# Amazon CloudWatch Logs

## Guía del usuario

# Amazon CloudWatch Logs: Guía del usuario

# Table of Contents

# Qué esi¿Qué es Amazon CloudWatch Logs?

Puede utilizar Amazon CloudWatch Logs para monitorizar, almacenar y obtener acceso a los archivos de registro desde instancias de Amazon Elastic Compute Cloud (Amazon EC2),AWS CloudTrail, Route 53 y otras fuentes.

CloudWatch Logs le permite centralizar los registros de todos los sistemas, aplicaciones yAWSque utilice, en un único servicio de gran escalabilidad. A continuación, puede verlos fácilmente, buscarlos códigos de error o patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para futuros análisis. CloudWatch Logs le permite ver todos los registros, independientemente de su origen, como un flujo único y coherente de eventos ordenados por tiempo, y puede consultarlos y ordenarlos en función de otras dimensiones, agruparlos por campos específicos, crear cálculos personalizados con un potente lenguaje de consulta y visualizar los registros datos en paneles.

## Features

- ConsultayOurLOGData: puede utilizar CloudWatch Logs Insights para buscar y analizar de forma interactiva sus datos de registro. Puede realizar consultas que le ayuden a responder de forma más eficaz a los problemas de funcionamiento. Insights de registros de CloudWatch Logs incluye un lenguaje de consulta específico con algunos comandos sencillos pero eficaces. Proporcionamos consultas de ejemplo, descripciones de comandos, autocompletado de consultas y detección de campos de registro para ayudarle a comenzar. Se incluyen ejemplos de consultas para varios tipos de registros de servicios de AWS. Para empezar, consulte Análisis de datos de registro con CloudWatch Logs Insights (p. 35).
- MonitorizaciónLOG de Amazon EC2inposturas: puede utilizar CloudWatch Logs para monitorizar aplicaciones y sistemas mediante datos de registro. Por ejemplo, CloudWatch Logs puede realizar, por ejemplo, el seguimiento de los errores presentes en los registros de las aplicaciones y enviarle una notificación cuando la tasa de errores supere el umbral que se especifique. CloudWatch Logs utiliza sus datos de registro para el monitoreo, de forma que no es necesario cambiar el código. Por ejemplo, puede monitorizar los registros de la aplicación para determinados términos literales (como, por ejemplo, "NullReferenceException") o contar el número de incidencias de un término literal en una posición particular en los datos de registro (como por ejemplo los códigos de estado "404" en un registro de acceso de Apache). Cuando se encuentra el término está buscando, CloudWatch Logs notifica los datos a una métrica de CloudWatch que especifique. Los datos de registro están cifrados mientras están en tránsito y cuando están en reposo. Para empezar, consulte Introducción a los registros de CloudWatch (p. 5).
- MonitorizaciónAWS CloudTrail LOGerejillas de ventilación: puede crear alarmas en CloudWatch y recibir notificaciones de la actividad del API particular registrada por CloudTrail y utilizar la notificación para llevar a cabo la resolución de problemas. Para empezar, consulteEnvío de eventos de CloudTrail a CloudWatch Logsen laAWS CloudTrailGuía del usuario de.
- RegistroretentionDe forma predeterminada, los registros se conservan de forma indefinida y no caducan nunca. Puede ajustar la política de retención para cada grupo de registros, manteniendo la retención indefinida o seleccionar un periodo de retención de entre 10 años y un día.
- ArchivadoLOGData: puede utilizar CloudWatch Logs para almacenar sus datos de registro en almacenamiento de larga duración. El agente CloudWatch Logs facilita la tarea de enviar de forma rápida, tanto los datos de registro cambiados como no cambiados desde un host al servicio de registros. Posteriormente, cuando lo necesite, podrá obtener acceso a los datos de log en su estado original.

- DNS de Route 53queries: puede utilizar CloudWatch Logs para registrar información sobre las consultas Route 53 recibe; Para obtener más información, consulteConsultas de DNS de registroen laGuía para desarrolladores de Amazon Route 53.

# RelacionadoAWS services

Los siguientes servicios se utilizan conjuntamente con CloudWatch Logs:

- AWS CloudTrailes un servicio web que le permite monitorizar las llamadas a la API de CloudWatch Logs para su cuenta, incluidas las llamadas realizadas porAWS Management Console,AWS Command Line Interface(AWS CLI), así como otros servicios. Cuando el registro de CloudTrail está activado, CloudTrail captura las llamadas a la API en su cuenta y envía los archivos de registro al bucket de Amazon S3 que especifique. Cada archivo de registro puede contener uno o varios registros, en función de la cantidad de acciones que se deben realizar para satisfacer una solicitud. Para obtener más información acerca deAWS CloudTrail, consulteQué esAWS CloudTrail?en laAWS CloudTrailGuía del usuario de. Para un ejemplo del tipo de datos que CloudWatch escribe en archivos de registro de CloudTrail, consulteAPI de registro de Amazon CloudWatch LogscALL ENAWS CloudTrail (p. 161).
- AWS Identity and Access Management(IAM)es un servicio web que le ayuda a controlar de forma segura el acceso aAWSrecursos para sus usuarios. Utilice IAM para controlar quién puede usar suAWS(autenticación), así como cuáles de ellos pueden usar y cómo pueden hacerlo (autorización). Para obtener más información, consulte¿Qué es IAM?en laIAM User Guide.
- Amazon Kinesis Data Streamses un servicio web que puede utilizar para una entrada y agregación de datos rápida y continua. 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¿Qué es Amazon Kinesis Data Streams?en laGuía del desarrollador de Amazon Kinesis Data Streams.
- AWS Lambda es un servicio web que puede utilizar para la creación de aplicaciones que respondan rápidamente a nueva información. Cargue su código de aplicación como funciones de Lambda y ejecuta el código en una infraestructura informática de alta disponibilidad y ejecuta la administración integral de los recursos informáticos, incluido el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, la implementación de parches de seguridad y código. Monitorear y registrar código. Lo único que tiene que hacer es suministrar el código en uno de los idiomas que admite Lambda. Para obtener más información, consulte ¿Qué es AWS Lambda? en la Guía para desarrolladores de AWS Lambda.

# Pricing

Cuando se inscribe enAWSpuede comenzar a utilizar CloudWatch Logs de forma gratuita utilizandoAWSCapa gratuita.

Se aplican las tarifas estándar para los registros almacenados por otros servicios que utilicen CloudWatch Logs (por ejemplo, registros de flujo de Amazon VPC y registros de Lambda).

Para obtener más información, consulte los precios de Amazon CloudWatch.

# Amazon CloudWatch Logsconcepts

A continuación, se describe la terminología y los conceptos que son básicos para que conozca y utilice los registros de CloudWatch.

Eventos de registro

Un evento de registro es un registro de algunas actividades guardado por la aplicación o el recurso que se está monitorizando. El evento de registro que entiende CloudWatch Logs contiene dos propiedades: la marca temporal de cuando se produjo el evento y el mensaje de eventos sin procesar. Los mensajes de evento deben estar cifrados con UTF-8.

Flujos de registro

Un flujo de registro es una secuencia de eventos de registro que comparten la misma fuente. En concreto, un flujo de registro en general, está pensado para representar la secuencia de eventos procedente de la instancia de aplicación o recurso que se monitoriza. Por ejemplo, un flujo de registro puede asociarse a un registro de acceso de Apache en un host específico. Cuando ya no necesita un flujo de registro, puede eliminarlo utilizando el comando aws logs delete-log-stream.

Grupos de registros

Los grupos de registros definen grupos de flujos de registro que comparten la misma configuración de retención, monitorización y control de acceso. Cada flujo de registro tiene que pertenecer a un grupo de registros. Por ejemplo, si tiene un flujo de registro diferente para los registros de acceso de Apache de cada host, puede agrupar estos flujos en un solo grupo de registros denominado `MyWebsite.com/Apache/access_log`.

No hay límites en el número de flujos de registro que pueden pertenecer a un grupo de registros.

Filtros de métricas

Puede utilizar filtros de métrica para extraer las observaciones de métricas de eventos introducidos y transformarlas en puntos de datos en una métrica de CloudWatch. Los filtros de métricas se asignan a grupos de registro y todos los filtros asignados a un grupo de registros se aplican a sus flujos de registro.

Configuración de retención

La configuración de retención se puede utilizar para especificar cuánto tiempo se conservan los eventos de registro en CloudWatch Logs. Los eventos de registro caducados se eliminarán automáticamente. De la misma forma que los filtros de métricas, los ajustes de retención también se asignan a los grupos de registro y la retención asignada a un grupo de registros se aplica a sus flujos de registro.

# GETsetup

Para utilizar los Amazon CloudWatch Logs, necesita unAWSaccount. SusAWSSu cuenta le permite utilizar servicios (por ejemplo, Amazon EC2) para generar registros 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).

## Signup para Amazon Web Services

Al crear unAWSSu cuenta, la inscribimos automáticamente en todos losAWSServicios de . Solo pagará por los servicios que utilice.

Si dispone de unAWSYa, 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 Amazon CloudWatchconsole

Inicie sesión en la consola de Amazon CloudWatch

1. Inicie sesión en la en laAWS Management Consoley abra la consola de CloudWatch enhttps://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambie la región. En la barra de navegación, elija la región donde tiene suAWSde AWS.
3. En el panel de navegación, elija Logs.

## Establezcaup Interfaz de línea de comandos de

Puede utilizar la herramientaAWS CLIpara realizar operaciones de CloudWatch Logs.

Para obtener información acerca de cómo instalar y configurar laAWS CLI, consulteConfiguración inicial de laAWSInterfaz de línea de comandos deen laAWS Command Line InterfaceGuía del usuario.

# Introducción a los registros de CloudWatch

Para recopilar registros de las instancias Amazon EC2 y los servidores locales en los CloudWatch Logs,AWSofrece dos opciones:

- Recomendado— El agente unificado de CloudWatch. Le permite recopilar registros y métricas avanzadas con un solo agente. Ofrece compatibilidad con distintos sistemas operativos, incluidos los servidores que ejecutan Windows Server. Este agente también proporciona un mejor rendimiento.

  Si utiliza el agente unificado para recopilar métricas de CloudWatch, el agente unificado permite la recopilación de métricas del sistema adicionales para la visibilidad en invitados. También admite la recopilación de métricas personalizadas mediante `StatsD` o `collectd`.

  Para obtener más información, consulteInstalación del agente de CloudWatchen laGuía del usuario de Amazon CloudWatch.
- Compatible, pero en el camino a la obsolescencia— El agente anterior de CloudWatch Logs, que admite la recopilación de registros de sólo servidores que ejecutan Linux. Si ya está utilizando ese agente, puede continuar haciéndolo. Sin embargo, el agente anterior requiere Python 2.7, 3.0 y 3.3. Dado que las instancias EC2 actuales no utilizan esas versiones de Python y que esas versiones están obsoletas y ya no se están parcheando,Le recomendamos encarecidamente que migre al agente de CloudWatch unificado.

  Cuando migra del agente de CloudWatch Logs al agente de CloudWatch unificado, el asistente de configuración del agente unificado puede leer el archivo de configuración del agente de CloudWatch Logs actual y configurar el nuevo agente para que recopile los mismos registros. Para obtener más información acerca del asistente, consulteCreación del archivo de configuración de agente de CloudWatch con el asistenteen laGuía del usuario de Amazon CloudWatch.

Contenido



## Utilice el agente unificado de CloudWatch para comenzar con los CloudWatch Logs

Para obtener más información sobre el uso del agente unificado de CloudWatch para comenzar con CloudWatch Logs, consulteRecopilar métricas y registros de instancias Amazon EC2 y servidores locales con el agente de CloudWatchen laGuía del usuario de Amazon CloudWatch. Realice los pasos indicados en esta sección para instalar, configurar e iniciar el agente. Si no va a utilizar el agente para recopilar métricas de CloudWatch, puede hacer caso omiso de las secciones que hagan referencia a ellas.

Si está utilizando actualmente el agente de CloudWatch Logs antiguo y desea realizar la migración para utilizar el nuevo agente unificado, le recomendamos que emplee el asistente incluido en el paquete del nuevo agente. Este asistente puede leer el archivo de configuración del agente de CloudWatch Logs y configurar el agente de CloudWatch para recopilar los mismos registros. Para obtener más información acerca del asistente, consulteCreación del archivo de configuración de agente de CloudWatch con el asistenteen laGuía del usuario de Amazon CloudWatch.

# Utilice el agente CloudWatch Logs anterior para comenzar con CloudWatch Logs

Al utilizar el agente de CloudWatch Logs le permite publicar datos de registro desde instancias de Amazon EC2 que ejecutan Linux o Windows Server y eventos registrados desdeAWS CloudTrail. Le recomendamos que utilice en su lugar el agente de CloudWatch unificado para publicar sus datos de registro. Para obtener más información sobre el nuevo agente, consulteRecopilar métricas y registros de instancias Amazon EC2 y servidores locales con el agente de CloudWatchen laGuía del usuario de Amazon CloudWatch. También puede seguir utilizando el agente de CloudWatch Logs anterior.

Contenido



## Requisitos previos de CloudWatch Logs

El agente de CloudWatch Logs requiere Python versión 2.7, 3.0 o 3.3 y cualquiera de las siguientes versiones de Linux:

- Amazon Linux versión 2014.03.02 o posterior. No se admite en Amazon Linux 2.
- Ubuntu Server versión 12.04, 14.04 o 16.04
- Versión CentOS 6, 6.3, 6.4, 6.5 o 7.0
- Red Hat Enterprise Linux (RHEL) versión 6.5 o 7.0
- Debian 8.0

## Inicio rápido de: Instalar y configurar el agente CloudWatch Logs en una instancia Linux de EC2 en ejecución

Tip

CloudWatch incluye un nuevo agente unificado que pueden recopilar tanto registros como métricas de los servidores locales y las instancias EC2. Si no es usuario del agente de CloudWatch Logs, le recomendamos que utilice el nuevo agente de CloudWatch unificado. Para obtener más información, consulte Introducción a los registros de CloudWatch (p. 5) .
El resto de esta sección explica el uso del agente de CloudWatch Logs de anterior.

# Configurar el agente de CloudWatch Logs anterior en una instancia Linux de EC2 en ejecución

Puede utilizar el instalador del agente de CloudWatch Logs en una instancia EC2 para instalar y configurar el agente de CloudWatch Logs. Una vez que se haya completado la instalación, los registros fluyen automáticamente desde la instancia al flujo de registros que crea al instalar el agente. El agente confirma que se ha iniciado y sigue en ejecución hasta que lo deshabilita.

Además de utilizar el agente de, también puede publicar datos de registro mediante la herramientaAWS CLI, el SDK de CloudWatch Logs o la API de CloudWatch Logs. La AWS CLI es más adecuada para la publicación de datos en la línea de comando o a través de scripts. El SDK de CloudWatch Logs es más adecuado para la publicación de datos de registro directamente desde aplicaciones o para crear su propia aplicación de publicación de registros.

## Paso 1: Configuración de su rol de IAM o usuario para CloudWatch Logs

El agente de CloudWatch Logs admite roles y usuarios de IAM. Si la instancia ya tiene un rol de IAM asociado, asegúrese de incluir la política de IAM a continuación. Si aún no dispone de un rol de IAM asignado a la instancia, puede utilizar sus credenciales de IAM para los siguientes pasos o bien puede asignar un rol de IAM a dicha instancia. Para obtener más información, consulte Attaching an IAM Role to an Instance.

### Para configurar su rol de IAM o usuario de para CloudWatch Logs

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija el rol seleccionando el nombre de rol (no seleccione la casilla de verificación junto al nombre).
4. Elija Attach Policies (Asociar políticas), Create Policy (Crear política).

   Se abrirá una nueva pestaña o ventana del navegador.
5. Seleccione la pestaña JSON y escriba el siguiente documento de política JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
    ],
      "Resource": [
        "*"
    ]
  }
 ]
}
```

6. Cuando haya terminado, seleccione Review policy. El validador de políticas notifica los errores de sintaxis.
7. En la página Review Policy (Revisar la política), escriba un Name (Nombre) y una Description (Descripción) (opcional) para la política que está creando. Revise la política Summary para ver los permisos concedidos por su política. A continuación, elija Create policy para guardar su trabajo.
8. Cierre la pestaña o ventana del navegador y vuelva a la página Add permissions (Agregar permisos) para su rol. Elija Refresh (Actualizar) y, a continuación, elija la política nueva para asociarla a su rol.

9. Elija Attach Policy.

## Paso 2: Instalar y configurar CloudWatch Logs en una instancia de Amazon EC2 existente

El proceso para instalar el agente de CloudWatch Logs varía en función de si su instancia de Amazon EC2 está ejecutando Amazon Linux, Ubuntu, CentOS o Red Hat. Utilice los pasos adecuados para la versión de Linux en su instancia.

### Para instalar y configurar CloudWatch Logs en una instancia de Amazon Linux existente

A partir de la AMI de Amazon Linux 2014.09, el agente de CloudWatch Logs está disponible como una instalación de RPM con el paquete awslogs. Las versiones anteriores de Amazon Linux pueden obtener acceso al paquete awslogs mediante la actualización de su instancia con el`sudo yum update -y`comando. Al instalar el paquete awslogs como RPM en lugar de utilizar el instalador de CloudWatch Logs, la instancia recibe actualizaciones de paquete regulares y parches deAWSsin tener que volver a instalar manualmente el agente CloudWatch Logs.

> **Warning**
>
> No actualice el agente de CloudWatch Logs utilizando el método de instalación de RPM si ha utilizado anteriormente el script de Python para instalar el agente. De hacerlo, podría provocar problemas de configuración que impidan que el agente de CloudWatch Logs envíe sus registros a CloudWatch.

1. Connect con la instancia de Amazon Linux. Para obtener más información, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   Para obtener más información acerca de los problemas de conexión, consulteSolución de problemas con la conexión a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.
2. Actualice su instancia de Amazon Linux para recoger los últimos cambios en los repositorios de paquetes.

   ```
   sudo yum update -y
   ```
3. Instale el paquete `awslogs`. Este es el método recomendado para instalar awslogs en instancias de Amazon Linux.

   ```
   sudo yum install -y awslogs
   ```
4. Edite el archivo `/etc/awslogs/awslogs.conf` para configurar los registros para realizar seguimiento. Para obtener más información sobre la edición de este archivo, consulte Registros de CloudWatchacaballeroreference (p. 164).
5. De forma predeterminada, el`/etc/awslogs/awscli.conf`hacia la región us-east-1. Para enviar los registros a una región diferente, edite la.`awscli.conf`y especifique esa región.
6. Inicie el servicio `awslogs`.

   ```
   sudo service awslogs start
   ```

   Si está ejecutando Amazon Linux 2, inicie el servicio `awslogs` con el siguiente comando.

   ```
   sudo systemctl start awslogsd
   ```
7. (Opcional) Compruebe el archivo `/var/log/awslogs.log` para ver si se han registrado errores al iniciar el servicio.

8. (Opcional) Ejecute el siguiente comando para iniciar el servicio `awslogs` en cada arranque del sistema.

```
sudo chkconfig awslogs on
```

   Si está ejecutando Amazon Linux 2, utilice el siguiente comando para iniciar el servicio en cada arranque del sistema.

```
sudo systemctl enable awslogsd.service
```

9. Debería ver el grupo de registros de nueva creación y el flujo de registros en la consola de CloudWatch después de que el agente haya estado en ejecución durante unos minutos.

   Para obtener más información, consulte VistalOGdatasen CloudWatch Logs (p. 60) .

### Para instalar y configurar CloudWatch Logs en una instancia de Ubuntu Server, CentOS o Red Hat

Si está utilizando una AMI que ejecuta Ubuntu Server, CentOS o Red Hat, utilice el siguiente procedimiento para instalar manualmente el agente de CloudWatch Logs en la instancia.

1. Conéctese a su instancia EC2. Para obtener más información, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   Para obtener más información acerca de los problemas de conexión, consulteSolución de problemas con la conexión a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

2. Ejecute el instalador del agente de CloudWatch Logs utilizando una de estas dos opciones. Puede ejecutarlo directamente desde Internet o descargar los archivos y ejecutarlo de forma independiente.

   > Note
   >
   > Si está ejecutando CentOS 6.x, Red Hat 6.x o Ubuntu 12.04, utilice los pasos para descargar y ejecutar el instalador independiente. La instalación del agente de CloudWatch Logs directamente desde Internet no es compatible con estos sistemas.

   > Note
   >
   > En Ubuntu, ejecute `apt-get update` antes de ejecutar los comandos siguientes.

   Para ejecutarlo directamente desde Internet, utilice los siguientes comandos y siga las instrucciones:

```
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py -O
```

```
sudo python ./awslogs-agent-setup.py --region us-east-1
```

   Si el comando anterior no funciona, pruebe lo siguiente:

```
sudo python3 ./awslogs-agent-setup.py --region us-east-1
```

   Para descargar y ejecutarlo de forma independiente, utilice los siguientes comandos y siga las instrucciones:

```
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py -O
```

```
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/AgentDependencies.tar.gz
 -O
```

```
tar xvf AgentDependencies.tar.gz -C /tmp/
```

```
sudo python ./awslogs-agent-setup.py --region us-east-1 --dependency-path /tmp/
AgentDependencies
```

Puede instalar el agente de CloudWatch Logs especificando las regiones us-east-1, us-west-1, us-west-2, ap-south-1, ap-northeast-2, ap-southeast-1, ap-southeast-1, ap-southeast-1, eu-central-1, eu-central-1, eu-west-1 o sa-east-1.

> **Note**
>
> Para obtener más información sobre la versión actual y el historial de versiones de `awslogs-agent-setup`, consulte CHANGELOG.txt.

El instalador del agente de CloudWatch Logs requiere cierta información durante el proceso de configuración. Antes de empezar, debe saber qué archivo de log monitorizar y su formato de marca temporal. También debe tener preparada la siguiente información.

| Elemento | Descripción |
|---|---|
| AWSID de clave de acceso | Pulse Intro si utiliza un rol de IAM. De lo contrario, escriba suAWSel ID de clave de acceso. |
| AWSclave de acceso secreta | Pulse Intro si utiliza un rol de IAM. De lo contrario, escriba suAWSLa clave de acceso secreta. |
| Nombre de región predeterminado | Pulse Intro. El valor predeterminado es us-east-2. Puede establecer esto en us-east-1, us-west-1, us-west-1, ap-south-1, ap-northeast-2, ap-southeast-1, ap-southeast-1, ap-southeast-2, ap-northeast-1, eu-central-1, eu-west-1, o sa-east-1. |
| Formato de salida predeterminado | Déjelo en blanco y pulse Intro. |
| Ruta del archivo de registro que cargar | La ubicación del archivo que contiene los datos de log que se van a enviar. El instalador le sugiere una ruta. |
| Nombre de grupo de registros de destino | El nombre de su grupo de registros. El instalador le sugiere un nombre de grupo de registros. |
| Nombre de flujo de registros de destino | De forma predeterminada, es el nombre del host. El instalador le sugiere un nombre de host. |
| Formato de marca temporal | Especifique el formato de la marca temporal en el archivo de log especificado. Elija personalizado para especificar su propio formato. |
| Posición inicial | Cómo se han cargado los datos. Establecerlo en start_of_file para cargar todo en el archivo de datos. Establézcalo en end_of_file para cargar solo los datos recién añadidos. |

Una vez que haya completado estos pasos, el instalador le preguntará si desea configurar otro archivo de log. Puede ejecutar el proceso tantas veces como desee para cada archivo de registro. Si no

tiene más archivos de registro que monitorizar, elija N cuando el instalador lo solicite para configurar otro registro. Para obtener más información sobre la configuración en el archivo de configuración del agente, consulte Registros de CloudWatchacaballeroreference (p. 164).

Note

No se admite configurar varias fuentes de registro para enviar datos a un único flujo de registro.

3. Debería ver el grupo de registros de nueva creación y el flujo de registros en la consola de CloudWatch después de que el agente haya estado en ejecución durante unos minutos.

   Para obtener más información, consulte VistalOGdatasen CloudWatch Logs (p. 60) .

# Inicio rápido de: Instalar y configurar el agente de CloudWatch Logs en una instancia EC2 Linux durante el lanzamiento

Tip

El agente de CloudWatch Logs antiguo descrito en esta sección se encuentra en vías de ser declarado obsoleto. Le recomendamos encarecidamente que utilice el nuevo agente de CloudWatch unificado que puede recopilar tanto registros como métricas. Además, el agente de CloudWatch Logs antiguo requiere Python 3.3 o versiones anteriores y estas versiones no están instaladas en las instancias EC2 nuevas de forma predeterminada. Para obtener más información sobre el agente de CloudWatch unificado, consulteInstalación del agente de CloudWatch.
El resto de esta sección explica el uso del agente de CloudWatch Logs de anterior.

## Instalación del agente de CloudWatch Logs de anterior en una instancia EC2 de Linux durante el lanzamiento

Puede utilizar los datos de usuario de Amazon EC2, una característica de Amazon EC2 que permite transferir información de parámetros a la instancia en el momento del lanzamiento, para instalar y configurar el agente de CloudWatch Logs en dicha instancia. Para transferir la información de instalación y configuración del agente de CloudWatch Logs a Amazon EC2, puede proporcionar el archivo de configuración en una ubicación de red, como un bucket de Amazon S3.

No se admite configurar varias fuentes de registro para enviar datos a un único flujo de registro.

Prerequisite

Cree un archivo de configuración de agente que describa todos los grupos de registro y flujos de registro. Se trata de un archivo de texto que describe los archivos de registro que monitorizar, así como los grupos de registro y los flujos de registro para añadirlos. El agente consume este archivo de configuración y comienza a monitorizar y a cargar todos los archivos de registro descritos en el mismo. Para obtener más información sobre la configuración en el archivo de configuración del agente, consulte Registros de CloudWatchacaballeroreference (p. 164).

A continuación se muestra un ejemplo de archivo de configuración del agente de para Amazon Linux 2

```
[general]
state_file = /var/lib/awslogs/state/agent-state

[/var/log/messages]
file = /var/log/messages
log_group_name = /var/log/messages
```

```
log_stream_name = {instance_id}
datetime_format = %b %d %H:%M:%S
```

A continuación se muestra un ejemplo de archivo de configuración del agente para Ubuntu

```
[general]
state_file = /var/awslogs/state/agent-state

[/var/log/syslog]
file = /var/log/syslog
log_group_name = /var/log/syslog
log_stream_name = {instance_id}
datetime_format = %b %d %H:%M:%S
```

Para configurar su rol de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Policies, Create Policy.
3. En la página Create Policy, en Create Your Own Policy, elija Select. Para obtener más información acerca de la creación de políticas personalizadas, consultePolíticas de IAM para Amazon EC2en laGuía del usuario de Amazon EC2 para instancias de Linux.
4. En la página Review Policy, en Policy Name, escriba un nombre para la política.
5. En Policy Document, pegue la siguiente política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::myawsbucket/*"
            ]
        }
    ]
}
```

6. Elija Create Policy (Crear política).
7. En el panel de navegación, seleccione Roles, Create New Role.
8. En la página Set Role Name, escriba un nombre de rol y, a continuación, elija Next Step.
9. En la página Select Role Type, elija Select junto a Amazon EC2.
10. En la página Attach Policy, en el encabezado de la tabla, elija Policy Type, Customer Managed.
11. Seleccione la política de IAM que ha creado y, a continuación, elijaPaso siguiente.
12. Elija Create Role (Crear rol).

Para obtener más información acerca de los usuarios y las políticas de IAM, consulteUsuarios y grupos de IAMyAdministración de políticas de IAMen laIAM User Guide.

Para lanzar una nueva instancia y habilitar CloudWatch Logs

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija Launch Instance.

   Para obtener más información, consulteLanzamiento de una instanciainGuía del usuario de Amazon EC2 para instancias de Linux.
3. En la páginaPaso 1: Elegir una imagen de máquina de Amazon (AMI)En, seleccione el tipo de instancia de Linux que lanzar y, a continuación, en laPaso 2: Página Choose an Instance Type, elijaSiguiente: Página Configure Instance Details (Configurar los detalles de la instancia).

   Asegúrese de que cloud-init se incluye en la imagen de máquina de Amazon (AMI). Las AMI de Amazon Linux y las AMI para Ubuntu y RHEL ya incluyen cloud-init, pero las AMI de CentOS y otros en el AWS Marketplace puede que no.
4. En la páginaPaso 3: Página Configure Instance Details (Configurar los detalles de la instancia), paraRol de IAM, seleccione el rol de IAM que ha creado.
5. En Advanced Details, en User data, pegue el siguiente script en el cuadro. A continuación, actualice el script cambiando el valor de la opción -c a la ubicación de su archivo de configuración del agente:

```
#!/bin/bash
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py -O
chmod +x ./awslogs-agent-setup.py
./awslogs-agent-setup.py -n -r us-east-1 -c s3://DOC-EXAMPLE-BUCKET1/my-config-file
```

6. Realice los demás cambios en la instancia, revise la configuración de lanzamiento y, a continuación, elija Launch.
7. Debería ver el grupo de registros de nueva creación y el flujo de registros en la consola de CloudWatch después de que el agente haya estado en ejecución durante unos minutos.

   Para obtener más información, consulte VistaIOGdatasen CloudWatch Logs (p. 60) .

# Inicio rápido de: Habilite las instancias de Amazon EC2 que ejecutan Windows Server 2016 para enviar los registros a CloudWatch Logs con el agente de CloudWatch Logs

Tip

CloudWatch incluye un nuevo agente unificado que pueden recopilar tanto registros como métricas de los servidores locales y las instancias EC2. Le recomendamos que utilice el nuevo agente de CloudWatch unificado de. Para obtener más información, consulte Introducción a los registros de CloudWatch (p. 5) .
El resto de esta sección explica el uso del agente de CloudWatch Logs de anterior.

# Habilite las instancias de Amazon EC2 que ejecutan Windows Server 2016 para enviar los registros a CloudWatch Logs utilizando el agente de CloudWatch Logs

Puede utilizar varios métodos para permitir que las instancias que ejecutan Windows Server 2016 envíen los registros a los registros de CloudWatch Logs. Los pasos de esta sección utilizan Systems Manager Run Command. Para obtener más información acerca de los otros métodos, consulte Sending Logs, Events, and Performance Counters to Amazon CloudWatch.

Pasos



## Descargue el archivo de configuración de muestra

Descargue el siguiente archivo de muestra en su equipo:`AWS.EC2.Windows.CloudWatch.json`.

## Configuración del archivo JSON para CloudWatch

Para determinar qué registros se enviarán a CloudWatch, especifique las opciones en un archivo de configuración. El proceso de creación de este archivo y especificación de las opciones puede tardar 30 minutos o más en completarse. Una vez que haya completado esta tarea una vez, podrá volver a utilizar el archivo de configuración en todas sus instancias.

Pasos



### Paso 1: Habilitar los CloudWatch Logs

En la parte superior del archivo JSON, cambie "false" a "true" en `IsEnabled`:

```
"IsEnabled": true,
```

### Paso 2: Configurar la configuración de CloudWatch

Especifique las credenciales, la región, el nombre de un grupo de registros y un espacio de nombres de flujo de registros. Esto permite que la instancia envíe datos de registros a CloudWatch Logs. Para enviar los mismos datos de log a diferentes ubicaciones, puede añadir secciones adicionales con ID únicos (por ejemplo, «CloudWatchLogs2" y CloudWatchLogs3") y una región diferente para cada ID.

Para configurar opciones para enviar datos de registros a CloudWatch Logs

1. En el archivo JSON, busque la sección `CloudWatchLogs`.

```
{
    "Id": "CloudWatchLogs",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "",
        "SecretKey": "",
        "Region": "us-east-1",
        "LogGroup": "Default-Log-Group",
        "LogStream": "{instance_id}"
    }
},
```

2. Deje los campos `AccessKey` y `SecretKey` en blanco. Configurará las credenciales mediante un rol de IAM.
3. Para`Region`, escriba la región a la que desea enviar los datos de log (por ejemplo,`us-east-2`).
4. En `LogGroup`, especifique el nombre del grupo de registros. Este nombre aparece en elGrupos de registrosen la consola de CloudWatch.
5. En `LogStream`, especifique el flujo de registros de destino. Este nombre aparece en elGrupos de registro > Streamsen la consola de CloudWatch.

   Si utiliza `{instance_id}`, el nombre del flujo de registro de destino predeterminado es el ID de esta instancia.

   Si especifica un nombre de flujo de registro que no existe, CloudWatch Logs lo crea automáticamente. Puede definir el nombre del flujo de registro mediante una cadena literal, las variables predefinidas `{instance_id}`, `{hostname}` y `{ip_address}`, o una combinación de ellas.

### Paso 3: Configurar los datos que se van a enviar

Puede enviar datos de registro de eventos, datos de Seguimiento de eventos para Windows (ETW) y otros datos de registro a CloudWatch Logs.

#### Para enviar datos de registro de eventos de aplicación de Windows a CloudWatch Logs

1. En el archivo JSON, busque la sección `ApplicationEventLog`.

```
{
    "Id": "ApplicationEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Application",
        "Levels": "1"
    }
},
```

2. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

### Para enviar datos de registros de seguridad a CloudWatch Logs

1. En el archivo JSON, busque la sección `SecurityEventLog`.

```
{
    "Id": "SecurityEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Security",
        "Levels": "7"
    }
},
```

2. En `Levels`, especifique **`7`** para cargar todos los mensajes.

### Para enviar datos de registros de eventos del sistema a CloudWatch Logs

1. En el archivo JSON, busque la sección `SystemEventLog`.

```
{
    "Id": "SystemEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "System",
        "Levels": "7"
    }
},
```

2. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

### Para enviar otros tipos de datos de registro de eventos a CloudWatch Logs

1. En el archivo JSON, añada una nueva sección. Cada sección debe tener un `Id` único.

```
{
    "Id": "Id-name",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Log-name",
        "Levels": "7"
    }
},
```

2. En `Id`, escriba un nombre para el registro que desea cargar (por ejemplo, **`WindowsBackup`**).
3. En `LogName`, escriba el nombre del registro que se va a cargar. Puede encontrar el nombre del registro como se indica a continuación.

a. Abra el Visor de eventos.

b. En el panel de navegación, elija Registros de aplicaciones y servicios.

c. Navegue hasta el registro y elija Actions, Properties.

4. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

### Para enviar datos de Seguimiento de eventos para Windows a los CloudWatch Logs

ETW (Seguimiento de eventos para Windows) proporciona un mecanismo de registro detallado y eficiente en el que las aplicaciones pueden escribir los registros. Cada ETW se controla mediante un administrador de sesiones que puede iniciar y parar la sesión de registro. Cada sesión tiene un proveedor y uno o varios consumidores.

1. En el archivo JSON, busque la sección `ETW`.

```
{
    "Id": "ETW",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Microsoft-Windows-WinINet/Analytic",
        "Levels": "7"
    }
},
```

2. En `LogName`, escriba el nombre del registro que se va a cargar.
3. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

### Para enviar registros personalizados (cualquier archivo de registro basado en texto) a CloudWatch Logs

1. En el archivo JSON, busque la sección `CustomLogs`.

```
{
    "Id": "CustomLogs",
```

```
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogDirectoryPath": "C:\\CustomLogs\\",
        "TimestampFormat": "MM/dd/yyyy HH:mm:ss",
        "Encoding": "UTF-8",
        "Filter": "",
        "CultureName": "en-US",
        "TimeZoneKind": "Local",
        "LineCount": "5"
    }
},
```

2. En `LogDirectoryPath`, escriba la ruta de la instancia donde se almacenan los registros.
3. En `TimestampFormat`, escriba el formato de marcas temporales que desea utilizar. Para obtener más información sobre los valores admitidos, consulte el tema Cadenas con formato de fecha y hora personalizado en MSDN.

   Important

   Su archivo de log de origen debe tener la marca temporal al principio de cada línea de log y debe haber un espacio en blanco tras dicha marca.
4. En `Encoding`, especifique la codificación del archivo que sea utilizar (por ejemplo, UTF-8). Para obtener una lista de los valores admitidos, consulte el tema Clase Encoding en MSDN.

   Note

   Utilice el nombre de codificación, no el nombre de visualización.
5. (Opcional) En `Filter`, escriba el prefijo de los nombres de registros. Deje en blanco este parámetro para monitorizar todos los archivos. Para obtener información sobre los valores admitidos, consulte el tema relacionado con la propiedad FileSystemWatcherFilter en MSDN.
6. (Opcional) En `CultureName`, especifique la configuración regional en la que se registra la marca temporal. Si `CultureName` está en blanco, se usa de forma predeterminada la misma configuración regional que utiliza actualmente su instancia de Windows. Para obtener más información sobre, consulte la columna `Language tag` en la tabla del tema relacionado con el comportamiento del producto en MSDN.

   Note

   No se admiten los valores `div`, `div-MV`, `hu` y `hu-HU`.
7. (Opcional) En `TimeZoneKind`, especifique `Local` o `UTC`. Puede configurar este valor para proporcionar información sobre la zona horaria cuando no se incluye ninguna información sobre esta en la marca temporal del log. Si este parámetro se deja en blanco y la marca temporal no incluye información sobre la zona horaria, CloudWatch Logs utiliza de forma predeterminada la zona horaria local. Se hace caso omiso a este parámetro si la marca temporal ya contiene información sobre la zona horaria.
8. (Opcional) En `LineCount`, especifique el número de líneas del encabezado para identificar el archivo de registro. Por ejemplo, los archivos de registro de IIS tienen encabezados prácticamente idénticos. Puede especificar **`5`**, que leería las tres primeras líneas del encabezado del archivo de registro para identificarlo. En los archivos de registro de IIS, la tercera línea es la marca de fecha y hora, pero la marca temporal no es siempre diferente entre los archivos de registro. Por este motivo, le recomendamos que incluya al menos una línea de datos de registro reales para identificar de forma única el archivo de registro.

