-01-12T20:07:03Z",
  "region": "us-east-2",
  "resources": [],
  "detail": {
    "check-name": "Load Balancer Optimization ",
    "check-item-detail": {
      "Instances in Zone a": "1",
      "Status": "Yellow",
      "Instances in Zone b": "0",
      "# of Zones": "2",
      "Region": "eu-central-1",
      "Load Balancer Name": "my-load-balance",
      "Instances in Zone e": null,
      "Instances in Zone c": null,
      "Reason": "Single AZ",
      "Instances in Zone d": null
    },
    "status": "WARN",
    "resource_id": "arn:aws:elasticloadbalancing:eu-central-1:123456789012:loadbalancer/my-load-balancer",
    "uuid": "aa12345f-55c7-498e-b7ac-123456789012"
  }
}

```

Claves de acceso expuestas

```
{
  "version": "0",
  "id": "1234abcd-ab12-123a-123a-1234567890ab",
  "detail-type": "Trusted Advisor Check Item Refresh Notification",
  "source": "aws.trustedadvisor",
  "account": "123456789012",
  "time": "2018-01-12T19:38:24Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "check-name": "Exposed Access Keys",
    "check-item-detail": {
      "Case ID": "12345678-1234-1234-abcd-1234567890ab",
      "Usage (USD per Day)": "0",
      "User Name (IAM or Root)": "my-username",
      "Deadline": "1440453299248",
      "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
      "Time Updated": "1440021299248",
      "Fraud Type": "Exposed",
      "Location": "www.example.com"
    },
    "status": "ERROR",
    "resource_id": "",
    "uuid": "aa12345f-55c7-498e-b7ac-123456789012"
  }
}
```

Eventos de WorkSpaces

Para obtener información acerca de los eventos de WorkSpaces, consulte [Monitorizar sus WorkSpaces mediante eventos CloudWatch](#) en la Guía de administración de Amazon WorkSpaces.

Eventos enviados a través de CloudTrail

También puede utilizar CloudWatch Events con servicios que no emiten eventos y que, por tanto, no figuran en esta página. AWS CloudTrail es un servicio que registra automáticamente eventos como AWS Lambda a la API. Puede crear reglas de CloudWatch Events que se desencadenen en función de la información capturada por CloudTrail. Para obtener más información acerca de CloudTrail, consulte [¿Qué es AWS CloudTrail?](#). Para obtener más información acerca de cómo crear una regla de CloudWatch Events que utilice CloudTrail, consulte [Creación de una regla de CloudWatch Events que se activa en función de una AWS API Llamada a la API AWS CloudTrail \(p. 8\)](#).

Todos los eventos que se entregan a través de CloudTrail tienen `AWS API Call via CloudTrail` como el valor de `detail-type`.

Algunas coincidencias en AWS puede notificar a CloudWatch Events tanto por el propio servicio como por CloudTrail, pero de diferentes maneras. Por ejemplo, una llamada a la API de Amazon EC2 que lanza o termina una instancia genera eventos disponibles para CloudWatch Events a través de CloudTrail. Sin embargo, los cambios de estado de las instancias de Amazon EC2, por ejemplo, de «en ejecución» a «terminando», son por sí mismos eventos de CloudWatch.

A continuación, se muestra un ejemplo de un evento enviado a través de CloudTrail. El evento lo generó la AWS API de llamada a Amazon S3 para crear un bucket.

```
{
```

```
"version": "0",
"id": "36eb8523-97d0-4518-b33d-ee3579ff19f0",
"detail-type": "AWS API Call via CloudTrail",
"source": "aws.s3",
"account": "123456789012",
"time": "2016-02-20T01:09:13Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2016-02-20T01:05:59Z"
      }
    }
  },
  "eventTime": "2016-02-20T01:09:13Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "CreateBucket",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.100.100.100",
  "userAgent": "[S3Console/0.4]",
  "requestParameters": {
    "bucketName": "bucket-test-iad"
  },
  "responseElements": null,
  "requestID": "9D767BCC3B4E7487",
  "eventID": "24ba271e-d595-4e66-a7fd-9c16cbf8abae",
  "eventType": "AwsApiCall"
}
```

AWS Los eventos de llamadas al API con un tamaño superior a 256 KB no se admiten. Para obtener más información sobre las llamadas a la API que puede utilizar como disparadores de reglas, consulte [Servicios compatibles con el historial de eventos de CloudTrail](#).

Envío y recepción de eventos entre cuentas de AWS

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede configurar su cuenta de AWS para enviar eventos a otras cuentas de AWS o para recibir eventos desde otras cuentas. Esto puede resultar útil si las cuentas pertenecen a la misma organización, o pertenecen a organizaciones que son socias o tienen una relación similar.

Si configura su cuenta para enviar o recibir eventos, puede especificar las cuentas individuales de AWS que pueden enviar eventos a la suya o recibirlos desde esta. Si utiliza la característica AWS Organizations, puede especificar una organización y conceder acceso a todas las cuentas de esta. Para obtener más información, consulte [¿Qué es AWS Organizations?](#) en la Guía del usuario de AWS Organizations.

El proceso general es el siguiente:

- En la página receptor, edite los permisos en la cuenta predeterminada Bus de eventos para permitir especificado AWS cuentas, una organización o todos los AWS para enviar eventos a la cuenta del receptor.
- En la cuenta remitente, configure una o varias reglas que tengan como destino el bus de eventos predeterminado de la cuenta receptora.

Si la cuenta de remitente tiene permisos para enviar eventos porque forma parte de un AWS Si tiene permisos, la cuenta remitente también debe tener un rol de IAM con políticas que le permitan enviar eventos a la cuenta receptora. Si utiliza la AWS Management Console para crear la regla destinada a la cuenta receptora, esta operación se realiza automáticamente. Si utiliza la AWS CLI, debe crear el rol manualmente.

- En la cuenta receptora, configure una o varias reglas que coincidan con eventos procedentes de la cuenta remitente.

La región de AWS en la que la cuenta receptora agrega permisos al bus de eventos predeterminado debe ser la misma en la que la cuenta remitente crea la regla para enviar eventos a la cuenta receptora.

Los eventos enviados de una cuenta a otra se cargan a la cuenta remitente como eventos personalizados. No se cobra nada a la cuenta receptora. Para obtener más información, consulte [Precios de Amazon CloudWatch](#).

Si una cuenta receptora configura una regla que envíe los eventos recibidos de una cuenta remitente a una tercera cuenta, estos eventos no se envían a la tercera cuenta.

Activación de su cuenta de AWS para recibir eventos de otras cuentas de AWS

Para recibir eventos desde otras organizaciones o cuentas, primero debe editar los permisos del bus de eventos predeterminado de su cuenta. El bus de eventos predeterminado acepta eventos de AWS servicios, otros autorizados AWS Cuentas, y `PutEvents` llama a.

Cuando edite los permisos del bus de eventos predeterminado para conceder permisos a otras cuentas de AWS, puede especificar las cuentas por el ID de cuenta o de organización. También puede elegir recibir eventos de AWS Cuentas.

Warning

Si decide recibir eventos de todas las cuentas de AWS, asegúrese de crear reglas que coincidan solo con los eventos que recibe de otras cuentas. Para crear reglas más seguras, asegúrese de que el patrón de eventos de cada regla contiene un campo `Account` con el ID de una o varias cuentas desde las que desea recibir eventos. Las reglas que tienen un patrón de eventos que contiene un campo `Account` (Cuenta) no coinciden con los eventos enviados desde cuentas que no aparecen en el campo `Account`. Para obtener más información, consulte [Patrones de eventos de CloudWatch](#) (p. 39).

Para activar su cuenta para recibir eventos de otras cuentas de AWS mediante la consola

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Event Buses, Add Permission.
3. Seleccionar AWS Cuenta o Organización.

Si elige `AWS Cuenta`, ingrese el valor de 12 dígitos `AWS ID` de la cuenta de desde la que desea recibir eventos. Para recibir eventos de todas las demás cuentas de AWS, seleccione `Everybody(*)` (Todos).

Si elige `Organization` (Organización), seleccione `My organization` (Mi organización) para conceder permisos a todas las cuentas de la organización de las que es miembro la cuenta actual. También puede elegir `Another organization` (Otra organización) y escribir el ID de esta. Al escribir el ID de organización, debe incluir el prefijo `o-`.

4. Elija Add (Agregar).
5. Repita estos pasos para añadir otras organizaciones o cuentas.

Para activar su cuenta para recibir eventos de otras cuentas de AWS mediante la AWS CLI

1. Para activar una cuenta de AWS específica para enviar eventos, ejecute el siguiente comando:

```
aws events put-permission --action events:PutEvents --statement-id MySid --principal SenderAccountID
```

Para habilitar una organización de AWS para enviar eventos, ejecute el siguiente comando:

```
aws events put-permission --action events:PutEvents --statement-id MySid --principal \* --condition '{"Type" : "StringEquals", "Key": "aws:PrincipalOrgID", "Value": "SenderOrganizationID"}'
```

Para activar todas las demás cuentas de AWS para enviar eventos, ejecute el siguiente comando:

```
aws events put-permission --action events:PutEvents --statement-id MySid --principal \*
```

Puede ejecutar `aws events put-permission` varias veces para conceder permisos tanto a las cuentas como a las organizaciones individuales de AWS, pero no puede especificar una cuenta y una organización individuales en un único comando.

2. Después de establecer los permisos para el bus de eventos predeterminado, puede utilizar opcionalmente el comando `describe-event-bus` para comprobar los permisos:

```
aws events describe-event-bus
```

Envío de eventos a otra cuenta de AWS

Para enviar eventos a otra cuenta, configure una regla de eventos de CloudWatch que tenga el bus de eventos predeterminado de AWS como destino. El bus de eventos predeterminado de esa cuenta receptora debe configurarse también para recibir eventos desde su cuenta.

Para enviar eventos desde su cuenta a otra cuenta de AWS mediante la consola

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create Rule.
3. En Event Source (Origen de eventos), elija Event Pattern (Patrón de eventos) y seleccione el nombre del servicio y los tipos de eventos que desea enviar a la otra cuenta.
4. Elija Add Target.
5. Para Objetivo, elija Bus de eventos en otro AWS account. En Account ID (ID de cuenta), escriba el ID de 12 dígitos de la cuenta de AWS a la que desea enviar eventos.
6. Se necesita un rol de IAM cuando esta cuenta remitente tiene permisos para enviar eventos porque la cuenta receptora concedió permisos a toda una organización.
 - Para crear un rol de IAM automáticamente, elija Create a new role for this specific resource (Crear un nuevo rol para este recurso específico).
 - De lo contrario, seleccione Use existing role (Usar rol existente). Elija un rol que ya tenga permisos suficientes para invocar la compilación. CloudWatch Events no concede permisos adicionales para el rol que seleccione.
7. En la parte inferior de la página, elija Configure Details.
8. Escriba un nombre y una descripción de la regla y seleccione Create Rule.

Para enviar eventos a otra cuenta de AWS mediante la AWS CLI

1. Si la cuenta remitente tiene permisos para enviar eventos porque forma parte de una organización de AWS a la que la cuenta receptora ha concedido permisos, la cuenta remitente también debe tener un rol con políticas que le permitan enviar eventos a la cuenta receptora. En este paso se explica cómo crear ese rol.

Si se concedió permiso a la cuenta remitente para enviar eventos mediante su ID de cuenta de AWS y no a través de una organización, este paso es opcional. Puede ir directamente al paso 2.

- a. Si se concedieron permisos a la cuenta remitente a través de una organización, cree el rol de IAM necesario. En primer lugar, cree un archivo denominado `assume-role-policy-document.json`, con el siguiente contenido:

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



```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "events.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
```

- b. Para crear el rol de , escriba el siguiente comando:

```
$ aws iam create-role \
--profile sender \
--role-name event-delivery-role \
--assume-role-policy-document file://assume-role-policy-document.json
```

- c. Cree un archivo denominado `permission-policy.json` con el siguiente contenido:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "events:PutEvents"
      ],
      "Resource": [
        "arn:aws:events:us-east-1:${receiver_account_id}:event-bus/default"
      ]
    }
  ]
}
```

- d. Escriba el siguiente comando para asociar esta política al rol:

```
$ aws iam put-role-policy \
--profile sender \
--role-name event-delivery-role \
--policy-name EventBusDeliveryRolePolicy \
--policy-document file://permission-policy.json
```

2. Utilice el comando `put-rule` para crear una regla que coincida con los tipos de eventos que se van a enviar a la otra cuenta.
3. Añada el bus de eventos predeterminado de la otra cuenta como destino de la regla.

Si se concedieron permisos a la cuenta remitente para enviar eventos por su ID de cuenta, no es necesario especificar un rol. Ejecute el siguiente comando :

```
aws events put-targets --rule NameOfRuleMatchingEventsToSend --targets
  "Id"="MyId", "Arn"="arn:aws:events:region:${ReceiverAccountID}:event-bus/default"
```

Si se concedieron permisos a la cuenta remitente para enviar eventos por su organización, especifique un rol, como en el ejemplo siguiente:

```
aws events put-targets --rule NameOfRuleMatchingEventsToSend --targets
  "Id"="MyId", "Arn"="arn:aws:events:region:${ReceiverAccountID}:event-bus/
default", "RoleArn"="arn:aws:iam:${sender_account_id}:role/event-delivery-role"
```

Escritura de reglas que coincidan con eventos de otra cuenta de AWS

Si su cuenta está configurada para recibir eventos de otras cuentas de AWS, puede escribir reglas que coincidan con esos eventos. Establezca el patrón de eventos de la regla para que coincida con los eventos que recibe de la otra cuenta.

A menos que especifique `account` en el patrón de eventos de una regla, cualquiera de las reglas de su cuenta, ya sean nuevas o existentes, que coincidan con los eventos que recibe de otras cuentas se activa en función de dichos eventos. Si recibe eventos de otra cuenta y desea que solamente se active una regla en ese patrón de eventos cuando se genere desde su propia cuenta, debe agregar `account` y especificar su propio ID de cuenta en el patrón de eventos de la regla.

Si configura su AWS para aceptar eventos de todos los AWS, le recomendamos encarecidamente que agregue `account` a cada regla de CloudWatch Events de su cuenta. Esto impide que las reglas de su cuenta se activen en eventos de cuentas desconocidas de AWS. Cuando especifique el campo `account` de la regla, puede especificar los ID de varias cuentas de AWS en dicho campo.

Para que se active una regla cuando se produzca un evento coincidente desde alguna cuenta de AWS a la que haya concedido permisos, no especifique `*` en el campo `account` de la regla. Si lo hace, no se encontrarán coincidencias de ningún evento, porque `*` no aparece nunca en el campo `account` de un evento. En lugar de ello, omita el campo `account` de la regla.

Para escribir una regla que coincida con eventos de otra cuenta mediante la consola

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Events, Create Rule.
3. En Event Source, seleccione Event Pattern y elija el nombre del servicio y los tipos de eventos con los que debe coincidir la regla.
4. Cerca de Event Pattern Preview, elija Edit.
5. En la ventana de edición, añada una línea `Account` que especifique cuáles son las cuentas de AWS que envían este evento con las que la regla debe coincidir. Por ejemplo, inicialmente, en la ventana de edición aparecía lo siguiente:

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ]
}
```

Añada lo siguiente para que la regla coincida con las notificaciones de volúmenes de EBS que envían las cuentas de AWS 123456789012 y 111122223333:

```
{
  "account": [
    "123456789012", "111122223333"
  ],
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ]
}
```

```
}
```

6. Después de editar el patrón de eventos, elija Save.
7. Termine de crear la regla de la forma habitual, definiendo uno o más destinos en su cuenta.

Para escribir una regla que coincida con eventos de otra cuenta de AWS mediante la AWS CLI

- Use el comando `put-rule`. En el campo `Account` del patrón de eventos de la regla, especifique el resto de cuentas de AWS con las que debe coincidir la regla. La siguiente regla de ejemplo coincide con los cambios en el estado de la instancia de Amazon EC2 en elAWS cuentas 123456789012 y 111122223333:

```
aws events put-rule --name "EC2InstanceStateChanges" --event-pattern "{\"account\":  
[\"123456789012\", \"111122223333\"],\"source\":[\"aws.ec2\"],\"detail-type\":[\"EC2  
Instance State-change Notification\"]}" --role-arn "arn:aws:iam::123456789012:role/  
MyRoleForThisRule"
```

Migrar una relación remitente-receptor para usar AWS Organizations

Si tiene una cuenta de remitente con permisos concedidos directamente a su ID de cuenta y ahora quiere revocar esos permisos y proporcionar a la cuenta de envío acceso mediante la concesión de permisos de acceso a una organización, debe adoptar algunos pasos adicionales. Estos pasos garantizan que los eventos de la cuenta del remitente pueden llegar a la cuenta del receptor. Esto se debe a que las cuentas a las que se concede permiso para enviar eventos a través de una organización también deben utilizar un rol de IAM para hacerlo.

Para añadir los permisos necesarios para migrar una relación remitente-receptor

1. En la cuenta remitente, cree un rol de IAM con políticas que lo habiliten para enviar eventos a la cuenta receptora.
 - a. Cree un archivo denominado `assume-role-policy-document.json`, con el siguiente contenido:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "events.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

- b. Para crear el rol de IAM, escriba el siguiente comando:

```
$ aws iam create-role \  
--profile sender \  
--role-name event-delivery-role \  
--assume-role-policy-document file://assume-role-policy-document.json
```

- c. Cree un archivo denominado `permission-policy.json` con el siguiente contenido:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "events:PutEvents"
      ],
      "Resource": [
        "arn:aws:events:us-east-1:${receiver_account_id}:event-bus/default"
      ]
    }
  ]
}
```

- d. Escriba el siguiente comando para asociar esta política al rol:

```
$ aws iam put-role-policy \
--profile sender \
--role-name event-delivery-role \
--policy-name EventBusDeliveryRolePolicy \
--policy-document file://permission-policy.json
```

2. Edite cada regla existente en la cuenta remitente que tenga el bus de eventos predeterminado de la cuenta receptora como destino. Edite la regla añadiendo el rol que ha creado en el paso 1 a la información de destino. Use el siguiente comando:

```
aws events put-targets --rule Rulename --targets
  "Id"="MyID", "Arn"="arn:aws:events:region:ReceiverAccountID:event-bus/
default", "RoleArn"="arn:aws:iam:${sender_account_id}:role/event-delivery-role"
```

3. En la cuenta del receptor, ejecute el siguiente comando para conceder permisos para las cuentas de la organización para enviar eventos a la cuenta del receptor:

```
aws events put-permission --action events:PutEvents --statement-id Sid-For-Organization
--principal \* --condition '{"Type" : "StringEquals", "Key": "aws:PrincipalOrgID",
"Value": "SenderOrganizationID"}'
```

Si lo prefiere, también puede revocar los permisos concedidos originalmente directamente a la cuenta del remitente:

```
aws events remove-permission --statement-id Sid-for-SenderAccount
```

Agregar eventos con PutEvents

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

La acción `PutEvents` envía a CloudWatch Events en una única solicitud. Para obtener más información, consulte [PutEvents](#) en la Referencia de la API Amazon CloudWatch Events y [put-events](#) en la AWS CLI Referencia de los comandos de la.

Cada solicitud `PutEvents` puede admitir un número limitado de entradas. Para obtener más información, consulte [Cuotas de eventos de CloudWatch \(p. 112\)](#). La operación `PutEvents` intenta procesar todas las entradas en el orden natural de la solicitud. Cada evento tiene un ID exclusivo que asigna el CloudWatch Events después de llamar a `PutEvents`.

El siguiente ejemplo de código Java envía dos eventos idénticos a CloudWatch Events:

```
PutEventsRequestEntry requestEntry = new PutEventsRequestEntry()
    .withTime(new Date())
    .withSource("com.mycompany.myapp")
    .withDetailType("myDetailType")
    .withResources("resource1", "resource2")
    .withDetail("{ \"key1\": \"value1\", \"key2\": \"value2\" }");

PutEventsRequest request = new PutEventsRequest()
    .withEntries(requestEntry, requestEntry);

PutEventsResult result = awsEventsClient.putEvents(request);

for (PutEventsResultEntry resultEntry : result.getEntries()) {
    if (resultEntry.getEventId() != null) {
        System.out.println("Event Id: " + resultEntry.getEventId());
    } else {
        System.out.println("Injection failed with Error Code: " +
            resultEntry.getErrorCode());
    }
}
```

El resultado `PutEvents` incluye una gama de entradas de respuesta. Cada entrada en la matriz de respuestas se correlaciona directamente con una entrada en la matriz de solicitudes siguiendo el orden natural, de arriba abajo de la solicitud y la respuesta. La matriz de respuesta `Entries` siempre incluye el mismo número de entradas que la matriz de solicitud.

Gestión de errores al utilizar PutEvents

De forma predeterminada, el error de entradas individuales en una solicitud no para el procesamiento de las siguientes entradas de la solicitud. Esto significa que una matriz Entradas de respuesta incluye tanto las entradas procesadas correctamente como las que no. Debe detectar las entradas procesadas sin éxito e incluirlas en una llamada siguiente.

Las entradas con resultado correcto incluyen el valor de ID y las entradas con resultado incorrecto incluyen los valores `ErrorCode` y `ErrorMessage`. El parámetro `ErrorCode` refleja el tipo de error. `ErrorMessage` proporciona más información detallada sobre el error. El ejemplo siguiente tiene tres entradas de resultados para una solicitud `PutEvents`. La segunda entrada ha generado un error y se refleja en la respuesta.

Ejemplo: Sintaxis de respuesta `PutEvents`

```
{
  "FailedEntryCount": 1,
  "Entries": [
    {
      "EventId": "11710aed-b79e-4468-a20b-bb3c0c3b4860"
    },
    {
      "ErrorCode": "InternalFailure",
      "ErrorMessage": "Internal Service Failure"
    },
    {
      "EventId": "d804d26a-88db-4b66-9eaf-9a11c708ae82"
    }
  ]
}
```

Las entradas que se procesan sin éxito se pueden incluir en las solicitudes `PutEvents` posteriores. En primer lugar, compruebe el parámetro `FailedRecordCount` en `PutEventsResult` para confirmar si se hay registros con error en la solicitud. En caso afirmativo, cada `Entry` que tenga un `ErrorCode` que no sea nulo se debe añadir a una solicitud posterior. Para un ejemplo de este tipo de controlador, consulte el siguiente código.

Ejemplo: Controlador de errores de `PutEvents`

```
PutEventsRequestEntry requestEntry = new PutEventsRequestEntry()
    .withTime(new Date())
    .withSource("com.mycompany.myapp")
    .withDetailType("myDetailType")
    .withResources("resource1", "resource2")
    .withDetail("{\"key1\": \"value1\", \"key2\": \"value2\" }");

List<PutEventsRequestEntry> putEventsRequestEntryList = new ArrayList<>();
for (int i = 0; i < 3; i++) {
    putEventsRequestEntryList.add(requestEntry);
}

PutEventsRequest putEventsRequest = new PutEventsRequest();
putEventsRequest.withEntries(putEventsRequestEntryList);
PutEventsResult putEventsResult = awsEventsClient.putEvents(putEventsRequest);

while (putEventsResult.getFailedEntryCount() > 0) {
    final List<PutEventsRequestEntry> failedEntriesList = new ArrayList<>();
    final List<PutEventsResultEntry> putEventsResultEntryList =
        putEventsResult.getEntries();
    for (int i = 0; i < putEventsResultEntryList.size(); i++) {
        final PutEventsRequestEntry putEventsRequestEntry =
            putEventsRequestEntryList.get(i);
        final PutEventsResultEntry putEventsResultEntry = putEventsResultEntryList.get(i);
        if (putEventsResultEntry.getErrorCode() != null) {
            failedEntriesList.add(putEventsRequestEntry);
        }
    }
    putEventsRequestEntryList = failedEntriesList;
    putEventsRequest.setEntries(putEventsRequestEntryList);
    putEventsResult = awsEventsClient.putEvents(putEventsRequest);
}
```