### Para enviar datos de registro de IIS a CloudWatch Logs

1. En el archivo JSON, busque la sección `IISLog`.

```
{
    "Id": "IISLogs",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\W3SVC1",
        "TimestampFormat": "yyyy-MM-dd HH:mm:ss",
        "Encoding": "UTF-8",
        "Filter": "",
        "CultureName": "en-US",
        "TimeZoneKind": "UTC",
        "LineCount": "5"
    }
},
```

2. En `LogDirectoryPath`, especifique la carpeta donde se almacenan los registros de IIS para un sitio individual (por ejemplo, `C:\inetpub\logs\LogFiles\W3SVC`*n*).

   Note

   Solo se admite el formato de registro W3C. Los formatos IIS, NCSA y personalizados no se admiten.

3. En `TimestampFormat`, escriba el formato de marcas temporales que desea utilizar. Para obtener más información sobre los valores admitidos, consulte el tema Cadenas con formato de fecha y hora personalizado en MSDN.
4. En `Encoding`, especifique la codificación del archivo que sea utilizar (por ejemplo, UTF-8). Para obtener información sobre los valores admitidos, consulte el tema relacionado con la clase Encoding en MSDN.

   Note

   Utilice el nombre de codificación, no el nombre de visualización.

5. (Opcional) En `Filter`, escriba el prefijo de los nombres de registros. Deje en blanco este parámetro para monitorizar todos los archivos. Para obtener información sobre los valores admitidos, consulte el tema relacionado con la propiedad FileSystemWatcherFilter en MSDN.
6. (Opcional) En `CultureName`, especifique la configuración regional en la que se registra la marca temporal. Si `CultureName` está en blanco, se usa de forma predeterminada la misma configuración regional que utiliza actualmente su instancia de Windows. Para obtener más información sobre los valores admitidos, consulte la columna `Language tag` en la tabla del tema relacionado con el comportamiento del producto en MSDN.

   Note

   No se admiten los valores `div`, `div-MV`, `hu` y `hu-HU`.

7. (Opcional) En `TimeZoneKind`, escriba `Local` o `UTC`. Puede configurar este valor para proporcionar información sobre la zona horaria cuando no se incluye ninguna información sobre esta en la marca temporal del log. Si este parámetro se deja en blanco y la marca temporal no incluye información sobre la zona horaria, CloudWatch Logs utiliza de forma predeterminada la zona horaria local. Se hace caso omiso a este parámetro si la marca temporal ya contiene información sobre la zona horaria.
8. (Opcional) En `LineCount`, especifique el número de líneas del encabezado para identificar el archivo de registro. Por ejemplo, los archivos de registro de IIS tienen encabezados prácticamente idénticos. Puede especificar **`5`**, que leería las cinco primeras líneas del encabezado del archivo de registro para identificarlo. En los archivos de registro de IIS, la tercera línea es la marca de fecha y hora, pero la marca temporal no es siempre diferente entre los archivos de registro. Por este motivo, le recomendamos que incluya al menos una línea de datos de registro reales para identificar de forma única el archivo de registro.

### Paso 4: Configuración del control de flujo

Cada tipo de datos debe tener un destino correspondiente en la sección `Flows`. Por ejemplo, para enviar el registro personalizado, el registro de ETW y el registro del sistema a CloudWatch Logs, agregue`(CustomLogs,ETW,SystemEventLog),CloudWatchLogs`a la`Flows`sección.

> Warning
>
> Si se añade un paso que no es válido se bloquea el flujo. Por ejemplo, si añade un paso de métrica de disco, pero la instancia no tiene ningún disco, se bloquean todos los pasos del flujo.

Puede enviar el mismo archivo de log a varios destinos. Por ejemplo, para enviar el registro de la aplicación a dos destinos diferentes definidos en la sección `CloudWatchLogs`, agregue `ApplicationEventLog,(CloudWatchLogs,CloudWatchLogs2)` a la sección `Flows`.

Para configurar el control de flujo

1. En el archivo `AWS.EC2.Windows.CloudWatch.json`, busque la sección `Flows`.

```
"Flows": {
    "Flows": [
      "PerformanceCounter,CloudWatch",
      "(PerformanceCounter,PerformanceCounter2), CloudWatch2",
      "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs",
      "CustomLogs, CloudWatchLogs2",
      "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"
    ]
}
```

2. En `Flows`, agregue todos los tipos de datos que desea cargar (por ejemplo, `ApplicationEventLog`) y su destino (por ejemplo, `CloudWatchLogs`).

### Paso 5: Guardar contenido JSON

Acaba de editar el archivo JSON. Guárdelo y pegue el contenido del archivo en un editor de texto en otra ventana. Necesitará el contenido del archivo en un paso posterior de este procedimiento.

## Crear un usuario y un rol de IAM para Systems Manager

Cuando se utiliza Systems Manager Run Command se necesita un rol de IAM para las credenciales de instancia. Este rol permite que Systems Manager de realice acciones en la instancia. Si lo desea, puede crear una única cuenta de usuario de IAM para configurar y ejecutar Systems Manager. Para obtener más información, consulteConfiguración de las funciones de seguridad para Systems Manageren laAWS Systems ManagerGuía del usuario de. Para obtener más información sobre cómo asociar un rol de IAM a una instancia existente, consulteAdjuntar un rol de IAM a una instanciaen laGuía del usuario de Amazon EC2 para instancias de Windows.

## Verifique los requisitos previos de Systems Manager

Antes de utilizar el comando de ejecución de Systems Manager para configurar la integración con CloudWatch Logs, verifique que las instancias cumplen los requisitos mínimos. Para obtener más información, consulteRequisitos previos de Systems Manageren laAWS Systems ManagerGuía del usuario de.

## Verifique el acceso a Internet

Las instancias Amazon EC2 de Windows Server y las instancias administradas deben tener acceso a Internet de salida para poder enviar datos de eventos y registros a CloudWatch. Para obtener más

información acerca de cómo configurar el acceso a Internet, consultePuertos de enlace a Interneten laAmazon VPC User Guide.

### Habilitar CloudWatch Logs mediante Systems Manager Run

Run Command le permite administrar la configuración de las instancias bajo demanda. Puede especificar un documento de Systems Manager, especificar parámetros y ejecutar el comando en una o varias instancias. El agente de SSM de la instancia procesa el comando y configura la instancia tal y como se especifica.

Para configurar la integración con CloudWatch Logs mediante Run Command

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Abra la consola de SSM en.https://console.aws.amazon.com/systems-manager/.
3. En el panel de navegación, elija Run Command.
4. Elija Run a command.
5. En Command document, elija AWS-ConfigureCloudWatch.
6. ParaInstancias de destino, elija las instancias que desea integrar con CloudWatch Logs. Si no ve ninguna instancia en esta lista, puede que no esté configurada para Run Command. Para obtener más información, consulteRequisitos previos de Systems Manageren laGuía del usuario de Amazon EC2 para instancias de Windows.
7. En Status, elija Enabled.
8. En Properties, copie y pegue el contenido JSON que creó en las tareas anteriores.
9. Complete los demás campos opcionales y elija Run.

Utilice el siguiente procedimiento para ver los resultados de la ejecución del comando en la consola de Amazon EC2.

Para ver la información de salida del comando en la consola

1. Seleccione un comando.
2. Elija la pestaña Output.
3. Elija View Output. La página de salida de comandos muestra los resultados de la ejecución de comandos.

## Inicio rápido de: Habilite las instancias de Amazon EC2 que ejecutan Windows Server 2012 y Windows Server 2008 para enviar los registros a los registros de CloudWatch Logs

> Tip
>
> CloudWatch incluye un nuevo agente unificado que pueden recopilar tanto registros como métricas de los servidores locales y las instancias EC2. Le recomendamos que utilice el nuevo agente de CloudWatch unificado de. Para obtener más información, consulte Introducción a los registros de CloudWatch (p. 5) .
> El resto de esta sección explica el uso del agente de CloudWatch Logs de anterior.

# Habilite las instancias de Amazon EC2 que ejecutan Windows Server 2012 y Windows Server 2008 para enviar los registros a los registros de CloudWatch Logs

Utilice los pasos siguientes para habilitar las instancias con Windows Server 2012 y Windows Server 2008 para enviar los registros a los registros a CloudWatch Logs.

## Descargue el archivo de configuración de muestra

Descargue el siguiente archivo JSON de muestra en su equipo: `AWS.EC2.Windows.CloudWatch.json`. Lo editará en los siguientes pasos.

## Configuración del archivo JSON para CloudWatch

Para determinar qué registros se enviarán a CloudWatch, especifique las opciones en el archivo de configuración JSON. El proceso de creación de este archivo y especificación de las opciones puede tardar 30 minutos o más en completarse. Una vez que haya completado esta tarea una vez, podrá volver a utilizar el archivo de configuración en todas sus instancias.

Pasos



### Paso 1: Habilitar los CloudWatch Logs

En la parte superior del archivo JSON, cambie "false" a "true" en `IsEnabled`:

```
"IsEnabled": true,
```

### Paso 2: Configurar la configuración de CloudWatch

Especifique las credenciales, la región, el nombre de un grupo de registros y un espacio de nombres de flujo de registros. Esto permite que la instancia envíe datos de registros a CloudWatch Logs. Para enviar los mismos datos de log a diferentes ubicaciones, puede añadir secciones adicionales con ID únicos (por ejemplo, «CloudWatchLogs2" y CloudWatchLogs3") y una región diferente para cada ID.

Para configurar opciones para enviar datos de registros a CloudWatch Logs

1. En el archivo JSON, busque la sección `CloudWatchLogs`.

```
{
    "Id": "CloudWatchLogs",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "AccessKey": "",
        "SecretKey": "",
        "Region": "us-east-1",
        "LogGroup": "Default-Log-Group",
        "LogStream": "{instance_id}"
    }
},
```

2. Deje los campos `AccessKey` y `SecretKey` en blanco. Configurará las credenciales mediante un rol de IAM.
3. Para`Region`, escriba la región a la que desea enviar los datos de log (por ejemplo,`us-east-2`).
4. En `LogGroup`, especifique el nombre del grupo de registros. Este nombre aparece en elGrupos de registrosen la consola de CloudWatch.
5. En `LogStream`, especifique el flujo de registros de destino. Este nombre aparece en elGrupos de registro > Streamsen la consola de CloudWatch.

   Si utiliza `{instance_id}`, el nombre del flujo de registro de destino predeterminado es el ID de esta instancia.

   Si especifica un nombre de flujo de registro que no existe, CloudWatch Logs lo crea automáticamente. Puede definir el nombre del flujo de registro mediante una cadena literal, las variables predefinidas `{instance_id}`, `{hostname}` y `{ip_address}`, o una combinación de ellas.

### Paso 3: Configurar los datos que se van a enviar

Puede enviar datos de registro de eventos, datos de Seguimiento de eventos para Windows (ETW) y otros datos de registro a CloudWatch Logs.

#### Para enviar datos de registro de eventos de aplicación de Windows a CloudWatch Logs

1. En el archivo JSON, busque la sección `ApplicationEventLog`.

```
{
    "Id": "ApplicationEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Application",
        "Levels": "1"
    }
},
```

2. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

#### Para enviar datos de registros de seguridad a CloudWatch Logs

1. En el archivo JSON, busque la sección `SecurityEventLog`.

```
{
    "Id": "SecurityEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Security",
        "Levels": "7"
    }
```

```
},
```

2. En `Levels`, especifique **`7`** para cargar todos los mensajes.

### Para enviar datos de registros de eventos del sistema a CloudWatch Logs

1. En el archivo JSON, busque la sección `SystemEventLog`.

```
{
    "Id": "SystemEventLog",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "System",
        "Levels": "7"
    }
},
```

2. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **`3`** carga mensajes de error (**`1`**) y mensajes de advertencia (**`2`**). Un valor **`7`** carga mensajes de error (**`1`**), mensajes de advertencia (**`2`**) y mensajes de información (**`4`**).

### Para enviar otros tipos de datos de registro de eventos a CloudWatch Logs

1. En el archivo JSON, añada una nueva sección. Cada sección debe tener un `Id` único.

```
{
    "Id": "Id-name",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Log-name",
        "Levels": "7"
    }
},
```

2. En `Id`, escriba un nombre para el registro que desea cargar (por ejemplo, **`WindowsBackup`**).
3. En `LogName`, escriba el nombre del registro que se va a cargar. Puede encontrar el nombre del registro como se indica a continuación.

   a. Abra el Visor de eventos.
   b. En el panel de navegación, elija Registros de aplicaciones y servicios.
   c. Navegue hasta el registro y elija Actions, Properties.
4. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **`1`**: cargar solo mensajes de error.
   - **`2`**: cargar solo mensajes de advertencia.
   - **`4`**: cargar solo mensajes de información.

Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **3** carga mensajes de error (**1**) y mensajes de advertencia (**2**). Un valor **7** carga mensajes de error (**1**), mensajes de advertencia (**2**) y mensajes de información (**4**).

### Para enviar datos de Seguimiento de eventos para Windows a los CloudWatch Logs

ETW (Seguimiento de eventos para Windows) proporciona un mecanismo de registro detallado y eficiente en el que las aplicaciones pueden escribir los registros. Cada ETW se controla mediante un administrador de sesiones que puede iniciar y parar la sesión de registro. Cada sesión tiene un proveedor y uno o varios consumidores.

1. En el archivo JSON, busque la sección `ETW`.

```
{
    "Id": "ETW",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogName": "Microsoft-Windows-WinINet/Analytic",
        "Levels": "7"
    }
},
```

2. En `LogName`, escriba el nombre del registro que se va a cargar.
3. En `Levels`, especifique el tipo de mensajes que desea cargar. Puede especificar uno de los siguientes valores:

   - **1**: cargar solo mensajes de error.
   - **2**: cargar solo mensajes de advertencia.
   - **4**: cargar solo mensajes de información.

   Puede combinar valores para incluir más de un tipo de mensaje. Por ejemplo, un valor **3** carga mensajes de error (**1**) y mensajes de advertencia (**2**). Un valor **7** carga mensajes de error (**1**), mensajes de advertencia (**2**) y mensajes de información (**4**).

### Para enviar registros personalizados (cualquier archivo de registro basado en texto) a CloudWatch Logs

1. En el archivo JSON, busque la sección `CustomLogs`.

```
{
    "Id": "CustomLogs",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogDirectoryPath": "C:\\CustomLogs\\",
        "TimestampFormat": "MM/dd/yyyy HH:mm:ss",
        "Encoding": "UTF-8",
        "Filter": "",
        "CultureName": "en-US",
        "TimeZoneKind": "Local",
        "LineCount": "5"
    }
},
```

2. En `LogDirectoryPath`, escriba la ruta de la instancia donde se almacenan los registros.

3. En `TimestampFormat`, escriba el formato de marcas temporales que desea utilizar. Para obtener más información sobre los valores admitidos, consulte el tema Cadenas con formato de fecha y hora personalizado en MSDN.

   Important

   Su archivo de log de origen debe tener la marca temporal al principio de cada línea de log y debe haber un espacio en blanco tras dicha marca.

4. En `Encoding`, especifique la codificación del archivo que sea utilizar (por ejemplo, UTF-8). Para obtener información sobre los valores admitidos, consulte el tema relacionado con la clase Encoding en MSDN.

   Note

   Utilice el nombre de codificación, no el nombre de visualización.

5. (Opcional) En `Filter`, escriba el prefijo de los nombres de registros. Deje en blanco este parámetro para monitorizar todos los archivos. Para obtener información sobre los valores admitidos, consulte el tema relacionado con la propiedad FileSystemWatcherFilter en MSDN.
6. (Opcional) En `CultureName`, especifique la configuración regional en la que se registra la marca temporal. Si `CultureName` está en blanco, se usa de forma predeterminada la misma configuración regional que utiliza actualmente su instancia de Windows. Para obtener más información sobre los valores admitidos, consulte la columna `Language tag` en la tabla del tema relacionado con el comportamiento del producto en MSDN.

   Note

   No se admiten los valores `div`, `div-MV`, `hu` y `hu-HU`.

7. (Opcional) En `TimeZoneKind`, especifique `Local` o `UTC`. Puede configurar este valor para proporcionar información sobre la zona horaria cuando no se incluye ninguna información sobre esta en la marca temporal del log. Si este parámetro se deja en blanco y la marca temporal no incluye información sobre la zona horaria, CloudWatch Logs utiliza de forma predeterminada la zona horaria local. Se hace caso omiso a este parámetro si la marca temporal ya contiene información sobre la zona horaria.
8. (Opcional) En `LineCount`, especifique el número de líneas del encabezado para identificar el archivo de registro. Por ejemplo, los archivos de registro de IIS tienen encabezados prácticamente idénticos. Puede especificar **`5`**, que leería las tres primeras líneas del encabezado del archivo de registro para identificarlo. En los archivos de registro de IIS, la tercera línea es la marca de fecha y hora, pero la marca temporal no es siempre diferente entre los archivos de registro. Por este motivo, le recomendamos que incluya al menos una línea de datos de registro reales para identificar de forma única el archivo de registro.

### Para enviar datos de registro de IIS a CloudWatch Logs

1. En el archivo JSON, busque la sección `IISLog`.

```
{
    "Id": "IISLogs",
    "FullName":
 "AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch",
    "Parameters": {
        "LogDirectoryPath": "C:\\inetpub\\logs\\LogFiles\\W3SVC1",
        "TimestampFormat": "yyyy-MM-dd HH:mm:ss",
        "Encoding": "UTF-8",
        "Filter": "",
        "CultureName": "en-US",
        "TimeZoneKind": "UTC",
        "LineCount": "5"
    }
```

```
},
```

2. En `LogDirectoryPath`, especifique la carpeta donde se almacenan los registros de IIS para un sitio individual (por ejemplo, `C:\inetpub\logs\LogFiles\W3SVCn`).

   Note

   Solo se admite el formato de registro W3C. Los formatos IIS, NCSA y personalizados no se admiten.

3. En `TimestampFormat`, escriba el formato de marcas temporales que desea utilizar. Para obtener más información sobre los valores admitidos, consulte el tema Cadenas con formato de fecha y hora personalizado en MSDN.
4. En `Encoding`, especifique la codificación del archivo que sea utilizar (por ejemplo, UTF-8). Para obtener información sobre los valores admitidos, consulte el tema relacionado con la clase Encoding en MSDN.

   Note

   Utilice el nombre de codificación, no el nombre de visualización.

5. (Opcional) En `Filter`, escriba el prefijo de los nombres de registros. Deje en blanco este parámetro para monitorizar todos los archivos. Para obtener información sobre los valores admitidos, consulte el tema relacionado con la propiedad FileSystemWatcherFilter en MSDN.
6. (Opcional) En `CultureName`, especifique la configuración regional en la que se registra la marca temporal. Si `CultureName` está en blanco, se usa de forma predeterminada la misma configuración regional que utiliza actualmente su instancia de Windows. Para obtener más información sobre los valores admitidos, consulte la columna `Language tag` en la tabla del tema relacionado con el comportamiento del producto en MSDN.

   Note

   No se admiten los valores `div`, `div-MV`, `hu` y `hu-HU`.

7. (Opcional) En `TimeZoneKind`, escriba `Local` o `UTC`. Puede configurar este valor para proporcionar información sobre la zona horaria cuando no se incluye ninguna información sobre esta en la marca temporal del log. Si este parámetro se deja en blanco y la marca temporal no incluye información sobre la zona horaria, CloudWatch Logs utiliza de forma predeterminada la zona horaria local. Se hace caso omiso a este parámetro si la marca temporal ya contiene información sobre la zona horaria.
8. (Opcional) En `LineCount`, especifique el número de líneas del encabezado para identificar el archivo de registro. Por ejemplo, los archivos de registro de IIS tienen encabezados prácticamente idénticos. Puede especificar **`5`**, que leería las cinco primeras líneas del encabezado del archivo de registro para identificarlo. En los archivos de registro de IIS, la tercera línea es la marca de fecha y hora, pero la marca temporal no es siempre diferente entre los archivos de registro. Por este motivo, le recomendamos que incluya al menos una línea de datos de registro reales para identificar de forma única el archivo de registro.

### Paso 4: Configuración del control de flujo

Cada tipo de datos debe tener un destino correspondiente en la sección `Flows`. Por ejemplo, para enviar el registro personalizado, el registro de ETW y el registro del sistema a CloudWatch Logs, agregue`(CustomLogs,ETW,SystemEventLog),CloudWatchLogs`a la`Flows`sección.

Warning

Si se añade un paso que no es válido se bloquea el flujo. Por ejemplo, si añade un paso de métrica de disco, pero la instancia no tiene ningún disco, se bloquean todos los pasos del flujo.

Puede enviar el mismo archivo de log a varios destinos. Por ejemplo, para enviar el registro de la aplicación a dos destinos diferentes definidos en la sección `CloudWatchLogs`, agregue `ApplicationEventLog,(CloudWatchLogs,CloudWatchLogs2)` a la sección `Flows`.

Para configurar el control de flujo

1. En el archivo `AWS.EC2.Windows.CloudWatch.json`, busque la sección `Flows`.

```
"Flows": {
    "Flows": [
      "PerformanceCounter,CloudWatch",
      "(PerformanceCounter,PerformanceCounter2), CloudWatch2",
      "(CustomLogs, ETW, SystemEventLog),CloudWatchLogs",
      "CustomLogs, CloudWatchLogs2",
      "ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"
    ]
}
```

2. En `Flows`, agregue todos los tipos de datos que desea cargar (por ejemplo, `ApplicationEventLog`) y su destino (por ejemplo, `CloudWatchLogs`).

Acaba de editar el archivo JSON. Lo utilizará en un paso posterior.

## Iniciar el agente

Para permitir que una instancia de Amazon EC2 que ejecuta Windows Server 2012 o Windows Server 2008 envíe registros a CloudWatch Logs, utilice el servicio EC2Config (`EC2Config.exe`). La instancia debe tener EC2Config 4.0 o posterior, y puede utilizar este procedimiento. Para obtener más información sobre el uso de una versión anterior de EC2Config, consulteUtilice EC2config 3.x o versiones anteriores para configurar CloudWatchen laGuía del usuario de Amazon EC2 para instancias de Windows

Para configurar CloudWatch mediante EC2Config 4.x

1. Compruebe la codificación de la`AWS.EC2.Windows.CloudWatch.json`que ha editado anteriormente en este procedimiento. Solo se admite la codificación UTF-8 sin BOM. A continuación, guarde el archivo en la siguiente carpeta de la instancia con Windows Server 2008 - 2012 R2: `C:\Program Files\Amazon\SSM\Plugins\awsCloudWatch\`.
2. Inicie o reinicie el agente SSM (`AmazonSSMAgent.exe`) mediante el panel de control de Windows Services o el siguiente comando de PowerShell:

```
PS C:\> Restart-Service AmazonSSMAgent
```

Una vez que el agente de SSM se reinicia, detecta el archivo de configuración y configura la instancia para la integración con CloudWatch. Si cambia los parámetros y valores del archivo de configuración local, debe reiniciar el agente de SSM para que detecte los cambios. Para deshabilitar la integración de CloudWatch en la instancia, cambie`IsEnabled`De a`false`Guarde los cambios en el archivo de configuración.

# Inicio rápido de: Instale el agente CloudWatch Logs conAWS OpsWorksy Chef

Puede instalar el agente CloudWatch Logs y crear flujos de registro medianteAWS OpsWorksy Chef, que es una herramienta de automatización de infraestructura en la nube y sistemas de terceros. Chef utiliza "recetas", que se escriben para instalar y configurar software en el equipo, y "libros de recetas", que son colecciones de recetas para realizar sus tareas de configuración y distribución de políticas. Para obtener más información, consulte Chef.

Los siguientes ejemplos de recetas muestran cómo monitorizar un archivo de registro en cada instancia EC2. Las recetas utilizan el nombre de stack como grupo de registros y el nombre de host de la instancia

como el nombre del flujo de registro. Si desea monitorizar varios archivos de log, tendrá que ampliar las recetas para crear varios grupos y flujos de logs.

## Paso 1: Cree recetas personalizadas.

Cree un repositorio para almacenar sus recetas.AWS OpsWorksadmite Git y Subversion o puede almacenar un archivo de almacenamiento en Amazon S3. La estructura de su repositorio de libros de recetas se describe enRepositorios de libros de recetasen laAWS OpsWorksGuía del usuario de. Los ejemplos que aparecen a continuación suponen que el libro de recetas se llama `logs`. La receta install.rb instala el agente de CloudWatch Logs. También puede descargar el libro de recetas de ejemplo (CloudWatchLogs-Cookbooks.zip).

Cree un archivo denominado metadata.rb que contiene el siguiente código:

```
#metadata.rb

name             'logs'
version          '0.0.1'
```

Cree el archivo de configuración de CloudWatch Logs:

```
#config.rb

template "/tmp/cwlogs.cfg" do
  cookbook "logs"
  source "cwlogs.cfg.erb"
  owner "root"
  group "root"
  mode 0644
end
```

Descargue e instalar el agente de CloudWatch Logs:

```
# install.rb

directory "/opt/aws/cloudwatch" do
  recursive true
end

remote_file "/opt/aws/cloudwatch/awslogs-agent-setup.py" do
  source "https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py"
  mode "0755"
end

  execute "Install CloudWatch Logs agent" do
  command "/opt/aws/cloudwatch/awslogs-agent-setup.py -n -r region -c /tmp/cwlogs.cfg"
  not_if { system "pgrep -f aws-logs-agent-setup" }
end
```

> **Note**
>
> En el ejemplo anterior, reemplace*región*Con uno de los siguientes: us-east-1, us-west-1, us-west-1, ap-south-1, ap-northeast-2, ap-southeast-1, ap-southeast-1, ap-southeast-1, eu-central-1, eu-central-1, eu-west-1, o sa-east-1.

Si se produce algún error en la instalación del agente, asegúrese de que el paquete `python-dev` está instalado. Si no lo está, utilice el siguiente comando e intente de nuevo la instalación del agente:

```
sudo apt-get -y install python-dev
```

Esta receta utiliza un archivo de plantilla cwlogs.cfg.erb que puede modificar para especificar distintos atributos como, por ejemplo, archivos que registrar. Para obtener más información sobre estos atributos, consulte Registros de CloudWatchacaballeroreference (p. 164).

```
[general]
# Path to the AWSLogs agent's state file. Agent uses this file to maintain
# client side state across its executions.
state_file = /var/awslogs/state/agent-state


## Each log file is defined in its own section. The section name doesn't
## matter as long as its unique within this file.
#
#[kern.log]
#
## Path of log file for the agent to monitor and upload.
#
#file = /var/log/kern.log
#
## Name of the destination log group.
#
#log_group_name = kern.log
#
## Name of the destination log stream.
#
#log_stream_name = {instance_id}
#
## Format specifier for timestamp parsing.
#
#datetime_format = %b %d %H:%M:%S
#
#

[<%= node[:opsworks][:stack][:name] %>]
datetime_format = [%Y-%m-%d %H:%M:%S]
log_group_name = <%= node[:opsworks][:stack][:name].gsub(' ','_') %>
file = <%= node[:cwlogs][:logfile] %>
log_stream_name = <%= node[:opsworks][:instance][:hostname] %>
```

La plantilla obtiene el nombre del stack y el nombre del host haciendo referencia a los atributos correspondientes en la configuración de stack e implementación JSON. El atributo que especifica el archivo que registrar se define en el archivo de atributos default.rb del libro de recetas cwlogs (logs/attributes/default.rb).

```
default[:cwlogs][:logfile] = '/var/log/aws/opsworks/opsworks-agent.statistics.log'
```

## Paso 2: Creación de unAWS OpsWorkspila

1. Abra el iconoAWS OpsWorksconsola de en.https://console.aws.amazon.com/opsworks/.
2. En OpsWorks Dashboard (Panel de OpsWorks), elija Add stack (Agregar pila)para crear una pila de AWS OpsWorks.
3. En la pantalla Add stack, elija Chef 11 stack.
4. En Stack name, escriba un nombre.
5. En Use custom Chef Cookbooks, elija Yes.
6. En Repository type, seleccione el tipo de repositorio que utiliza. Si está utilizando el ejemplo anterior, elija Http Archive.
7. En Repository URL, escriba el repositorio donde guardó el libro de recetas que creó en el paso anterior. Si está utilizando el ejemplo anterior, escriba **`https://s3.amazonaws.com/aws-cloudwatch/downloads/CloudWatchLogs-Cookbooks.zip`**.

8. Elija Add Stack para crear la pila.

## Paso 3: Ampliar su rol de IAM

Para usar CloudWatch Logs con suAWS OpsWorks, tiene que ampliar el rol de IAM utilizado por sus instancias.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Policies, Create Policy.
3. En la página Create Policy, en Create Your Own Policy, elija Select. Para obtener más información acerca de la creación de políticas personalizadas, consultePolíticas de IAM para Amazon EC2en laGuía del usuario de Amazon EC2 para instancias de Linux.
4. En la página Review Policy, en Policy Name, escriba un nombre para la política.
5. En Policy Document, pegue la siguiente política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
    ],
    "Resource": [
      "arn:aws:logs:*:*:*"
    ]
  }
 ]
}
```

6. Elija Create Policy (Crear política).
7. En el panel de navegación, elija Roles y, a continuación, en el panel de contenido, en Role Name (Nombre de rol), seleccione el nombre del rol de instancia que utiliza su pila de AWS OpsWorks. Puede encontrar el utilizado por su stack en la configuración de stack (el valor predeterminado es `aws-opsworks-ec2-role`).

   Note

   Elija el nombre del rol, no la casilla de verificación.
8. En la pestaña Permissions, en Managed Policies, seleccione Attach Policy.
9. En la página Attach Policy, en el encabezado de la tabla (junto a Filter y Search), elija Policy Type, Customer Managed Policies.
10. ParaPolíticas administradas por el cliente, seleccione la política de IAM de que ha creado anteriormente y elijaAsociación de políticas de.

    Para obtener más información acerca de los usuarios y las políticas de IAM, consulteUsuarios y grupos de IAMyAdministración de políticas de IAMen laIAM User Guide.

## Paso 4: Añadir una capa

1. Abra el iconoAWS OpsWorksconsola de en.https://console.aws.amazon.com/opsworks/.
2. En el panel de navegación, elija Layers.

3. En el panel de contenido, seleccione una capa y elija Add layer.
4. En la pestaña OpsWorks, en Layer type, elija Custom.
5. En los campos Name y Short name, escriba el nombre breve y largo de la capa y, a continuación, elija Add layer.
6. En la pestaña Recipes (Recetas), en Custom Chef Recipes (Recetas de Chef personalizadas), hay varios encabezados (Setup, Configure, Deploy, Undeploy, and Shutdown), que corresponden a eventos de ciclo de vida de AWS OpsWorks. AWS OpsWorks dispara eventos en estos puntos clave en el ciclo de vida de la instancia, que ejecuta las recetas asociadas.

   Note

   Si los encabezados anteriores no son visibles, en Custom Chef Recipes, elija edit.
7. Escriba logs::config, logs::install junto a Setup, elija + para añadirlo a la lista y, a continuación, elija Save.

   AWS OpsWorks ejecuta esta receta en cada una de las nuevas instancias de esta capa, justo después del arranque de la instancia.

## Paso 5: Adición de una instancia

La capa solo controla cómo configurar las instancias. Ahora es necesario agregar algunas instancias a la capa e iniciarlas.

1. Abra el iconoAWS OpsWorksconsola de en.https://console.aws.amazon.com/opsworks/.
2. En el panel de navegación, elija Instances y, a continuación, bajo su capa, elija + Instance.
3. Acepte la configuración predeterminada y elija Add Instance para añadir la instancia a la capa.
4. En la columna Actions de la fila, haga clic en start para comenzar la instancia.

   AWS OpsWorkslanza una nueva instancia EC2 y configura CloudWatch Logs. El estado de la instancia cambia a en línea cuando está listo.

## Paso 6: Ver sus registros

Debería ver el grupo de registros de nueva creación y el flujo de registros en la consola de CloudWatch después de que el agente haya estado en ejecución durante unos minutos.

Para obtener más información, consulte VistalOGdatasen CloudWatch Logs (p. 60) .

# Informar del estado del agente CloudWatch Logs

Utilice el siguiente procedimiento para informar del estado del agente de CloudWatch Logs en la instancia EC2.

### Para informar del estado del agente

1. Conéctese a su instancia EC2. Para obtener más información, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   Para obtener más información acerca de los problemas de conexión, consulteSolución de problemas con la conexión a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux
2. En el símbolo del sistema, escriba el siguiente comando:

```
sudo service awslogs status
```

Si está ejecutando Amazon Linux 2, escriba el siguiente comando:

```
sudo service awslogsd status
```

3. Compruebe la/var/log/awslogs.logPara ver si hay errores, advertencias o problemas con el agente de CloudWatch Logs.

# Iniciar el agente CloudWatch Logs

Si el agente de CloudWatch Logs en la instancia EC2 no comienza automáticamente después de la instalación o en caso de parar el agente de, puede utilizar el siguiente procedimiento para iniciar el agente.

Para iniciar el agente de

1. Conéctese a su instancia EC2. Para obtener más información, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   Para obtener más información acerca de los problemas de conexión, consulteSolución de problemas con la conexión a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.
2. En el símbolo del sistema, escriba el siguiente comando:

```
sudo service awslogs start
```

   Si está ejecutando Amazon Linux 2, escriba el siguiente comando:

```
sudo service awslogsd start
```

# Detener el agente CloudWatch Logs

Utilice el siguiente procedimiento para parar el agente de CloudWatch Logs en la instancia EC2.

Para detener el agente

1. Conéctese a su instancia EC2. Para obtener más información, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   Para obtener más información acerca de los problemas de conexión, consulteSolución de problemas con la conexión a la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.
2. En el símbolo del sistema, escriba el siguiente comando:

```
sudo service awslogs stop
```

   Si está ejecutando Amazon Linux 2, escriba el siguiente comando:

```
sudo service awslogsd stop
```

# Inicio rápido de: UsarAWS CloudFormationpara comenzar con CloudWatch Logs

AWS CloudFormation le permite describir y aprovisionar sus recursos de AWS en formato JSON. Las ventajas de este método incluyen la posibilidad de administrar una colección deAWScomo una sola unidad, y replicar fácilmente suAWSen las regiones.

Al aprovisionar AWS mediante AWS CloudFormation, debe crear plantillas que describan los recursos de AWS que utilizar. El siguiente ejemplo es un fragmento de plantilla que crea un grupo de registro y un filtro de métricas que cuenta las incidencias de 404 y envía este recuento al grupo de registro.