Envío de eventos con AWS CLI

Puede utilizar AWS CLI para enviar eventos personalizados. El siguiente ejemplo pone un evento personalizado en CloudWatch Events:

```
aws events put-events \  
--entries '[{"Time": "2016-01-14T01:02:03Z", "Source": "com.mycompany.myapp", "Resources":  
["resource1", "resource2"], "DetailType": "myDetailType", "Detail": "{ \"key1\":  
\"value1\", \"key2\": \"value2\" }"}]'
```

También puede crear un archivo (por ejemplo `entries.json`) como el siguiente:

```
[  
  {  
    "Time": "2016-01-14T01:02:03Z",  
    "Source": "com.mycompany.myapp",  
    "Resources": [  
      "resource1",  
      "resource2"  
    ],  
    "DetailType": "myDetailType",  
    "Detail": "{ \"key1\": \"value1\", \"key2\": \"value2\" }"  
  }  
]
```

Puede utilizar AWS CLI para leer las entradas procedentes de este archivo y enviar eventos. En el símbolo del sistema, escriba:

```
aws events put-events --entries file://entries.json
```

Cálculo de tamaños de entrada de evento PutEvents

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede inyectar eventos personalizados en CloudWatch Events con la herramienta `PutEventsaction`. Puede inyectar varios eventos utilizando la acción `PutEvents` siempre que el tamaño total de entrada sea inferior a 256 KB. Puede calcular el tamaño de entrada de eventos de antemano siguiendo los pasos que se indican a continuación. A continuación, puede incluir en un lote varios eventos en una única solicitud para mayor eficacia.

Note

La restricción de tamaño se impone en la entrada. Aunque la entrada tenga un tamaño inferior a la restricción, eso no significa que el evento de CloudWatch Events sea inferior a este tamaño. Al contrario, el tamaño del evento será siempre mayor que el tamaño de la entrada por los

caracteres necesarios y las claves de la representación JSON del evento. Para obtener más información, consulte [Patrones de eventos de CloudWatch](#) (p. 39).

El tamaño `PutEventsRequestEntry` se calcula del siguiente modo:

- Si se especifica el parámetro `Time`, se mide como 14 bytes.
- Los parámetros `Source` y `DetailType` se miden como el número de bytes para sus formatos cifrados con UTF-8.
- Si se especifica el parámetro `Detail`, se mide como el número de bytes para su formato cifrado con UTF-8.
- Si se especifica el parámetro `Resources`, cada entrada se mide como el número de bytes para sus formatos cifrados con UTF-8.

El siguiente ejemplo de código Java calcula el tamaño de un objeto `PutEventsRequestEntry` dado:

```
int getSize(PutEventsRequestEntry entry) {
    int size = 0;
    if (entry.getTime() != null) {
        size += 14;
    }
    size += entry.getSource().getBytes(StandardCharsets.UTF_8).length;
    size += entry.getDetailType().getBytes(StandardCharsets.UTF_8).length;
    if (entry.getDetail() != null) {
        size += entry.getDetail().getBytes(StandardCharsets.UTF_8).length;
    }
    if (entry.getResources() != null) {
        for (String resource : entry.getResources()) {
            if (resource != null) {
                size += resource.getBytes(StandardCharsets.UTF_8).length;
            }
        }
    }
    return size;
}
```


Uso de CloudWatch Events con los puntos de enlace de la VPC

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar su AWS, puede establecer una conexión privada entre su VPC y CloudWatch Events. Puede utilizar esta conexión para habilitar CloudWatch Events (Eventos de CloudWatch) y comunicarse con sus recursos en la VPC sin pasar por la Internet pública.

Amazon VPC es un AWS Servicio de que se puede utilizar para lanzar AWS recursos de en una red virtual que usted defina. Con una VPC, puede controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red. Para conectar su VPC a CloudWatch Events, debe definir un punto de enlace de la VPC de la interfaz para CloudWatch Events. Este tipo de punto de enlace le permite conectar la VPC a los servicios de AWS. El punto de enlace ofrece conectividad escalable de confianza con CloudWatch Events sin necesidad de utilizar una gateway de Internet, una instancia de conversión de las direcciones de red (NAT) o una conexión de VPN. Para obtener más información, consulte [Qué es Amazon VPC](#) en la Guía del usuario de Amazon VPC.

Los puntos de enlace de la VPC de tipo interfaz utilizan la tecnología de AWS PrivateLink, una tecnología de AWS que permite la comunicación privada entre los servicios de AWS mediante una interfaz de red elástica con direcciones IP privadas. Para obtener más información, consulte [Nuevo —AWS PrivateLink para AWS Servicios](#).

Los siguientes pasos son para usuarios de Amazon VPC. Para obtener más información, consulte [Introducción](#) en la Guía del usuario de Amazon VPC.

Availability

Actualmente, CloudWatch Events admite puntos de conexión de la VPC en las regiones siguientes:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)

- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- South America (São Paulo)

Creación de un punto de enlace de la VPC para eventos de CloudWatch

Para comenzar a utilizar CloudWatch Events con su VPC, cree un punto de enlace de la VPC de tipo interfaz para CloudWatch Events. El nombre del servicio que debe elegir es región com.amazonaws.**región**.events. Para obtener más información, consulte [Creación de un punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

No necesita cambiar la configuración de CloudWatch Events. CloudWatch Events llama a otros AWS Servicios de con puntos de conexión públicos o puntos de conexión de la VPC de tipo interfaz privados, lo que esté en uso. Por ejemplo, si crea un punto de enlace de la VPC de tipo interfaz para CloudWatch Events y ya tiene una regla de CloudWatch Events que envía notificaciones a Amazon SNS cuando se activa, las notificaciones comienzan a circular a través del punto de enlace de la VPC de tipo interfaz.

Control del acceso al punto de enlace de la VPC de CloudWatch Events

Una política de punto de enlace de la VPC es una política de recursos de IAM que puede asociar a un punto de enlace cuando crea o modifica el punto de enlace. Si no asocia una política al crear un punto de enlace, se asociará automáticamente una política predeterminada que conceda acceso completo al servicio. Una política de punto de enlace no anula ni sustituye a las políticas de usuario de IAM o las políticas específicas de los servicios. Se trata de una política independiente para controlar el acceso desde el punto de enlace al servicio especificado.

Las políticas de punto de conexión deben escribirse en formato JSON.

Para obtener más información, consulte [Controlar el acceso a servicios con puntos de enlace de la VPC](#) en la Guía del usuario de Amazon VPC.

A continuación, se muestra un ejemplo de una política de punto de enlace para CloudWatch Events. Esta política permite los usuarios que se conectan a CloudWatch Events a través de la VPC enviar eventos a CloudWatch Events y les impide realizar otras acciones de CloudWatch Events.

```
{
  "Statement": [
    {
      "Sid": "PutOnly",
      "Principal": "*",
      "Action": [
        "events:PutEvents"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

}

Para modificar la política de punto de enlace de la VPC para CloudWatch Events

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Endpoints (Puntos de enlace).
3. Si todavía no ha creado el punto de enlace para CloudWatch Events, elija Creación de un punto de enlace. A continuación, seleccione com.amazonaws.**región**.events y elija Create endpoint (Crear punto de enlace).
4. Seleccione el punto de enlace com.amazonaws.**región**.events y elija la pestaña Policy (Política) en la mitad inferior de la pantalla.
5. Elija Edit Policy (Editar política) y realice los cambios en la política.

Monitorización del uso con métricas de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

CloudWatch Events envía métricas a Amazon CloudWatch cada minuto.

Métricas de CloudWatch Events

El espacio de nombres de `AWS/Events` incluye las siguientes métricas.

En todas estas métricas, se utiliza el recuento (Count) como unidad. Por lo tanto, las estadísticas más útiles son Sum y SampleCount.

Métrica	Descripción
<code>DeadLetterInvocations</code>	<p>Mide el número de veces que no se invoca el destino de una regla en respuesta a un evento. Esto incluye las invocaciones que harían que se activara la misma regla de nuevo, lo que provocaría un bucle infinito.</p> <p>Dimensiones válidas: RuleName</p> <p>Unidades: Recuento</p>
<code>Invocations</code>	<p>Mide el número de veces que se invoca un destino para una regla en respuesta a un evento. Incluye las llamadas que se realizaron correctamente e incorrectamente, pero no incluye los intentos limitados o repetidos hasta que producen definitivamente un error. No incluye las <code>DeadLetterInvocations</code>.</p> <p>Note</p> <p>Amazon CloudWatch Events solo envía esta métrica a CloudWatch si tiene un valor distinto de cero.</p> <p>Dimensiones válidas: RuleName</p> <p>Unidades: Recuento</p>
<code>FailedInvocations</code>	<p>Mide el número de invocaciones que produjeron definitivamente un error. No incluye las invocaciones que se reintentaron o que se realizaron correctamente tras un reintento. Tampoco incluye las invocaciones con errores que se cuentan en <code>DeadLetterInvocations</code>.</p> <p>Dimensiones válidas: RuleName</p> <p>Unidades: Recuento</p>

Métrica	Descripción
<code>TriggeredRules</code>	Mide el número de reglas desencadenadas correspondientes a cualquier evento. Dimensiones válidas: <code>RuleName</code> Unidades: Recuento
<code>MatchedEvents</code>	Mide el número de eventos correspondientes a cualquier regla. Dimensiones válidas: Ninguna Unidades: Recuento
<code>ThrottledRules</code>	Mide el número de reglas desencadenadas que se limitaron. Dimensiones válidas: <code>RuleName</code> Unidades: Recuento

Dimensiones de las métricas de eventos de CloudWatch

Las métricas de CloudWatch Events tienen una dimensión, que se indica a continuación.

Dimensión	Descripción
<code>RuleName</code>	Filtra las métricas disponibles por nombre de regla.

Reglas administradas por Amazon CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Otros AWS Los servicios de pueden crear y administrar reglas de CloudWatch Events en su AWS Cuenta de que se necesitan para determinadas funciones de dichos servicios. Se denominan reglas administradas.

Si un servicio crea una regla administrada, también puede crear una política de IAM que conceda permisos a dicho servicio para crear la regla. Las políticas de IAM creadas de esta manera se asignan de forma reducida con permisos de nivel de recursos, para permitir la creación solo de las reglas necesarias.

Puede eliminar reglas administradas mediante la opción Force delete (Forzar eliminación). Hágalo así únicamente si está seguro de que el otro servicio ya no necesita la regla. De lo contrario, eliminar una regla administrada hace que las características que dependen de él dejen de funcionar.

Seguridad para eventos de Amazon CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Para obtener información sobre la seguridad de CloudWatch Events de [Seguridad en Amazon EventBridge](#).

Etiquetado de sus recursos de Amazon CloudWatch Events

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Una etiqueta es un atributo personalizado que usted o AWS asignan a un recurso de AWS. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un campo opcional denominado valor de etiqueta (por ejemplo, `111122223333` o `Production`). Omitir el valor de etiqueta es lo mismo que usar una cadena vacía. Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

Las etiquetas le ayudan a hacer lo siguiente:

- Identificar y organizar sus recursos de AWS. Muchos servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, podría asignar la misma etiqueta a una regla de CloudWatch Events que se asigne a una instancia EC2.
- Realizar un seguimiento de los costos de AWS. Estas etiquetas se activan en el panel de AWS Billing and Cost Management. AWS usa las etiquetas para clasificar los costos y enviar un informe mensual de asignación de costos. Para obtener más información, consulte [Uso de etiquetas de asignación de costos](#) en la [Guía del usuario de AWS Billing and Cost Management](#).

En las siguientes secciones se ofrece más información acerca de las etiquetas de CloudWatch Events.

Recursos admitidos en eventos de CloudWatch

Los siguientes recursos de CloudWatch Events admiten el etiquetado:

- Reglas

Para obtener información acerca de cómo añadir y administrar etiquetas, consulte [Administración de etiquetas \(p. 107\)](#).

Administración de etiquetas

Las etiquetas se componen de las propiedades `value` y `key` de un recurso. Puede utilizar la consola de CloudWatch, la consola de AWS CLI o la API de CloudWatch Events para agregar, editar o eliminar los

valores de estas propiedades. Para obtener información sobre cómo trabajar con etiquetas, consulte lo siguiente:

- [TagResource](#), [UntagResource](#), y [ListTagsForResource](#) en la Referencia de API de Amazon CloudWatch Events
- [tag-resource](#), [untag-resource](#), y [list-tags-for-resource](#) en la Referencia de la CLI de Amazon CloudWatch
- [Uso de Tag Editor](#) en la Guía del usuario de Resource Groups

Convenciones de nomenclatura y uso de las etiquetas

Las siguientes convenciones básicas de nomenclatura y uso se aplican al uso de etiquetas con recursos de CloudWatch Events:

- Cada recurso puede tener un máximo de 50 etiquetas.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- La longitud máxima de la clave de etiqueta es de 128 caracteres Unicode en UTF-8.
- La longitud máxima del valor de etiqueta es de 256 caracteres Unicode en UTF-8.
- Los caracteres permitidos son letras, números y espacios representables en UTF-8, además de los siguientes caracteres: . : + = @ _ / - (guion).
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Como práctica recomendada, decida una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos los tipos de recursos. Por ejemplo, decida si se va a utilizar `Costcenter`, `costcenter` o `CostCenter` y utilice la misma convención para todas las etiquetas. Procure no utilizar etiquetas similares con un tratamiento de mayúsculas y minúsculas incoherente.
- El prefijo `aws:` está prohibido para las etiquetas, ya que está reservado para su uso por parte de AWS. Las claves y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas que tengan este prefijo no cuentan para la cuota de etiquetas por recurso.

Registro de llamadas al API de Amazon CloudWatch Events con AWS CloudTrail

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Amazon CloudWatch Events se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un usuario de AWS en CloudWatch Events. CloudTrail captura las llamadas a la API realizadas por o en nombre de su AWS account. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de CloudWatch y las llamadas de código a las operaciones de la API de CloudWatch Events. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de CloudWatch. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a CloudWatch Events, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información sobre CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la [AWS CloudTrail Guía del usuario](#).

Temas

- [Información de eventos de CloudWatch en CloudTrail \(p. 109\)](#)
- [Ejemplo: Entradas de archivos de registro de CloudWatch \(p. 110\)](#)

Información de eventos de CloudWatch en CloudTrail

CloudTrail está habilitado en su AWS al crearla. Cuando se produce una actividad de eventos compatible en CloudWatch Events, dicha actividad se registra en un evento de CloudTrail junto con otros eventos AWS de servicios de en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Ver eventos con el historial de eventos de CloudTrail](#).

Para mantener un registro continuo de los eventos de la AWS, incluidos los eventos de CloudWatch Events, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la AWS y entrega los archivos de registro al bucket de Amazon S3 que se especifique. También puede configurar otros dispositivos de AWS para analizar en profundidad

y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [Consulte Servicios e integraciones compatibles con CloudTrail.](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas](#)

CloudWatch Events admite el registro de las siguientes acciones como eventos en los archivos de log de CloudTrail:

- [DeleteRule](#)
- [DescribeEventBus](#)
- [DescribeRule](#)
- [DisableRule](#)
- [EnableRule](#)
- [ListRuleNamesByTarget](#)
- [ListRules](#)
- [ListTargetsByRule](#)
- [PutPermission](#)
- [PutRule](#)
- [PutTargets](#)
- [RemoveTargets](#)
- [TestEventPattern](#)

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#).

Ejemplo: Entradas de archivos de registro de CloudWatch

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon S3 que se especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

La siguiente entrada de archivo de registro de CloudTrail muestra un usuario que ha llamado a CloudWatch EventsPutRuleaction.

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-11-17T23:56:15Z"
      }
    }
  },
  "eventTime": "2015-11-18T00:11:28Z",
  "eventSource": "events.amazonaws.com",
  "eventName": "PutRule",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS CloudWatch Console",
  "requestParameters": {
    "description": "",
    "name": "cttest2",
    "state": "ENABLED",
    "eventPattern": "{\"source\": [\"aws.ec2\"], \"detail-type\": [\"EC2 Instance State-change Notification\"]}",
    "scheduleExpression": ""
  },
  "responseElements": {
    "ruleArn": "arn:aws:events:us-east-1:123456789012:rule/cttest2"
  },
  "requestID": "e9caf887-8d88-11e5-a331-3332aa445952",
  "eventID": "49d14f36-6450-44a5-a501-b0fdcdfaeb98",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-10-07",
  "recipientAccountId": "123456789012"
}
```

Cuotas de eventos de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Amazon CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Para obtener información sobre las cuotas de servicio de CloudWatch Events y EventBridge, consulte [Cuotas de Amazon EventBridge](#).