```
"WebServerLogGroup": {
    "Type": "AWS::Logs::LogGroup",
    "Properties": {
        "RetentionInDays": 7
    }
},

"404MetricFilter": {
    "Type": "AWS::Logs::MetricFilter",
    "Properties": {
        "LogGroupName": {
            "Ref": "WebServerLogGroup"
        },
        "FilterPattern": "[ip, identity, user_id, timestamp, request, status_code = 404,
 size, ...]",
        "MetricTransformations": [
            {
                "MetricValue": "1",
                "MetricNamespace": "test/404s",
                "MetricName": "test404Count"
            }
        ]
    }
}
```

Se trata de un ejemplo básico. Puede configurar implementaciones de CloudWatch Logs mucho más ricas utilizandoAWS CloudFormation. Para obtener más información acerca de los ejemplos de plantillas, consulteFragmentos de la plantilla de Amazon CloudWatch Logsen laAWS CloudFormationGuía del usuario de. Para obtener más información acerca de cómo empezar a utilizarla, consulteIntroducción aAWS CloudFormationen laAWS CloudFormationGuía del usuario de.

# Análisis de datos de registro con CloudWatch Logs Insights

CloudWatch Logs Insights le permite buscar y analizar de forma interactiva sus datos de registro en Amazon CloudWatch Logs. Puede realizar consultas que le ayuden a responder de forma más eficaz a los problemas de funcionamiento. Si se produce un problema, puede utilizar CloudWatch Logs Insights para identificar posibles causas y validar soluciones implementadas.

CloudWatch Logs Insights incluye un lenguaje de consultas específico con algunos comandos sencillos pero eficaces. CloudWatch Logs Insights proporciona consultas de ejemplo, descripciones de comandos, finalización automática de consultas y detección de campos de registro para ayudarle a empezar. Se incluyen ejemplos de consultas para varios tipos de registros de servicios de AWS.

CloudWatch Logs Insights descubre automáticamente los campos en los registros deAWSservicios como Amazon Route 53,AWS Lambda,AWS CloudTraily Amazon VPC, y cualquier aplicación o registro personalizado que emite eventos de registro como JSON.

Puede utilizar CloudWatch Logs Insights para buscar datos de registro enviados a CloudWatch Logs el 5 de noviembre de 2018 o posteriormente.

Una única solicitud puede consultar hasta 20 grupos de registros. Las consultas expiran después de 15 minutos, si no se han completado. Los resultados de las consultas están disponibles durante 7 días.

Puede guardar las consultas que haya creado. Esto puede ayudarle a ejecutar consultas complejas cuando lo necesite, sin tener que volver a crearlas cada vez que desee ejecutarlas.

CloudWatch Logs Insights Las consultas de Insights incurren en cargos en función del volumen de datos consultados. Para obtener más información, consulte los precios de Amazon CloudWatch.

> **Important**
>
> Si su equipo de seguridad de red no permite el uso de sockets de web, no puede acceder a la parte de CloudWatch Logs Insights de la consola de CloudWatch. Puede utilizar las capacidades de consulta CloudWatch Logs Insights con API. Para obtener más información, consulteStartQueryen laReferencia de la API de Amazon CloudWatch Logs.

Contenido

- Ver consultas o historial de consultas en ejecución (p. 59)

# Registros admitidos y campos descubiertos

Los informes de CloudWatch Logs Insights admiten todo tipo de registros. Para cada sesión enviada a CloudWatch Logs, se generan automáticamente cinco campos del sistema:

- `@message` contiene el evento de registro sin analizar ni procesar. Esto equivale al campo `message` en InputLogEvent.
- `@timestamp` contiene la marca de tiempo del evento incluida en el campo `timestamp` del evento de registro. Esto equivale al campo `timestamp` en InputLogEvent.
- `@ingestionTime`contiene la hora a la que recibió el evento de registro por CloudWatch Logs.
- `@logStream` contiene el nombre del flujo de registros al que se añadió el evento de registro. Las secuencias de registro se utilizan para agrupar registros por el mismo proceso que los generó.
- `@log` es un identificador de grupo de registro con el formato *`account-id`*`:`*`log-group-name`*. Puede ser útil en consultas de varios grupos de registro para identificar a qué grupo de registro pertenece un evento determinado.

CloudWatch Logs Insights inserta el@al principio de los campos que genera.

Para muchos tipos de registro, CloudWatch Logs también detecta automáticamente los campos de registro contenidos en los registros. Estos campos de detección automática se muestran en la siguiente tabla.

Para otros tipos de registros con campos que CloudWatch Logs Insights no detecta automáticamente, puede utilizar la herramienta**`parse`**Para extraer y crear campos efímeros para su uso en esa consulta. Para obtener más información, consulte Sintaxis de consulta CloudWatch Logs Insights (p. 41) .

Si el nombre de un campo de registro detectado comienza con el@, CloudWatch Logs Insights lo muestra con un@anexado al principio. Por ejemplo, si un nombre de campo de registro es `@example.com`, este nombre de campo se muestra como `@@example.com`.

| Log type (Tipo de registro) | Campos de registro detectados |
|---|---|
| Registros de flujo de Amazon VPC | `@timestamp`, `@logStream`, `@message`, `accountId`, `endTime`, `interfaceId`, `logStatus`, `startTime`, `version`, `action`, `bytes`, `dstAddr`, `dstPort`, `packets`, `protocol`, `srcAddr`, `srcPort` |
| Registros de Route 53 | `@timestamp`, `@logStream`, `@message`, `edgeLocation`, `hostZoneId`, `protocol`, `queryName`, `queryTimestamp`, `queryType`, `resolverIp`, `responseCode`, `version` |
| Troncos de Lambda | `@timestamp`, `@logStream`, `@message`, `@requestId`, `@duration`, `@billedDuration`, `@type`, `@maxMemoryUsed`, `@memorySize`<br><br>Si una línea de registro de Lambda contiene un ID de seguimiento de X-Ray, también incluye los campos siguientes:`@xrayTraceId`y`@xraySegmentId`.<br><br>CloudWatch Logs Insights descubre automáticamente los campos de registro en registros de Lambda, pero solo para el primer fragmento JSON integrado en cada evento de registro. Si un evento de registro de Lambda contiene varios fragmentos JSON, puede analizar y extraer los campos de registro con la herramienta**`parse`**comando. Para obtener más información, consulte Campos de registros JSON (p. 37) . |

| Log type (Tipo de registro) | Campos de registro detectados |
| --- | --- |
| Registros de CloudTrail<br><br>Registros en formato JSON | Para obtener más información, consulte Campos de registros JSON (p. 37) . |
| Otros tipos de registros | `@timestamp`, `@ingestionTime`, `@logStream`, `@message`, `@log`. |

# Campos de registros JSON

CloudWatch Logs Insights representa los campos JSON anidados que utilizan la notación de puntos. En el siguiente ejemplo de evento JSON, el campo `type` del objeto JSON `userIdentity` se representa como `userIdentity.type`.

Las matrices JSON se aplanan en una lista de nombres de campos y valores. Por ejemplo, para especificar el valor de `instanceId` para que el primer elemento `requestParameters.instancesSet`, utilice `requestParameters.instancesSet.items.0.instanceId`.

CloudWatch Logs Insights puede extraer un máximo de 1000 campos de eventos de registro de un registro JSON. Para campos adicionales que no se extraen, puede utilizar el comando parse para analizar estos campos desde el evento de registro sin analizar en el campo de mensaje.

```
{ "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn: aws: iam: : 123456789012: user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21: 22: 54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools1.6.12.2",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-abcde123"
                }
            ]
        }
    },
    "responseElements": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-abcde123",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
```

```
                    "code": 80,
                    "name": "stopped"
                }
            }
        ]
    }
}
```

# Tutorial: Ejecutar y modificar una consulta de muestra de

El siguiente tutorial le ayuda a familiarizarse con CloudWatch Logs Insights. Ejecute una consulta de muestra y, a continuación, verá cómo modificarla y volverla a ejecutar.

Para ejecutar una consulta, debe disponer ya de registros almacenados en CloudWatch Logs. Si ya está utilizando CloudWatch Logs y tiene configurados grupos de registro y flujos de registros, está listo para comenzar. Es posible que también ya tenga registros si utiliza servicios comoAWS CloudTrail, Amazon Route 53 o Amazon VPC y ha configurado los registros de dichos servicios para ir a CloudWatch Logs. Para obtener más información sobre el envío de registros a CloudWatch Logs, consulteIntroducción a los registros de CloudWatch (p. 5).

Las consultas en CloudWatch Logs Insights devuelven un conjunto de campos de eventos de registro, o el resultado de una agregación matemática u otra operación realizada en eventos de registro. Este tutorial muestra una consulta que devuelve una lista de eventos de registro.

## Ejecutar una consulta de muestra de

Comience por ejecutar una consulta de muestra.

### Para ejecutar una consulta de ejemplo de CloudWatch Logs Insights

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.

   Cerca de la parte superior de la pantalla se encuentra el editor de consultas. La primera vez que se abre CloudWatch Logs Insights, este cuadro contiene una consulta predeterminada que devuelve los 20 eventos de registro más recientes.
3. Seleccione uno o varios grupos de registros que va a consultar, encima del editor de consultas. Para ayudarle a encontrar los grupos de registro, puede introducir texto en la barra de búsqueda y CloudWatch Logs mostrará los grupos de registro coincidentes en la barra de búsqueda.

   Al seleccionar un grupo de registros, CloudWatch Logs Insights detecta automáticamente los campos de los datos del grupo de registros. Para ver estos campos detectados, seleccione Fields (Campos) a la derecha de la página.
4. (Opcional) Utilice el selector de tiempo situado en la parte superior derecha para seleccionar el periodo de tiempo que desea consultar.
5. Elija Run (Ejecutar).

   Aparecen los resultados de la consulta. En este ejemplo, los resultados son los últimos 20 eventos de registro de cualquier tipo.

   CloudWatch Logs también muestra un gráfico de barras de eventos de registro en este grupo de registros con el paso del tiempo. Este gráfico de barras muestra la distribución de los eventos en el grupo de registros que coincide con la consulta y el intervalo de tiempo, no solo los eventos que se muestran en la tabla.

6. Para ver todos los campos de uno de los eventos de registro devueltos, elija el icono que aparece a la izquierda de ese evento de registro.

# Modificar la consulta de muestra de

En este tutorial, debe modificar la consulta de muestra para mostrar los 50 eventos de registro más recientes.

Si aún no ha ejecutado el tutorial anterior, hágalo ahora. Este tutorial comienza donde finaliza el tutorial anterior.

> **Note**
>
> Algunas consultas de muestra proporcionadas con CloudWatch Logs Insights utilizan`head`or`tail`Comandos en lugar de`limit`. Estos comandos están obsoletos y se han sustituido por `limit`. Utilice `limit` en lugar de `head` o `tail` en todas las consultas que escriba.

### Para modificar la consulta de ejemplo de CloudWatch Logs Insights

1. En el editor de consultas, cambie 20 a 50 y, a continuación, elija Run (Ejecutar).

   Aparecen los resultados de la nueva consulta. Suponiendo que haya suficientes datos en el grupo de registros en el intervalo de tiempo predeterminado, ahora hay 50 eventos de registro en la lista.
2. (Opcional) Puede guardar las consultas que haya creado. Para guardar esta consulta, elija Save (Guardar). Para obtener más información, consulte Guardar y volver a ejecutar consultas de CloudWatch Logs Insights (p. 54) .

# Agregar un comando de filtro a la consulta de muestra de

En este tutorial se muestra cómo realizar un cambio más potente en la consulta en el editor de consultas. En este tutorial, se filtran los resultados de la consulta anterior en función de un campo de los eventos de registro recuperados.

Si aún no ha ejecutado los tutoriales anteriores, hágalo ahora. Este tutorial comienza donde finaliza el tutorial anterior.

### Para añadir un comando de filtro a la consulta anterior

1. Decida un campo que filtrar. Para ver los campos más frecuentes que CloudWatch Logs ha detectado en los eventos de registro contenidos en los grupos de registro seleccionados en los últimos 15 minutos y el porcentaje de esos eventos de registro en los que aparece cada campo, seleccioneCamposen la parte derecha de la página.

   Para ver los campos contenidos en un evento de registro determinado, elija el icono que aparece a la izquierda de dicha fila.

   El campo awsRegion podría aparecer en su evento de registro, en función de los eventos que se encuentren en sus registros. En el resto de este tutorial, utilizaremos awsRegion como campo de filtro, pero puede utilizar un campo diferente si ese campo no está disponible.
2. En el editor de consultas, coloque el cursor después de 50 y pulse Intro.
3. En la nueva línea, introduzca | (la barra vertical) y un espacio. Los comandos de una consulta de CloudWatch Logs Insights deben ir separados por el carácter de barra.
4. Escriba **`filter awsRegion="us-east-1"`**.

5. Elija Run (Ejecutar).

   La consulta se ejecuta de nuevo, y ahora muestra el 50 resultados más recientes que coinciden con el nuevo filtro.

   Si filtra en otro campo diferente y recibe un resultado erróneo, es posible que sea necesario aplicar escape al nombre de campo. Si el nombre de campo incluye caracteres no alfanuméricos, debe volver a poner acentos graves (') antes y después del nombre de campo: por ejemplo, **`error-code`="102"**).

   Debe utilizar los caracteres graves para los nombres de campo que contengan caracteres no alfanuméricos, pero no para los valores. Los valores siempre van entre comillas («).

incluye potentes capacidades de consulta, incluidos varios comandos y compatibilidad con expresiones regulares, operaciones matemáticas y operaciones estadísticas. Para obtener más información, consulte Sintaxis de consulta CloudWatch Logs Insights (p. 41) .

# Tutorial: Ejecutar una consulta con una función de agregación

En este tutorial, se ejecuta una consulta que devuelve los resultados de ejecutar funciones de agregación en los informes de registro.

Para ejecutar una consulta de agregación

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. Seleccione uno o varios grupos de registro encima del editor de consultas. Para ayudarle a encontrar los grupos de registro, introduzca texto en la barra de búsqueda y CloudWatch Logs mostrará los grupos de registro coincidentes en la barra de búsqueda.
4. En el editor de consultas, elimine la consulta que se muestra actualmente y, a continuación, escriba lo siguiente y elija Run (Ejecutar). Sustituya fieldname por el nombre de campo que aparece en el área Fields (Campos) a la derecha de la pantalla.

   ```
   stats count(*) by fieldname
   ```

   Los resultados muestran el número de eventos de registro en el grupo de registro recibidas por CloudWatch Logs que contienen cada valor diferente para el nombre de campo que eligió.

# Tutorial: Ejecutar una consulta que produzca una visualización agrupada por campos de registro

Cuando ejecuta una consulta que utiliza el método`stats`Para agrupar los resultados devueltos por los valores de uno o varios campos de las entradas de registro, puede ver los resultados como un gráfico de barras, un gráfico circular, un gráfico de líneas o un gráfico de áreas apiladas. De este modo, podrá consultar de un modo más eficaz las tendencias de los registros.

Para ejecutar una consulta para visualización

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

2. En el panel de navegación, elija  Insights.
3. Seleccione uno o varios grupos de registros que va a consultar.
4. En el editor de consultas, elimine el contenido actual y escriba la siguiente función `stats`. Después seleccione Run query (Ejecutar consulta).

```
stats count(*) by @logStream
    | limit 100
```

   Los resultados muestran el número de eventos del grupo de registros por cada secuencia de registro. Los resultados tienen un límite de 100 filas.
5. Elija la pestaña Visualization (Visualización).
6. Seleccione la flecha situada junto a Line (Línea) y, a continuación, elija Bar (Barra).

   Aparece el gráfico de barras, con una barra por cada secuencia de registro del grupo de registros.

# Tutorial: Ejecutar una consulta que produce una visualización de series de tiempo

Cuando ejecuta una consulta que utiliza el método`bin()`Para agrupar los resultados devueltos por un período de tiempo, puede ver los resultados como un gráfico de líneas, un gráfico de áreas apiladas, un gráfico circular o un gráfico de barras. De este modo, podrá consultar de un modo más eficaz las tendencias de los eventos de registro con el paso del tiempo

Para ejecutar una consulta para visualización

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. Seleccione uno o varios grupos de registros que va a consultar.
4. En el editor de consultas, elimine el contenido actual y escriba la siguiente función `stats`. Después seleccione Run query (Ejecutar consulta).

```
stats count(*) by bin(30s)
```

   Los resultados muestran el número de eventos de registro en el grupo de registro recibidas por CloudWatch Logs durante cada período de 30 segundos.
5. Elija la pestaña Visualization (Visualización).

   Los resultados se muestran como un gráfico de líneas. Para cambiar a un gráfico de barras, a un gráfico circular o a un gráfico de áreas apiladas, elija la flecha situada junto aLíneaen la parte superior izquierda de la gráfica.

# Sintaxis de consulta CloudWatch Logs Insights

CloudWatch Logs Insights admite un lenguaje de consultas que puede utilizar para realizar consultas en sus grupos de registros. Cada consulta puede incluir uno o varios comandos de consulta separados por caracteres de barra vertical tipo Unix (`|`).

Se admiten seis comandos de consulta, junto con muchas funciones y operaciones de apoyo, incluidas expresiones regulares, operaciones aritméticas, operaciones de comparación, funciones numéricas, funciones de fecha y hora, funciones de cadena y funciones genéricas.

Los comentarios también se admiten. Las líneas en una consulta que empiezan por el carácter # se pasan por alto.

Los campos que empiezan con el@son generados por CloudWatch Logs Insights. Para obtener más información acerca de los campos que CloudWatch Logs detecta y genera automáticamente, consulteRegistros admitidos y campos descubiertos (p. 36).

# Comandos de consulta de CloudWatch Logs

En la siguiente tabla se muestran los seis comandos de consulta admitidos junto con ejemplos básicos. Para obtener consultas de muestra más potentes, consulte Consultas de ejemplo (p. 56).

| Comando | Descripción | Ejemplos |
|---|---|---|
| **`display`** | Especifica qué campos se mostrarán en los resultados de la consulta. Si especificas este comando más de una vez en la consulta, solo se utilizarán los campos especificados en el último caso. | En el siguiente ejemplo se utiliza el campo`@message`y crea los campos efímeros`loggingType`y`loggingMessage`Para usar en la consulta. Filtra los eventos a solo aquellos con`ERROR`como el valor de`loggingType`, pero a continuación sólo muestra el`loggingMessage`de esos eventos en los resultados.<br>`fields @message | parse @message "[*] *" as loggingType, loggingMessage | filter loggingType = "ERROR" | display loggingMessage` |
| **`fields`** | Recupera los campos especificados de eventos de registro para su visualización.<br><br>Puede utilizar funciones y operaciones dentro de un comando fields para modificar los valores de campo para mostrarlos y crear nuevos campos para utilizarlos en el resto de la consulta. | En el siguiente ejemplo, se muestran los campos`foo-bar`,`action`, y el valor absoluto de la diferencia entre`f3`y`f4`para todos los eventos de registro en el grupo de registros.<br>`fields `foo-bar`, action, abs(f3-f4)`<br><br>En el ejemplo siguiente se crea y muestra un campo efímero`opStatus`. El valor de`opStatus`para cada entrada de registro es la concatenación de los valores de`Operation`y`StatusCode`, con un guión entre esos valores.<br>`fields concat(Operation, '-', StatusCode) as opStatus` |
| **`filter`** | Filtra los resultados de una consulta basándose en una o varias condiciones. Puede utilizar una amplia variedad de operadores y expresiones en la ventana**`filter`**comando. Para obtener más información, consulte the section | En el siguiente ejemplo, se recuperan los campos`f1`,`f2`, y`f3`Para todos los eventos de registro con un valor superior a 2000 en el`duration`.<br>`fields f1, f2, f3 | filter (duration>2000)` |

| Comando | Descripción | Ejemplos |
|---|---|---|
| | called “Coincide y expresiones regulares en el comando filter” (p. 46) . | En el siguiente ejemplo, también se presenta una consulta válida, pero los resultados no muestran campos separados. En su lugar, los resultados muestran el`@timestamp`y todos los datos de registro en el`@message`Para todos los eventos de registro donde la duración es superior a 2000.<br>`filter (duration>2000)`<br>En el siguiente ejemplo, se recuperan los campos`f1`y`f2`para todos los eventos de registro donde`f1`es 10 o`f3`es más de 25.<br>`fields f1, f2 \| filter (f1=10 or f3>25)`<br>En el siguiente ejemplo se devuelve eventos de registro donde el campo`statusCode`tiene un valor entre 200 y 299.<br>`fields f1 \| filter statusCode like /2\d\d/`<br>El siguiente ejemplo devuelve eventos de registro que tienen un`statusCode`de «300", «400" o «500".<br>`fields @timestamp, @message \| filter statusCode in [300,400,500]`<br>Este último ejemplo devuelve eventos de registro que no tienen`Type`campos con valores de «foo», «bar» o «1".<br>`fields @timestamp, @message \| filter Type not in ["foo","bar",1]` |
| **`stats`** | Calcula estadísticas acumuladas basadas en los valores de los campos de registro. Cuando utilice `stats`, también puede utilizar `by` para especificar uno o varios criterios que se van a utilizar para agrupar datos al calcular las estadísticas.<br>Se admiten varios operadores estadísticos, entre los que se incluyen `sum()`, `avg()`, `count()`, `min()` y `max()`. | En el siguiente ejemplo, se calcula el valor medio de`f1`Para cada valor único de`f2`.<br>`stats avg (f1) by f2` |

| Comando | Descripción | Ejemplos |
| --- | --- | --- |
| **`sort`** | Ordena los eventos de registro recuperados. Se admite tanto el orcen ascendente (`asc`) como el descendente (`desc`). | En el siguiente ejemplo, se ordenan los eventos devueltos en orden descendente en función del valor de`f1`y muestra los campos`f1`,`f2`, y`f3`.<br>`fields f1, f2, f3 \| sort f1 desc` |
| **`limit`** | Especifica el número de eventos de registro devueltos por la consulta.<br><br>Puede usarlo para limitar los resultados a un número pequeño y, de este modo, ver un conjunto reducido de resultados relevantes. También puede utilizar `limit` con un número comprendido entre 1000 y 10 000 para incrementar el número de filas de resultados de la consulta que van a aparecer en la consola a una cantidad mayor que el valor predeterminado, que es de 1000 filas.<br><br>Si no especifica ningún límite, de forma predeterminada, la consulta mostrará un máximo de 1000 filas. | En el siguiente ejemplo, se ordenan los eventos en orden descendente en función del valor de`@timestamp`y muestra los campos`f1`y`f2`para los primeros 25 eventos por orden de clasificación. En este caso el orden es por marca temporal comenzando por el más reciente, por lo que se devuelven los 25 eventos más recientes.<br>`sort @timestamp desc \| limit 25 \| display f1, f2` |

| Comando | Descripción | Ejemplos |
| --- | --- | --- |
| **parse** | Extrae datos de un campo de registro y crea uno o varios campos efímeros que puede procesar más adelante en la consulta.`parse`acepta expresiones glob y expresiones regulares.<br><br>Para expresiones glob, proporcione el comando `parse` con una cadena constante (caracteres entre comillas simples o dobles), donde cada fragmento de texto de la variable se ha sustituido por un asterisco (*). Estos se extraen en campos efímeros y se les da un alias después de la palabra clave `as`, en orden posicional.<br><br>Incluya expresiones regulares en barras diagonales (/). Dentro de la expresión, cada parte de la cadena coincidente que se va a extraer se incluye en un grupo de captura determinado. Un ejemplo de un grupo de captura es `(?<name>.*)`, donde `name` es el nombre y `.*` es el patrón. | Utilizando esta línea de registro única a modo de ejemplo:<br><br>`25 May 2019 10:24:39,474 [ERROR] {foo=2, bar=data} The error was: DataIntegrityException`<br><br>Los dos siguientes`parse`Las expresiones hacen lo siguiente: los campos efímeros`level`,`config`, y`exception`se crean.`level`tiene un valor de`ERROR`,`config`tiene un valor de`{foo=2, bar=data}`, y`exception`tiene un valor de`DataIntegrityException`. En el primer ejemplo se utiliza una expresión glob y en el segundo se utiliza una expresión regular.<br><br>`parse @message "[*] * The error was: *" as level, config, exception`<br><br>`parse @message /\[(?<level>\S+)\]\s+(?<config>\{.*\})\s+The error was: (?<exception>\S+)/`<br><br>En el siguiente ejemplo se utiliza una expresión regular para extraer los campos efímeros `user2`, `method2` y `latency2` desde el campo de registro `@message` y devolver la latencia media para cada combinación única de `method2` y `user2`.<br><br>`parse @message /user=(?<user2>.*?), method:(?<method2>.*?), latency := (?<latency2>.*?)/ \| stats avg(latency2) by method2, user2` |

Notas sobre los comandos de consulta de la tabla anterior

Las reglas, directrices y sugerencias siguientes se aplican a los comandos de consulta de la tabla anterior.

- Cualquier campo de registro denominado en una consulta que tenga caracteres distintos del signo @, el punto (.) y caracteres alfanuméricos debe ir entre caracteres de acento grave (`). Por ejemplo, el nombre de campo `foo-bar` debe estar entre caracteres de acento grave porque incluye un carácter no alfanumérico.
- Ambos**`fields`**y**`display`**Para especificar los campos que deben mostrarse en los resultados de la consulta. Las diferencias entre ambos son las siguientes:
  - Puede utilizar el**`display`**Para especificar qué campos se mostrarán en los resultados. Puede utilizar el**`fields`**con el comandocomopara crear nuevos campos efímeros utilizando funciones y los campos que están en el evento de registro. Por ejemplo,`fields ispresent(resolverArn) as`

`isRes`crea un campo efímero llamado`isRes`que se puede usar en el resto de la consulta. El valor de`isRes`es 0 o 1 dependiendo de si o no`resolverArn`es un campo descubierto en el evento de registro.

- Si tiene varios**`fields`**y no incluya un**`display`**, los campos especificados en todos los**`fields`** `commands are displayed.`
- Si tiene varios**`display`**, solo los campos especificados en el**`display` `command are displayed.`**

# Coincide y expresiones regulares en el comando filter

Puede usar operadores de comparación (=,! =, <, <=, >, >=), operadores booleanos (`and`,`or`, y`not`) y expresiones regulares en el**`filter`**comando.

Puede utilizar `in` para probar la pertenencia a un conjunto. Coloque una matriz con los elementos que desee comprobar inmediatamente después de `in`. Puede usar `not` con `in`. Coincidencia de cadenas usando`in`deben ser coincidencias completas de cadena.

Para filtrar por subcadenas, puede usar`like`or`=~`(signo igual seguido de una tilde) en el`filter`comando. Para una coincidencia de subcadena usando`like`or`=~`Incluya también la subcadena para que coincidencia entre comillas dobles o simples. Para realizar la coincidencia de expresiones regulares, debe incluir la expresión para que coincidencia con barras diagonales. La consulta devuelve solo los eventos de registro que coincidan con los criterios establecidos.

Ejemplos

Los tres ejemplos siguientes devuelven todos los eventos en que `f1` contiene la palabra `Exception`. Los dos primeros ejemplos utilizan expresiones regulares. El tercer ejemplo utiliza una coincidencia de subcadenas. Los tres ejemplos distinguen entre mayúsculas y minúsculas.

```
fields f1, f2, f3 | filter f1 like /Exception/
```

```
fields f1, f2, f3 | filter f1 =~ /Exception/
```

```
fields f1, f2, f3 | filter f1 like "Exception"
```

En el siguiente ejemplo se cambia la búsqueda de «Exception» para que no distinga mayúsculas y minúsculas.

```
fields f1, f2, f3 | filter f1 like /(?i)Exception/
```

En el siguiente ejemplo se utiliza una expresión regular. Devuelve todos los eventos en los que `f1` es exactamente la palabra `Exception`. La consulta no distingue entre mayúsculas y minúsculas.

```
fields f1, f2, f3 | filter f1 =~ /^(?i)Exception$/
```

# Uso de alias en consultas

Puede utilizar `as` para crear uno o varios alias en una consulta. Los alias se admiten en los comandos `fields`, `stats` y `sort`.

Puede crear alias para campos de registro y para los resultados de operaciones y funciones.

Ejemplos

Los siguientes ejemplos muestran el uso de alias en los comandos de consulta.

```
fields abs(myField) as AbsoluteValuemyField, myField2
```

Devuelve el valor absoluto de `myField` como `AbsoluteValuemyField` y también devuelve el campo `myField2`.

```
stats avg(f1) as myAvgF1 | sort myAvgF1 desc
```

Calcula la media de los valores de `f1` como `myAvgF1` y los devuelve en orden descendente por dicho valor.

# Usar comentarios en consultas

Puede comentar las líneas en una consulta mediante el carácter #. Las líneas que empiezan por el carácter # se pasan por alto. Esto puede resultar útil para documentar su consulta o para no tener en cuenta temporalmente parte de una consulta compleja de una llamada, sin eliminar esa línea.

En el siguiente ejemplo, se pasa por alto la segunda línea de la consulta.

```
fields @timestamp, @message
    # | filter @message like /delay/
    | limit 20
```

# Funciones y operaciones admitidas

El lenguaje de consultas es compatible con muchos tipos de operaciones y funciones, tal y como se muestra en las siguientes tablas.

Operaciones de comparación

Puede utilizar las operaciones de comparación en el comando `filter` y como argumentos para otras funciones. Las operaciones de comparación aceptan todos los tipos de datos como argumentos y devuelven un resultado booleano.

```
= != < <= > >=
```

Operadores booleanos

Puede utilizar los operadores booleanos **`and`**, **`or`**, y **`not`**. Solo puede utilizar estos operadores booleanos en funciones que devuelven un valor booleano.

Operaciones aritméticas

Puede utilizar operaciones aritméticas en los comandos `filter` y `fields` y como argumentos para otras funciones. Las operaciones aritméticas aceptan tipos de datos numéricos como argumentos y devuelven resultados numéricos.

| Operation | Descripción |
|---|---|
| `a + b` | Suma |
| `a - b` | Resta |
| `a * b` | Multiplicación |

| Operation | Descripción |
|---|---|
| `a / b` | División |
| `a ^ b` | Potencia. `2 ^ 3` devuelve `8` |
| `a % b` | Resto o módulo. `10 % 3` devuelve `1` |

Numeric operations

Puede utilizar operaciones numéricas en los comandos `filter` y `fields` y como argumentos para otras funciones. Las operaciones numéricas aceptan tipos de datos numéricos como argumentos y devuelven resultados numéricos.

| Operation | Tipo de resultado | Descripción |
|---|---|---|
| `abs(a: number)` | número | Valor absoluto. |
| `ceil(a: number)` | número | Redondeo a valor máximo (el número entero menor que es mayor que el valor de `a`). |
| `floor(a: number)` | número | Redondeo a valor mínimo (el número entero más alto que es menor que el valor de `a`). |
| `greatest(a: number, ...numbers: number[])` | número | Devuelve el valor más alto. |
| `least(a: number, ...numbers: number[])` | número | Devuelve el valor más bajo. |
| `log(a: number)` | número | Registro natural. |
| `sqrt(a: number)` | número | Raíz cuadrada. |

Funciones generales

Puede utilizar funciones generales en los comandos `filter` y `fields` y como argumentos para otras funciones.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `ispresent(fieldName: LogField)` | booleano | Devuelve `true` si el campo existe. |
| `coalesce(fieldName: LogField, ...fieldNames: LogField[])` | LogField | Devuelve el primer valor no nulo de la lista. |

Funciones de cadena

Puede utilizar funciones de cadena en los comandos `filter` y `fields` y como argumentos para otras funciones.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `isempty(fieldName: string)` | booleano | Devuelve `true` si el campo no se encuentra o es una cadena vacía. |
| `isblank(fieldName: string)` | booleano | Devuelve `true` si el campo no se encuentra, es una cadena vacía o solo contiene espacio en blanco. |
| `concat(str: string, ...strings: string[])` | string | Concatena las cadenas. |
| `ltrim(str: string)`<br>`ltrim(str: string, trimChars: string)` | string | Si la función no tiene un segundo argumento, elimina espacios en blanco desde la izquierda de la cadena. Si la función tiene un segundo argumento de cadena, no elimina espacios en blanco. En su lugar, elimina los caracteres de `trimChars` desde la izquierda de `str`. Por ejemplo, `ltrim("xyZxyfooxyZ","xyZ")` devuelve `"fooxyZ"`. |
| `rtrim(str: string)`<br>`rtrim(str: string, trimChars: string)` | string | Si la función no tiene un segundo argumento, elimina espacios en blanco a la derecha de la cadena. Si la función tiene un segundo argumento de cadena, no elimina espacios en blanco. En su lugar, elimina los caracteres de `trimChars` desde la derecha de `str`. Por ejemplo, `rtrim("xyZfooxyxyZ","xyZ")` devuelve `"xyZfoo"`. |
| `trim(str: string)`<br>`trim(str: string, trimChars: string)` | string | Si la función no tiene un segundo argumento, elimina espacios en blanco de ambos extremos de la cadena. Si la función tiene un segundo argumento de cadena, no elimina espacios en blanco. En su lugar, elimina los caracteres de `trimChars` desde ambos lados de `str`. Por ejemplo, `trim("xyZxyfooxyxyZ","xyZ")` devuelve `"foo"`. |
| `strlen(str: string)` | número | Devuelve la longitud de la cadena puntos de código Unicode. |
| `toupper(str: string)` | string | Convierte la cadena en mayúsculas. |

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `tolower(str: string)` | string | Convierte la cadena de caracteres en minúsculas. |
| `substr(str: string, startIndex: number)`<br><br>`substr(str: string, startIndex: number, length: number)` | string | Devuelve una subcadena del índice especificado por el argumento numérico al final de la cadena. Si la función tiene un segundo argumento numérico, contiene la longitud de la subcadena que debe recuperarse. Por ejemplo, `substr("xyZfooxyZ",3, 3)` devuelve `"foo"`. |
| `replace(str: string, searchValue: string, replaceValue: string)` | string | Sustituye todas las instancias de `searchValue` en `str` por `replaceValue`. Por ejemplo, `replace("foo","o","0")` devuelve `"f00"`. |
| `strcontains(str: string, searchValue: string)` | número | Devuelve 1 si `str` contiene `searchValue` y 0 en los demás casos. |

Funciones DateTime

Puede utilizar funciones de fecha y hora en los comandos `filter` y `fields` y como argumentos para otras funciones. Puede utilizar estas funciones para crear buckets de hora para consultas con funciones de agregación.

Como parte de las funciones de fecha y hora, puede utilizar períodos de tiempo que constan de un número y, a continuación, `m` para minutos o `h` para horas. Por ejemplo, `10m` es 10 minutos y `1h` es 1 hora.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `bin(period: Period)` | Marca temporal | Redondea el valor de `@timestamp` según el periodo indicado y, a continuación, trunca. |
| `datefloor(timestamp: Timestamp, period: Period)` | Marca temporal | Trunca la marca temporal según el periodo indicado. Por ejemplo, `datefloor(@timestamp, 1h)` trunca todos los valores de `@timestamp` en la parte inferior de la hora. |
| `dateceil(timestamp: Timestamp, period: Period)` | Marca temporal | Redondea hacia arriba la marca temporal según el periodo indicado y, a continuación, trunca. Por ejemplo, `dateceil(@timestamp, 1h)` trunca todos los valores de `@timestamp` en la parte superior de la hora. |
| `fromMillis(fieldName: number)` | Marca temporal | Interpreta el campo de entrada como el número de milisegundos desde la fecha de inicio de Unix y lo convierte en una marca de tiempo. |

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `toMillis(fieldName: Timestamp)` | número | Convierte la marca de tiempo que se encontró en el campo con nombre asignado en un número que representa los milisegundos desde la fecha de inicio de Unix. |

Funciones de dirección IP

Puede utilizar funciones de cadena de dirección IP en los comandos `filter` y `fields` y como argumentos para otras funciones.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `isValidIp(fieldName: string)` | booleano | Devuelve `true` si el campo es una dirección IPv4 o IPv6 válida. |
| `isValidIpV4(fieldName: string)` | booleano | Devuelve `true` si el campo es una dirección IPv4 válida. |
| `isValidIpV6(fieldName: string)` | booleano | Devuelve `true` si el campo es una dirección IPv6 válida. |
| `isIpInSubnet(fieldName: string, subnet: string)` | booleano | Devuelve `true` si el campo es una dirección IPv4 o IPv6 válida dentro de la subred v4 o v6 especificada. Cuando especifique la subred, utilice la notación CIDR, como `192.0.2.0/24` o `2001:db8::/32`. |
| `isIpv4InSubnet(fieldName: string, subnet: string)` | booleano | Devuelve `true` si el campo es una dirección IPv4 válida dentro de la subred v4 especificada. Cuando especifique la subred, utilice la notación CIDR, como `192.0.2.0/24`. |
| `isIpv6InSubnet(fieldName: string, subnet: string)` | booleano | Devuelve `true` si el campo es una dirección IPv6 válida dentro de la subred v6 especificada. Cuando especifique la subred, utilice la notación CIDR, como `2001:db8::/32`. |

Funciones de agregación de estadísticas

Puede utilizar las funciones de agregación en el comando `stats` y como argumentos para otras funciones.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `avg(fieldName: NumericLogField)` | número | La media de los valores en el campo especificado. |
| `count()`<br><br>`count(fieldName: LogField)` | número | Cuenta los eventos de registro.`count()`(o`count(*)`) cuenta todos los eventos devueltos por la consulta, mientras que`count(fieldName)`Cuenta todos los registros que incluyen el nombre de campo especificado. |

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `count_distinct(fieldName: LogField)` | número | Devuelve el número de valores únicos para el campo. Si el campo tiene una cardinalidad muy alta (contiene muchos valores únicos), el valor devuelto por `count_distinct` es solo una aproximación. |
| `max(fieldName: LogField)` | LogFieldValue | El máximo de los valores para este campo de registro en los registros consultados. |
| `min(fieldName: LogField)` | LogFieldValue | El mínimo de los valores para este campo de registro en los registros consultados. |
| `pct(fieldName: LogFieldValue, percent: number)` | LogFieldValue | Un percentil indica el peso relativo de un valor en un conjunto de datos. Por ejemplo, `pct(@duration, 95)` devuelve el valor `@duration` en que el 95 % de los valores de `@duration` son inferiores a este valor y un 5 por ciento son superiores a este valor. |
| `stddev(fieldName: NumericLogField)` | número | El desvío estándar de los valores en el campo especificado. |
| `sum(fieldName: NumericLogField)` | número | La suma de los valores en el campo especificado. |

Funciones sin agregación de estadísticas

Puede utilizar las funciones de no agregación en el comando `stats` y como argumentos para otras funciones.

| Función | Tipo de resultado | Descripción |
|---|---|---|
| `earliest(fieldName: LogField)` | LogField | Devuelve el valor de `fieldName` desde el evento de registro que tiene la primera marca temporal en los registros consultados. |
| `latest(fieldName: LogField)` | LogField | Devuelve el valor de `fieldName` desde el evento de registro que tiene la última marca temporal en los registros consultados. |
| `sortsFirst(fieldName: LogField)` | LogField | Devuelve el valor de `fieldName` que ordena en primer lugar los registros consultados. |
| `sortsLast(fieldName: LogField)` | LogField | Devuelve el valor de `fieldName` que ordena al final los registros consultados. |

# Visualización de datos de registro en gráficos

Puede utilizar visualizaciones (por ejemplo, gráficos de barras, gráficos de líneas y gráficos de áreas apiladas) para identificar patrones con mayor eficacia en los datos de registro. CloudWatch Logs Insights genera visualizaciones para las consultas que utilizan el`stats`Funciones de agregación y una o varias

funciones de agregación. Para obtener más información, consulte Aggregation Functions in the Stats Command (p. 51) .

Todas estas consultas pueden generar gráficos de barras. Si la consulta utiliza la función `bin()` para agrupar los datos en función de un mismo campo a lo largo del tiempo, también puede ver gráficos de líneas y gráficos de áreas apiladas.

Temas



# Visualización de datos de series temporales

Las visualizaciones de series temporales funcionan con las consultas que tienen las siguientes características:

- La consulta contiene una o varias funciones de agregación. Para obtener más información, consulte Aggregation Functions in the Stats Command (p. 51) .
- La consulta utiliza la función `bin()` para agrupar los datos por un campo.

Estas consultas pueden generar gráficos de líneas, gráficos de áreas apiladas, gráficos de barras y gráficos circulares.

Ejemplos

Para ver un tutorial completo, consulte the section called “Tutorial: Ejecutar una consulta que produce una visualización de series de tiempo” (p. 41).

Aquí hay más consultas de ejemplo que funcionan para la visualización de series temporales.

La siguiente consulta genera una visualización de los valores medios del campo `myfield1`, con un punto de datos creado cada cinco minutos. Cada punto de datos es la agregación de las medias de los valores `myfield1` de los registros de los últimos cinco minutos.