Para obtener más información, consulte los siguientes temas.

- [Amazon EventBridge](#)
- [Service Quotas de EventBridge](#)
- [Referencia del API de Amazon EventBridge](#)

Solución de problemas de CloudWatch

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. Los eventos de CloudWatch y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge proporciona más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

Puede utilizar los pasos de esta sección para solucionar problemas de CloudWatch.

Temas

- [Mi regla se ha activado pero no se ha invocado mi función de Lambda \(p. 113\)](#)
- [Acabo de crear o modificar una regla, pero no coincidía con un evento de prueba \(p. 114\)](#)
- [Mi regla no se activa automáticamente en el momento especificado en ScheduleExpression \(p. 115\)](#)
- [Mi regla no se activó a la hora esperada \(p. 115\)](#)
- [Mi regla coincide con las llamadas al API de IAM pero no se ha activado \(p. 115\)](#)
- [Mi regla no funciona, ya que el rol de IAM asociado a la regla no se tiene en cuenta cuando se activa la regla \(p. 116\)](#)
- [He creado una regla con un EventPattern que se supone que coincide con un recurso, pero no veo ningún evento que coincida con la regla \(p. 116\)](#)
- [La entrega de mi evento al destino ha sufrido un retraso \(p. 116\)](#)
- [Algunos eventos no se entregaron en mi destino \(p. 116\)](#)
- [Mi regla se activó más de una vez en respuesta a un único evento. ¿Qué garantía ofrece CloudWatch Events para activar reglas o enviar eventos a los destinos? \(p. 117\)](#)
- [Cómo evitar bucles infinitos \(p. 117\)](#)
- [Mis eventos no se entregan en la cola de de Amazon SQS de destino \(p. 117\)](#)
- [Mi regla se activa pero no veo ningún mensaje publicado en mi tema de Amazon SNS \(p. 118\)](#)
- [Mi tema de Amazon SNS sigue teniendo permisos para eventos de CloudWatch incluso después de haber eliminado la regla asociada al tema de Amazon SNS \(p. 119\)](#)
- [Qué claves de condición de IAM puedo utilizar con CloudWatch Events \(p. 119\)](#)
- [Cómo puedo saber si las reglas de CloudWatch Events están rotas \(p. 119\)](#)

Mi regla se ha activado pero no se ha invocado mi función de Lambda

Asegúrese de tener establecido los permisos adecuados para su función de Lambda. Ejecute el comando siguiente AWS CLI (sustituya el nombre de la función por su función de y utilice el `AWSRegion` en la que se encuentra su función):

```
aws lambda get-policy --function-name MyFunction --region us-east-1
```

Debería ver un resultado similar a este:

```
{
  "Policy": "{\"Version\":\"2012-10-17\",
    \"Statement\":[
      {\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:events:us-
east-1:123456789012:rule/MyRule\"}},
      \"Action\":\"lambda:InvokeFunction\",
      \"Resource\":\"arn:aws:lambda:us-east-1:123456789012:function:MyFunction\",
      \"Effect\":\"Allow\",
      \"Principal\":{\"Service\":\"events.amazonaws.com\"},
      \"Sid\":\"MyId\"}
    ]
  },
  \"Id\":\"default\"}
}
```

Si ve lo siguiente:

```
A client error (ResourceNotFoundException) occurred when calling the GetPolicy operation:
The resource you requested does not exist.
```

O si ve el resultado, pero no puede localizar `events.amazonaws.com` como entidad de confianza en la política, ejecute el siguiente comando:

```
aws lambda add-permission \
--function-name MyFunction \
--statement-id MyId \
--action 'lambda:InvokeFunction' \
--principal events.amazonaws.com \
--source-arn arn:aws:events:us-east-1:123456789012:rule/MyRule
```

Note

Si la política es incorrecta, también puede editar la regla en la consola de CloudWatch Events eliminando y, a continuación, volviéndola a añadir a la regla. La consola de CloudWatch establecerá los permisos adecuados en el destino.

Si utiliza un alias o versión de Lambda específica, debe añadir el `--qualifier` parámetro de `aws lambda get-policy` y `aws lambda add-permission` comandos.

```
aws lambda add-permission \
--function-name MyFunction \
--statement-id MyId \
--action 'lambda:InvokeFunction' \
--principal events.amazonaws.com \
--source-arn arn:aws:events:us-east-1:123456789012:rule/MyRule
--qualifier alias or version
```

Otra razón por la que la función Lambda podría producir un error de activación es si la política que aparece cuando se ejecuta `get-policy` contiene `SourceAccount` field. Una configuración `SourceAccount` evita que CloudWatch Events pueda invocar la función.

Acabo de crear o modificar una regla, pero no coincidía con un evento de prueba

Al realizar un cambio en una regla o en sus destinos, los eventos entrantes podrían no comenzar o parar de inmediato la asignación a reglas nuevas o actualizadas. Espere un breve período de tiempo para que

los cambios surtan efecto. Si, después de este breve período, los eventos todavía no se asignan, también puede comprobar las métricas de CloudWatch para la regla como `TriggeredRules`, `Invocations`, y `FailedInvocations` Para depuración adicional. Para obtener más información sobre estas métricas, consulte [Dimensiones y métricas de Amazon CloudWatch Events](#) en la Guía del usuario de Amazon CloudWatch.

Si la regla se dispara por un evento de un servicio de AWS, también puede utilizar la acción `TestEventPattern` para probar el patrón de eventos de la regla con un evento de prueba para asegurarse de que el patrón de eventos de la configuración se ha establecido correctamente. Para obtener más información, consulte `TestEventPattern` en la Referencia al API de Amazon CloudWatch Events.

Mi regla no se activa automáticamente en el momento especificado en ScheduleExpression

`ScheduleExpressions` están en UTC. Asegúrese de que ha establecido la programación para que la regla se active automáticamente en la zona horaria UTC. Si la expresión `ScheduleExpression` es correcta siga, a continuación, los pasos indicados en [Acabo de crear o modificar una regla, pero no coincidía con un evento de prueba](#) (p. 114).

Mi regla no se activó a la hora esperada

CloudWatch Events no admite la configuración a una hora de inicio exacta cuando se crea una regla para ejecutarla en cada periodo de tiempo. La cuenta atrás hasta la hora de ejecución comienza en cuanto se crea la regla.

Puede utilizar una expresión Cron para invocar destinos a una hora especificada. Por ejemplo, puede utilizar una expresión Cron para crear una regla que se activa cada cuatro horas exactamente en el minuto 0. En la consola de CloudWatch, usaría la expresión cron `0 0/4 * * ? *`, y con el AWS CLI usarías la expresión `cron(0 0/4 * * ? *)`. Por ejemplo, para crear una regla denominada `TestRule` que se activa cada cuatro horas utilizando la AWS CLI escribiría lo siguiente en el símbolo del sistema:

```
aws events put-rule --name TestRule --schedule-expression 'cron(0 0/4 * * ? *)'
```

Puede utilizar la expresión Cron `0/5 * * * ? *` para activar una regla cada cinco minutos. Por ejemplo:

```
aws events put-rule --name TestRule --schedule-expression 'cron(0/5 * * * ? *)'
```

CloudWatch Events no proporciona precisión de segundo nivel en expresiones de programación. La mejor resolución al utilizar una expresión Cron es un minuto. Debido a la naturaleza distribuida de los eventos de CloudWatch y los servicios de destino, el retraso entre el momento en que la regla programada se activa y el momento en que el servicio de destino realiza la ejecución del recurso de destino puede ser de varios segundos. La regla programada se activará dentro de ese minuto, pero no en el segundo 0 preciso.