```
stats avg(myfield1) by bin(5m)
```

La siguiente consulta genera una visualización de los tres valores basados en diferentes campos, con un punto de datos creado cada cinco minutos. La visualización se genera porque la consulta contiene las funciones de agregación y utiliza `bin()` como campo de agrupación.

```
stats avg(myfield1), min(myfield2), max(myfield3) by bin(5m)
```

Restricciones de gráfico de líneas y gráfico de áreas apiladas

Las consultas que agregan información de entradas de registro pero no utilizan la función `bin()` pueden generar gráficos de barras. Sin embargo, las consultas no pueden generar gráficos de líneas ni gráficos de áreas apiladas. Para obtener más información sobre estos tipos de consultas, visite the section called “Visualización de datos de registro agrupados por campos” (p. 53).

# Visualización de datos de registro agrupados por campos

Puede generar gráficos de barras para consultas que utilizan la función `stats` y una o varias funciones de agregación. Para obtener más información, consulte Aggregation Functions in the Stats Command (p. 51) .

Para ver la visualización, ejecute la consulta. A continuación, elija la pestaña Visualization (Visualización), seleccione la flecha situada junto a Line (Línea) y haga clic en Bar (Barra). Las visualizaciones de los gráficos de barras tienen un límite máximo de 100 barras.

Ejemplos

Para ver un tutorial completo, consulte the section called “Tutorial: Ejecutar una consulta que produzca una visualización agrupada por campos de registro” (p. 40). Los párrafos siguientes incluyen más consultas de ejemplo de visualizaciones por campos.

La siguiente consulta de registro de flujo de VPC busca el número medio de bytes transferidos por sesión en cada dirección de destino.

```
stats avg(bytes) by dstAddr
```

También puede generar un gráfico que contenga varias barras para cada valor resultante. Por ejemplo, la siguiente consulta de registro de flujo de VPC busca el número medio y máximo de bytes transferidos por sesión en cada dirección de destino.

```
stats avg(bytes), max(bytes) by dstAddr
```

La siguiente consulta busca el número de registros de Amazon Route 53 para cada tipo de consulta.

```
stats count(*) by queryType
```

# Guardar y volver a ejecutar consultas de CloudWatch Logs Insights

Cuando haya creado una consulta, puede guardarla para volver a ejecutarla más adelante. Las consultas guardadas se conservan en una estructura de carpetas para ayudarle a mantenerlas organizadas. Puede guardar hasta 1000 consultas de CloudWatch Logs Insights por región y cuenta.

Para guardar una consulta, debe haber iniciado sesión en un rol que tenga el permiso `logs:PutQueryDefinition`. Para ver una lista de consultas guardadas, debe haber iniciado sesión en un rol que tenga el permiso `logs:DescribeQueryDefinitions` .

### Para guardar una consulta

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. En el editor de consultas, cree una consulta.
4. Seleccione Save.

   Si no ve unSave (Guardar)Debe cambiar al nuevo diseño para la consola de CloudWatch Logs. Para ello:

   a. En el panel de navegación, seleccione Log groups (Grupos de registro).
   b. Elija Try the new design (Probar el nuevo diseño).
   c. En el panel de navegación, seleccione Insights y vuelva al paso 3 de este procedimiento.
5. Escriba un nombre para la consulta.

6. (Opcional) Elija una carpeta en la que desee guardar la consulta. Seleccione Create new (Crear nueva) para crear una carpeta. Si crea una carpeta nueva, puede utilizar caracteres de barra (/) en el nombre de la carpeta para definir una estructura de carpetas. Por ejemplo, poner nombre a una carpeta nueva **`folder-level-1/folder-level-2`** crea una carpeta de nivel superior llamada **`folder-level-1`**, con otra carpeta llamada **`folder-level-2`** dentro de esa carpeta. La consulta se guarda en **`folder-level-2`**.
7. (Opcional) Cambie los grupos de registro de la consulta o el texto de la consulta.
8. Seleccione Save.

### Para ejecutar una consulta guardada

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. A la derecha, elija Queries (Consultas).
4. Seleccione la consulta de la lista Saved queries (Consultas guardadas) . Aparece en el editor de consultas.
5. Elija Run (Ejecutar).

### Para guardar una nueva versión de una consulta guardada

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. A la derecha, elija Queries (Consultas).
4. Seleccione la consulta de la lista Saved queries (Consultas guardadas) . Aparece en el editor de consultas.
5. Modifique la consulta. Si necesita ejecutarla para comprobar su trabajo, elija Run query (Ejecutar consulta).
6. Cuando esté listo para guardar la nueva versión, elija Actions (Acciones), Save as (Guardar como).
7. Escriba un nombre para la consulta.
8. (Opcional) Elija una carpeta en la que desee guardar la consulta. Seleccione Create new (Crear nueva) para crear una carpeta. Si crea una carpeta nueva, puede utilizar caracteres de barra (/) en el nombre de la carpeta para definir una estructura de carpetas. Por ejemplo, poner nombre a una carpeta nueva **`folder-level-1/folder-level-2`** crea una carpeta de nivel superior llamada **`folder-level-1`**, con otra carpeta llamada **`folder-level-2`** dentro de esa carpeta. La consulta se guarda en **`folder-level-2`**.
9. (Opcional) Cambie los grupos de registro de la consulta o el texto de la consulta.
10. Seleccione Save.

Para eliminar una consulta, debe haber iniciado sesión en un rol que tenga el permiso `logs:DeleteQueryDefinition`.

### Para editar o eliminar una consulta guardada

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. A la derecha, elija Queries (Consultas).
4. Seleccione la consulta de la lista Saved queries (Consultas guardadas) . Aparece en el editor de consultas.
5. Elija Actions (Acciones), Edit (Editar) o Actions (Acciones), Delete (Eliminar).

# Consultas de ejemplo

En esta sección se incluyen ejemplos de consultas que muestran la potencia de CloudWatch Logs Insights.

Consultas generales

Buscar los 25 eventos de registro añadidos más recientemente.

```
fields @timestamp, @message | sort @timestamp desc | limit 25
```

Obtener una lista del número de excepciones por hora.

```
filter @message like /Exception/
    | stats count(*) as exceptionCount by bin(1h)
    | sort exceptionCount desc
```

Obtener una lista de eventos de registro que no son excepciones.

```
fields @message | filter @message not like /Exception/
```

Consultas de registros de Lambda Logs

Determinar la cantidad de memoria sobreaprovisionada.

```
filter @type = "REPORT"
    | stats max(@memorySize / 1000 / 1000) as provisonedMemoryMB,
        min(@maxMemoryUsed / 1000 / 1000) as smallestMemoryRequestMB,
        avg(@maxMemoryUsed / 1000 / 1000) as avgMemoryUsedMB,
        max(@maxMemoryUsed / 1000 / 1000) as maxMemoryUsedMB,
        provisonedMemoryMB - maxMemoryUsedMB as overProvisionedMB
```

Crear un informe de latencia.

```
filter @type = "REPORT" |
    stats avg(@duration), max(@duration), min(@duration) by bin(5m)
```

Consultas de registros de flujo de Amazon VPC

Buscar las 15 primeras transferencias de paquete en hosts:

```
stats sum(packets) as packetsTransferred by srcAddr, dstAddr
    | sort packetsTransferred  desc
    | limit 15
```

Busca las 15 primeras transferencias de bytes en los hosts de una determinada subred.

```
filter isIpv4InSubnet(srcAddr, "192.0.2.0/24")
    | stats sum(bytes) as bytesTransferred by dstAddr
    | sort bytesTransferred desc
    | limit 15
```

Busque las direcciones IP con UDP como protocolo de transferencia de datos.

```
filter protocol=17 | stats count(*) by srcAddr
```

Buscar direcciones IP donde los registros de flujo se han omitido durante la ventana de captura.

```
filter logStatus="SKIPDATA"
    | stats count(*) by bin(1h) as t
    | sort t
```

Consultas de registros de Route 53 Log

Buscar la distribución de registros por hora por tipo de consulta.

```
stats count(*) by queryType, bin(1h)
```

Buscar los 10 solucionadores de DNS con el mayor número de solicitudes.

```
stats count(*) as numRequests by resolverIp
    | sort numRequests desc
    | limit 10
```

Buscar el número de registros por dominio y subdominio donde el servidor no pudo completar la solicitud de DNS.

```
filter responseCode="SERVFAIL" | stats count(*) by queryName
```

Consultas de registros de CloudTrail

Buscar el número de entradas de registro por cada servicio, tipo de evento yAWSRegión .

```
stats count(*) by eventSource, eventName, awsRegion
```

Buscar los hosts de Amazon EC2 de que se iniciaron o detuvieron en un determinadoAWSRegión .

```
filter (eventName="StartInstances" or eventName="StopInstances") and region="us-east-2"
```

Busque elAWSRegiones, nombres de usuario y ARN de los usuarios de IAM de creados recientemente.

```
filter eventName="CreateUser"
    | fields awsRegion, requestParameters.userName, responseElements.user.arn
```

Buscar el número de registros en los que se ha producido una excepción al llamar a la API `UpdateTrail`.

```
filter eventName="UpdateTrail" and ispresent(errorCode)
    | stats count(*) by errorCode, errorMessage
```

Ejemplos del comando para analizar

Utilice una expresión glob para extraer los campos efímeros `@user`, `@method` y `@latency` desde el campo de registro `@message` y devolver la latencia media para cada combinación única de `@method` y `@user`.

```
parse @message "user=*, method:*, latency := *" as @user,
    @method, @latency | stats avg(@latency) by @method,
    @user
```

Utilice una expresión regular para extraer los campos efímeros `@user2`, `@method2` y `@latency2` desde el campo de registro `@message` y devolver la latencia media para cada combinación única de `@method2` y `@user2`.

```
parse @message /user=(?<user2>.*?), method:(?<method2>.*?),
    latency := (?<latency2>.*?)/ | stats avg(latency2) by @method2,
    @user2
```

Extrae los campos efímeros `loggingTime`, `loggingType` y `loggingMessage`, los filtra para registrar los eventos que contienen cadenas `ERROR` o `INFO` y, a continuación, muestra solo los campos `loggingMessage` y `loggingType` para los eventos que contienen una cadena `ERROR`.

```
FIELDS @message
    | PARSE @message "* [*] *" as loggingTime, loggingType, loggingMessage
    | FILTER loggingType IN ["ERROR", "INFO"]
    | DISPLAY loggingMessage, loggingType = "ERROR" as isError
```

# Agregar consulta al panel o exportar resultados de consulta

Después de ejecutar una consulta, puede agregar la consulta a un panel de CloudWatch o copiar los resultados en el portapapeles.

Las consultas agregadas a los paneles se ejecutan automáticamente cada vez que carga el panel y cada vez que el panel se actualiza. Estas consultas se contabilizan para el límite de 10 consultas de CloudWatch Logs Insights.

### Para añadir resultados de consultas a un panel

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. Elija uno o varios grupos de registros y ejecute una consulta.
4. Elija Add to dashboard (Añadir a panel).
5. Seleccione el panel o elija Create new (Crear nuevo) para crear un nuevo panel para los resultados de la consulta.
6. Seleccione el tipo de widget que desea utilizar para los resultados de la consulta.
7. Escriba un nombre para el widget.
8. Elija Add to dashboard (Añadir a panel).

### Para copiar los resultados de la consulta en el portapapeles o descargar los resultados de la consulta

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. Elija uno o varios grupos de registros y ejecute una consulta.
4. Elija Export results (Exportar resultados) y, a continuación, elija la opción que desee.

# Ver consultas o historial de consultas en ejecución

Puede ver las consultas en curso, así como su historial de consultas recientes.

Las consultas que se están ejecutando actualmente incluyen consultas añadidas a un panel. Está limitado a 10 consultas de CloudWatch Logs Insights por cuenta, incluidas consultas añadidas a paneles.

### Para ver su historial de consultas recientes

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija  Insights.
3. SeleccionarHistorial de laSi está utilizando el nuevo diseño para la consola CloudWatch Logs. Si está utilizando el diseño antiguo, elija Actions (Acciones), View query history for this account (Ver historial de consultas de esta cuenta).

   Aparece una lista de consultas recientes. Puede volver a ejecutar cualquiera de ellas seleccionando la consulta y eligiendo Run (Ejecutar).

   UNDEREstado, muestra CloudWatch LogsEn cursoPara cualquier consulta que se esté ejecutando.

# Uso delOGgrupos ylOGstreams

Un flujo de registro es una secuencia de eventos de registro que comparten la misma fuente. Cada origen independiente de registros en CloudWatch Logs constituye un flujo de registros independiente.

Un grupo de logs es un grupo de flujos de logs que comparten la misma configuración de retención, monitorización y control de acceso. Puede definir grupos de logs y especificar los flujos que deben incluirse en cada uno. No hay límites en el número de flujos de registro que pueden pertenecer a un grupo de registros.

Utilice los procedimientos de esta sección para trabajar con grupos y flujos de logs.

## Creación de unlOGgrupo en CloudWatch Logs

Cuando instale el agente de CloudWatch Logs en una instancia de Amazon EC2 utilizando los pasos en las secciones anteriores de la Guía del usuario de Amazon CloudWatch Logs, el grupo de registros se crea como parte de ese proceso. También puede crear un grupo de registros directamente en la consola de CloudWatch.

Para crear un grupo de registros

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija Actions (Acciones) y, a continuación, elija Create log group (Crear grupo de registros).
4. Escriba el nombre del grupo de registros y, a continuación, elija Create log group (Crear grupo de registros).

## Sendlogs a unlOGgroup

CloudWatch Logs recibe automáticamente los eventos de registro de variosAWSServicios de . También puede enviar otros eventos de registro a CloudWatch Logs mediante uno de los métodos siguientes:

- Agente de CloudWatch: el agente unificado de CloudWatch puede enviar métricas y registros a CloudWatch Logs. Para obtener información acerca de la instalación y uso del agente de CloudWatch, consulteRecopilación de métricas y registros de instancias Amazon EC2 y servidores locales con el agente de CloudWatchen laGuía del usuario de Amazon CloudWatch.
- AWS CLI—ElPut-log-eventscarga lotes de eventos de registro a CloudWatch Logs.
- Mediante programación— ElPutLogEventsAPI le permite cargar lotes de eventos de registro mediante programación en CloudWatch Logs.

## VistalOGdatasen CloudWatch Logs

Puede ver y desplazarse a través de datos de registro flujo a flujo cuando los envía a CloudWatch Logs. Puede especificar el intervalo de tiempo para los datos de log que desee ver.

Para ver los datos del registro

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

2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. En Log Groups, elija el grupo de registros para ver los flujos.
4. En la lista de grupos de registros, elija el nombre del grupo de registros que desea ver.
5. En la lista de flujos de registros, elija el nombre del flujo de registros que desea ver.
6. Para cambiar la forma en que se muestran los datos de registro, lleve a cabo alguna de las siguientes operaciones:

   - Para expandir un único evento de registro, elija la flecha situada junto a ese evento de registro.
   - Para ampliar todos los eventos de registro y verlos como texto sin formato, por encima de la lista de eventos de registro, elija Text.
   - Para filtrar los eventos de registro, escriba el filtro de búsqueda que desee en el campo de búsqueda. Para obtener más información, consulte CrearmmétricasfROMlOGerejillas de ventilaciónucantarfilters (p. 72).
   - Para ver los datos de registro de un intervalo de fechas y horas especificado, junto al filtro de búsqueda, elija la flecha situada al lado de la fecha y hora. Para especificar un intervalo de fechas y horas, elija Absolute (Absoluto). Para elegir un número predefinido de minutos, horas, días o semanas, elija Relative (Relativo). También puede cambiar entre zona horaria UTC y zona horaria local.

# BúsquedaIOGdataucantarfilterpatterns

Puede buscar los datos de registro utilizando Filtrar ypatternsyntax (p. 73). Puede buscar todos los flujos de registros dentro de un grupo de registros o mediante la AWS CLI también puede buscar flujos de registro específicos. Cuando se ejecuta cada búsqueda, devuelve hasta la primera página de los datos encontrados y un token para recuperar la siguiente página de datos o para continuar buscando. Si no se devuelve ningún resultado, puede seguir buscando.

Puede definir el intervalo de tiempo que desea consultar para limitar el alcance de la búsqueda. Podría empezar por un intervalo mayor para ver las líneas de registro que le interesan y, a continuación, acortar el intervalo de tiempo al ámbito para ver los registros en el intervalo de tiempo que le interese.

También puede pasar directamente desde las métricas extraídas de los registros a los registros correspondientes.

## BúsquedaIOGenTraysucantar elconsole

Puede buscar las entradas de registro que cumplan los criterios especificados mediante la consola.

### Para buscar sus registros utilizando la consola

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. En Log Groups (Grupos de registros), elija el nombre del grupo de registros que contiene el flujo de registros que desea buscar.
4. En Log Streams (Flujos de registros), elija el nombre del flujo de registros que desea buscar.
5. En Log events (Eventos de registros), escriba la sintaxis del filtro que se va a utilizar.

### Para buscar todas las entradas de registro durante un intervalo de tiempo utilizando la consola

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).

3. En Log Groups (Grupos de registros), elija el nombre del grupo de registros que contiene el flujo de registros que desea buscar.
4. Elija Search Log Group (Buscar grupos de registros).
5. En Log events (Eventos de registros), seleccione el intervalo de fecha y hora e introduzca la sintaxis del filtro.

# BúsquedalOGenTraysucantar elAWS CLI

Puede buscar las entradas de registro que cumplan los criterios especificados mediante la AWS CLI.

Para buscar entradas de registro mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando filter-log-events. Usar`--filter-pattern`Para limitar los resultados al patrón de filtros especificado y`--log-stream-names`para limitar los resultados a los flujos de registro especificados.

```
aws logs filter-log-events --log-group-name my-group [--log-stream-
names LIST_OF_STREAMS_TO_SEARCH] [--filter-pattern VALID_METRIC_FILTER_PATTERN]
```

Para buscar entradas de registro durante un intervalo de tiempo determinado mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando filter-log-events:

```
aws logs filter-log-events --log-group-name my-group [--log-stream-
names LIST_OF_STREAMS_TO_SEARCH] [--start-time 1482197400000] [--end-time 1482217558365]
 [--filter-pattern VALID_METRIC_FILTER_PATTERN]
```

# Tabla dinámica desdemmétricas alogs

Puede acceder a determinadas entradas de registro desde otras partes de la consola.

### Para acceder desde widgets del panel a registros

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Dashboards (Paneles).
3. Elija un panel.
4. En el widget, elija el icono View logs (Ver registros) y, a continuación, elija View logs in this time range (Ver registros en este intervalo de tiempo). Si hay más de un filtro de métricas, seleccione uno de la lista. Si hay más filtros de métricas de los que podemos mostrar en la lista, elija More metric filters y seleccione o busque un filtro de métricas.

### Para acceder desde métricas a registros

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (Métricas).
3. En el campo de búsqueda en la pestaña All metrics, escriba el nombre de la métrica y pulse Intro.
4. Seleccione una o varias métricas de los resultados de la búsqueda.
5. Elija Actions (Acciones), View logs (Ver registros). Si hay más de un filtro de métricas, seleccione uno de la lista. Si hay más filtros de métricas de los que podemos mostrar en la lista, elija More metric filters y seleccione o busque un filtro de métricas.

## Troubleshooting

La búsqueda tarda demasiado tiempo en completarse

Si tiene una gran cantidad de datos de registro, la búsqueda podría tardar mucho tiempo en completarse. Para acelerar la búsqueda, puede hacer lo siguiente:

- Si utiliza la AWS CLI, puede limitar la búsqueda a solo los flujos de registro que le interesen. Por ejemplo, si su grupo de registros de tiene 1000 flujos de registro, pero solo desea ver tres flujos de registro que sabe que son relevantes, puede usar la AWS CLI para limitar la búsqueda únicamente a los tres flujos de registro dentro del grupo de registros.
- Utilice un intervalo de tiempo más corto, más granular, lo que reduce la cantidad de datos que se van a buscar y acelera la consulta.

# CambiarlOGdatarEtention en CloudWatch Logs

De forma predeterminada, los datos de registro se almacenan en CloudWatch Logs. Sin embargo, puede configurar durante cuánto tiempo almacenar los datos de registro en un grupo de registros. Cualquier dato anterior a la configuración de retención actual se elimina automáticamente. Puede cambiar la retención de registro de cada grupo de registros cuando lo desee.

Para cambiar la configuración de retención de registros

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Busque el grupo de logs que desea actualizar.
4. En la columna Expire Events After para ese grupo de registros, elija la configuración de retención actual, por ejemplo Never Expire.
5. En Edit Retention (Editar retención), en Retention (Retención), elija un valor de retención de registros y, a continuación, elija Ok (Aceptar).

# EtiquetarlOGgGrupos en Amazon CloudWatch Logs

Puede asignar sus propios metadatos a los grupos de registro que crea en Amazon CloudWatch Logs en la forma deetiquetas. Una etiqueta es un par clave-valor definido por el usuario para un grupo de registros. El uso de las etiquetas es una forma sencilla y potente para administrar los recursos de AWS y organizar los datos, incluidos los datos de facturación.

> Note
>
> CloudWatch Logs no admite directivas de IAM que impidan que los usuarios asignen etiquetas especificadas a grupos de registro mediante el`aws:Resource/key-name`o`aws:TagKeys`Claves de condición de Para obtener más información acerca del uso de etiquetas para controlar el acceso, consulteControl de acceso a los recursos de Amazon Web Services mediante etiquetas.

Contenido

# Etiquetarbasics

Utiliza elAWS CLILa API de CloudWatch Logs

- Agregar etiquetas a un grupo de registros al crearlo
- Agregar etiquetas a un grupo de registros existente
- Enumerar las etiquetas para un grupo de registros
- Eliminar las etiquetas de un grupo de registros

Puede utilizar las etiquetas para categorizar los grupos de registros. Por ejemplo, puede clasificarlas en categorías por objetivo, propietario o entorno. Dado que define la clave y el valor de cada etiqueta, puede crear un conjunto de categorías personalizadas para satisfacer sus necesidades específicas. Por ejemplo, podría definir un conjunto de etiquetas que le ayude a realizar un seguimiento de los grupos de registro por propietario y aplicaciones asociadas. Estos son algunos ejemplos de etiquetas:

- Proyecto: Nombre de proyecto
- Propietario: Nombre
- Propósito: Prueba de carga
- : Aplicación Nombre de la aplicación
- : Producción

# Seguimiento decOstosucantartagging

Puede utilizar etiquetas para categorizar y hacer un seguimiento de los costos de AWS. Cuando se aplican etiquetas a laAWS, incluidos los grupos de registro, suAWSEl informe de asignación de costos de incluye el uso y los costos agregados por etiquetas. Puede aplicar etiquetas que representen categorías de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) para estructurar los costos entre diferentes servicios. Para obtener más información, consulteUso de etiquetas de asignación de costos para informes de facturación personalizadosen laAWS Billing and Cost ManagementGuía del usuario.

# Etiquetarrestrictions

Se aplican las siguientes restricciones a las etiquetas.

## Restricciones básicas

- El número máximo de etiquetas por grupo de registro es 50.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No se pueden cambiar o editar etiquetas para un grupo de registros eliminado.

## Limitaciones de clave de etiqueta

- Cada clave de etiqueta debe ser única. Si añade una etiqueta con una clave que ya está en uso, la nueva etiqueta sobrescribe el par clave-valor existente.
- Una clave de etiqueta no puede comenzar por `aws:` porque este prefijo está reservado para su uso por AWS. AWS crea etiquetas cuyo nombre comienza por este prefijo por usted, pero usted no puede editarlas ni eliminarlas.
- Las claves de etiqueta deben tener entre 1 y 128 caracteres Unicode de longitud.
- Las claves de etiqueta deben constar de los siguientes caracteres: Letras Unicode, números, espacios en blanco y los caracteres especiales siguientes:`_ . / = + - @`.

Restricciones de valor de etiqueta

- Los valores de etiqueta deben tener entre 0 y 255 caracteres Unicode de longitud.
- Los valores de etiqueta pueden estar en blanco. De lo contrario, deben constar de los siguientes caracteres: Letras Unicode, números, espacios en blanco y cualquiera de los caracteres especiales siguientes:`_ . / = + - @`.

## EtiquetadolOGgruposucantar elAWS CLI

Puede añadir, enumerar y eliminar etiquetas con la AWS CLI. Para ver ejemplos, consulte la documentación siguiente:

create-log-group

Crea un grupo de registros. Si lo desea, puede añadir etiquetas al crear el grupo de registros.

tag-log-group

Añade o actualiza las etiquetas para el grupo de registros especificado.

list-tags-log-group

Muestra las etiquetas para el grupo de registros especificado.

untag-log-group

Elimina las etiquetas del grupo de registro especificado.

## EtiquetadolOGgruposuCómo cantar la API de CloudWatch Logs

Puede agregar, enumerar y eliminar etiquetas con la API de CloudWatch Logs. Para ver ejemplos, consulte la documentación siguiente:

CreateLogGroup

Crea un grupo de registros. Si lo desea, puede añadir etiquetas al crear el grupo de registros.

TagLogGroup

Añade o actualiza las etiquetas para el grupo de registros especificado.

ListTagsLogGroup

Muestra las etiquetas para el grupo de registros especificado.

UntagLogGroup

Elimina las etiquetas del grupo de registro especificado.

# EncryptlOGdATA en CloudWatch LogsucantarAWS Key Management Service

Los datos del grupo de registros siempre se cifran en CloudWatch Logs. Opcionalmente, puede utilizarAWS Key Management Servicepara este cifrado. Si lo hace, el cifrado se realiza utilizando unaAWS KMSclave maestra del cliente (CMK). El cifrado usando AWS KMS se habilita en el nivel del grupo de

registro, asociando una CMK con un grupo de registros, ya sea al crear el grupo de registros o después de que exista.

> Important
>
> CloudWatch Logs ahora admite el contexto de cifrado, usando`kms:EncryptionContext:aws:logs:arn`como clave y el ARN del grupo de registros como valor de esa clave. Si tiene grupos de registro que ya ha cifrado con una CMK y desea restringir la CMK para que se utilice con una sola cuenta y grupo de registro, debe asignar una nueva CMK que incluya una condición en la política de IAM. Para obtener más información, consulte AWS KMS keys yencryptioncontext (p. 69).

Después de asociar una CMK con un grupo de registros, todos los datos recién introducidos para el grupo de registro se cifran mediante la CMK. Estos datos se almacenan en formato cifrado durante todo el periodo de retención. Cuando se solicita CloudWatch Logs descifra estos datos. Cuando se solicitan datos cifrados, los CloudWatch Logs deben tener permisos para la CMK.

Después de desvincular una CMK de un grupo de registros, CloudWatch Logs cifra datos recién introducidos utilizando el método de cifrado predeterminado de CloudWatch Logs. Todos los datos previamente ingeridos que se cifraron con el CMK permanecen cifrados con el CMK.

> Important
>
> solo CloudWatch Logs K simétricas. No utilice una CMK asimétrica para cifrar los datos de los grupos de registros. Para obtener más información, consulte Uso de claves simétricas y asimétricas.

# Limits

- Para realizar los siguientes pasos, debe tener los siguientes permisos: `kms:CreateKey`, `kms:GetKeyPolicy` y `kms:PutKeyPolicy`.
- Después de asociar o desvincular una CMK desde un grupo de registros, puede tardar hasta cinco minutos en que la operación surta efecto.
- Si revoca el acceso de CloudWatch Logs a una CMK asociada o elimina una CMK asociada, los datos cifrados en CloudWatch Logs no se pueden recuperar.
- No puede asociar una CMK a un grupo de registros mediante la consola de CloudWatch.

# Paso 1: Creación de unAWS KMSCMK

Para crear una CMK de AWS KMS, utilice el siguiente comando create-key:

```
aws kms create-key
```

La salida contiene la ID de clave y el nombre de recurso de Amazon (ARN) de la CMK. A continuación, se muestra un ejemplo del resultado:

```
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
```

```
        "CreationDate": 1478910250.94,
        "Arn": "arn:aws:kms:us-west-2:123456789012:key/6f815f63-e628-448c-8251-
e40cb0d29f59",
        "AWSAccountId": "123456789012",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

# Paso 2: Establezcapemisiones en el CMK

De forma predeterminada, todas las CMK de AWS KMS son privadas. Sólo el propietario del recurso puede utilizarlo para cifrar y descifrar datos. Sin embargo, el propietario del recurso puede conceder permisos para que otros usuarios y recursos accedan a la CMK. Con este paso, otorgará a la entidad principal del servicio CloudWatch permiso para utilizar la CMK. La entidad principal del servicio debe estar en la mismaAWSRegión en la que está almacenada la CMK.

Como práctica recomendada, recomendamos que restrinja el uso de la clave únicamente a las cuentas de AWS o grupos de registro que especifique.

En primer lugar, guarde la política predeterminada para su CMK como `policy.json` utilizando el siguiente comando get-key-policy:

```
aws kms get-key-policy --key-id key-id --policy-name default --output text > ./policy.json
```

Abra el archivo `policy.json` en un editor de texto y agregue la sección en negrita desde una de las instrucciones siguientes. Separe la instrucción existente de la nueva instrucción con una coma. Estas instrucciones utilizan`Condition`Para mejorar la seguridad de laAWS KMSLa clave de. Para obtener más información, consulte AWS KMS keys yencryptioncontext (p. 69).

La sección `Condition` de este ejemplo restringe la clave a un ARN único de grupo de registros.

```
{
 "Version": "2012-10-17",
    "Id": "key-default-1",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::Your_account_ID:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "ArnEquals": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:log-group:log-group-name"
                }
            }
        }
    ]
}
```

La`Condition`en este ejemplo limita el uso de laAWS KMSPara la cuenta especificada, pero se puede utilizar para cualquier grupo de registro.

```
{
    "Version": "2012-10-17",
    "Id": "key-default-1",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::Your_account_ID:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
    ]
}
```

Por último, añada la política actualizada utilizando el siguiente comando put-key-policy:

```
aws kms put-key-policy --key-id key-id --policy-name default --policy file://policy.json
```

# Paso 3: Associate unalOGgagrupación con una CMK

Puede asociar una CMK a un grupo de registros al crearlo o posteriormente.

Para averiguar si un grupo de registro ya tiene un CMK asociado, utilice el siguiente comando describe-log-groups:

```
aws logs describe-log-groups --log-group-name-prefix "log-group-name-prefix"
```

Si la salida incluye un campo `kmsKeyId`, el grupo de registro se asocia con la clave mostrada para el valor de ese campo.

Para asociar la CMK con un grupo de registros al crearlo

Utilice el comando create-log-group como se indica a continuación:

```
aws logs create-log-group --log-group-name my-log-group --kms-key-id "key-arn"
```

Para asociar la CMK con un grupo de registros existente

Utilice el comando associate-kms-key como se indica a continuación:

```
aws logs associate-kms-key --log-group-name my-log-group --kms-key-id "key-arn"
```

# Paso 4: Desasociación de unalOGgrupo de una CMK

Para desvincular la CMK asociada a un grupo de registros, utilice el siguiente comando disassociate-kms-key:

```
aws logs disassociate-kms-key --log-group-name my-log-group
```

# AWS KMS keys yencryptioncontext

Para mejorar la seguridad de suAWS Key Management Servicey los grupos de registro cifrados, CloudWatch Logs coloca ahora ARN de grupo de registros como parte de lacontexto de cifradoutilizado para cifrar sus datos de registro. El contexto de cifrado es un conjunto de pares clave-valor que se utilizan como datos autenticados adicionales. El contexto de cifrado permite utilizar condiciones de política de IAM para limitar el acceso a laAWS KMSClave porAWScuenta y grupo de registro. Para obtener más información, consulteContexto de cifradoyElementos de política de JSON de IAM: Condición.

Le recomendamos que utilice diferentes claves CMK para cada uno de los grupos de registro cifrados.

Si tiene un grupo de registros que cifró anteriormente y ahora desea cambiar el grupo de registros para utilizar una nueva CMK que funcione solo para ese grupo de registros, siga estos pasos.

### Para convertir un grupo de registros cifrado para utilizar una CMK con una política que lo limite a ese grupo de registros

1. Escriba el siguiente comando para encontrar el ARN de la CMK actual del grupo de registros:

   ```
   aws logs describe-log-groups
   ```

   La salida incluye la siguiente línea. Tome nota del ARN. Tiene que usarlo en el paso 7.

   ```
   ...
   "kmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/01234567-89ab-
   cdef-0123-456789abcdef"
   ...
   ```

2. Escriba el siguiente comando para crear una nueva CMK:

   ```
   aws kms create-key
   ```

3. Escriba el siguiente comando para guardar la política de la nueva clave en un archivo `policy.json`:

```
aws kms get-key-policy --key-id new-key-id --policy-name default --output text > ./
policy.json
```

4. Utilice un editor de texto para abrir `policy.json` y agregar una expresión `Condition` a la política:

```
{
    "Version": "2012-10-17",
    "Id": "key-default-1",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::ACCOUNT-ID:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:REGION:ACCOUNT-
ID:log-
group:LOG-GROUP-NAME"
                }
            }
        }
    ]
}
```

5. Escriba el siguiente comando para agregar la política actualizada a la nueva CMK:

```
aws kms put-key-policy --key-id new-key-ARN --policy-name default --policy file://
policy.json
```

6. Escriba el siguiente comando para asociar la política al grupo de registros:

```
aws logs associate-kms-key --log-group-name my-log-group --kms-key-id new-key-ARN
```

Ahora CloudWatch Logs cifra todos los datos nuevos utilizando la nueva CMK.

7. A continuación, revoque todos los permisos excepto `Decrypt` en la antigua CMK. En primer lugar, escriba el siguiente comando para recuperar la política anterior:

```
aws kms get-key-policy --key-id old-key-ARN --policy-name default --output text > ./
policy.json
```

8. Utilice un editor de texto para abrir `policy.json` y eliminar todos los valores de la lista `Action`, excepto `kms:Decrypt*`

```
{
    "Version": "2012-10-17",
    "Id": "key-default-1",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::REGION:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*"
            ],
            "Resource": "*"
        }
    ]
}
```

9. Escriba el siguiente comando para agregar la política actualizada a la CMK antigua:

```
aws kms put-key-policy --key-id old-key-ARN --policy-name default --policy file://
policy.json
```

# CrearmmétricasfROMlOGerejillas de ventilaciónucantarfilters

Puede buscar y filtrar los datos de registro que entran en CloudWatch Logs creando uno o variosFiltros métricas. Los filtros de métricas definen los términos y los patrones que hay que buscar en los datos de registro a medida que se envían a CloudWatch Logs. CloudWatch Logs utiliza estos filtros de métricas para convertir los datos de registro en métricas numéricas de CloudWatch que puede representar gráficamente o en las que puede configurar una alarma.

Al crear una métrica a partir de un filtro de registro, también puede optar por asignar dimensiones y una unidad a la métrica. Si especifica una unidad, asegúrese de especificar la correcta al crear el filtro. El cambio de unidad para el filtro más tarde no tendrá ningún efecto.

Puede utilizar cualquier tipo de estadística de CloudWatch, incluidas las estadísticas de percentiles, al visualizar estas métricas o al configurar alarmas.

> Note
>
> Las métricas admiten estadísticas de percentiles solo si ninguno de sus valores es negativo. Si configura el filtro de métricas para que pueda notificar números negativos, las estadísticas de percentiles no estarán disponibles para esa métrica cuando tenga valores de números negativos. Para obtener más información, consulte Percentiles.

Los filtros no pueden filtrar datos retroactivamente. Los filtros solo publican los puntos de datos de métricas para eventos que ocurran después de la creación del filtro. Los resultados filtrados devuelven las primeras 50 líneas, que no se mostrarán si la marca temporal en los resultados filtrados es anterior al momento de la creación de la métrica.

Contenido



## Concepts

Cada filtro de métrica se compone de los siguientes elementos principales:

valor predeterminado

El valor registrado en el filtro de métricas durante un periodo cuando no se encuentra ningún registro coincidente. Al configurar este valor como 0, garantiza que los datos se registran durante cada periodo, lo que impide métricas "irregulares" con periodos en los que no hay datos.

Si asigna dimensiones a una métrica creada por un filtro de métrica, no puede asignar un valor predeterminado a esa métrica.

Dimensiones de

Las dimensiones son los pares clave-valor que definen aún más una métrica. Puede asignar dimensiones a la métrica creada a partir de un filtro de métrica. Dado que las dimensiones forman parte del identificador único de una métrica, si extrae un par único nombre/valor de los registros, está creando una nueva variación de esa métrica.

patrón de filtro

Una descripción simbólica de cómo debe interpretar CloudWatch Logs los datos en cada evento de registro. Por ejemplo, una entrada de registro puede contener las marcas temporales, direcciones IP, cadenas, etc. Puede utilizar el patrón para especificar lo que hay que buscar en el archivo de registro.

nombre de métrica

El nombre de la métrica de CloudWatch en la que se debe publicar la información de registro monitorizada. Por ejemplo, puede publicar en un métrica denominada ErrorCount.

espacio de nombres de métrica

El espacio de nombres de destino de la nueva métrica de CloudWatch.

valor de métrica

El valor numérico para publicar en la métrica cada vez que se encuentra un registro coincidente. Por ejemplo, si está contando las incidencias de un término determinado como "Error", el valor será "1" para cada incidencia. Si está contando los bytes transferidos, puede incrementar según el número real de bytes encontrados en el evento de registro.

# Filtrar ypatternsyntax

Se pueden utilizar filtros de métricas para buscar y comparar términos, frases o valores incluidos en los eventos de registro. Cuando un filtro de métricas encuentra uno de los términos, frases o valores en los eventos de registro, puede incrementar el valor de una métrica de CloudWatch. Por ejemplo, puede crear un filtro de métrica que busque la palabra ERROR en los eventos de registro y cuente cuántas veces aparece.

También puede optar por asignar cotas y una unidad a la métrica. Por ejemplo, si la métrica cuenta la palabraERROR DEen sus eventos de registro, también puede establecerErrorCodecomo una dimensión para que pueda ver no solo el recuento total de eventos de registro que incluyenERROR DEsino también ver los datos filtrados por los que se informa el código de error.

Note

Si especifica una unidad, asegúrese de especificar la correcta al crear el filtro. El cambio de unidad para el filtro más tarde no tendrá ningún efecto.

Los filtros de métricas también pueden extraer valores numéricos de eventos de registro delimitados por espacio, como la latencia de las solicitudes web. En estos ejemplos, puede incrementar el valor de la métrica según el valor numérico real extraído del registro.

Puede utilizar operadores condicionales y caracteres comodín para crear coincidencias exactas. Antes de crear un filtro de métricas, puede probar los patrones de búsqueda en la consola de CloudWatch. Las secciones siguientes explican la sintaxis de filtro de métricas de forma más detallada.

## Coincidenciaterms enlOGevents

Para buscar un término en los eventos de registro, utilice el término como patrón del filtro de métricas. Puede especificar varios términos en un patrón de filtro de métricas, pero todos los términos deben

aparecer en un evento de registro para que exista una coincidencia. Los filtros de métricas distinguen entre mayúsculas y minúsculas.

Los términos de filtros de métricas que incluyen caracteres distintos de los alfanuméricos o guion bajo deben ir escritos entre comillas dobles ("").

Para excluir un término, utilice un signo menos (-) delante del término.

Ejemplo 1: Coincidir todo

El patrón de filtro "" coincide con todos los eventos de registro.

Ejemplo 2: Periodo único

El patrón de filtro "ERROR" coincide con mensajes de eventos de registro que contienen este término, como los siguientes:

- [ERROR] A fatal exception has occurred
- Saliendo con ERRORCODE: -1

Ejemplo 3: Incluir un término y excluir un término

En el ejemplo anterior, si cambia el patrón de filtro a "ERROR" - "Exiting", se excluirá el mensaje de evento de registro "Exiting with ERRORCODE: -1".

Ejemplo 4: Varios términos

El patrón de filtro "ERROR Exception" coincide con los mensajes de eventos de registro que contienen ambos términos, como los siguientes:

- [ERROR] Caught IllegalArgumentException
- [ERROR] Unhandled Exception

El patrón de filtro "Failed to process the request" coincide con los mensajes de eventos de registro que contienen todos los términos, como los siguientes:

- [WARN] Failed to process the request
- [ERROR] Unable to continue: No se pudo procesar la solicitud

## ORpatternmatching

Puede comparar términos en filtros basados en texto con la coincidencia de patrones OR. Utilice un signo de interrogación para OR, como por ejemplo `?term`.

Observe los tres ejemplos de evento de registro que aparecen a continuación. `ERROR` coincide con los ejemplos 1 y 2. `?ERROR ?WARN` coincide con los ejemplos 1, 2 y 3, ya que todos ellos incluyen la palabra ERROR, o la palabra WARN. `ERROR WARN` solo se coincide con el ejemplo 1, ya que es el único que contiene estas dos palabras. ERROR -WARN coincide con el ejemplo 2, ya que coincide con una cadena que contiene ERROR pero no contiene WARN.

1. `ERROR WARN message`
2. `ERROR message`
3. `WARN message`

Puede comparar términos con la coincidencia de patrones OR en filtros delimitados por espacios. Con filtros delimitados por espacios, `w1` significa la primera palabra en el evento de registro, `w2` significa la

segunda palabra, y así sucesivamente. En los patrones de ejemplo siguientes, [W1=Error, w2] coincide con los patrones 1 y 2 porque ERROR es la primera palabra, y [W1=Error || W1=Warn, w2] coincide con los patrones 1, 2 y 3. [W1! =Error&&w1! =WARN, w2] no coincide con ninguna de las líneas porque todas contienen ERROR o WARN.

1. ERROR WARN mensaje
2. ERROR mensaje
3. WARN mensaje

Puede comparar términos con la coincidencia de patrones OR en filtros JSON. En los patrones de ejemplo siguientes, {$.foo = bar} coincide con el patrón 1, {$.foo = baz } coincide con el patrón 2 y {$.foo = bar || $.foo = baz } coincide con los patrones 1 y 2.

1. {"foo": "bar"}
2. {"foo": "baz"}

## Coincidenciaterms en JSONlOGevents

Puede extraer valores de eventos de registros JSON. Para extraer valores de eventos de registro JSON, tiene que crear un filtro de métrica basado en cadena. No se admiten las cadenas que contengan notación científica. Los elementos en los datos de eventos de registro JSON deben coincidir exactamente con el filtro de métricas. Es posible que desee crear filtros de métricas en eventos de registro JSON para indicar lo siguiente:

- Se produce un determinado evento. Por ejemplo eventName es "UpdateTrail".
- La IP se encuentra fuera de una subred conocida. Por ejemplo, sourceIPAddress no está dentro de ningún intervalo de subred conocido.
- Son verdaderas una combinación de dos o más de las condiciones anteriores. Por ejemplo, el eventName es «UpdateTrail» y recipientAccountId es 123456789012.

### Uso demétricofilters aextractvalues de JSONlOGevents

Puede utilizar filtros de métricas para extraer valores de eventos de registro JSON. Un filtro de métricas comprueba los registros entrantes y modifica un valor numérico cuando el filtro encuentra una coincidencia en los datos de registro. Al crear un filtro de métricas, puede incrementar simplemente un recuento cada vez que el texto coincidente se encuentre en un registro, o puede extraer valores numéricos del registro y utilizarlos para incrementar el valor de las métricas.

#### Coincidencia de JSONtermsucantarmétricofilters

La sintaxis del filtro de métricas para eventos de registro JSON utiliza el formato siguiente:

```
{ SELECTOR EQUALITY_OPERATOR STRING }
```

El filtro de métricas debe ir escrito entre llaves { }, para indicar que se trata de una expresión JSON. El filtro de métricas contiene las siguientes partes:

SELECTOR

Especifica la propiedad de JSON que comprobar. Los selectores de propiedades siempre empiezan por un signo de dólar ($), lo que significa la raíz de JSON. Los selectores de propiedades son cadenas alfanuméricas que también admiten los caracteres "-" y "_". Los elementos de matriz se indican con la sintaxis [NUMBER] y deben cumplir una propiedad. Algunos ejemplos son: $.eventId, $.users[0], $.users[0].id, $.requestParameters.instanceId.

EQUALITY_OPERATOR

Puede ser = o !=-.

STRING

Una cadena con o sin comillas. Puede utilizar el carácter comodín asterisco "*" para que coincida con cualquier texto, delante o detrás de un término de búsqueda. Por ejemplo, *Event coincidirá con PutEvent y GetEvent. Event* coincidirá con EventId y EventName. Ev*ent solo coincidirá con la cadena real Ev*ent. Las cadenas que constan solo de caracteres alfanuméricos no se tienen que escribir entre comillas. Las cadenas que tienen caracteres Unicode y de otro tipo, por ejemplo, "@","$", "\", etc. se deben escribir entre comillas dobles para que sean válidas.

### JSONmétricofilterexamples

A continuación se muestra un ejemplo JSON:

```
{
  "eventType": "UpdateTrail",
  "sourceIPAddress": "111.111.111.111",
  "arrayKey": [
        "value",
        "another value"
  ],
  "objectList": [
       {
         "name": "a",
         "id": 1
       },
       {
         "name": "b",
         "id": 2
       }
  ],
  "SomeObject": null,
  "ThisFlag": true
}
```

Las siguientes filtros coincidirían:

```
{ $.eventType = "UpdateTrail" }
```

Filtro sobre el tipo de evento UpdateTrail.

```
{ $.sourceIPAddress != 123.123.* }
```

Filtro sobre la dirección IP que está fuera del prefijo de subred 123.123.

```
{ $.arrayKey[0] = "value" }
```

El filtro en la primera entrada en arrayKey es "value". Si arrayKey no es una matriz será falso.

```
{ $.objectList[1].id = 2 }
```

Filtro en la segunda entrada en objectList con una propiedad denominada id = 2. Si objectList no es una matriz será falso. Si los elementos en objectList no son objetos o no tiene una propiedad de ID, será falso.

```
{ $.SomeObject IS NULL }
```

Filtro en SomeObject se ha definido como nulo. Esto solo será verdadero si el objeto especificado se ha definido en nulo.

```
{ $.SomeOtherObject NOT EXISTS }
```

Filtro en SomeOtherObject inexistente. Esto solo será verdadero si el objeto especificado no existe en los datos de registro.

```
{ $.ThisFlag IS TRUE }
```

Los filtros en ThisFlag con valor TRUE. Esto también funciona para filtros booleanos que comprobarán el valor FALSE.

### JSONcompoundconditions

Puede combinar varias condiciones en una expresión compuesta con OR (||) y AND (&&). Se permite el uso de paréntesis y la sintaxis sigue el orden estándar de operaciones () > && > ||.

```
{
    "user": {
        "id": 1,
        "email": "John.Stiles@example.com"
    },
    "users": [
        {
         "id": 2,
         "email": "John.Doe@example.com"
        },
        {
         "id": 3,
         "email": "Jane.Doe@example.com"
        }
    ],
    "actions": [
        "GET",
        "PUT",
        "DELETE"
    ],
    "coordinates": [
        [0, 1, 2],
        [4, 5, 6],
        [7, 8, 9]
    ]
}
```

### Examples

```
{ ($.user.id = 1) && ($.users[0].email = "John.Doe@example.com") }
```

Coincide con el JSON anterior.

```
{ ($.user.id = 2 && $.users[0].email = "nonmatch") || $.actions[2] = "GET" }
```

No coincide con el JSON anterior.

```
{ $.user.email = "John.Stiles@example.com" || $.coordinates[0][1] = nonmatch &&
 $.actions[2] = nomatch }
```

Coincide con el JSON anterior.

```
{ ($.user.email = "John.Stiles@example.com" || $.coordinates[0][1] = nonmatch) &&
 $.actions[2] = nomatch }
```

No coincide con el JSON anterior.

### JSONspecialconsiderations

El SELECTOR debe apuntar a un nodo de valor (cadena o número) en el JSON. Si apunta a una matriz o a un objeto, el filtro no se aplicará, ya que el formato de registro no coincide con el filtro. Por ejemplo, tanto {$.users = 1} como {$.users != 1} no coincidirán con un evento de registro en el que los usuarios están en una matriz:

```
{
  "users": [1, 2, 3]
}
```

### Numéricocomparisons

La sintaxis de filtro de métricas admite la concordancia exacta en comparaciones numéricas. Se admiten las siguientes comparaciones numéricas: **<**, **>**, **>=**, **<=**, **=**, **!=**

Los filtros numéricos tienen una sintaxis de

```
{ SELECTOR NUMERIC_OPERATOR NUMBER }
```

El filtro de métricas debe ir escrito entre llaves { }, para indicar que se trata de una expresión JSON. El filtro de métricas contiene las siguientes partes:

SELECTOR

Especifica la propiedad de JSON que comprobar. Los selectores de propiedades siempre empiezan por un signo de dólar ($), lo que significa la raíz de JSON. Los selectores de propiedades son cadenas alfanuméricas que también admiten los caracteres "-" y "_". Los elementos de matriz se indican con la sintaxis [NUMBER] y deben cumplir una propiedad. Algunos ejemplos son: $.latency, $.numbers[0], $.errorCode, $.processes[4].averageRuntime.

NUMERIC_OPERATOR

Puede ser uno de los siguientes: **=**, **!=**, **<**, **>**, **<=** o **>=**.

NUMBER

Un número entero con un signo + o - opcional, un decimal con un signo + o - opcional o un número en notación científica, que es un entero o un decimal con un signo + o - opcional, seguido de "e", seguido de un entero con un signo + o - opcional.

Ejemplos:

```
{ $.latency >= 500 }
{ $.numbers[0] < 10e3 }
{ $.numbers[0] < 10e-3 }
{ $.processes[4].averageRuntime <= 55.5 }
{ $.errorCode = 400 }
{ $.errorCode != 500 }
{ $.latency > +1000 }
```

# Uso demétricofilters aextractvalues desritmodelimadalOGevents

Puede utilizar filtros de métricas para extraer valores de eventos de registro delimitados por espacios. Los caracteres entre un par de corchetes [] o dos comillas dobles ("") se tratan como un campo único. Por ejemplo:

```
127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] "GET /apache_pb.gif HTTP/1.0" 200 1534
127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] "GET /apache_pb.gif HTTP/1.0" 500 5324
127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] "GET /apache_pb.gif HTTP/1.0" 200 4355
```

Para especificar un patrón de filtro de métricas que analice eventos delimitados por espacios, el patrón de filtro de métricas tiene que especificar los campos con un nombre, separado por comas, con todo el patrón entre corchetes. Por ejemplo: [ip, user, username, timestamp, request, status_code, bytes].

En los casos en que no sabe el número de campos, puede utilizar la notificación abreviada utilizando puntos suspensivos (…). Por ejemplo:

```
[..., status_code, bytes]
[ip, user, ..., status_code, bytes]
[ip, user, ...]
```

También puede añadir condiciones a los campos para que solo los eventos de registro que coincidan con todas las condiciones coincidan con los filtros. Por ejemplo:

```
[ip, user, username, timestamp, request, status_code, bytes > 1000]
[ip, user, username, timestamp, request, status_code = 200, bytes]
[ip, user, username, timestamp, request, status_code = 4*, bytes]
[ip, user, username, timestamp, request = *html*, status_code = 4*, bytes]
```

Puede utilizar `&&` como operador AND lógico y `||` como operador OR lógico, como en los siguientes ejemplos:

```
[ip, user, username, timestamp, request, status_code = 4* && bytes > 1000]
[ip, user, username, timestamp, request, status_code = 403 || status_code = 404, bytes]
```

CloudWatch Logs son compatibles con los campos condicionales de cadena y número. En los campos de cadena, puede utilizar los operadores = o != con un asterisco (*).

En el caso de los campos numéricos, puede utilizar los operadores **>**, **<**, **>=**, **<=**, = y !=.

Si utiliza un filtro delimitado por espacios, los campos extraídos se asignan a los nombres de los campos delimitados por espacios (tal como se expresa en el filtro) al valor de cada uno de estos campos. Si no va a utilizar un filtro delimitado por espacios, estará vacío.

Filtro de ejemplo:

```
[..., request=*.html*, status_code=4*,]
```

Evento de registro de ejemplo para el filtro:

```
127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html HTTP/1.0\" 404 1534
```

Los campos extraídos para el evento de registro y patrón de filtros:

```
{
   "$status_code": "404",
```

```
   "$request": "GET /products/index.html HTTP/1.0",
   "$7": "1534",
   "$4": "10/Oct/2000:13:25:15 -0700",
   "$3": "frank",
   "$2": "-",
   "$1": "127.0.0.1"
}
```

# Settinghowthemetricvaluechangeswhenmatchesarefound

Cuando un filtro de métricas encuentra uno de los términos, frases o valores coincidentes en los eventos de registro, incrementa el recuento de la métrica de CloudWatch de según la cantidad que especifique en el valor de la métrica. El valor de las métricas se acumula y registra cada minuto.

Si los registros se introducen durante un periodo de tiempo de un minuto, pero no se encuentran coincidencias, se notifica el valor especificado para el valor predeterminado (si lo hubiera). Sin embargo, si no se introducen eventos de registro durante un periodo de un minuto, no se notifica ningún valor.

Especificar un valor predeterminado, aunque sea 0, contribuye a garantizar que los datos se notifican con más frecuencia, lo que contribuye a evitar las métricas irregulares cuando no se encuentran coincidencias.

Por ejemplo, suponga que existe un grupo de registros que publica dos registros cada minuto y el valor de la métrica es 1 y el valor predeterminado es 0. Si se encuentran coincidencias en ambas entradas de registro en el primer minuto, el valor de la métrica para ese minuto es 2. Si no hay coincidencias en los registros publicados en el segundo minuto, se utiliza el valor predeterminado 0 para ambos registros y el valor de la métrica de ese minuto es 0.

Si no especifica ningún valor predeterminado, no se registran datos para ninguno de los periodos en los que no se encuentran coincidencias de patrón.

Si asigna dimensiones a una métrica creada por un filtro de métrica, no puede asignar un valor predeterminado a esa métrica.

# Publishingnumericalvaluesfound inlogentries

En vez de contar solo el número de los elementos coincidentes encontrados en los registros, también puede utilizar el filtro de métricas para publicar los valores en función de los valores numéricos encontrados en los registros. El siguiente procedimiento muestra cómo publicar una métrica con la latencia encontrada en la solicitud JSON `metricFilter: { $.latency = * } metricValue: $.latency`.

### Para publicar una métrica con la latencia en una solicitud JSON

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija `Actions`, Create metric filter (Crear filtro de métricas).
4. En Filter Pattern (Patrón de filtro), escriba **`{ $.latency = * }`** y, a continuación, elija Next (Siguiente).
5. En Metric Name, escriba myMetric.
6. En Metric Value (Valor de métrica), escriba **`$.latency`**.
7. En Default Value (Valor predeterminado) escriba 0 y, a continuación, elija Next (Siguiente). La especificación de un valor predeterminado garantiza que los datos se comuniquen incluso durante períodos en los que ningún evento de registro coincida con el filtro. Esto evita que las métricas sean irregulares o falten cuando se ingieren registros, pero no coinciden con el filtro.
8. Elija Create metric filter (Crear filtro de métricas).

El siguiente evento de registro publicaría un valor de 50 en la métrica myMetric tras la creación del filtro.

```
{
"latency": 50,
"requestType": "GET"
}
```

# Publicar dimensiones con las métricas

Cuando publica una métrica generada a partir de valores encontrados en eventos de registro JSON o eventos de registro delimitados por espacios, también puede publicar dimensiones con la métrica. Puede publicar hasta tres dimensiones con una métrica generada por un filtro de métrica. Para obtener más información acerca de las dimensiones, consulteDimensiones.

> Warning
>
> Las métricas extraídas de eventos de registro se cargan como métricas personalizadas. Para evitar cargas elevadas inesperadas, no especifique campos de alta cardinalidad, como`IPAddress`o`requestID`como dimensiones. Cada valor diferente encontrado para una dimensión se trata como una métrica independiente y acumula cargos como una métrica personalizada independiente.
> Para evitar cargos accidentales elevados, es posible que Amazon deshabilite un filtro de métrica si genera 1000 pares de nombre/valor diferentes para las dimensiones especificadas en un plazo determinado.
> También puede configurar una alarma de facturación para avisarle si los cargos son superiores a los esperados. Para obtener más información, consulteCrear una alarma de facturación para monitorizar la estimación deAWSCargos.

## Publicar dimensiones con métricas de eventos de registro JSON

Para ver cómo especificar dimensiones para un filtro de métrica para eventos de registro JSON, empecemos por mirar un filtro de ejemplo y un evento de registro de ejemplo para el filtro.

Ejemplo de filtro:

```
{ $.eventType = "*" && $.sourceIPAddress != 123.123.*}
```

Ejemplo de evento de registro:

```
{"eventType": "UpdateTrail",
  "sourceIPAddress": "111.111.111.111",
  "arrayKey": [
        "value",
        "another value"
  ],
  "objectList": [
       {"name": "a",
         "id": 1
       },
       {"name": "b",
         "id": 2
       }
  ],
  "SomeObject": null,
  "ThisFlag": true
}
```

Este filtro de ejemplo incrementa la métrica siempre que un evento de registro incluya cualquiera de los campos enumerados en el filtro.

```
[ $.eventType, $.sourceIPAddress ]
```

Al crear el filtro de métrica, puede especificar cualquiera de los campos del filtro como una dimensión. Por ejemplo, para establecer el tipo de evento como dimensión, especifique lo siguiente como dimensión al configurar el filtro de métrica.

```
"EventType" : $.eventType
```

Esta métrica tiene una dimensión llamada`EventType`, y los valores de las dimensiones son los tipos de eventos que se encuentran en los eventos de registro, como`UpdateTrail`en este evento de registro de ejemplo.

## Publicar dimensiones con métricas de eventos de registro delimitados por espacios.

Para ver cómo especificar dimensiones para un filtro de métrica para eventos de registro delimitados por espacios, empecemos por mirar un filtro de ejemplo y un evento de registro de ejemplo para el filtro.

Ejemplo de filtro:

```
[ip, server, username, timestamp, request, status_code, bytes > 1000]
```

Ejemplo de evento de registro:

```
127.0.0.1 Prod frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html HTTP/1.0\" 404 1534
```

Este filtro de ejemplo incrementa la métrica siempre que un evento de registro incluya cualquiera de los campos enumerados en el filtro. Para el evento de registro de ejemplo mostrado anteriormente, el filtro busca los siguientes campos y valores.

```
{
   "$status_code": "404",
   "$request": "GET /products/index.html HTTP/1.0",
   "$bytes": "1534",
   "$timestamp": "10/Oct/2000:13:25:15 -0700",
   "$username": "frank",
   "$server": "Prod",
   "$ip": "127.0.0.1"
}
```

Al crear el filtro de métrica, puede especificar cualquiera de estos campos como una dimensión. Por ejemplo, para establecer el nombre del servidor como dimensión, debe especificar la siguiente dimensión cuando configure el filtro de métrica.

```
"Server" : $server
```

Esta métrica tiene una dimensión llamada`Server`, y los valores de las dimensiones son los nombres de servidor que se encuentran en los eventos de registro, como`Prod`en este evento de registro de ejemplo.

# Crearmétricofilters

Los siguientes procedimientos y ejemplos muestran cómo crear filtros de métricas.

Ejemplos



# Crear un filtro de métricas para un grupo de registros.

Para crear un filtro de métricas para un grupo de registros, siga los pasos que se indican a continuación.

Para crear un filtro de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre del grupo de registros.
4. Elija `Actions`, Create metric filter (Crear filtro de métricas).
5. Parapatrón de filtro, escriba el patrón de filtro que se va a utilizar. Para obtener más información, consulte Filtrar ypatternsyntax (p. 73) .
6. Para probar el patrón de filtro, enPattern de prueba, introduzca uno o más eventos de registro para usar para probar el patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en elMensajes de eventos de registro.
7. SeleccionarSiguientey, a continuación, escriba un nombre para el filtro.
8. UNDERDetalles de métrica, paraespacio de nombres de métrica, escriba un nombre para el espacio de nombres de CloudWatch en el que se publicará la métrica. Si este espacio de nombres no existe todavía, asegúrese de queCrear nuevosestá seleccionada.
9. ParaNombre de métrica, escriba un nombre para la nueva métrica de.
10. ParaValor de la métrica, si el filtro de métrica está contando las ocurrencias de las palabras clave en el filtro, escriba 1. Esto incrementa la métrica en 1 por cada evento de registro que incluye una de las palabras clave.

    También puede introducir un token como**`$size`**. Esto incrementa la métrica por el valor del número en el`size`para cada evento de registro que contenga un`size`.
11. (Opcional) ParaUnidad, seleccione una unidad para asignar a la métrica. Si no especifica una unidad, la unidad se define como`None`.
12. (Opcional) Introduzca los nombres y los tokens de hasta tres dimensiones para la métrica.

    Si asigna dimensiones a una métrica creada por un filtro de métrica, no puede asignar un valor predeterminado a esa métrica.
13. Elija Create metric filter (Crear filtro de métricas).

# Ejemplo: RecuentolOGevents

El tipo de monitorización de evento de registro más sencillo consiste en contar el número de eventos de registro que se producen. Es posible que desee hacerlo para llevar un recuento de todos los eventos, para crear un monitor de estilo "latido" o simplemente para practicar la creación de filtros de métricas.

En el siguiente ejemplo de CLI, un filtro de métrica denominado MyAppAccessCount se aplica al grupo de registro MyApp/access.log para crear la métrica EventCount en el espacio de nombres de CloudWatch

MyNamespace. El filtro está configurado para que compare cualquier contenido de eventos de registro y para aumentar la métrica en "1".

Para crear un filtro de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre de un grupo de registros.
4. Elija `Actions`, Create metric filter (Crear filtro de métricas).
5. Deje Filter Pattern (Patrón de filtro) y Select Log Data to Test (Seleccionar los datos de registro para probar) en blanco.
6. Elija Next (Siguiente), y, a continuación, en Filter Name (Nombre de filtro), escriba **`EventCount`**.
7. En Metric Details (Detalles de métrica), en Metric Namespace (Espacio de nombres de métrica), escriba **`MyNameSpace`**.
8. En Nombre de métrica, escriba **`MyAppEventCount`**.
9. Confirme que el Metric Value (Valor métrico) es 1. Esto especifica que el recuento se incrementa en 1 para cada evento de registro.
10. En Default Value (Valor predeterminado) escriba 0 y, a continuación, elija Next (Siguiente). Al especificar un valor predeterminado se garantiza que los datos se registren incluso durante los periodos en los que no se producen eventos de registro, lo que impide que haya métricas irregulares en las que a veces no existen datos.
11. Elija Create metric filter (Crear filtro de métricas).

Para crear un filtro de métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs put-metric-filter \
  --log-group-name MyApp/access.log \
  --filter-name EventCount \
  --filter-pattern " " \
  --metric-transformations \
  metricName=MyAppEventCount,metricNamespace=MyNamespace,metricValue=1,defaultValue=0
```

Puede probar esta nueva política publicando cualesquiera datos de eventos. Debería ver los puntos de datos publicados en la métrica MyAppAccessEventCount.

Para publicar datos de eventos mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs put-log-events \
  --log-group-name MyApp/access.log --log-stream-name TestStream1 \
  --log-events \
    timestamp=1394793518000,message="Test event 1" \
    timestamp=1394793518000,message="Test event 2" \
    timestamp=1394793528000,message="This message also contains an Error"
```

# Ejemplo: Recuentooccurrencias de unterm

Los eventos de registro suelen incluir mensajes importantes que desea contar, quizás referentes al éxito o fracaso de las operaciones. Por ejemplo, puede producirse un error y registrarse en un archivo de registro si falla una determinada operación. Es posible que desee monitorizar estas entradas para comprender la evolución de sus errores.

En el ejemplo siguiente, se crea un filtro de métricas para monitorizar el término Error. La política se ha creado y se ha añadido al grupo de registros.MyApp/message.log. CloudWatch Logs publica un punto de datos en la métrica personalizada de CloudWatch ErrorCount en laMyApp/message.logCon un valor de «1" para cada evento que contenga Error. Si ningún evento contiene la palabra Error, entonces se publica un valor 0. Cuando se representan estos datos gráficamente en la consola de CloudWatch, asegúrese de utilizar la estadística de suma.

Después de crear un filtro de métricas, puede ver la métrica en la consola de CloudWatch. Cuando seleccione la métrica que desea ver, seleccione el espacio de nombres de métrica que coincida con el nombre del grupo de registros. Para obtener más información, consulte Viewing Available Metrics (Visualización de las métricas disponibles).

Para crear un filtro de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre del grupo de registros.
4. Elija Actions (Acciones), Create metric filter (Crear filtro de métricas).
5. En Filter pattern (Patrón de filtro), escriba **`Error`**.

   Note

   Todas las entradas de Filter Pattern distinguen entre mayúsculas y minúsculas.
6. Para probar el patrón de filtro, enPattern de prueba, introduzca uno o más eventos de registro para usar para probar el patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en elMensajes de eventos de registro.
7. Elija Next (Siguiente), y, a continuación, en la página Filter Name (Asignar métrica), en Filter Name (Nombre de filtro), escriba **`MyAppErrorCount`**.
8. En Metric Details, en Metric Namespace, escriba MyNameSpace.
9. En Metric Name, escriba ErrorCount.
10. Confirme que el Metric Value (Valor métrico) es 1. Esto especifica que el recuento se incrementa en 1 para cada evento de registro que contenga "Error".
11. En Default Value (Valor predeterminado) escriba 0 y, a continuación, elija Next (Siguiente).
12. Elija Create metric filter (Crear filtro de métricas).

Para crear un filtro de métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs put-metric-filter \
  --log-group-name MyApp/message.log \
  --filter-name MyAppErrorCount \
  --filter-pattern 'Error' \
  --metric-transformations \
      metricName=ErrorCount,metricNamespace=MyNamespace,metricValue=1,defaultValue=0
```

Puede probar esta nueva política publicando eventos que contengan la palabra "Error" en el mensaje.

Para publicar eventos mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando. Tenga en cuenta que los patrones distinguen entre mayúsculas y minúsculas.

```
aws logs put-log-events \
  --log-group-name MyApp/access.log --log-stream-name TestStream1 \
```

```
  --log-events \
    timestamp=1394793518000,message="This message contains an Error" \
    timestamp=1394793528000,message="This message also contains an Error"
```

# Ejemplo: Recuento HTTP 404codes

Mediante CloudWatch Logs, puede monitorizar cuántas veces los servidores Apache devuelven una respuesta HTTP 404, que es el código de respuesta de página no encontrada. Es posible que le interese monitorizar esto para saber con qué frecuencia los visitantes no encuentran el recurso que buscan. Supongamos que los registros se estructuran para incluir la siguiente información para cada evento de registro (visita al sitio):

- Dirección IP del solicitante
- Identidad RFC 1413
- Nombre de usuario
- Marca temporal
- Solicitar método con recurso solicitado y protocolo
- Código de respuesta HTTP para solicitud
- Bytes transferidos en solicitud

Un ejemplo de esto podría ser el siguiente:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 404 2326
```

Podría especificar una regla que intente comparar eventos con dicha estructura para errores HTTP 404, tal y como se muestra en el ejemplo siguiente:

Para crear un filtro de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija `Actions`, Create metric filter (Crear filtro de métricas).
4. En Filter pattern (Patrón de filtro), escriba **`[IP, UserInfo, User, Timestamp, RequestInfo, StatusCode=404, Bytes]`**.
5. Para probar el patrón de filtro, enPattern de prueba, introduzca uno o más eventos de registro para usar para probar el patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en elMensajes de eventos de registro.
6. Elija Next (Siguiente), y, a continuación, para Filter name (Nombre de filtro), escriba HTTP404Errors.
7. En Metric Details (Detalles de métrica), en Metric Namespace (Espacio de nombres de métrica), escriba **`MyNameSpace`**.
8. En Metric name (Nombre de métrica), escriba **`ApacheNotFoundErrorCount`**.
9. Confirme que el Metric Value (Valor métrico) es 1. Esto especifica que el recuento se incrementa en 1 para cada evento de Error 404.
10. En Default Value (Valor predeterminado) escriba 0 y, a continuación, elija Next (Siguiente).
11. Elija Create metric filter (Crear filtro de métricas).

Para crear un filtro de métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs put-metric-filter \
```

```
  --log-group-name MyApp/access.log \
  --filter-name HTTP404Errors \
  --filter-pattern '[ip, id, user, timestamp, request, status_code=404, size]' \
  --metric-transformations \
      metricName=ApacheNotFoundErrorCount,metricNamespace=MyNamespace,metricValue=1
```

En este ejemplo, se han utilizado caracteres literales como los corchetes izquierdo y derecho, las comillas dobles y la cadena de caracteres 404. El patrón tiene que coincidir con todo el mensaje de evento de registro para que el evento de registro se tenga en cuenta para monitorización.

Puede verificar la creación del filtro de métricas a través del comando describe-metric-filters. Debería ver un resultado con un aspecto similar al siguiente:

```
aws logs describe-metric-filters --log-group-name MyApp/access.log

{
    "metricFilters": [
        {
            "filterName": "HTTP404Errors",
            "metricTransformations": [
                {
                    "metricValue": "1",
                    "metricNamespace": "MyNamespace",
                    "metricName": "ApacheNotFoundErrorCount"
                }
            ],
            "creationTime": 1399277571078,
            "filterPattern": "[ip, id, user, timestamp, request, status_code=404, size]"
        }
    ]
}
```

Ahora puede publicar unos cuantos eventos manualmente:

```
aws logs put-log-events \
--log-group-name MyApp/access.log --log-stream-name hostname \
--log-events \
timestamp=1394793518000,message="127.0.0.1 - bob [10/Oct/2000:13:55:36 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 404 2326" \
timestamp=1394793528000,message="127.0.0.1 - bob [10/Oct/2000:13:55:36 -0700] \"GET /
apache_pb2.gif HTTP/1.0\" 200 2326"
```

Poco después de colocar estos eventos de registro de ejemplo, puede recuperar la métrica denominada en la consola de CloudWatch como ApacheNotFoundErrorCount.

# Ejemplo: Recuento HTTP 4xxcodes

Como en el ejemplo anterior, es posible que desee monitorizar los registros de acceso al servicio web y monitorizar los niveles del código de respuesta HTTP. Por ejemplo, es posible que desee monitorizar todos los errores de nivel HTTP 400. Sin embargo, es posible que no desee especificar un nuevo filtro de métrica para cada código devuelto.

El siguiente ejemplo muestra cómo crear una métrica que incluya todas las respuestas de código HTTP de nivel 400 desde registro de acceso utilizando el formato de registro de acceso de Apache desde el ejemplo Ejemplo: Recuento HTTP 404codes (p. 86).

Para crear un filtro de métricas mediante la consola de CloudWatch

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

2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre del grupo de registros para el servidor Apache.
4. Elija `Actions`, Create metric filter (Crear filtro de métricas).
5. Parapatrón de filtrointroduzca, escriba**`[ip, id, user, timestamp, request, status_code=4*, size]`**.
6. Para probar el patrón de filtro, enPattern de prueba, introduzca uno o más eventos de registro para usar para probar el patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en elMensajes de eventos de registro.
7. SeleccionarSiguientey, a continuación, paraNombre del filtro, escriba**`HTTP4xxErrors`**.
8. UNDERDetalles de métrica, paraespacio de nombres de métricaintroduzca, escriba**`MyNameSpace`**.
9. ParaNombre de métricaintroduzca, escribaHttp4xxErr.
10. ParaValor de la métricaEscriba 1. Esto especifica que el recuento se incrementa en 1 para cada evento de registro que contenga un error 4xx.
11. ParaValor predeterminadoEscriba 0 y, a continuación, elijaSiguiente.
12. Elija Create metric filter (Crear filtro de métricas).

Para crear un filtro de métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs put-metric-filter \
  --log-group-name MyApp/access.log \
  --filter-name HTTP4xxErrors \
  --filter-pattern '[ip, id, user, timestamp, request, status_code=4*, size]' \
  --metric-transformations \
  metricName=HTTP4xxErrors,metricNamespace=MyNamespace,metricValue=1,defaultValue=0
```

Puede utilizar los siguientes datos en llamadas PutEvents para probar esta regla. Si no elimina la regla de monitorización en el ejemplo anterior, generará dos métricas diferentes.

```
127.0.0.1 - - [24/Sep/2013:11:49:52 -0700] "GET /index.html HTTP/1.1" 404 287
127.0.0.1 - - [24/Sep/2013:11:49:52 -0700] "GET /index.html HTTP/1.1" 404 287
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /~test/ HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /favicon.ico HTTP/1.1" 404 308
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /favicon.ico HTTP/1.1" 404 308
127.0.0.1 - - [24/Sep/2013:11:51:34 -0700] "GET /~test/index.html HTTP/1.1" 200 3
```

# Ejemplo: Extraer campos de un registro de Apache y asignar dimensiones

A veces, en lugar de contar, se recomienda utilizar valores dentro de eventos de registro individuales para valores de métricas. Este ejemplo muestra cómo puede crear una regla de extracción para crear una métrica que mida los bytes transferidos por un servidor web Apache.

Esta regla de extracción coincide con los siete campos del evento de registro. El valor de la métrica es el valor del séptimo token coincidente. Puede consultar la referencia al token como "$7" en el campo `metricValue` de la regla de extracción.