Mi regla coincide con las llamadas al API de IAM pero no se ha activado

El servicio de IAM solo está disponible en la región EE. UU. Este (Norte de Virginia), por tanto cualquier AWS Los eventos de llamada al API desde IAM solo están disponibles en esa región.

Para obtener más información, consulte [Ejemplos de eventos de CloudWatch Events de servicios admitidos](#) (p. 44).

Mi regla no funciona, ya que el rol de IAM asociado a la regla no se tiene en cuenta cuando se activa la regla

Los roles de IAM para reglas solo se utilizan para eventos relacionados con flujos de Kinesis. Para funciones de Lambda y temas de Amazon SNS, debe proporcionar permisos basados en recursos.

Asegúrese de que los puntos de enlace regionales de AWS STS estén habilitados. CloudWatch Events habla con el AWS STS para asumir el rol de IAM que ha proporcionado. Para obtener más información, consulte [Activación y desactivación de AWS STS en una región](#) en la Guía del usuario de IAM.

He creado una regla con un EventPattern que se supone que coincide con un recurso, pero no veo ningún evento que coincida con la regla

La mayoría de los servicios en AWS tratan los dos puntos (:) o la barra diagonal (/) como el mismo carácter en los nombres de recursos de Amazon (ARN). Sin embargo, CloudWatch Events utiliza una coincidencia exacta en las reglas y los patrones de eventos. Asegúrese de usar los caracteres de ARN correctos cuando cree patrones de eventos, de modo que se ajusten a la sintaxis de ARN del evento de la correspondencia.

Además, no todos los eventos tienen datos en el campo de recursos (como los eventos de llamada API de CloudTrail).

La entrega de mi evento al destino ha sufrido un retraso

CloudWatch Events intenta enviar un evento a un destino durante un máximo de 24 horas, excepto en aquellos casos en que el recurso de destino esté restringido. El primer intento se realiza en cuanto el evento llega en el flujo de transmisión. No obstante, si el servicio de destino está teniendo problemas, CloudWatch Events reprograma automáticamente otra entrega en el futuro. Si han transcurrido 24 horas desde la llegada del evento, no se programan más intentos y `FailedInvocations` se publica en CloudWatch. Le recomendamos que cree una alarma de CloudWatch en `FailedInvocations` Métrica de.

Algunos eventos no se entregaron en mi destino

Si un destino de una regla de CloudWatch Events está restringido durante un tiempo prolongado, es posible que CloudWatch Events no pueda reintentar la entrega. Por ejemplo, si el destino no está

aprovisionado para gestionar el tráfico de eventos entrantes y el servicio de destino está limitado a las solicitudes que realiza CloudWatch Events realiza en su nombre, es posible que CloudWatch Events no reintente la entrega.

Mi regla se activó más de una vez en respuesta a un único evento. ¿Qué garantía ofrece CloudWatch Events para activar reglas o enviar eventos a los destinos?

En casos excepcionales, la misma regla se puede activar más de una vez para un solo evento o tiempo programado, o el mismo destino se puede invocar más de una vez para una regla activada determinada.

Cómo evitar bucles infinitos

En CloudWatch Events es posible crear reglas que producen bucles infinitos, en los que una regla se activa repetidamente. Por ejemplo, una regla puede detectar que las ACL han cambiado en un bucket de S3 y activar software para cambiarlas al estado deseado. Si la regla no se ha escrito minuciosamente, un nuevo cambio de las ACL vuelve a activar la regla, lo que crea un bucle infinito.

Para evitarlo, escriba las reglas de modo que las acciones ya desencadenadas no vuelvan a activar una misma regla. Por ejemplo, la regla puede activarse solo si las ACL tienen un estado incorrecto, en lugar de después de cualquier cambio.

Un bucle infinito puede generar cargos superiores a los esperados rápidamente. Le recomendamos que utilice la función de presupuestos, que le avisa cuando los cargos superan la cuota especificada. Para obtener más información, consulte [Gestión de costos con presupuestos](#).

Mis eventos no se entregan en la cola de de Amazon SQS de destino

La cola de Amazon SQS podría estar cifrada. Si crea una regla con una cola de Amazon SQS cifrada como destino, debe tener incluida la siguiente sección en su política de claves de KMS para que el evento se envíe correctamente a laencryptedqueue.

```
{
    "Sid": "Allow CWE to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "events.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

Mi regla se activa pero no veo ningún mensaje publicado en mi tema de Amazon SNS

Asegúrese de tener establecido el permiso adecuado para su tema de Amazon SNS. Ejecute el comando siguiente AWS CLI (sustituya el tema de ARN por su tema y utilice el AWS Región en la que se encuentra el tema):

```
aws sns get-topic-attributes --region us-east-1 --topic-arn "arn:aws:sns:us-east-1:123456789012:MyTopic"
```

Debería ver unos atributos de política similares a los siguientes:

```
{"Version\":\"2012-10-17\",
 \"Id\":\"__default_policy_ID\",
 \"Statement\":[{\"Sid\":\"__default_statement_ID\",
 \"Effect\":\"Allow\",
 \"Principal\":{\"AWS\":\"*\"},
 \"Action\":[\"SNS:Subscribe\",
 \"SNS:ListSubscriptionsByTopic\",
 \"SNS>DeleteTopic\",
 \"SNS:GetTopicAttributes\",
 \"SNS:Publish\",
 \"SNS:RemovePermission\",
 \"SNS:AddPermission\",
 \"SNS:Receive\",
 \"SNS:SetTopicAttributes\"],
 \"Resource\":\"arn:aws:sns:us-east-1:123456789012:MyTopic\",
 \"Condition\":{\"StringEquals\":{\"AWS:SourceOwner\":\"123456789012\"}},{\"Sid\":
 \"Allow_Publish_Events\",
 \"Effect\":\"Allow\",
 \"Principal\":{\"Service\":\"events.amazonaws.com\"},
 \"Action\":\"sns:Publish\",
 \"Resource\":\"arn:aws:sns:us-east-1:123456789012:MyTopic\"}]}
```

Si ve una política similar a la siguiente, solo tiene el conjunto de políticas predeterminado:

```
{"Version\":\"2008-10-17\",
 \"Id\":\"__default_policy_ID\",
 \"Statement\":[{\"Sid\":\"__default_statement_ID\",
 \"Effect\":\"Allow\",
 \"Principal\":{\"AWS\":\"*\"},
 \"Action\":[\"SNS:Subscribe\",
 \"SNS:ListSubscriptionsByTopic\",
 \"SNS>DeleteTopic\",
 \"SNS:GetTopicAttributes\",
 \"SNS:Publish\",
 \"SNS:RemovePermission\",
 \"SNS:AddPermission\",
 \"SNS:Receive\",
 \"SNS:SetTopicAttributes\"],
 \"Resource\":\"arn:aws:sns:us-east-1:123456789012:MyTopic\",
 \"Condition\":{\"StringEquals\":{\"AWS:SourceOwner\":\"123456789012\"}}}]}
```

Si no ve `events.amazonaws.com` con el permiso `Publish` en la política, utilice la AWS CLI para establecer el atributo de la política de temas.

Copie la política actual y agregue la siguiente instrucción a la lista de instrucciones:

```
{\"Sid\":\"Allow_Publish_Events\",
```

Amazon CloudWatch Events Guía del usuario
Mi tema de Amazon SNS sigue teniendo permisos
para eventos de CloudWatch incluso después de haber
eliminado la regla asociada al tema de Amazon SNS

```
\ "Effect\" : \"Allow\" , \"Principal\" : { \"Service\" : \"events.amazonaws.com\" } ,  
  \"Action\" : \"sns:Publish\" ,  
  \"Resource\" : \"arn:aws:sns:us-east-1:123456789012:MyTopic\" }
```

La nueva política debería tener un aspecto similar al de la política que se describió anteriormente.

Establezca los atributos del tema a través de AWS CLI:

```
aws sns set-topic-attributes --region us-east-1 --topic-arn "arn:aws:sns:us-  
east-1:123456789012:MyTopic" --attribute-name Policy --attribute-value NEW_POLICY_STRING
```

Note

Si la política es incorrecta, también puede editar la regla en la consola de CloudWatch Events eliminando y, a continuación, volviéndola a añadir a la regla. CloudWatch Events establece los permisos adecuados en el destino.

Mi tema de Amazon SNS sigue teniendo permisos para eventos de CloudWatch incluso después de haber eliminado la regla asociada al tema de Amazon SNS

Al crear una regla con Amazon SNS como destino, CloudWatch Events añade el permiso a su tema de Amazon SNS en su nombre. Si elimina la regla poco después de crearla, CloudWatch Events podría no poder eliminar el permiso de su tema de Amazon SNS. Si esto ocurre, puede eliminar el permiso del tema mediante la [Atributos de tema de configuración de Amazon SNS](#) Comando de.

Qué claves de condición de IAM puedo utilizar con CloudWatch Events

CloudWatch Events admite [AWS Claves de condición generales](#) (consulte [Claves disponibles](#) en la Guía del usuario de IAM), además de las siguientes claves de condición específicas del servicio.

Cómo puedo saber si las reglas de CloudWatch Events están rotas

Puede utilizar la siguiente alarma para que le avise cuando las reglas de CloudWatch Events estén rotas.

Para crear una alarma que avise cuando las reglas estén rotas

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija Create Alarm (Crear alarma). En el panel CloudWatch Metrics by Category, seleccione Events Metrics.
3. En la lista de métricas, seleccione FailedInvocations.

4. Encima del gráfico, seleccione **Statistic**, **Sum**.
5. En **Period**, elija un valor; por ejemplo, 5 minutos. Seleccione **Next** (Siguiente).
6. En **Alarm Threshold**, en **Name**, escriba un nombre único para la alarma; por ejemplo, **myFailedRules**. En **Description**, escriba una descripción de la alarma; por ejemplo, Reglas que no proporcionan eventos a los destinos.
7. En **is**, seleccione **>=** y **1**. En **for**, escriba **10**.
8. En **Actions** (Acciones), en **Whenever this alarm** (Siempre que esta alarma), elija **State is ALARM** (El estado es ALARMA).
9. Para **Enviar notificación a**Para, seleccione un tema de Amazon SNS existente o cree uno nuevo. Para crear un nuevo tema de , elija **New list**. Escriba un nombre para el nuevo tema de Amazon SNS, por ejemplo: **MyFailedRules**.
10. En **Email list**, escriba una lista separada por comas con las direcciones de correo electrónico a las que se van a enviar notificaciones cuando la alarma cambie al estado **ALARM**.
11. Elija **Create Alarm** (Crear alarma).

Historial de revisión

Note

Amazon EventBridge es la forma preferida de administrar sus eventos. CloudWatch Events y EventBridge son el mismo servicio subyacente y la misma API, pero EventBridge ofrece más funciones. Los cambios que realice en CloudWatch o EventBridge aparecerán en cada consola. Para obtener más información, consulte [Amazon EventBridge](#).

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del usuario de Eventos de CloudWatch a partir de junio de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

update-history-change	update-history-description	update-history-date
Compatibilidad con el etiquetado (p. 121)	Ahora puede etiquetar algunos recursos de CloudWatch Events. Para obtener más información, consulte Recursos para Amazon CloudWatch Events en la Guía del usuario de Amazon CloudWatch Events.	21 de marzo de 2019
Compatibilidad con los puntos de enlace de la VPC de Amazon (p. 121)	A partir de ahora, puede establecer una conexión privada entre su VPC y CloudWatch Events. Para obtener más información, consulte Uso de eventos de CloudWatch con los puntos de enlace de la VPC en la Guía del usuario de Amazon CloudWatch Events.	28 de junio de 2018

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de Amazon CloudWatch Events.

Cambio	Descripción	Fecha de la versión
CodeBuild como un objetivo	Se ha agregado CodeBuild como destino de las reglas de evento. Para obtener más información, consulte Tutorial: Programar compilaciones automatizadas con CodeBuild (p. 32) .	13 de diciembre de 2017
AWS Batch como destino	Se agregó AWS Batch como destino de las reglas de evento. Para obtener más información, consulte Eventos de AWS Batch .	8 de septiembre de 2017
CodePipeline yAWS GlueEventos de	Se ha agregado compatibilidad con eventos de CodePipeline yAWS Glue. Para obtener más información, consulte Eventos de CodePipeline (p. 47) y AWS Glue Events (p. 59) .	8 de septiembre de 2017

Cambio	Descripción	Fecha de la versión
Eventos CodeBuild y CodeCommit	Se ha agregado compatibilidad con eventos de CodeBuild y CodeCommit. Para obtener más información, consulte Eventos de CodeBuild (p. 46) .	3 de agosto de 2017
Destinos adicionales admitidos	CodePipeline y Amazon Inspector pueden ser destinos de eventos.	29 de junio de 2017
Compatibilidad para enviar y recibir eventos entre cuentas de AWS	Un cuenta de AWS puede enviar eventos a otra cuenta de AWS. Para obtener más información, consulte Envío y recepción de eventos entre cuentas de AWS (p. 89) .	29 de junio de 2017
Destinos adicionales admitidos	Ahora puede establecer dosAWS como objetivos para acciones de eventos: Máquinas de estado de Amazon EC2 (a través de Run Command) y Step Functions. Para obtener más información, consulte Introducción a Amazon CloudWatch Events (p. 6) .	7 de marzo de 2017
Amazon EMR Events	Se ha agregado compatibilidad con eventos para Amazon EMR. Para obtener más información, consulte Eventos de Amazon EMR (p. 50) .	7 de marzo de 2017
AWSEventos Health	Se ha agregado compatibilidad con eventos paraAWSHealth. Para obtener más información, consulte AWS Health Events (p. 64) .	1 de diciembre de 2016
Amazon Elastic Container Service	Se ha agregado compatibilidad con eventos para Amazon ECS. Para obtener más información, consulte Eventos de Amazon Elastic Container Service (p. 50) .	21 de noviembre de 2016
Eventos de AWS Trusted Advisor	Se ha agregado compatibilidad con eventos para Trusted Advisor. Para obtener más información, consulte AWS Trusted Advisor Events (p. 85) .	18 de noviembre de 2016
Amazon Elastic Block Store	Se ha agregado compatibilidad con eventos para Amazon EBS. Para obtener más información, consulte Eventos de Amazon EBS (p. 49) .	14 de noviembre de 2016
Eventos de AWS CodeDeploy	Se ha agregado compatibilidad con eventos para CodeDeploy. Para obtener más información, consulte AWS CodeDeploy Events (p. 46) .	9 de septiembre de 2016
Eventos programados con granularidad de 1 minuto	Se ha agregado compatibilidad con eventos programados con granularidad de 1 minuto. Para obtener más información, consulte Expresiones Cron (p. 35) y Expresiones de frecuencia (p. 38) .	19 de abril de 2016
Colas de Amazon Simple Queue Service como destinos	Se ha agregado compatibilidad con colas de Amazon SQS como destinos. Para obtener más información, consulte ¿Qué es Amazon CloudWatch Events? (p. 1) .	30 de marzo de 2016

Cambio	Descripción	Fecha de la versión
Eventos de Auto Scaling	Se ha agregado compatibilidad con eventos para enlaces de ciclo de vida de Auto Scaling. Para obtener más información, consulte Eventos de Auto Scaling de Amazon EC2 (p. 49) .	24 de febrero de 2016
Nuevo servicio	Versión inicial de CloudWatch Events.	14 de enero de 2016

AWSGlosario

Contiene la más recienteAWSterminología, consulte la [AWSGlosario](#) en laAWSReferencia general de.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.