En este ejemplo también se muestra cómo asignar dimensiones a la métrica que se está creando.

Para crear un filtro de métricas mediante la consola de CloudWatch

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

2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre del grupo de registros para el servidor Apache.
4. Elija `Actions`, Create metric filter (Crear filtro de métricas).
5. Parapatrón de filtrointroduzca, escriba**`[ip, id, user, timestamp, request, status_code, size]`**.
6. Para probar el patrón de filtro, enPattern de prueba, introduzca uno o más eventos de registro para usar para probar el patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en elMensajes de eventos de registro.
7. SeleccionarSiguientey, a continuación, paraNombre del filtro, escriba**`size`**.
8. UNDERDetalles de métrica, paraespacio de nombres de métricaintroduzca, escriba**`MyNameSpace`**. Debido a que este es un nuevo espacio de nombres, asegúrese de queCrear nuevosestá seleccionada.
9. ParaNombre de métricaintroduzca, escriba**`BytesTransferred`**
10. ParaValor de la métricaintroduzca, escriba**`$size`**.
11. ParaUnidad, seleccioneBytes.
12. Para Dimension Name, escriba **`IP`**.
13. ParaValor de dimensión, escriba**`$.ip`**Y, a continuación, elijaSiguiente.
14. Elija Create metric filter (Crear filtro de métricas).

Para crear este filtro de métricas mediante laAWS CLI

En el símbolo del sistema, ejecute el siguiente comando

```
aws logs put-metric-filter \
--log-group-name MyApp/access.log \
 --filter-name BytesTransferred \
 --filter-pattern '[ip, id, user, timestamp, request, status_code, size]' \
 --metric-transformation  \
 metricName=BytesTransferred,metricNamespace=MyNamespace,metricValue=$size
```

```
aws logs put-metric-filter \
--log-group-name MyApp/access.log \
--filter-name BytesTransferred \
--filter-pattern '[ip, id, user, timestamp, request, status_code, size]' \
--metric-transformation  \
metricName=BytesTransferred,metricNamespace=MyNamespace,metricValue=
$size,unit=Bytes,dimensions='{EventType=$eventtype}'
```

> **Note**
>
> En este comando, utilice este formato para especificar varias dimensiones.
>
> ```
> aws logs put-metric-filter \
> --log-group-name my-log-group-name \
> --filter-name my-filter-name \
> --filter-pattern 'my-filter-pattern' \
> --metric-transformation  \
> metricName=my-metric-name,metricNamespace=my-metric-namespace,metricValue=my-
> token,unit=unit,dimensions='{dimension1=$dim,dimension2=$dim2,dim3=$dim3}''
> ```

Puede utilizar los siguientes datos en llamadas PutLogEvents para probar esta regla. Esto genera dos métricas diferentes si no elimina la regla de monitorización en el ejemplo anterior.

```
127.0.0.1 - - [24/Sep/2013:11:49:52 -0700] "GET /index.html HTTP/1.1" 404 287
```

```
127.0.0.1 - - [24/Sep/2013:11:49:52 -0700] "GET /index.html HTTP/1.1" 404 287
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /~test/ HTTP/1.1" 200 3
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /favicon.ico HTTP/1.1" 404 308
127.0.0.1 - - [24/Sep/2013:11:50:51 -0700] "GET /favicon.ico HTTP/1.1" 404 308
127.0.0.1 - - [24/Sep/2013:11:51:34 -0700] "GET /~test/index.html HTTP/1.1" 200 3
```

# Listamétricofilters

Puede enumerar todos los filtros de métricas de un grupo de registros.

Para mostrar filtros de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. En el panel de contenido, en la lista de grupos de registros, en la columna Metric Filters, elija el número de filtros.

   La pantalla Log Groups > Filters for muestra todos los filtros de métricas asociados con el grupo de registros.

Para mostrar filtros de métricas con la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs describe-metric-filters --log-group-name MyApp/access.log
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "metricFilters": [
        {
            "filterName": "HTTP404Errors",
            "metricTransformations": [
                {
                    "metricValue": "1",
                    "metricNamespace": "MyNamespace",
                    "metricName": "ApacheNotFoundErrorCount"
                }
            ],
            "creationTime": 1399277571078,
            "filterPattern": "[ip, id, user, timestamp, request, status_code=404, size]"
        }
    ]
}
```

# Eliminación de unmétricofilter

Una política se identifica por su nombre y el grupo de registros al que pertenece.

Para eliminar un filtro de métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).

3. En el panel de contenido, en la secciónFiltro de métricas, elija el número de filtros de métrica para el grupo de registros.
4. UNDERFiltros de métricas, active la casilla de verificación situada a la derecha del nombre del filtro que desea eliminar. A continuación, elija Delete (Eliminar).
5. Cuando se le pida confirmación, seleccione Delete (Eliminar).

Para eliminar un filtro de métricas con la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws logs delete-metric-filter --log-group-name MyApp/access.log \
 --filter-name MyFilterName
```

# En tiempo realprocessing delOGdata consubscriptions

Puede utilizar las suscripciones para obtener acceso a la fuente en tiempo real de eventos de registros de CloudWatch Logs y enviarlos a otros servicios como, por ejemplo, un flujo de Amazon Kinesis, un flujo de Amazon Kinesis Data Firehose oAWS Lambdapara procesamiento personalizado, análisis o carga en otros sistemas. Cuando los eventos de registro se envían al servicio de recepción, están codificados en Base64 y comprimidos con el formato gzip.

Para empezar a suscribirse a eventos de registro, cree el recurso de recepción como, por ejemplo, un flujo de Kinesis, donde se enviarán los eventos. Un filtro de suscripción define el patrón de filtros que utilizar para filtrar los eventos de registro que se envían alAWSUn recurso de, así como información sobre adónde se van a enviar los eventos de registro coincidentes.

Cada grupo de registros puede tener hasta dos filtros de suscripción asociados.

> Note
>
> Si el servicio de destino devuelve un error reintentable, como una excepción de limitación controlada o una excepción de servicio reintentable (HTTP 5xx, por ejemplo), CloudWatch Logs continúa reintentando la entrega durante un máximo de 24 horas. CloudWatch Logs no intenta volver a entregar si el error es un error no retryable, como AccessDeniedException o ResourceNotFoundException.

También produce métricas de CloudWatch Logs sobre el reenvío de eventos de registro a suscripciones. Para obtener más información, consulteDimensiones y métricas de Amazon CloudWatch Logs.

> Note
>
> Kinesis Data Firehose no está disponible en Asia Pacífico (Osaka).

Contenido



# Concepts

Cada filtro de suscripción se compone de los siguientes elementos principales:

nombre de grupo de registro

> El grupo de registros al que asociar el filtro de suscripción. Todos los eventos de registros cargados en este grupo de registros estarían sujetos al filtro de suscripción y los que coinciden con el filtro se entregarían al servicio de destino que recibe los eventos de registro coincidentes.

patrón de filtro

> Una descripción simbólica de cómo debe interpretar los registros de CloudWatch Logs los datos de cada evento de registro, junto con las expresiones de filtrado que restringen lo que se envía al destinoAWSRecurso. Para obtener más información acerca de la sintaxis del patrón de filtro, consulte Filtrar ypatternsyntax (p. 73).

arn de destino

El nombre de recurso de Amazon (ARN) del flujo de Kinesis, el flujo de Kinesis Data Firehose o la función Lambda que desee utilizar como destino de la fuente de suscripción.

arn de rol

Un rol de IAM que concede a CloudWatch Logs los permisos necesarios para incluir datos en el destino elegido. Este rol no es necesario para destinos de Lambda porque CloudWatch Logs puede obtener los permisos necesarios desde los ajustes de control de acceso en la propia función Lambda.

distribución

El método utilizado para distribuir los datos de registro al destino, cuando el destino es un flujo de Amazon Kinesis. De forma predeterminada, los datos de registro se agrupan por flujo de registro. Para obtener una distribución más uniforme, puede agrupar los datos de registro de forma aleatoria.

# Uso de CloudWatch Logssubscriptionfilters

Puede usar un filtro de suscripción con Kinesis, Lambda o Kinesis Data Firehose. Los registros que se envían a un servicio de recepción mediante un filtro de suscripción están codificados en Base64 y comprimidos con el formato gzip.

Ejemplos

- Ejemplo 1: Suscripciónfiltres con Kinesis (p. 93)
- Ejemplo 2: Suscripciónfilters conAWS Lambda (p. 97)
- Ejemplo 3: SuscripciónfLos productos de Amazon Kinesis Data Firehose (p. 99)

## Ejemplo 1: Suscripciónfiltres con Kinesis

En el siguiente ejemplo se asocia un filtro de suscripción a un grupo de registros que contieneAWS CloudTrailpara tener todas las actividades registradas realizadas por «Root»AWSentregadas a una secuencia de Kinesis llamada «RootAccess». Para obtener más información acerca de cómo enviarAWS CloudTrailPara CloudWatch Logs, consulteEnvío de eventos de CloudTrail a CloudWatch Logsen laAWS CloudTrailGuía del usuario.

Note

Antes de crear el flujo de Kinesis, calcule el volumen de los datos de log que se generarán. Asegúrese de crear un flujo de Kinesis con fragmentos suficientes para gestionar este volumen. Si el flujo no dispone de suficientes fragmentos, se limitará el flujo de registros. Para obtener más información acerca de los límites de volumen del flujo de Kinesis, consulteLímites de Amazon Kinesis Data Streams.

Para crear un filtro de suscripción para Kinesis

1. Para crear una secuencia de Kinesis de destino utilizando el siguiente comando:

```
$ C:\>  aws kinesis create-stream --stream-name "RootAccess" --shard-count 1
```

2. Espere hasta que el flujo de Kinesis esté Activo (esto podría tardar un minuto o dos). Puede utilizar las siguientes Kinesis KinesisDescripción de una secuenciapara comprobar el comandoStreamDescription.StreamStatusPropiedad. Además, anote el valor StreamDescription.StreamARN, ya que lo necesitará en un paso posterior:

```
aws kinesis describe-stream --stream-name "RootAccess"
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "StreamDescription": {
        "StreamStatus": "ACTIVE",
        "StreamName": "RootAccess",
        "StreamARN": "arn:aws:kinesis:us-east-1:123456789012:stream/RootAccess",
        "Shards": [
            {
                "ShardId": "shardId-000000000000",
                "HashKeyRange": {
                    "EndingHashKey": "340282366920938463463374607431768211455",
                    "StartingHashKey": "0"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
                    "49551135218688818456679503831981458784591352702181572610"
                }
            }
        ]
    }
}
```

3. Cree el rol de IAM que concederá permiso a CloudWatch Logs para incluir datos en su flujo de Kinesis. En primer lugar, tendrá que crear una política de confianza en un archivo (por ejemplo, `~/TrustPolicyForCWL.json`). Utilice un editor de texto para crear esta política. No utilice la consola de IAM para crearla.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.region.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

4. Usarcreate-rolePara crear el rol de IAM, especificando el archivo de política de confianza. Anote el valor de Role.Arn devuelto, ya que también lo necesitará más tarde:

```
aws iam create-role --role-name CWLtoKinesisRole --assume-role-policy-document file://
~/TrustPolicyForCWL.json
```

A continuación, se muestra un ejemplo de la salida.

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                    "Service": "logs.region.amazonaws.com"
                }
            }
        },
        "RoleId": "AAOIIAH450GAB4HC5F431",
        "CreateDate": "2015-05-29T13:46:29.431Z",
        "RoleName": "CWLtoKinesisRole",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/CWLtoKinesisRole"
    }
```

```
}
```

5. Cree una política de permisos para definir las acciones que CloudWatch Logs puede realizar en su cuenta. En primer lugar, creará una política de permisos en un archivo (por ejemplo, `~/PermissionsForCWL.json`). Utilice un editor de texto para crear esta política. No utilice la consola de IAM para crearla.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:region:123456789012:stream/RootAccess"
    }
  ]
}
```

6. Asocie la política de permisos con el rol utilizando el siguiente comando put-role-policy:

```
aws iam put-role-policy  --role-name CWLtoKinesisRole  --policy-name Permissions-
Policy-For-CWL  --policy-document file://~/PermissionsForCWL.json
```

7. Después de que Kinesis Stream esté enActivaEl estado de y haya creado el rol de IAM, puede crear el filtro de suscripción de CloudWatch Logs. El filtro de suscripción inicia de inmediato el flujo de datos de registro en tiempo real desde el grupo de registros elegido a su flujo de Kinesis:

```
aws logs put-subscription-filter \
    --log-group-name "CloudTrail" \
    --filter-name "RootAccess" \
    --filter-pattern "{$.userIdentity.type = Root}" \
    --destination-arn "arn:aws:kinesis:region:123456789012:stream/RootAccess" \
    --role-arn "arn:aws:iam::123456789012:role/CWLtoKinesisRole"
```

8. Después de configurar el filtro de suscripción, CloudWatch Logs reenvía todos los eventos de registro entrantes que coinciden con el patrón de filtro a su flujo de Kinesis. Puede verificar que esto está ocurriendo tomando un iterador de fragmentos de Kinesis y utilizando el comando get-records de Kinesis para obtener algunos registros de Kinesis:

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

```
{
    "ShardIterator":
    "AAAAAAAAAAFGU/
kLvNggvndHq2UIFOw5PZc6F01s3e3afsSscRM70JSbjIefg2ub07nk1y6CDxYR1UoGHJNP4m4NFUetzfL+wev
+e2P4djJg4L9wmXKvQYoE+rMUiFq+p4Cn3IgvqOb5dRA0yybNdRcdzvnC35KQANoHzzahKdRGb9v4scv+3vaq+f
+OIK8zM5My8ID+g6rMo7UKWeI4+IWiK2OSh0uP"
}
```

```
aws kinesis get-records --limit 10 --shard-iterator "AAAAAAAAAAFGU/
kLvNggvndHq2UIFOw5PZc6F01s3e3afsSscRM70JSbjIefg2ub07nk1y6CDxYR1UoGHJNP4m4NFUetzfL+wev
+e2P4djJg4L9wmXKvQYoE+rMUiFq+p4Cn3IgvqOb5dRA0yybNdRcdzvnC35KQANoHzzahKdRGb9v4scv+3vaq+f
+OIK8zM5My8ID+g6rMo7UKWeI4+IWiK2OSh0uP"
```

Tenga en cuenta que es posible que tenga que realizar esta llamada varias veces antes de que Kinesis comience a devolver los datos.

Cabe esperar ver una respuesta en una gama de registros. LaDatosEl atributo en un registro de Kinesis está cifrado en Base64 y comprimido con el formato gzip. Puede examinar los datos sin procesar desde la línea de comando utilizando los siguientes comandos de Unix:

```
echo -n "<Content of Data>" | base64 -d | zcat
```

Los datos descodificados y descomprimidos en Base64 se formatean como JSON con la siguiente estructura:

```
{
    "owner": "111111111111",
    "logGroup": "CloudTrail",
    "logStream": "111111111111_CloudTrail_us-east-1",
    "subscriptionFilters": [
        "Destination"
    ],
    "messageType": "DATA_MESSAGE",
    "logEvents": [
        {
            "id": "31953106606966983378809025079804211143289615424298221568",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424298221569",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424298221570",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
        }
    ]
}
```

Los elementos clave en la estructura de datos anterior son los siguientes:

owner

LaAWSEl ID de cuenta de los datos de registro de origen.

logGroup

El nombre del grupo de registros de los datos de registro de origen.

logStream

El nombre del flujo de registros de los datos de registro de origen.

subscriptionFilters

La lista de nombres de filtros de suscripción que coincide con los datos de registro de origen.

messageType

Los mensajes de datos utilizarán el tipo "DATA_MESSAGE". A veces CloudWatch Logs puede emitir registros de Kinesis con un tipo «CONTROL_MESSAGE», principalmente para comprobar si el destino es accesible.

logEvents

Los datos de registro reales, representados como un conjunto de registros de eventos de registro. La propiedad "id" es un identificador único de cada evento de registro.

# Ejemplo 2: Suscripciónfilters conAWS Lambda

En este ejemplo, creará un filtro de suscripción de CloudWatch Logs que envía datos de registro a suAWS Lambdafunción.

Note

Antes de crear la función Lambda, calcule el volumen de los datos de log que se generarán. Asegúrese de crear una función que pueda gestionar este volumen. Si la función no dispone de suficiente volumen, se limitará el flujo de registros. Para obtener más información acerca de los límites de Lambda, consulteAWS LambdaLímites.

Para crear un filtro de suscripción para Lambda

1. Cree la función AWS Lambda.

   Asegúrese de haber configurado el rol de ejecución de Lambda. Para obtener más información, consultePaso 2.2: Creación de un rol de IAM (rol de ejecución)en laAWS LambdaGuía para desarrolladores.
2. Abra un editor de texto y cree un archivo denominado `helloWorld.js` con el siguiente contenido:

```
var zlib = require('zlib');
exports.handler = function(input, context) {
    var payload = Buffer.from(input.awslogs.data, 'base64');
    zlib.gunzip(payload, function(e, result) {
        if (e) {
            context.fail(e);
        } else {
            result = JSON.parse(result.toString('ascii'));
            console.log("Event Data:", JSON.stringify(result, null, 2));
            context.succeed();
        }
    });
};
```

3. Comprima el archivo helloWorld.js y guárdelo con el nombre `helloWorld.zip`.
4. Utilice el siguiente comando, donde el rol es el rol de ejecución de Lambda que configuró en el primer paso:

```
aws lambda create-function \
    --function-name helloworld \
    --zip-file fileb://file-path/helloWorld.zip \
    --role lambda-execution-role-arn \
    --handler helloWorld.handler \
    --runtime nodejs12.x
```

5. Conceda a CloudWatch Logs el permiso para ejecutar su función. Utilice el siguiente comando, sustituyendo la cuenta del marcador por su propia cuenta y el grupo de registros del marcador por el grupo de registros que procesar:

```
aws lambda add-permission \
    --function-name "helloworld" \
    --statement-id "helloworld" \
    --principal "logs.region.amazonaws.com" \
```

```
    --action "lambda:InvokeFunction" \
    --source-arn "arn:aws:logs:region:123456789123:log-group:TestLambda:*" \
    --source-account "123456789012"
```

6. Cree un filtro de suscripción utilizando el siguiente comando, sustituyendo la cuenta del marcador por su propia cuenta y el grupo de registros del marcador por el grupo de registros que procesar:

```
aws logs put-subscription-filter \
    --log-group-name myLogGroup \
    --filter-name demo \
    --filter-pattern "" \
    --destination-arn arn:aws:lambda:region:123456789123:function:helloworld
```

7. (Opcional) Probar mediante un evento de registro de ejemplo. En el símbolo del sistema, ejecute el siguiente comando, que pone un mensaje de registro sencillo en el flujo suscrito.

   Para consultar la salida de su función de Lambda, diríjase a la función de Lambda donde verá la salida en /aws/lambda/helloworld:

```
aws logs put-log-events --log-group-name myLogGroup --log-stream-name stream1 --log-
events "[{\"timestamp\":<CURRENT TIMESTAMP MILLIS> , \"message\": \"Simple Lambda
 Test\"}]"
```

   Cabe esperar ver una respuesta en una gama de Lambda. LaDatosEl atributo en el registro de Lambda está cifrado en Base64 y comprimido con el formato gzip. La carga útil real que recibe Lambda está en el siguiente formato`{ "awslogs": {"data": "BASE64ENCODED_GZIP_COMPRESSED_DATA"} }`Puede examinar los datos sin procesar desde la línea de comando utilizando los siguientes comandos de Unix:

```
echo -n "<BASE64ENCODED_GZIP_COMPRESSED_DATA>" | base64 -d | zcat
```

   Los datos descodificados y descomprimidos en Base64 se formatean como JSON con la siguiente estructura:

```
{
    "owner": "123456789012",
    "logGroup": "CloudTrail",
    "logStream": "123456789012_CloudTrail_us-east-1",
    "subscriptionFilters": [
        "Destination"
    ],
    "messageType": "DATA_MESSAGE",
    "logEvents": [
        {
            "id": "31953106606966983378809025079804211143289615424298221568",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424298221569",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424298221570",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root
\"}"
```

```
        }
    ]
}
```

Los elementos clave en la estructura de datos anterior son los siguientes:

owner

LaAWSEl ID de cuenta de los datos de registro de origen.

logGroup

El nombre del grupo de registros de los datos de registro de origen.

logStream

El nombre del flujo de registros de los datos de registro de origen.

subscriptionFilters

La lista de nombres de filtros de suscripción que coincide con los datos de registro de origen.

messageType

Los mensajes de datos utilizarán el tipo "DATA_MESSAGE". A veces CloudWatch Logs puede emitir registros de Lambda con un tipo «CONTROL_MESSAGE», principalmente para comprobar si el destino es accesible.

logEvents

Los datos de registro reales, representados como un conjunto de registros de eventos de registro. La propiedad "id" es un identificador único de cada evento de registro.

# Ejemplo 3: SuscripciónfLos productos de Amazon Kinesis Data Firehose

En este ejemplo, creará una suscripción de CloudWatch Logs que envíe eventos de registro entrantes que coincidan con su filtros definidos a su flujo de entrega de Amazon Kinesis Data Firehose. Los datos enviados desde los registros de CloudWatch a Amazon Kinesis Data Firehose ya están comprimidos mediante la compresión de nivel 6 de gzip, por lo que no es necesario utilizar la compresión dentro de su flujo de entrega de Kinesis Data Firehose.

Note

Antes de crear el flujo de Kinesis Data Firehose, calcule el volumen de los datos de log que se generarán. Asegúrese de crear un flujo de Kinesis Data Firehose que pueda gestionar este volumen. Si el flujo no puede gestionar el volumen, se limitará el flujo de registros. Para obtener más información acerca de los límites de volumen de flujo de Kinesis Data Firehose, consulteLímites de datos de Amazon Kinesis Data Firehose.

Para crear un filtro de suscripción para Kinesis Data Firehose

1. Para crear un depósito de Amazon Simple Storage Service (Amazon S3). Le recomendamos que utilice un bucket creado específicamente para CloudWatch Logs. Sin embargo, si desea utilizar un bucket existente, vaya al paso 2.

   Ejecute el siguiente comando, sustituyendo el marcador de región por la región que desee utilizar:

```
aws s3api create-bucket --bucket my-bucket --create-bucket-configuration
 LocationConstraint=region
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "Location": "/my-bucket"
}
```

2. Cree el rol de IAM que concederá permiso a Amazon Kinesis Data Firehose para incluir datos en su bucket de Amazon S3.

   Para obtener más información, consulteControl del acceso con Amazon Kinesis Data Firehoseen laGuía del desarrollador de Amazon Kinesis Data Firehose.

   En primer lugar, utilice un editor de texto para crear una política de confianza en un archivo`~/TrustPolicyForFirehose.json`como sigue, sustituyendoaccount-idCon suAWSID de cuenta:

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "firehose.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": { "StringEquals": { "sts:ExternalId":"account-id" } }
  }
}
```

3. Usarcreate-rolePara crear el rol de IAM, especificando el archivo de política de confianza. Anote el valor de Role.Arn devuelto, ya que lo necesitará en un paso posterior:

```
aws iam create-role \
      --role-name FirehosetoS3Role \
      --assume-role-policy-document file://~/TrustPolicyForFirehose.json

{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                    "Service": "firehose.amazonaws.com"
                }
            }
        },
        "RoleId": "AAOIIAH450GAB4HC5F431",
        "CreateDate": "2015-05-29T13:46:29.431Z",
        "RoleName": "FirehosetoS3Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/FirehosetoS3Role"
    }
}
```

4. Cree una política de permisos para definir las acciones que Kinesis Data Firehose puede realizar en su cuenta. En primer lugar, utilice un editor de texto para crear una política de permisos en un archivo `~/PermissionsForFirehose.json`:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "s3:AbortMultipartUpload",
          "s3:GetBucketLocation",
```

```
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListBucketMultipartUploads",
            "s3:PutObject" ],
        "Resource": [
            "arn:aws:s3:::my-bucket",
            "arn:aws:s3:::my-bucket/*" ]
    }
  ]
}
```

5. Asocie la política de permisos con el rol utilizando el siguiente comando put-role-policy:

```
aws iam put-role-policy --role-name FirehosetoS3Role --policy-name Permissions-Policy-
For-Firehose --policy-document file://~/PermissionsForFirehose.json
```

6. Cree un flujo de entrega de Kinesis Data Firehose como se indica a continuación, sustituyendo los valores de marcador deRoleARNyBucketARNcon el rol y los ARN de bucket que ha creado:

```
aws firehose create-delivery-stream \
   --delivery-stream-name 'my-delivery-stream' \
   --s3-destination-configuration \
  '{"RoleARN": "arn:aws:iam::123456789012:role/FirehosetoS3Role", "BucketARN":
 "arn:aws:s3:::my-bucket"}'
```

Tenga en cuenta que Kinesis Data Firehose utiliza automáticamente un prefijo en formato AAAA/MM/DD/HH UTC para objetos de Amazon S3 entregados. Puede especificar un prefijo adicional que añadir delante del prefijo de formato de hora. Si el prefijo termina con una barra inclinada (/), aparece como una carpeta en el bucket de Amazon S3.

7. Espere hasta que el flujo se active (esto podría tardar unos minutos). Puede usar Kinesis Data Firehosedescribe-delivery-streampara comprobar el comandoDeliveryStreamDescription.DeliveryStreamStatusPropiedad. Además, anote el valor DeliveryStreamDescription.DeliveryStreamARN, ya que lo necesitará en un paso posterior:

```
aws firehose describe-delivery-stream --delivery-stream-name "my-delivery-stream"
{
    "DeliveryStreamDescription": {
        "HasMoreDestinations": false,
        "VersionId": "1",
        "CreateTimestamp": 1446075815.822,
        "DeliveryStreamARN": "arn:aws:firehose:us-east-1:123456789012:deliverystream/
my-delivery-stream",
        "DeliveryStreamStatus": "ACTIVE",
        "DeliveryStreamName": "my-delivery-stream",
        "Destinations": [
            {
                "DestinationId": "destinationId-000000000001",
                "S3DestinationDescription": {
                    "CompressionFormat": "UNCOMPRESSED",
                    "EncryptionConfiguration": {
                        "NoEncryptionConfig": "NoEncryption"
                    },
                    "RoleARN": "delivery-stream-role",
                    "BucketARN": "arn:aws:s3:::my-bucket",
                    "BufferingHints": {
                        "IntervalInSeconds": 300,
                        "SizeInMBs": 5
                    }
                }
            }
```

```
        ]
    }
}
```

8. Cree el rol de IAM que concederá permiso a CloudWatch Logs para incluir datos en su flujo de entrega de Kinesis Data Firehose. En primer lugar, utilice un editor de texto para crear una política de confianza en un archivo `~/TrustPolicyForCWL.json`:

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.region.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

9. Usarcreate-rolePara crear el rol de IAM, especificando el archivo de política de confianza. Anote el valor de Role.Arn devuelto, ya que lo necesitará en un paso posterior:

```
aws iam create-role \
      --role-name CWLtoKinesisFirehoseRole \
      --assume-role-policy-document file://~/TrustPolicyForCWL.json

{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                    "Service": "logs.region.amazonaws.com"
                }
            }
        },
        "RoleId": "AAOIIAH450GAB4HC5F431",
        "CreateDate": "2015-05-29T13:46:29.431Z",
        "RoleName": "CWLtoKinesisFirehoseRole",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/CWLtoKinesisFirehoseRole"
    }
}
```

10. Cree una política de permisos para definir las acciones que CloudWatch Logs puede realizar en su cuenta. En primer lugar, utilice un editor de texto para crear un archivo de política de permisos (por ejemplo, `~/PermissionsForCWL.json`):

```
{
    "Statement":[
      {
        "Effect":"Allow",
        "Action":["firehose:*"],
        "Resource":["arn:aws:firehose:region:123456789012:*"]
      }
    ]
}
```

11. Asocie la política de permisos con el rol utilizando el comando put-role-policy:

```
aws iam put-role-policy --role-name CWLtoKinesisFirehoseRole --policy-name Permissions-Policy-For-CWL --policy-document file://~/PermissionsForCWL.json
```

12. Después de que el flujo de entrega de Amazon Kinesis Data Firehose esté en estado activo y haya creado el rol de IAM, puede crear el filtro de suscripción de CloudWatch Logs. El filtro de suscripción inicia de inmediato el flujo de datos de registro en tiempo real desde el grupo de registros elegido a su flujo de entrega de Amazon Kinesis Data Firehose:

```
aws logs put-subscription-filter \
    --log-group-name "CloudTrail" \
    --filter-name "Destination" \
    --filter-pattern "{$.userIdentity.type = Root}" \
    --destination-arn "arn:aws:firehose:region:123456789012:deliverystream/my-delivery-
stream" \
    --role-arn "arn:aws:iam::123456789012:role/CWLtoKinesisFirehoseRole"
```

13. Después de configurar el filtro de suscripción, CloudWatch Logs reenviará todos los eventos de registro entrantes que coinciden con el patrón de filtro a su flujo de entrega de Amazon Kinesis Data Firehose. Los datos comenzarán a aparecer en su Amazon S3 en función del intervalo de búfer de tiempo definido en el flujo de entrega de Amazon Kinesis Data Firehose. Una vez que haya transcurrido el tiempo suficiente, puede verificar los datos comprobando su bucket de Amazon S3.

```
aws s3api list-objects --bucket 'my-bucket' --prefix 'firehose/'
{
    "Contents": [
        {
            "LastModified": "2015-10-29T00:01:25.000Z",
            "ETag": "\"a14589f8897f4089d3264d9e2d1f1610\"",
            "StorageClass": "STANDARD",
            "Key": "firehose/2015/10/29/00/my-delivery-stream-2015-10-29-00-01-21-
a188030a-62d2-49e6-b7c2-b11f1a7ba250",
            "Owner": {
                "DisplayName": "cloudwatch-logs",
                "ID": "1ec9cf700ef6be062b19584e0b7d84ecc19237f87b5"
            },
            "Size": 593
        },
        {
            "LastModified": "2015-10-29T00:35:41.000Z",
            "ETag": "\"a7035b65872bb2161388ffb63dd1aec5\"",
            "StorageClass": "STANDARD",
            "Key": "firehose/2015/10/29/00/my-delivery-
stream-2015-10-29-00-35-40-7cc92023-7e66-49bc-9fd4-fc9819cc8ed3",
            "Owner": {
                "DisplayName": "cloudwatch-logs",
                "ID": "1ec9cf700ef6be062b19584e0b7d84ecc19237f87b6"
            },
            "Size": 5752
        }
    ]
}
```

```
aws s3api get-object --bucket 'my-bucket' --key 'firehose/2015/10/29/00/my-delivery-
stream-2015-10-29-00-01-21-a188030a-62d2-49e6-b7c2-b11f1a7ba250' testfile.gz

{
    "AcceptRanges": "bytes",
    "ContentType": "application/octet-stream",
    "LastModified": "Thu, 29 Oct 2015 00:07:06 GMT",
    "ContentLength": 593,
    "Metadata": {}
}
```

Los datos en el objeto de Amazon S3 se comprimen con el formato gzip. Puede examinar los datos sin procesar desde la línea de comando utilizando el siguiente comando de Unix:

```
zcat testfile.gz
```

# Entre países accountlOGdatasharing consubscriptions

Puedes colaborar con un propietario de unAWSy recibir sus eventos de registro en suAWS, como una transmisión de Amazon Kinesis o Amazon Kinesis Data Firehose (esto se conoce como intercambio de datos entre cuentas). Por ejemplo, estos datos de eventos de registro se pueden leer desde un flujo de Kinesis o Kinesis Data Firehose centralizado para realizar el procesamiento y análisis personalizados. El procesamiento personalizado resulta especialmente útil al colaborar y analizar datos en muchas cuentas.

Por ejemplo, el grupo de seguridad de información de una empresa podría desear analizar datos de detección de intrusiones en tiempo real o de comportamientos anómala para poder realizar una auditoría de cuentas en todas las divisiones de la empresa recopilando sus registros de producción federada para procesamiento central. Un flujo en tiempo real de datos de eventos en dichas cuentas se puede montar y enviar a los grupos de seguridad de información que pueden utilizar Kinesis para adjuntar los datos a sus sistemas de análisis de seguridad existentes.

Note

Kinesis Data Firehose no está disponible en Asia Pacífico (Osaka).

Temas



## Entre países accountlOGdatasharing usando Kinesis Kinesis

Para compartir los datos de registro entre cuentas, es necesario establecer un emisor y receptor de datos de registro:

- remitente de datos de registro: obtiene la información de destino del destinatario y permite a CloudWatch Logs saber que está listo para enviar sus eventos de registros al destino especificado. En los procedimientos del resto de esta sección, el remitente de los datos de registro se muestra con un número de cuenta de AWS ficticio de 111111111111.
- Receptor de datos de registro: configura un destino que encapsula un flujo de Kinesis y permite a CloudWatch Logs saber que el destinatario desea recibir datos de registro. El destinatario a continuación, comparte la información sobre su destino con el remitente. En los procedimientos del resto de esta sección, el destinatario de los datos de registro se muestra con un número de cuenta de AWS ficticio de 999999999999.

Para empezar a recibir eventos de registro de usuarios de cuenta cruzada, el destinatario de los datos de registro crea primero un destino de CloudWatch Logs. Cada destino consta de los siguientes elementos fundamentales:

Nombre de destino

El nombre del destino que desea crear.

ARN de destino

El nombre de recurso de Amazon (ARN) delAWSUn recurso de que desea utilizar como destino de la fuente de suscripción.

ARN de rol

UnaAWS Identity and Access ManagementUn rol de (IAM) que concede a CloudWatch Logs los permisos necesarios para incluir datos en el flujo de Kinesis elegido.

Política de acceso

Un documento de política de IAM (en formato JSON, escrito con la gramática de política de IAM) que rige el conjunto de los usuarios a los que se les permite escribir en su destino.

El grupo de registro y el destino deben estar en el mismoAWSRegión . Sin embargo, elAWSUn recurso de al que apunta el destino puede estar ubicado en una región diferente. En los ejemplos de las secciones siguientes, todos los recursos específicos de la región se crean en EE.UU. Este (Norte de Virginia).

Temas



# Creación de undestination

Important

Todos los pasos de este procedimiento deben realizarse en la cuenta del destinatario de los datos de registro.

Para este ejemplo, la cuenta de destinatario de datos de registro tiene unAWSID de cuenta 999999999999, mientras que el remitente de datos de registroAWSEl ID de la cuenta es 1111111111.

En este ejemplo se crea un destino mediante un flujo de Kinesis denominado RecipientStream y un rol que permite a CloudWatch Logs escribir datos en el mismo.

## Para crear un destino

1. Cree un flujo de destino en Kinesis. En el símbolo del sistema, escriba:

```
aws kinesis create-stream --stream-name "RecipientStream" --shard-count 1
```

2. Espere hasta que el flujo de Kinesis se active. Puede utilizar el comando aws kinesis describe-stream para comprobar la propiedad StreamDescription.StreamStatus. Además, tenga en cuenta laStreamDescription.StreamARNValor CloudWatch Logs

```
aws kinesis describe-stream --stream-name "RecipientStream"
{
  "StreamDescription": {
    "StreamStatus": "ACTIVE",
```

```
    "StreamName": "RecipientStream",
    "StreamARN": "arn:aws:kinesis:us-east-1:999999999999:stream/RecipientStream",
    "Shards": [
      {
        "ShardId": "shardId-000000000000",
        "HashKeyRange": {
          "EndingHashKey": "340282366920938463463374607431768EXAMPLE",
          "StartingHashKey": "0"
        },
        "SequenceNumberRange": {
          "StartingSequenceNumber":
 "49551135218688818456679503831981458784591352702 18EXAMPLE"
        }
      }
    ]
  }
}
```

El flujo puede tardar un minuto o dos en mostrarse en el estado activo.

3. Cree el rol de IAM que concederá permiso a CloudWatch Logs para incluir datos en su flujo de Kinesis. En primer lugar, deberá crear una política de confianza en un archivo ~/TrustPolicyForCWL.json. Utilice un editor de texto para crear este archivo de política; no utilice la consola de IAM.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.region.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

4. Usaraws iam create-rolePara crear el rol de IAM, especificando el archivo de política de confianza. Anote el valor Role.Arn devuelto porque que también se transferirá a CloudWatch Logs posteriormente:

```
aws iam create-role \
    --role-name CWLtoKinesisRole \
    --assume-role-policy-document file://~/TrustPolicyForCWL.json

{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Action": "sts:AssumeRole",
                "Effect": "Allow",
                "Principal": {
                    "Service": "logs.region.amazonaws.com"
                }
            }
        },
        "RoleId": "AAOIIAH450GAB4HC5F431",
        "CreateDate": "2015-05-29T13:46:29.431Z",
        "RoleName": "CWLtoKinesisRole",
        "Path": "/",
        "Arn": "arn:aws:iam::999999999999:role/CWLtoKinesisRole"
    }
}
```

5. Cree una política de permisos para definir qué acciones puede llevar a cabo CloudWatch Logs en su cuenta. En primer lugar, utilice un editor de texto para crear una política de permisos en un archivo ~/PermissionsForCWL.json:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:region:999999999999:stream/RecipientStream"
    }
  ]
}
```

6. Asocie la política de permisos con el rol utilizando el comando aws iam put-role-policy:

```
aws iam put-role-policy \
    --role-name CWLtoKinesisRole \
    --policy-name Permissions-Policy-For-CWL \
    --policy-document file://~/PermissionsForCWL.json
```

7. Después de que el flujo de Kinesis esté en estado activo y haya creado el rol de IAM, puede crear el destino de CloudWatch Logs.

   a. Este paso no asociará una política de acceso a su destino y solo es el primer paso de los dos que completan la creación de un destino. Anote el valor de DestinationArn que se devuelve en la carga:

```
aws logs put-destination \
    --destination-name "testDestination" \
    --target-arn "arn:aws:kinesis:region:999999999999:stream/RecipientStream" \
    --role-arn "arn:aws:iam::999999999999:role/CWLtoKinesisRole"

{
  "DestinationName" : "testDestination",
  "RoleArn" : "arn:aws:iam::999999999999:role/CWLtoKinesisRole",
  "DestinationArn" : "arn:aws:logs:us-
east-1:999999999999:destination:testDestination",
  "TargetArn" : "arn:aws:kinesis:us-east-1:999999999999:stream/RecipientStream"
}
```

   b. Una vez que se haya completado el paso 7a, en la cuenta del destinatario de los datos de registro, asocie una política de acceso con el destino. Esta política permite que la cuenta del remitente de los datos de registro (111111111111) tenga acceso al destino en la cuenta del destinatario de los datos de registro (999999999999). Puede utilizar un editor de texto para incluir esta política en el archivo ~/AccessPolicy.json:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "111111111111"
      },
      "Action" : "logs:PutSubscriptionFilter",
      "Resource" : "arn:aws:logs:region:999999999999:destination:testDestination"
    }
  ]
}
```

Note

Si varias cuentas están enviando registros a este destino, cada cuenta de remitente debe aparecer por separado en la política. Esta política no admite la especificación `*` como `Principal` o el uso de la clave global `aws:PrincipalOrgId`.

c. Esto crea una política que define quién tiene acceso de escritura al destino. Esta política debe especificar la acción logs:PutSubscriptionFilter para obtener acceso al destino. Los usuarios entre varias cuentas utilizarán la acción PutSubscriptionFilter para enviar eventos de registro al destino:

```
aws logs put-destination-policy \
    --destination-name "testDestination" \
    --access-policy file://~/AccessPolicy.json
```

Esta directiva de acceso permite a los usuarios en elAWSCuenta con ID 111111111111 para llamarPutSubscriptionFiltercontra el destino con ARN arn:aws:logs:*región*:999999999999:Destination:TestDestination. Cualquier otro intento de usuario de llamar a PutSubscriptionFilter en este destino se rechazará.

Para validar los privilegios de un usuario frente a una política de acceso, consulteUso del validador de políticasen laGuía del usuario de IAM.

## Creación de unsubscriptionfilter

Después de crear un destino, la cuenta del destinatario de los datos de registro puede compartir el ARN de destino (arn:aws:logs:us-east-1:999999999999:destination:testDestination) con otras cuentas de AWS para que puedan enviar eventos de registro al mismo destino. A continuación, los usuarios de estas otras cuentas remitentes crean un filtro de suscripción en sus grupos de registros respectivos frente a este destino. El filtro de suscripción inicia de inmediato el flujo de datos de registro en tiempo real desde el grupo de registros elegido al destino especificado.

En el siguiente ejemplo, se crea un filtro de suscripción en una cuenta de envío. El filtro está asociado a un grupo de registros que contieneAWS CloudTraileventos para que cada actividad registrada realizada por «Root»AWSLas credenciales se entregan en el destino creado anteriormente. Ese destino encapsula una secuencia de Kinesis llamada «RecipientStream». Para obtener más información acerca de cómo enviarAWS CloudTrailPara CloudWatch Logs, consulteEnvío de eventos de CloudTrail a CloudWatch Logsen laAWS CloudTrailGuía del usuario.

```
aws logs put-subscription-filter \
    --log-group-name "CloudTrail" \
    --filter-name "RecipientStream" \
    --filter-pattern "{$.userIdentity.type = Root}" \
    --destination-arn "arn:aws:logs:region:999999999999:destination:testDestination"
```

El grupo de registro y el destino deben estar en el mismoAWSRegión . Sin embargo, el destino puede apuntar a unAWSUn recurso de Kinesis que está ubicado en una región diferente.

## Validación del valor defBaja delOGevents

Después de crear el filtro de suscripción, CloudWatch Logs reenvía todos los eventos de registro entrantes que coinciden con el patrón de filtro al flujo de Kinesis que se encapsula en el flujo de destino denominado»RecipientStream«. El propietario del destino puede verificar que esto sucede utilizando elaws kinesis get-shard-iteratorpara tomar un fragmento de Kinesis y usar el comandoaws kinesis get-recordspara obtener algunos registros de Kinesis:

```
aws kinesis get-shard-iterator \
```

```
      --stream-name RecipientStream \
      --shard-id shardId-000000000000 \
      --shard-iterator-type TRIM_HORIZON

{
    "ShardIterator":
    "AAAAAAAAAAFGU/
kLvNggvndHq2UIFOw5PZc6F01s3e3afsSscRM70JSbjIefg2ub07nk1y6CDxYR1UoGHJNP4m4NFUetzfL+wev
+e2P4djJg4L9wmXKvQYoE+rMUiFq+p4Cn3IgvqOb5dRA0yybNdRcdzvnC35KQANoHzzahKdRGb9v4scv+3vaq+f
+OIK8zM5My8ID+g6rMo7UKWeI4+IWiKEXAMPLE"
}

aws kinesis get-records \
      --limit 10 \
      --shard-iterator
      "AAAAAAAAAAFGU/
kLvNggvndHq2UIFOw5PZc6F01s3e3afsSscRM70JSbjIefg2ub07nk1y6CDxYR1UoGHJNP4m4NFUetzfL+wev
+e2P4djJg4L9wmXKvQYoE+rMUiFq+p4Cn3IgvqOb5dRA0yybNdRcdzvnC35KQANoHzzahKdRGb9v4scv+3vaq+f
+OIK8zM5My8ID+g6rMo7UKWeI4+IWiKEXAMPLE"
```

Note

Es posible que tenga que volver a ejecutar el comando get-records varias veces antes de que Kinesis comience a devolver los datos.

Debería ver una respuesta con una gama de registros de Kinesis. El atributo de datos en el registro de Kinesis está comprimido en formato gzip y cifrado en Base64. Puede examinar los datos sin procesar desde la línea de comando utilizando el siguiente comando de Unix:

```
echo -n "<Content of Data>" | base64 -d | zcat
```

Los datos descodificados y descomprimidos en Base64 se formatean como JSON con la siguiente estructura:

```
{
    "owner": "111111111111",
    "logGroup": "CloudTrail",
    "logStream": "111111111111_CloudTrail_us-east-1",
    "subscriptionFilters": [
        "RecipientStream"
    ],
    "messageType": "DATA_MESSAGE",
    "logEvents": [
        {
            "id": "31953106606966983378809025079804211143289615424 29EXAMPLE",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424 29EXAMPLE",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root\"}"
        },
        {
            "id": "31953106606966983378809025079804211143289615424 29EXAMPLE",
            "timestamp": 1432826855000,
            "message": "{\"eventVersion\":\"1.03\",\"userIdentity\":{\"type\":\"Root\"}"
        }
    ]
}
```

Los elementos fundamentales de esta estructura de datos son los siguientes:

owner

LaAWSEl ID de cuenta de los datos de registro de origen.

logGroup

El nombre del grupo de registros de los datos de registro de origen.

logStream

El nombre del flujo de registros de los datos de registro de origen.

subscriptionFilters

La lista de nombres de filtros de suscripción que coincide con los datos de registro de origen.

messageType

Los mensajes de datos utilizarán el tipo "DATA_MESSAGE". A veces CloudWatch Logs puede emitir registros de Kinesis con un tipo «CONTROL_MESSAGE», principalmente para comprobar si el destino es accesible.

logEvents

Los datos de registro reales, representados como un conjunto de registros de eventos de registro. La propiedad ID es un identificador único de cada evento de registro.

## Modificación dedestinaciónmembership enruntime

Puede encontrar situaciones en las que tenga que añadir o eliminar la pertenencia de algunos usuarios de un destino de su propiedad. Puede utilizar la función de`put-destination-policy`En su destino con una nueva política de acceso. En el siguiente ejemplo, una cuenta 111111111111 añadida anteriormente deja de enviar más datos de registro y se habilita la cuenta 222222222222.

1. Obtenga la política que está asociada actualmente al destino testDestination y anote la AccessPolicy:

```
aws logs describe-destinations \
    --destination-name-prefix "testDestination"

{
 "Destinations": [
   {
     "DestinationName": "testDestination",
     "RoleArn": "arn:aws:iam::999999999999:role/CWLtoKinesisRole",
     "DestinationArn": "arn:aws:logs:region:999999999999:destination:testDestination",
     "TargetArn": "arn:aws:kinesis:region:999999999999:stream/RecipientStream",
     "AccessPolicy": "{\"Version\": \"2012-10-17\", \"Statement\":
 [{\"Sid\": \"\", \"Effect\": \"Allow\", \"Principal\": {\"AWS\":
 \"111111111111\"}, \"Action\": \"logs:PutSubscriptionFilter\", \"Resource\":
 \"arn:aws:logs:region:123456789012:destination:testDestination\"}] }"
   }
 ]
}
```

2. Actualice la política para reflejar que la cuenta 111111111111 está detenida y que la cuenta 222222222222 está habilitada. Incluya esta política en el archivo ~/NewAccessPolicy.json:

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

```
      "Principal" : {
        "AWS" : "222222222222"
      },
      "Action" : "logs:PutSubscriptionFilter",
      "Resource" : "arn:aws:logs:region:999999999999:destination:testDestination"
    }
  ]
}
```

3. Llame a PutDestinationPolicy para asociar la política definida en el archivo NewAccessPolicy.json con el destino:

```
aws logs put-destination-policy \
--destination-name "testDestination" \
--access-policy file://~/NewAccessPolicy.json
```

   Esto finalmente deshabilitará los eventos de registro del ID de cuenta 111111111111. Registrar eventos desde el ID de cuenta222222222222Comience a fluir al destino en cuanto el propietario de la cuenta222222222222Crea un filtro de suscripción.

# Entre países accountlOGdatasCómo utilizar Kinesis Data Firehose

Para compartir los datos de registro entre cuentas, es necesario establecer un emisor y receptor de datos de registro:

- remitente de datos de registro: obtiene la información de destino del destinatario y permite a CloudWatch Logs saber que está listo para enviar sus eventos de registros al destino especificado. En los procedimientos del resto de esta sección, el remitente de los datos de registro se muestra con un número de cuenta de AWS ficticio de 111111111111.
- Receptor de datos de registro: configura un destino que encapsula un flujo de Kinesis y permite a CloudWatch Logs saber que el destinatario desea recibir datos de registro. El destinatario a continuación, comparte la información sobre su destino con el remitente. En los procedimientos del resto de esta sección, el destinatario de los datos de registro se muestra con unAWSnúmero de cuenta 222222222222.

El ejemplo de esta sección utiliza una secuencia de entrega de Kinesis Data Firehose con almacenamiento de Amazon S3. También puede configurar flujos de entrega de Kinesis Data Firehose con diferentes configuraciones. Para obtener más información, consulteCreación de una secuencia de entrega de Kinesis Data Firehose.

El grupo de registro y el destino deben estar en el mismoAWSRegión . Sin embargo, elAWSUn recurso de al que apunta el destino puede estar ubicado en una región diferente.

> Note
>
> Esta función no está disponible en Asia Pacífico (Osaka) porque Kinesis Data Firehose no está disponible en esa región.

Temas

- Modificación dedestinaciónmembership enruntime (p. 117)

# Paso 1: Creación de un Firehose de datos Kinesis Data Firehosedeliverystream

Important

Todos los pasos en el paso 1 deben realizarse en la cuenta del destinatario de los datos de registro.
En los siguientes ejemplos, EE.UU. Este (Norte de Virginia) se utiliza en los comandos de ejemplo. Reemplace esto por la región correcta para su implementación de.

Para crear un flujo de entrega de Kinesis Data Firehose que utilizar como destino

1. Cree un bucket de Amazon S3:

```
aws s3api create-bucket --bucket firehose-test-bucket1 --create-bucket-configuration
 LocationConstraint=us-east-1
```

2. Cree el rol de IAM que concede a Kinesis Data Firehose para incluir datos en el bucket de.

   a. En primer lugar, utilice un editor de texto para crear una política de confianza en un archivo~/`TrustPolicyForFirehose.json`.

```
{ "Statement": { "Effect": "Allow", "Principal": { "Service":
 "firehose.amazonaws.com" }, "Action": "sts:AssumeRole", "Condition":
 { "StringEquals": { "sts:ExternalId":"222222222222" } } } }
```

   b. Cree el rol de IAM, especificando el archivo de política de confianza que acaba de crear.

```
aws iam create-role \
    --role-name FirehosetoS3Role \
    --assume-role-policy-document file://~/TrustPolicyForFirehose.json
```

   c. El resultado de este comando tendrá un aspecto similar al siguiente: Anote el nombre del rol y el ARN del rol.

```
{
    "Role": {
        "Path": "/",
        "RoleName": "FirehosetoS3Role",
        "RoleId": "AROAR3BXASEKW7K635M53",
        "Arn": "arn:aws:iam::222222222222:role/FirehosetoS3Role",
        "CreateDate": "2021-02-02T07:53:10+00:00",
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Effect": "Allow",
                "Principal": {
                    "Service": "firehose.amazonaws.com"
                },
                "Action": "sts:AssumeRole",
                "Condition": {
                    "StringEquals": {
                        "sts:ExternalId": "222222222222"
                    }
                }
            }
        }
    }
```

```
}
```

3. Introduzca el siguiente comando para crear el flujo de entrega de Kinesis Data Firehose. Reemplazar*mi-role-arn*y*mi-cubo-arn*Con los valores correctos para su implementación de.

```
aws firehose create-delivery-stream \
   --delivery-stream-name 'my-delivery-stream' \
   --s3-destination-configuration \
  '{"RoleARN": "arn:aws:iam::222222222222:role/FirehosetoS3Role", "BucketARN":
 "arn:aws:s3:::firehose-test-bucket1"}'
```

El resultado debería tener un aspecto similar al siguiente:

```
{
    "DeliveryStreamARN": "arn:aws:firehose:us-east-1:222222222222:deliverystream/my-
delivery-stream"
}
```

## Paso 2: Creación de undestination

Important

Todos los pasos de este procedimiento deben realizarse en la cuenta del destinatario de los datos de registro.

Para crear un destino

1. Espere hasta que el flujo de Kinesis Data Firehose creado enPaso 1: Creación de un Firehose de datos Kinesis Data Firehosedeliverystream (p. 112)se activa. Puede utilizar el siguiente comando para comprobar laStreamDescription.StreamStatusPropiedad.

```
aws firehose describe-delivery-stream --delivery-stream-name "my-delivery-stream"
```

Además, tenga en cuenta laDeliveryStreamDescription.DeliveryStreamarn, ya que tendrá que utilizarlo en un paso posterior. Resultado de ejemplo de este comando:

```
{
    "DeliveryStreamDescription": {
        "DeliveryStreamName": "my-delivery-stream",
        "DeliveryStreamARN": "arn:aws:firehose:us-east-1:222222222222:deliverystream/
my-delivery-stream",
        "DeliveryStreamStatus": "ACTIVE",
        "DeliveryStreamEncryptionConfiguration": {
            "Status": "DISABLED"
        },
        "DeliveryStreamType": "DirectPut",
        "VersionId": "1",
        "CreateTimestamp": "2021-02-01T23:59:15.567000-08:00",
        "Destinations": [
            {
                "DestinationId": "destinationId-000000000001",
                "S3DestinationDescription": {
                    "RoleARN": "arn:aws:iam::222222222222:role/FirehosetoS3Role",
                    "BucketARN": "arn:aws:s3:::firehose-test-bucket1",
                    "BufferingHints": {
                        "SizeInMBs": 5,
                        "IntervalInSeconds": 300
                    },
                    "CompressionFormat": "UNCOMPRESSED",
```

```
                    "EncryptionConfiguration": {
                        "NoEncryptionConfig": "NoEncryption"
                    },
                    "CloudWatchLoggingOptions": {
                        "Enabled": false
                    }
                },
                "ExtendedS3DestinationDescription": {
                    "RoleARN": "arn:aws:iam::222222222222:role/FirehosetoS3Role",
                    "BucketARN": "arn:aws:s3:::firehose-test-bucket1",
                    "BufferingHints": {
                        "SizeInMBs": 5,
                        "IntervalInSeconds": 300
                    },
                    "CompressionFormat": "UNCOMPRESSED",
                    "EncryptionConfiguration": {
                        "NoEncryptionConfig": "NoEncryption"
                    },
                    "CloudWatchLoggingOptions": {
                        "Enabled": false
                    },
                    "S3BackupMode": "Disabled"
                }
            }
        ],
        "HasMoreDestinations": false
    }
}
```

El flujo de entrega puede tardar un minuto o dos en mostrarse en el estado activo.

2. Cuando el flujo de entrega de esté activo, cree el rol de IAM que concederá el permiso a CloudWatch Logs para incluir datos en su flujo de Kinesis Data Firehose. En primer lugar, deberá crear una política de confianza en un archivo ~/TrustPolicyForCWL.json. Utilice un editor de texto para crear esta política. Para obtener más información acerca de los puntos de enlace de CloudWatch Logs, consulteCuotas y puntos de enlace de Amazon CloudWatch Logs.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.us-east-1.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

3. Usaraws iam create-rolePara crear el rol de IAM, especificando el archivo de política de confianza que acaba de crear.

```
aws iam create-role \
                        --role-name CWLtoKinesisFirehoseRole \
      --assume-role-policy-document file://~/TrustPolicyForCWL.json
```

A continuación, se muestra un ejemplo de salida. Tome nota del valor de`Role.Arn`, ya que tendrá que utilizarlo en un paso posterior.

```
{
    "Role": {
        "Path": "/",
        "RoleName": "CWLtoKinesisFirehoseRole",
        "RoleId": "AROAR3BXASEKYJYWF243H",
        "Arn": "arn:aws:iam::222222222222:role/CWLtoKinesisFirehoseRole",
        "CreateDate": "2021-02-02T08:10:43+00:00",
```

```
        "AssumeRolePolicyDocument": {
            "Statement": {
                "Effect": "Allow",
                "Principal": {
                    "Service": "logs.us-east-1.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }
        }
    }
}
```

4. Cree una política de permisos para definir qué acciones puede llevar a cabo CloudWatch Logs en su cuenta. En primer lugar, utilice un editor de texto para crear una política de permisos en un archivo~/PermisionesForcWL.json:

```
{
    "Statement":[
      {
        "Effect":"Allow",
        "Action":["firehose:*"],
        "Resource":["arn:aws:firehose:region:222222222222:*"]
      }
    ]
}
```

5. Asocie la política de permisos con el rol escribiendo el siguiente comando:

```
aws iam put-role-policy --role-name CWLtoKinesisFirehoseRole --policy-name Permissions-
Policy-For-CWL --policy-document file://~/PermissionsForCWL.json
```

6. Después de que el flujo de entrega de Kinesis Data Firehose esté en estado activo y haya creado el rol de IAM, puede crear el destino de CloudWatch Logs.

   a. Este paso no asociará una política de acceso a su destino y solo es el primer paso de los dos que completan la creación de un destino. Anote la función de lasdestination.arnque se devuelve en la carga:

```
aws logs put-destination \
    --destination-name "testFirehoseDestination" \
    --target-arn "arn:aws:firehose:us-east-1:222222222222:deliverystream/my-
delivery-stream" \
    --role-arn "arn:aws:iam::222222222222:role/CWLtoKinesisFirehoseRole"

{
    "destination": {
        "destinationName": "testFirehoseDestination",
        "targetArn": "arn:aws:firehose:us-east-1:222222222222:deliverystream/my-
delivery-stream",
        "roleArn": "arn:aws:iam::222222222222:role/CWLtoKinesisFirehoseRole",
        "arn": "arn:aws:logs:us-
east-1:222222222222:destination:testFirehoseDestination"}
}
```

   b. Después de completar el paso anterior, en la cuenta del destinatario de los datos de registro (22222222222222), asocie una política de acceso al destino. Esta política permite que la cuenta del remitente de los datos de registro (111111111111111111111111) tenga acceso al destino en la cuenta del destinatario de los datos de registro (222222222222). Puede utilizar un editor de texto para incluir esta política en el archivo ~/AccessPolicy.json:

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

```
  "Statement" : [
    {
      "Sid" : "",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "111111111111"
      },
      "Action" : "logs:PutSubscriptionFilter",
      "Resource" : "arn:aws:logs:us-
east-1:222222222222:destination:testFirehoseDestination"
    }
  ]
}
```

c. Esto crea una política que define quién tiene acceso de escritura al destino. Esta política debe especificar la acción logs:PutSubscriptionFilter para obtener acceso al destino. Los usuarios entre varias cuentas utilizarán la acción PutSubscriptionFilter para enviar eventos de registro al destino:

```
aws logs put-destination-policy \
    --destination-name "testFirehoseDestination" \
    --access-policy file://~/AccessPolicy.json
```

## Paso 3: Creación de unsubscriptionfilter

Cambie a la cuenta de envío, que es 111111111111 en este ejemplo. Ahora creará el filtro de suscripción en la cuenta de envío. En este ejemplo, el filtro está asociado a un grupo de registros que contieneAWS CloudTraileventos para que cada actividad registrada realizada por «Root»AWSLas credenciales se entregan en el destino creado anteriormente. Para obtener más información acerca de cómo enviarAWS CloudTrailPara CloudWatch Logs, consulteEnvío de eventos de CloudTrail a CloudWatch Logsen laAWS CloudTrailGuía del usuario.

```
aws logs put-subscription-filter \
    --log-group-name "aws-cloudtrail-logs-111111111111-300a971e" \
    --filter-name "firehose_test" \
    --filter-pattern "{$.userIdentity.type = AssumedRole}" \
    --destination-arn "arn:aws:logs:us-
east-1:222222222222:destination:testFirehoseDestination"
```

El grupo de registro y el destino deben estar en el mismoAWSRegión . Sin embargo, el destino puede apuntar a unAWSUn recurso de Kinesis Data Firehose que está ubicado en una región diferente.

## Validación del valor defBaja delOGevents

Después de crear el filtro de suscripción, CloudWatch Logs reenvía todos los eventos de registro entrantes que coinciden con el patrón de filtro al flujo de entrega de Kinesis Data Firehose. Los datos comienzan a aparecer en su depósito de Amazon S3 en función del intervalo de tiempo que se establece en la secuencia de entrega de Kinesis Data Firehose. Una vez que haya transcurrido el tiempo suficiente, puede verificar los datos comprobando el bucket de Amazon S3. Para comprobar el depósito de, escriba el siguiente comando:

```
aws s3api list-objects --bucket 'firehose-test-bucket1'
```

El resultado de ese comando será similar al siguiente:

```
{
    "Contents": [
        {
```

```
            "Key": "2021/02/02/08/my-delivery-
stream-1-2021-02-02-08-55-24-5e6dc317-071b-45ba-a9d3-4805ba39c2ba",
            "LastModified": "2021-02-02T09:00:26+00:00",
            "ETag": "\"EXAMPLEa817fb88fc770b81c8f990d\"",
            "Size": 198,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "firehose+2test",
                "ID": "EXAMPLE27fd05889c665d2636218451970ef79400e3d2aecca3adb1930042e0"
            }
        }
    ]
}
```

A continuación, puede recuperar un objeto específico del depósito introduciendo el siguiente comando. Reemplace el valor de`key`con el valor que encontró en el comando anterior.

```
aws s3api get-object --bucket 'firehose-test-bucket1' --key '2021/02/02/08/my-delivery-
stream-1-2021-02-02-08-55-24-5e6dc317-071b-45ba-a9d3-4805ba39c2ba' testfile.gz
```

Los datos en el objeto de Amazon S3 se comprimen con el formato gzip. Puede examinar los datos sin procesar desde la línea de comando utilizando uno de los siguientes comandos:

Linux:

```
zcat testfile.gz
```

macOS:

```
zcat <testfile.gz
```

## Modificación dedestinaciónmembership enruntime

Puede encontrar situaciones en las que tenga que añadir o eliminar remitentes de registros de un destino de su propiedad. Puede utilizar la acción PutDestinationPolicy en su destino con la nueva política de acceso. En el siguiente ejemplo, una cuenta añadida anteriormente1111111111Se detiene el envío de más datos de registro y cuenta3333333333está habilitado.

1. Obtenga la política que está asociada actualmente al destino testDestination y anote la AccessPolicy:

```
aws logs describe-destinations \
    --destination-name-prefix "testFirehoseDestination"

{
    "destinations": [
        {
            "destinationName": "testFirehoseDestination",
            "targetArn": "arn:aws:firehose:us-east-1:222222222222:deliverystream/my-
delivery-stream",
            "roleArn": "arn:aws:iam:: 222222222222:role/CWLtoKinesisFirehoseRole",
            "accessPolicy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement
\" : [\n    {\n      \"Sid\" : \"\",\n      \"Effect\" : \"Allow\",\n
 \"Principal\" : {\n        \"AWS\" : \"111111111111 \"\n      },\n      \"Action
\" : \"logs:PutSubscriptionFilter\",\n      \"Resource\" : \"arn:aws:logs:us-
east-1:222222222222:destination:testFirehoseDestination\"\n    }\n  ]\n}\n\n",
            "arn": "arn:aws:logs:us-east-1:
 222222222222:destination:testFirehoseDestination",
            "creationTime": 1612256124430
        }
```

```
    ]
}
```

2. Actualice la política para reflejar esa cuenta1111111111se detiene, y esa cuenta3333333333está habilitado. Incluya esta política en el archivo ~/NewAccessPolicy.json:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "333333333333 "
      },
      "Action" : "logs:PutSubscriptionFilter",
      "Resource" : "arn:aws:logs:us-
east-1:222222222222:destination:testFirehoseDestination"
    }
  ]
}
```

3. Utilice el siguiente comando para asociar la política definida en laNewAccessPolicy.jsoncon el destino:

```
aws logs put-destination-policy \
    --destination-name "testFirehoseDestination" \

    --access-policy file://~/NewAccessPolicy.json
```

Esto finalmente deshabilita los eventos de registro del ID de cuenta1111111111. Registrar eventos desde el ID de cuenta3333333333Comience a fluir al destino en cuanto el propietario de la cuenta3333333333Crea un filtro de suscripción.

# AWS serviciosthatpublishIA CloudWatch Logs

Los siguientes ejemplos deAWSpublican registros en CloudWatch Logs. Para obtener información acerca de los registros que envían estos servicios, consulte la documentación enlazada.

| Servicio | Documentación |
| --- | --- |
| Amazon API Gateway | Configuración del registro de API de CloudWatch en API Gateway |
| MySQL de Amazon Aurora | Publicación de registros de Amazon Aurora MySQL en Amazon CloudWatch Logs |
| AWS CloudHSM | MonitoreoAWS CloudHSMRegistros de auditoría en Amazon CloudWatch Logs |
| AWS CloudTrail | Supervisión de archivos de registro de CloudTrail con Amazon CloudWatch Logs |
| Amazon Cognito | Creación del rol de IAM de CloudWatch Logs |
| Amazon Connect | Registro y monitorización de Amazon Connect |
| AWS DataSync | Permitir a DataSync para cargar registros en grupos de registros de Amazon CloudWatch |
| AWS Elastic Beanstalk | Uso de Elastic Beanstalk con Amazon CloudWatch Logs |
| Amazon Elastic Container Service | Uso de CloudWatch Logs con instancias de contenedor |
| Amazon Elastic Kubernetes Service | Registro de plano de control de Amazon Elastic Kubernetes Service |
| Amazon ElastiCache for Redis | Entrega de registro |
| AWS Fargate | Uso del controlador de registros awslogs |
| AWS Glue | Registro continuo para trabajos de AWS Glue |
| AWS IoT | Supervisión con CloudWatch Logs |
| AWS Lambda | Acceso a Amazon CloudWatch Logs AWS Lambda |
| Amazon Macie | Supervisión de trabajos de detección de datos confidenciales con Amazon CloudWatch Logs |
| Amazon MQ | Configuración de Amazon MQ para publicar registros de auditoría y generales en Amazon CloudWatch Logs |
| AWS OpsWorks | Uso de Amazon CloudWatch Logs conAWS OpsWorksPilas |

| Servicio | Documentación |
| --- | --- |
| Amazon Relational Database Service | Publicación de registros de PostgreSQL en Amazon CloudWatch Logs |
| AWSRobomaker | AWS Nodos ROS de CloudWatch de Robomaker con soporte sin conexión |
| Amazon Route 53 | Registro y supervisión en Amazon Route 53 |
| Amazon SageMaker | Registrar eventos de Amazon SageMaker con Amazon CloudWatch |
| Amazon Simple Notification Service | Vista de CloudWatch Logs |
| Amazon VPC | Logs de flujo de VPC |

# Habilitación de registros desdeAWSServicios de

Aunque muchos servicios publican registros solo en CloudWatch Logs, algunosAWSpueden publicar registros directamente en Amazon Simple Storage Service o Amazon Kinesis Data Firehose. Si su requisito principal para los registros es el almacenamiento o el procesamiento en uno de estos servicios, puede conseguir fácilmente que el servicio que produce los registros los envíe directamente a Amazon S3 o Kinesis Data Firehose sin necesidad de configuración adicional.

Aunque los registros se publican directamente en Amazon S3 o Kinesis Data Firehose, se aplican cargos de. Para obtener más información, consulteTroncos vendidosen elRegistrosenPrecios de Amazon CloudWatch.

Permisos

Algunos de estosAWSutilizan una infraestructura común para enviar sus registros a CloudWatch Logs, Amazon S3 o Kinesis Data Firehose. Para habilitar la deAWSEstos servicios se muestran en la siguiente tabla para enviar sus registros a estos destinos, debe iniciar sesión como usuario con ciertos permisos.

Además, se deben conceder permisos aAWSPara habilitar el envío de los registros.AWSpuede crear automáticamente esos permisos cuando se configuran los registros, o puede crearlos usted mismo primero antes de configurar el registro.

Si eliges tenerAWSconfigura automáticamente los permisos y las directivas de recursos necesarios cuando usted o alguien de su organización configura por primera vez el envío de registros, a continuación, el usuario que está configurando el envío de registros debe tener ciertos permisos, como se explica más adelante en esta sección. Como alternativa, puede crear las directivas de recursos usted mismo y, a continuación, los usuarios que configuran el envío de registros no necesitan tantos permisos.

En la tabla siguiente se resumen los tipos de registros y los destinos de registro a los que se aplica la información de esta sección.

| Log type (Tipo de registro) | CloudWatch Logs (p. 122) | Amazon S3 (p. 123) | Kinesis Data Firehose (p. 125) |
|---|---|---|---|
| Logs de acceso a Amazon API Gateway | ✓ | | |
| Registros de métricas de calidad de medios de Amazon Chime y registros de mensajes SIP | ✓ | | |
| CloudFront: registros de acceso | | ✓ | |
| Registros de Amazon ElastiCache for Redis | ✓ | | ✓ |
| AWS Global Accelerator Registros de flujo de | | ✓ | |
| Registro de bróker de Amazon MSK | ✓ | ✓ | ✓ |
| AWS Network Firewall logs | ✓ | ✓ | ✓ |
| Registros de acceso del Network Load Balancer | | ✓ | |

| Log type (Tipo de registro) | CloudWatch Logs (p. 122) | Amazon S3 (p. 123) | Kinesis Data Firehose (p. 125) |
|---|---|---|---|
| Registros de consulta de Amazon Route 53 | ✓ | ✓ | ✓ |
| Eventos de trabajador de Amazon SageMaker | ✓ | | |
| Archivos de fuente de datos de instancias de spot de EC2 | | ✓ | |
| AWS Step Functions Historial del flujo | ✓ | | |
| AWS Storage Gateway registros de auditoría y registros de estado | ✓ | | |
| Registro de flujo de Amazon Virtual Private Cloud | | ✓ | |

En las siguientes secciones se proporcionan más detalles para cada uno de estos destinos.

# Registros enviados a CloudWatch Logs

> **Important**
>
> Cuando configure los tipos de registro en la siguiente lista para que se envíen a CloudWatch Logs,AWScrea o cambia las directivas de recursos asociadas con el grupo de registros que recibe los registros, si es necesario. Siga leyendo esta sección para ver los detalles.

Esta sección se aplica cuando se envían los siguientes tipos de registros a CloudWatch Logs:

- Logs de acceso a Amazon API Gateway
- AWS Storage Gatewayregistros de auditoría y registros de estado
- Registros de métricas de calidad de medios de Amazon Chime y registros de mensajes SIP
- Registros de Amazon ElastiCache for Redis
- Registro de Amazon Managed Streaming for Apache Kafka
- AWSRegistro de Network Firewall
- Registros de consulta de Amazon Route 53
- Eventos de trabajador de Amazon SageMaker
- AWS Step Functionshistorial de flujo de trabajo rápido e historial de flujo de trabajo

### Permisos de usuario

Para poder configurar el envío de cualquiera de estos tipos de registros a CloudWatch Logs por primera vez, debe iniciar sesión en una cuenta con los siguientes permisos.

- `logs:CreateLogDelivery`
- `logs:PutResourcePolicy`
- `logs:DescribeResourcePolicies`
- `logs:DescribeLogGroups`

Si alguno de estos tipos de registros ya se está enviando a un grupo de registros en CloudWatch Logs, entonces para configurar el envío de otro de estos tipos de registros a ese mismo grupo de registros, solo necesita la`logs:CreateLogDelivery`Permiso.

Directiva de recursos de grupo de registro

El grupo de registros al que se envían los registros debe tener una directiva de recursos que incluya determinados permisos. Si el grupo de registros actualmente no tiene una directiva de recursos, y el usuario que configura el registro tiene el`logs:PutResourcePolicy`,`logs:DescribeResourcePolicies`, y`logs:DescribeLogGroups`permisos para el grupo de registro y, a continuación,AWScrea automáticamente la siguiente directiva al comenzar a enviar los registros a CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:0123456789:log-group:my-log-group:log-stream:*"
      ]
    }
  ]
}
```

Si el grupo de registros tiene una directiva de recursos, pero esa directiva no contiene la instrucción mostrada en la directiva anterior, y el usuario que configura el registro tiene el`logs:PutResourcePolicy`,`logs:DescribeResourcePolicies`, y`logs:DescribeLogGroups`para el grupo de registros, esa instrucción se anexa a la directiva de recursos del grupo de registros.

Consideraciones de límite de tamaño de directiva de recursos de grupo

Estos servicios deben enumerar cada grupo de registro al que están enviando registros en la política de recursos y las políticas de recursos de CloudWatch Logs están limitadas a 5120 caracteres. Un servicio que envía registros a un gran número de grupos de registros podría alcanzar este límite.

Para mitigar el problema, CloudWatch Logs monitorea el tamaño de las políticas de recursos utilizadas por el servicio que envía registros y, cuando detecta que una política se acerca al límite de tamaño de 5120 caracteres, CloudWatch Logs habilita automáticamente`/aws/vendedlogs/*`en la directiva de recursos para ese servicio. A continuación, puede comenzar a usar grupos de registro con nombres que comiencen por`/aws/vendedlogs/`como los destinos de los registros de estos servicios.

# Registros enviados a Amazon S3

> **Important**
>
> Cuando configure los tipos de registro en la siguiente lista para enviarlos a Amazon S3,AWScrea o cambia las directivas de recursos asociadas con el depósito de S3 que recibe los registros, si es necesario. Siga leyendo esta sección para ver los detalles.

Esta sección se aplica cuando se envían los siguientes tipos de registros a Amazon S3:

- Registros de acceso de CloudFront y registros de acceso de streaming CloudFront utiliza un modelo de permisos diferente al de los demás servicios de esta lista. Para obtener más información, consulte Permisos necesarios para configurar el registro estándar y el acceso a los archivos de registro.
- Fuente de datos de instancias de spot de Amazon EC2
- Registros de flujo de AWS Global Accelerator
- Registro de Amazon Managed Streaming for Apache Kafka
- Registros de acceso del Network Load Balancer
- AWSRegistro de Network Firewall
- Registro de flujo de Amazon Virtual Private Cloud

Los registros publicados directamente en Amazon S3 se publican en un bucket existente que especifique. Se crean uno o varios archivos de registro cada cinco minutos en el bucket especificado.

Cuando entrega registros por primera vez a un depósito de Amazon S3, el servicio que entrega registros registra al propietario del depósito para asegurarse de que los registros se entregan solo a un depósito perteneciente a esta cuenta. Como resultado, para cambiar el propietario del depósito de Amazon S3, debe volver a crear o actualizar la suscripción de registro en el servicio de origen.

Permisos de usuario

Para poder configurar el envío de cualquiera de estos tipos de registros a Amazon S3 por primera vez, debe iniciar sesión en una cuenta con los siguientes permisos.

- `logs:CreateLogDelivery`
- `S3:GetBucketPolicy`
- `S3:PutBucketPolicy`

Si alguno de estos tipos de registros ya se está enviando a un bucket de Amazon S3, entonces para configurar el envío de otro de estos tipos de registros al mismo bucket, solo necesita tener `logs:CreateLogDelivery` Permiso.

Política de recursos de bucket de S3

El depósito de S3 al que se envían los registros debe tener una directiva de recursos que incluya determinados permisos. Si el depósito actualmente no tiene una directiva de recursos y el usuario que configura el registro tiene la propiedad `S3:GetBucketPolicy` y `S3:PutBucketPolicy` permisos para el depósito y, a continuación, AWS crea automáticamente la siguiente política cuando empiece a enviar los registros a Amazon S3.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-bucket"
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Si el depósito tiene una directiva de recursos, pero esa directiva no contiene la instrucción mostrada en la directiva anterior, y el usuario que configura el registro tiene el`S3:GetBucketPolicy`y`S3:PutBucketPolicy`para el bucket, esa instrucción se anexa a la directiva de recursos del bucket.

# Registro enviado a Kinesis Data Firehose

Esta sección se aplica cuando se envían los siguientes tipos de registros a Kinesis Data Firehose:

- Registros de Amazon ElastiCache for Redis
- Registro de Amazon Managed Streaming for Apache Kafka
- AWSRegistro de Network Firewall
- Registros de consulta de Amazon Route 53

Permisos de usuario

Para poder configurar el envío de cualquiera de estos tipos de registros a Kinesis Data Firehose por primera vez, debe iniciar sesión en una cuenta con los siguientes permisos.

- `logs:CreateLogDelivery`
- `firehose:TagDeliveryStream`
- `iam:CreateServiceLinkedRole`

Si alguno de estos tipos de registros ya se está enviando a Kinesis Data Firehose, entonces para configurar el envío de otro de estos tipos de registros a Kinesis Data Firehose solo necesita tener el`logs:CreateLogDelivery`y`firehose:TagDeliveryStream`Permisos.

Roles de IAM utilizados para permisos

Debido a que Kinesis Data Firehose no utiliza directivas de recursos,AWSutiliza roles de IAM al configurar estos registros para que se envíen a Kinesis Data Firehose.AWScrea un rol vinculado al servicio denominadoAWSServiceRoleForLogDelivery. Este rol vinculado al servicio incluye los siguientes permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:ListTagsForDeliveryStream"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/LogDeliveryEnabled": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

Este rol vinculado a servicios otorga permiso para todas las transmisiones de entrega de Kinesis Data Firehose que tienen la propiedad`LogDeliveryEnabled`etiqueta establecida en`true`.AWSproporciona esta etiqueta a la secuencia de entrega de destino cuando configura el registro.

Este rol vinculado al servicio también tiene una política de confianza que permite`delivery.logs.amazonaws.com`Para asumir el rol vinculado al servicio necesario. Esta política de confianza es la siguiente:

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

# Las actualizaciones de CloudWatch LogsAWSPolíticas administradas de

Ver detalles sobre las actualizaciones deAWSDesde que este servicio comenzó CloudWatch Logs realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de CloudWatch Logs.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Política de rol vinculado al servicio AWSServiceRoleForLogDelivery (p. 125) actualización de una política existente | CloudWatch Logs cambiaron los permisos de la directiva de IAM asociada con elAWSServiceRoleForLogDeliveryUn rol vinculado al servicio. Se realizó el siguiente cambio:<br>• La`firehose:ResourceTag/LogDeliveryEnabled": "true"`la clave de condición se cambió a`aws:ResourceTag/LogDeliveryEnabled": "true"`. | 15 de julio de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| CloudWatch Logs comenzó a controlar los cambios | CloudWatch Logs comenzó a controlar los cambios enAWSPolíticas administradas. | 10 de junio de 2021 |

# Exporting (Exportando)lOGdATA a Amazon S3

Puede exportar los datos de registro desde sus grupos de registro a un bucket de Amazon S3 y utilizarlos en el procesamiento y análisis personalizado o para cargar en otros sistemas.

Exportación de datos de registro a buckets de Amazon S3AWS KMSno es compatible.

Para iniciar el proceso de exportación, debe crear un bucket de S3 para almacenar los datos de registro exportados. Puede almacenar los archivos exportados en el bucket de Amazon S3 y definir reglas de ciclo de vida de Amazon S3 para que los archivos exportados se archiven o eliminen automáticamente.

Se admite la exportación a buckets de S3 que están cifrados con AES-256. No se admite la exportación a buckets de S3 que están cifrados con SSE-KMS. Para obtener más información, consulte ¿Cómo puedo habilitar el cifrado predeterminado para un bucket de S3?

Puede exportar los registros de varios grupos de registro o varios intervalos de tiempo en el mismo bucket de S3. Para separar los datos de registro de cada tarea de exportación, puede especificar un prefijo que se utilizará como key prefix de Amazon S3 para todos los objetos exportados.

Los datos de registro pueden tardar hasta 12 horas en estar disponibles para la exportación. Para el análisis casi en tiempo real de datos de registro, consulte Análisis de datos de registro con CloudWatch Logs Insights (p. 35) o En tiempo realprocessing delOGdata consubscriptions (p. 92) en su lugar.

> Note
>
> A partir del 15 de febrero de 2019, la característica de exportación a Amazon S3 requiere que los interlocutores tengans3:PutObjectAcceso al bucket de destino.

Contenido



# Concepts

Antes de comenzar, conviene familiarizarse con los siguientes conceptos de exportación:

nombre de grupo de registro

> El nombre del grupo de registro asociado a la tarea de exportación. Los datos de registro de este grupo de registros se exportarán al bucket de Amazon S3 especificado.

desde (marca temporal)

> Una marca temporal necesaria expresada como el número de milisegundos desde el 1 de enero de 1970 00:00:00 UTC. Se exportarán todos los eventos de registro en el grupo de registro recibidos después de este momento.

hasta (marca temporal)

> Una marca temporal necesaria expresada como el número de milisegundos desde el 1 de enero de 1970 00:00:00 UTC. Se exportarán todos los eventos de registro en el grupo de registro recibidos antes de este momento.

bucket de destino

El nombre del bucket de Amazon S3 asociado a la tarea de exportación. Este bucket se utiliza para exportar los datos de registro desde el grupo de registro especificado.

prefijo de destino

Un atributo opcional que se utiliza como prefijo de clave de S3 para todos los objetos exportados. Esto le ayuda a crear una organización similar a carpetas en su bucket.

# ExportlOGdATA a Amazon S3ucantar elconsole

En el siguiente ejemplo, utilizará la consola de Amazon CloudWatch para exportar todos los datos de un grupo de Amazon CloudWatch Logs denominado`my-log-group`Un bucket de Amazon S3`my-exported-logs`.

Exportación de datos de registro a buckets de Amazon S3AWS KMSno es compatible.

## Paso 1: Creación de un Amazon S3bucket

Le recomendamos que utilice un bucket creado específicamente para CloudWatch Logs. Sin embargo, si desea utilizar un bucket existente, puede pasar al paso 2.

Note

El bucket de Amazon S3 debe residir en la misma región que los datos de registro que se van a exportar. CloudWatch Logs no admite la exportación de datos a buckets de Amazon S3 en una región distinta.

Para crear un bucket de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Si es necesario, cambie la región. En la barra de navegación, elija la región donde residen los CloudWatch Logs.
3. Seleccione la opción Create Bucket.
4. En Bucket Name (Nombre del bucket), escriba un nombre para el bucket.
5. ParaRegión, seleccione la región donde residen los datos de CloudWatch Logs.
6. Seleccione Create.

## Paso 2: Creación de un IAMuser confullaccess a Amazon S3 y CloudWatch Logs

En los pasos siguientes, creará el usuario de IAM con los permisos necesarios.

Para crear el usuario de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Elija Users (Usuarios), Add user (Añadir usuario).
3. Escriba un nombre de usuario, como ***`CWLExportUser`***.
4. Seleccione ambosAcceso programáticoyAWS Management ConsoleAcceso a.
5. Elija Autogenerated password (Contraseña generada automáticamente) o Custom password (Contraseña personalizada).
6. Seleccione Next (Siguiente): Permisos.

7. Elija Attach existing policies directly (Asociar políticas existentes directamente) y asocie las políticas `AmazonS3FullAccess` y `CloudWatchLogsFullAccess` al usuario. Puede utilizar el cuadro de búsqueda para buscar las políticas.
8. Seleccione Next (Siguiente): Tags (Etiquetas):,Siguiente: Review (Revisar)y, a continuación,Creación de usuario.

# Paso 3: EstablezcapLas misiones en Amazon S3bucket

De forma predeterminada, todos los buckets y objetos de Amazon S3 son privados. Solo el propietario del recurso y la cuenta de AWS que creó el bucket pueden tener acceso a ese bucket y a los objetos que contiene. No obstante, el propietario del recurso puede elegir conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Cuando establezca la política, le recomendamos que incluya una cadena generada aleatoriamente como prefijo para el bucket, de manera que solo se exporten al bucket los flujos de registros deseados.

Para definir permisos en un bucket de Amazon S3

1. En la consola de Amazon S3, elija el bucket que ha creado en el paso 1.
2. Elija Permissions (Permisos), Bucket policy (Política de bucket).
3. En la ventana Bucket Policy Editor (Editor de políticas de bucket), añada alguna de las políticas siguientes. Cambie `my-exported-logs` por el nombre de su bucket de S3· y `random-string` por una cadena de caracteres generados aleatoriamente. Asegúrese de especificar el punto de enlace de la región correcta en Principal (Entidad principal).

   - Si el bucket está en su cuenta, añada la siguiente política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
          "Action": "s3:GetBucketAcl",
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs",
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
      },
      {
          "Action": "s3:PutObject" ,
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
          "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
      }
    ]
}
```

   - Si el bucket está en otra cuenta, utilice la siguiente política en su lugar. Incluye una instrucción adicional que utiliza el usuario de IAM de que creó en el paso anterior.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
          "Action": "s3:GetBucketAcl",
          "Effect": "Allow",
```

```
            "Resource": "arn:aws:s3:::my-exported-logs",
            "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
        },
        {
            "Action": "s3:PutObject" ,
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
            "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
            "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
        },
        {
            "Action": "s3:PutObject" ,
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
            "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
            "Principal": { "AWS": "arn:aws:iam::SendingAccountID:user/CWLExportUser" }
        }
    ]
}
```

4. Elija Save para definir la política que acaba de añadir como política de acceso en su bucket. Esta política permite a CloudWatch Logs exportar datos de registro a su bucket de Amazon S3. El propietario del bucket tiene permisos completos en todos los objetos exportados.

   Warning

   Si el bucket existente ya tiene una o varias políticas asociadas, añada las instrucciones para que los CloudWatch Logs a dicha política o políticas. Le recomendamos que evalúe el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que van a tener acceso al bucket.

# Paso 4: Creación de unexporttask

En este paso se crea la tarea de exportación para exportar los registros desde un grupo de registros.

Para exportar datos a Amazon S3

1. Inicie sesión como el usuario de IAM que creó enPaso 2: Creación de un IAMUser confullaccess a Amazon S3 y CloudWatch Logs.
2. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
3. En el panel de navegación, seleccione Log groups (Grupos de registro).
4. En la pantalla Log Groups (Grupos de registros) elija el nombre del grupo de registros.
5. SeleccionarActions,Exportar datos a Amazon S3.
6. En la páginaExportar datos a Amazon S3Pantalla, enDefinición de exportación de datos, defina el intervalo de tiempo para los datos que exportar usandoDesdeyPara.
7. Si su grupo de registros tiene varios flujos de registro, puede proporcionar un prefijo de flujo de registro para limitar los datos del grupo de registro a un flujo específico. Elija Advanced (Avanzadas) y, a continuación, en Stream prefix (Prefijo del flujo), escriba el prefijo del flujo de registros.
8. UNDERElija Choose S3, elija la cuenta asociada con el bucket de Amazon S3.
9. ParaNombre del bucket de S3, elija un bucket de Amazon S3.
10. En Export data to (Prefijo del bucket de S3), escriba la cadena generada aleatoriamente que especificó en la política del bucket.
11. SeleccionarExportPara exportar los datos de registro a Amazon S3.
12. Para ver el estado de los datos de registro que ha exportado a Amazon S3, elijaActionsy luegoVer todas las exportaciones a Amazon S3.

# ExportlOGdATA a Amazon S3ucantar elAWS CLI

En el siguiente ejemplo, utilizará una tarea de exportación para exportar todos los datos de un grupo de registros de CloudWatch Logs denominado`my-log-group`Un bucket de Amazon S3`my-exported-logs`. En este ejemplo se presupone que ya ha creado un grupo denominado `my-log-group`.

Exportación de datos de registro a buckets de Amazon S3AWS KMSno es compatible.

## Paso 1: Creación de un Amazon S3bucket

Le recomendamos que utilice un bucket creado específicamente para CloudWatch Logs. Sin embargo, si desea utilizar un bucket existente, puede pasar al paso 2.

> **Note**
>
> El bucket de Amazon S3 debe residir en la misma región que los datos de registro que se van a exportar. CloudWatch Logs no admite la exportación de datos a buckets de Amazon S3 en una región distinta.

Para crear un bucket de Amazon S3AWS CLI

En el símbolo del sistema, ejecute el siguiente comando create-bucket, donde `LocationConstraint` es la región en la que se exportan los datos de registro.

```
aws s3api create-bucket --bucket my-exported-logs --create-bucket-configuration
 LocationConstraint=us-east-2
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "Location": "/my-exported-logs"
}
```

## Paso 2: Creación de un IAMuser confullaccess a Amazon S3 y CloudWatch Logs

En los pasos siguientes, creará el usuario de IAM con los permisos necesarios.

Para crear el usuario y asignarle permisos

1. Para crear el usuario de IAM, introduzca el siguiente comando.

   ```
   aws iam create-user --user-name CWLExportUser
   ```

2. Asocie las políticas administradas de IAM al usuario de IAM que acaba de crear.

   ```
   export S3POLICYARN=$(aws iam list-policies --query 'Policies[?
   PolicyName==`AmazonS3FullAccess`].{ARN:Arn}' --output text)
   ```

   ```
   export CWLPOLICYARN=$( aws iam list-policies --query 'Policies[?
   PolicyName==`CloudWatchLogsFullAccess`].{ARN:Arn}' --output text)
   ```

   ```
   aws iam attach-user-policy --user-name CWLExportUser --policy-arn $S3POLICYARN
   ```

```
aws iam attach-user-policy --user-name CWLExportUser --policy-arn $CWLPOLICYARN
```

3. Confirme que se han asociado las dos políticas administradas.

```
aws iam list-attached-user-policies --user-name CWLExportUser
```

4. Configure elAWS CLIpara incluir las credenciales de IAM del*CWLExportUser*Usuario de IAM Para obtener más información, consulte Configuración de la AWS CLI.

# Paso 3: EstablezcapLas misiones en Amazon S3bucket

De forma predeterminada, todos los buckets y objetos de Amazon S3 son privados. Solo el propietario del recurso y la cuenta que creó el bucket pueden tener acceso a ese bucket y a los objetos que contiene. No obstante, el propietario del recurso puede elegir conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Para definir permisos en un bucket de Amazon S3

1. Cree un archivo denominado `policy.json` y agregue la siguiente política de acceso, cambiando `Resource` por el nombre de su bucket de S3 y `Principal` por el punto de enlace de la región a la que va a exportar los datos de registro. Utilice un editor de texto para crear este archivo de política. No utilice la consola de IAM.

   - Si el bucket está en su cuenta, utilice la siguiente política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:GetBucketAcl",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::my-exported-logs",
            "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
        },
        {
            "Action": "s3:PutObject" ,
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::my-exported-logs/*",
            "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
            "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
        }
    ]
}
```

   - Si el bucket está en otra cuenta, utilice la siguiente política en su lugar. Incluye una instrucción adicional que utiliza el usuario de IAM de que creó en el paso anterior.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
          "Action": "s3:GetBucketAcl",
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs",
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
```

```
      },
      {
          "Action": "s3:PutObject" ,
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
          "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
      },
      {
          "Action": "s3:PutObject" ,
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
          "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
          "Principal": { "AWS": "arn:aws:iam::SendingAccountID:user/CWLExportUser" }
      }
    ]
}
```

- Si el bucket de se encuentra en una cuenta distinta y utiliza un rol de IAM en lugar de un usuario de IAM, utilice la siguiente política en su lugar.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
          "Action": "s3:GetBucketAcl",
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs",
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
      },
      {
          "Action": "s3:PutObject" ,
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
          "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
          "Principal": { "Service": "logs.us-west-2.amazonaws.com" }
      },
      {
          "Action": "s3:PutObject" ,
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::my-exported-logs/random-string/*",
          "Condition": { "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-
control" } },
          "Principal": { "AWS": "arn:aws:iam::SendingAccountID:role/CWLExportUser" }
      }
    ]
}
```

2. Defina la política que acaba de añadir como política de acceso en su bucket con el comando put-bucket-policy. Esta política permite a CloudWatch Logs exportar datos de registro a su bucket de Amazon S3. El propietario del bucket tendrá permisos completos en todos los objetos exportados.

```
aws s3api put-bucket-policy --bucket my-exported-logs --policy file://policy.json
```

Warning

Si el bucket existente ya tiene una o varias políticas asociadas, añada las instrucciones para que los CloudWatch Logs a dicha política o políticas. Le recomendamos que evalúe el

conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que van a tener acceso al bucket.

# Paso 4: Creación de unexporttask

Después de crear la tarea de exportación para exportar registros desde un grupo de registros, la tarea de exportación podría llevar de unos segundos a unas horas, en función del tamaño de los datos que se van a exportar.

Para crear una tarea de exportación mediante la AWS CLI

En el símbolo del sistema, utilice el siguiente comando create-export-task para crear la tarea de exportación.

```
aws logs create-export-task --profile CWLExportUser --task-name "my-log-group-09-10-2015"
 --log-group-name "my-log-group" --from 1441490400000 --to 1441494000000 --destination "my-
exported-logs" --destination-prefix "export-task-output"
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "taskId": "cda45419-90ea-4db5-9833-aade86253e66"
}
```

# Paso 5: describeexporttasks

Después de crear una tarea de exportación, puede obtener el estado actual de la tarea.

Para describir tareas de exportación utilizando la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando describe-export-tasks.

```
aws logs --profile CWLExportUser describe-export-tasks --task-id "cda45419-90ea-4db5-9833-
aade86253e66"
```

A continuación, se muestra un ejemplo del resultado.

```
{
   "exportTasks": [
   {
      "destination": "my-exported-logs",
      "destinationPrefix": "export-task-output",
      "executionInfo": {
         "creationTime": 1441495400000
      },
      "from": 1441490400000,
      "logGroupName": "my-log-group",
      "status": {
         "code": "RUNNING",
         "message": "Started Successfully"
      },
      "taskId": "cda45419-90ea-4db5-9833-aade86253e66",
      "taskName": "my-log-group-09-10-2015",
      "tTo": 1441494000000
   }]
}
```

Puede utilizar el comando `describe-export-tasks` de tres formas diferentes:

- Sin filtros: Muestra todas las tareas de exportación, en orden de creación inverso.
- Filtrar por ID de tarea: Muestra la tarea de exportación, si existe, con el ID especificado.
- Filtrar por estado de tarea: Muestra las tareas de exportación con el estado especificado.

Por ejemplo, utilice el siguiente comando para filtrar por el estado `FAILED`.

```
aws logs --profile CWLExportUser describe-export-tasks --status-code "FAILED"
```

A continuación, se muestra un ejemplo del resultado.

```
{
   "exportTasks": [
   {
      "destination": "my-exported-logs",
      "destinationPrefix": "export-task-output",
      "executionInfo": {
         "completionTime": 1441498600000
         "creationTime": 1441495400000
      },
      "from": 1441490400000,
      "logGroupName": "my-log-group",
      "status": {
         "code": "FAILED",
         "message": "FAILED"
      },
      "taskId": "cda45419-90ea-4db5-9833-aade86253e66",
      "taskName": "my-log-group-09-10-2015",
      "to": 1441494000000
   }]
}
```

# Paso 6: Cancelar unaexporttask

Puede cancelar una tarea de exportación si se encuentra en el estado `PENDING` o `RUNNING`.

Para cancelar una tarea de exportación mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando cancel-export-task:

```
aws logs --profile CWLExportUser cancel-export-task --task-id "cda45419-90ea-4db5-9833-
aade86253e66"
```

Puede utilizar el comando describe-export-tasks para comprobar que la tarea se ha cancelado correctamente.

# Log Streaming CloudWatch LogsdATA a Amazon Elasticsearch Service

Puede configurar un grupo de registros de CloudWatch Logs para transmitir datos que recibe a su clúster de Amazon Elasticsearch Service (Amazon ES) casi en tiempo real a través de una suscripción de CloudWatch Logs. Para obtener más información, consulte En tiempo realprocessing delOGdata consubscriptions (p. 92).

En función de la cantidad de datos de registro que se vayan a transmitir, es posible que desee establecer un límite de ejecuciones simultáneas en la función. Para obtener más información, consulte Límite de ejecuciones simultáneas en el nivel de función.

> Note
>
> La transmisión de grandes cantidades de datos de CloudWatch Logs a Amazon ES podría dar lugar a elevados cargos por uso. Le recomendamos crear un presupuesto en la consola de administración de costos y facturación. Para obtener más información, consulte Gestión de costos con presupuestos.

## Prerequisites

Antes de comenzar, cree un dominio de Amazon ES. El dominio de Amazon ES puede tener acceso público o acceso de VPC, pero no puede modificar el tipo de acceso después de que se cree el dominio. Es posible que desee revisar su configuración de dominios de Amazon ES más adelante y modificar la configuración del clúster en función de la cantidad de datos que procesará el clúster.

Para obtener más información acerca de Amazon ES, consulte laGuía para desarrolladores de Amazon Elasticsearch Service.

Para crear un dominio de Amazon ES

En el símbolo del sistema, ejecute el siguiente comando create-elasticsearch-domain:

```
aws es create-elasticsearch-domain --domain-name my-domain
```

## Suscripción a unalOGgRoup a Amazon ES

Puede utilizar la consola de CloudWatch para suscribir un grupo de registros a Amazon ES.

Para suscribir un grupo de registros a Amazon ES

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Log groups (Grupos de registro).
3. Elija el nombre del grupo de registros.

4. SeleccionarActions,Crear filtro de suscripción de Elasticsearch search search search.
5. Elija si desea transmitir a un clúster de esta cuenta u otra cuenta.
6. ParaCluster de Amazon ES, elija el clúster que creó en el paso anterior.
7. UNDERFunción Lambda, paraFunción de ejecución de IAM de LambdaEn, elija el rol de IAM que debe utilizar Lambda a la hora de ejecutar llamadas a Amazon ES y, a continuación, elijaSiguiente.

   La función de IAM que elija deberá cumplir estos requisitos:

   - Debo tener `lambda.amazonaws.com` en la relación de confianza.
   - Debe incluir la política siguiente:

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Action": [
                   "es:*"
               ],
               "Effect": "Allow",
               "Resource": "arn:aws:es:region:account-id:domain/target-domain-name/*"
           }
       ]
   }
   ```

   - Si el dominio de Amazon ES de destino utiliza el acceso VPC, la función debe tener laAWSLambdaVPCAccessExecutionRoleAsociación de políticas en. Esta política administrada por Amazon concede a Lambda acceso a la VPC del cliente, permitiendo que Lambda escriba en el punto de enlace de Amazon ES de la VPC.
8. En Formato de registro, elija un formato de registro.
9. En Patrón de filtro de suscripción, escriba los términos o el patrón que desea buscar en los eventos de registros. Esto garantiza que envíe solo los datos que le interesan en su clúster de Amazon ES. Para obtener más información, consulte CrearmmétricasfROMlOGerejillas de ventilaciónucantarfilters (p. 72).
10. (Opcional) En Seleccionar datos de registro para probar, seleccione un flujo de registros y, a continuación, elija Patrón de prueba para verificar que el filtro de búsqueda devuelve los resultados esperados.
11. Elija Iniciar streaming.

# Seguridad en Amazon CloudWatch Logs

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube – AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener más información acerca de los programas de conformidad que se aplican a WorkSpaces, consulteAWSServicios de conformidad en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon CloudWatch Logs. Muestra cómo configurar Amazon CloudWatch Logs para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otrosAWSServicios de CloudWatch Logs que le ayudan a supervisar y proteger sus recursos de CloudWatch

Contenido



# DatospRotection en Amazon CloudWatch Logs

LaAWS Modelo de responsabilidad compartidaSe aplica a la protección de datos en Amazon CloudWatch Logs. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS . Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de AWS que utiliza usted. Para obtener más información acerca de la privacidad de datos, consulte las Preguntas frecuentes sobre privacidad de datos. Para obtener información acerca de la protección de datos en Europa, consulte la publicación de blog The AWS Shared Responsability Model and GDPR en el Blog de seguridad de AWS.

Para fines de protección de datos, recomendamos proteger Cuenta de AWS y configurar cuentas de usuario individuales conAWS Identity and Access Management(IAM). De esta manera, solo se otorgan

a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También le recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Le recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que le ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 cuando accede a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información acerca de los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaje con CloudWatch Logs u otrosAWSutilizando la consola, API,AWS CLI, o bienAWSSDK. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

## Cifrado enrest

CloudWatch Logs protege los datos en reposo a través del cifrado. Todos los grupos de registro están cifrados. De forma predeterminada, el servicio CloudWatch Logs administra las claves de cifrado del lado del servidor.

Si desea administrar las claves que se emplean para cifrar y descifrar los registros, utilice las claves maestras del cliente (CMK) de AWS Key Management Service. Para obtener más información, consulte EncryptlOGdATA en CloudWatch LogsucantarAWS Key Management Service (p. 65) .

## Cifrado en transit

CloudWatch Logs utiliza cifrado de extremo a extremo de los datos en tránsito. El servicio CloudWatch Logs administra las claves de cifrado del lado del servidor.

# Identity and Access Management para Amazon CloudWatch Logs

El acceso a Amazon CloudWatch Logs requiere credenciales deAWSPuede utilizar para autenticar las solicitudes. Estas credenciales deben tener permisos para obtener acceso aAWSRecursos de, como por ejemplo para recuperar datos de CloudWatch Logs sobre sus recursos en la nube. En las siguientes secciones presentamos más detalles sobre cómo usarAWS Identity and Access Management(IAM)Para ayudar a CloudWatch Logs sus recursos controlando quién puede obtener acceso a ellos:

- Authentication (p. 141)
- Control de acceso (p. 142)

# Authentication

Puede obtener acceso a AWS con los siguientes tipos de identidades:

- AWSUsuario raíz de la cuenta de— Cuando te inscribes enAWS, proporciona una dirección de correo electrónico y la contraseña asociada a suAWSaccount. Estas son las credenciales raíz y proporcionan acceso completo a todos los recursos de AWS.

  Important

  Por motivos de seguridad, le recomendamos que utilice las credenciales raíz solo para crear un usuario administrador, que es un usuario de IAM con permiso total para administrar su cuenta de AWS. Después, podrá utilizar este usuario administrador para crear otros usuarios y roles de IAM con permisos limitados. Para obtener más información, consulte Prácticas recomendadas de IAM y Creación de un grupo y usuario administrador en la Guía del usuario de IAM.

- Usuario de IAM— UnUsuario de IAMes simplemente una identidad dentro de suAWSCuenta de que tiene permisos personalizados específicos (por ejemplo, permisos para ver métricas en CloudWatch Logs). Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión enAWScomo las páginas webAWS Management Console,AWSForos de debate de, o elAWS SupportCenter.

  Además de un nombre de usuario y una contraseña, también puede generar claves de acceso para cada usuario. Puede utilizar estas claves cuando obtenga acceso a los servicios de AWS mediante programación, ya sea a través de uno de los SDK o mediante la AWS Command Line Interface (AWS CLI). El SDK y las herramientas de CLI usan claves de acceso para firmar criptográficamente su solicitud. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. Soporta CloudWatch LogsSignature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información acerca de la autenticación de solicitudes de, consulteProceso de firma Signature Version 4en laAWSReferencia general de.

- Rol de IAM— UnRol de IAMes otra identidad de IAM que puede crear en su cuenta de que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Un rol de IAM le permite obtener claves de acceso temporal que se pueden utilizar para tener acceso aAWSServicios y recursos de. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

  - Acceso de usuarios federados: en lugar de crear un usuario de IAM, puede usar identidades de usuario preexistentes deAWS Directory Service, el directorio de usuarios de la compañía o un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.

  - Acceso entre cuentas: puede utilizar un rol de IAM de su cuenta para conceder otroAWSPermisos de cuenta para tener acceso a los recursos de su cuenta. Para ver un ejemplo, consulte .Tutorial: Delegar el acceso entreAWSCuentas que utilizan roles de IAMen laIAM User Guide.

  - AWSAcceso a servicios de :: puede utilizar un rol de IAM de su cuenta para conceder unAWSPermisos de servicio para tener acceso a los recursos de su cuenta. Por ejemplo, puede crear un rol que permita a Amazon Redshift obtener acceso a un bucket de Amazon S3 en su nombre y cargar en un clúster de Amazon Redshift los datos almacenados en el bucket de. Para obtener más

información, consulteCreación de un rol para delegar permisos a unAWSService (Servicio)enIaIAM User Guide.

- Aplicaciones que se ejecutan en Amazon EC2En lugar de almacenar claves de acceso en la instancia EC2 para que las usen aplicaciones que se ejecutan en la instancia y queAWSSolicitudes de API de, puede usar un rol de IAM para administrar credenciales temporales para estas aplicaciones. Para asignar una función de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a dicha instancia. Un perfil de instancia contiene la función y permite a los programas que se encuentran en ejecución en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de roles para aplicaciones en Amazon EC2 en la Guía del usuario de IAM.

# Control de acceso

Aunque disponga de credenciales válidas para autenticar las solicitudes, si no tiene permisos, no podrá crear recursos de CloudWatch Logs ni obtener acceso a ellos. Por ejemplo, debe disponer de permisos para crear flujos de registro, crear grupos de registro, etc.

En las secciones siguientes se describe cómo administrar los permisos para CloudWatch Logs. Le recomendamos que lea primero la información general.

- Información general sobre la administración de permisos de acceso a los recursos de CloudWatch Logs (p. 142)
- Usar políticas basadas en identidad (políticas de IAM) para CloudWatch Logs (p. 146)
- Referencia de permisos CloudWatch Logs (p. 151)

# Información general sobre la administración de permisos de acceso a los recursos de CloudWatch Logs

Todos losAWSes propiedad de un recurso de Cuenta de AWS Y los permisos para crear o tener acceso a un recurso se rigen por políticas de permisos. Los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y funciones). Algunos servicios (como AWS Lambda) también permiten asociar políticas de permisos con los recursos.

> Note
>
> Un registroAdministrador de cuentas(o usuario administrador de IAM) es un usuario con privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

Temas

- CloudWatch Logs recursos y operaciones (p. 143)
- Titularidad de los recursos (p. 143)
- Administración del acceso a los recursos (p. 143)
- Especificar elementos de la política: Acciones, efectos y entidades principales (p. 145)
- Especificación de las condiciones de una política (p. 146)

## CloudWatch Logs recursos y operaciones

En CloudWatch Logs, los recursos principales son grupos de registros, flujos de registro y destinos. CloudWatch Logs no admite subrecursos (otros recursos para su uso con el recurso principal).

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla:

| Tipo de recurso | Formato de ARN |
| --- | --- |
| Grupo de registros | arn:aws:logs:*región*:*ID-de-cuenta*:log-group:*nombre_de_grupo_de_registros* |
| Flujo de registro | arn:aws:logs:*región*:*ID-de-cuenta*:log-group:*nombre_de_grupo_de_registros*:log-stream:*nombre_de_flujo_de_registro* |
| Destino | arn:aws:logs:*región*:*ID-de-cuenta*:destination:*nombre_de_destino* |

Para obtener más información sobre los ARN, consulteARN deinIAM User Guide. Para obtener información acerca de los ARN de CloudWatch Logs, consulteNombres de recursos de Amazon (ARN)inReferencia general de Amazon Web Services. Para ver un ejemplo de una política que abarca los CloudWatch Logs, consulteUsar políticas basadas en identidad (políticas de IAM) para CloudWatch Logs (p. 146).

CloudWatch Logs proporciona un conjunto de operaciones para trabajar con los recursos de CloudWatch Logs. Para ver la lista de las operaciones disponibles, consulte Referencia de permisos CloudWatch Logs (p. 151).

## Titularidad de los recursos

La cuenta de AWS es la propietaria de los recursos que se crean en ella, independientemente de quién los haya creado. En concreto, el propietario de los recursos es la cuenta de AWS de la entidad principal (es decir, la cuenta raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Los siguientes ejemplos ilustran cómo funciona:

- Si usa las credenciales de la cuenta raíz de suAWSPara crear un grupo de registros, la cuenta deAWSes la propietaria del recurso de CloudWatch Logs.
- Si crea un usuario de IAM en suAWSy conceder permisos para crear recursos de CloudWatch Logs a ese usuario, el usuario podrá crear recursos de CloudWatch Logs. Sin embargo, suAWSLa cuenta de a la que pertenece el usuario será la propietaria de los recursos de CloudWatch Logs.
- Si crea un rol de IAM en suAWSCon permisos para crear recursos de CloudWatch Logs, cualquier persona que pueda asumir ese rol podrá crear recursos de CloudWatch Logs. SusAWSLa cuenta de a la que pertenece el rol será la propietaria de los recursos de CloudWatch Logs.

## Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> Note
>
> En esta sección se explica cómo se usa IAM en el contexto de los Logs de CloudWatch. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa

de IAM, consulte¿Qué es IAM?en laIAM User Guide. Para obtener más información acerca de la sintaxis y descripciones de las políticas de IAM, consulteReferencia de política de IAMen laIAM User Guide.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. CloudWatch Logs admite políticas basadas en identidad y políticas basadas en recursos para destinos, que se utilizan para habilitar suscripciones entre cuentas. Para obtener más información, consulte Entre países esaccountlOGdatasharing consubscriptions (p. 104) .

Temas

- Permisos de grupo de registro e información de colaborador (p. 144)
- Políticas basadas en identidad (políticas de IAM) (p. 144)
- Políticas basadas en recursos (p. 145)

## Permisos de grupo de registro e información de colaborador

Contributor Insights es una característica de CloudWatch que le permite analizar datos de grupos de registros y crear series temporales que muestren datos de colaboradores. Puede ver métricas acerca de los colaboradores Top-N, el número total de colaboradores únicos y su uso. Para obtener más información, consulta Uso de Contributor Insights para analizar datos de alta cardinalidad.

Cuando concede a un usuario el`cloudwatch:PutInsightRule`y`cloudwatch:GetInsightRuleReport`, ese usuario puede crear una regla que evalúe cualquier grupo de registros en CloudWatch Logs y, a continuación, vea los resultados. Los resultados pueden contener datos de colaborador para esos grupos de registro. Asegúrese de conceder estos permisos solo a los usuarios que puedan ver estos datos.

## Políticas basadas en identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o grupo de su cuenta: para conceder permisos a un usuario para ver registros en la consola de CloudWatch Logs, puede asociar una política de permisos a un usuario o a un grupo al que pertenezca el usuario.
- Asociar una política de permisos a un rol (conceder permisos entre cuentas): puede asociar una política de permisos basada en identidad a un rol de IAM para conceder permisos entre cuentas. Por ejemplo, el administrador de la Cuenta A puede crear una función para conceder permisos entre cuentas a otra cuenta de AWS (por ejemplo, a la Cuenta B) o a un servicio de AWS, tal y como se indica a continuación:
  1. El administrador de la Cuenta A crea un rol de IAM y asocia una política de permisos a dicho rol, que concede permisos sobre los recursos de la Cuenta A.
  2. El administrador de la Cuenta A asocia una política de confianza al rol que identifica la Cuenta B como la entidad principal que puede asumir el rol.
  3. A continuación, el administrador de la Cuenta B puede delegar permisos para asumir el rol a cualquier usuario de la Cuenta B. De este modo, los usuarios de la Cuenta B podrán crear recursos y obtener acceso a ellos en la Cuenta A. La entidad principal de la política de confianza también puede ser la entidad principal de un servicio de AWS si desea conceder permisos para asumir el rol a un servicio de AWS.

  Para obtener más información acerca del uso de IAM para delegar permisos, consulteAdministración de accesosen laIAM User Guide.

A continuación, se muestra un ejemplo de política que concede permisos para la`logs:PutLogEvents`,`logs:CreateLogGroup`, y`logs:CreateLogStream`acciones de todos los

recursos de us-east-1. Para grupos de registros, CloudWatch Logs admite identificar recursos específicos utilizando los ARN de recursos (también conocidos como permisos de nivel de recurso) de algunas de las acciones de API. Si desea incluir todos los grupos de registros, debe especificar el carácter comodín (*).

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"",
         "Effect":"Allow",
         "Action":[
            "logs:PutLogEvents",
            "logs:CreateLogGroup",
            "logs:CreateLogStream"
         ],
         "Resource":"arn:aws:logs:us-east-1:*:*"
      }
   ]
}
```

Para obtener más información acerca del uso de políticas basadas en identidad con CloudWatch Logs, consulteUsar políticas basadas en identidad (políticas de IAM) para CloudWatch Logs (p. 146). Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

### Políticas basadas en recursos

CloudWatch Logs admite políticas basadas en recursos para destinos, que se puede utilizar para habilitar suscripciones entre cuentas. Para obtener más información, consulte Creación de undestination (p. 105) . Los destinos se pueden crear utilizando el API PutDestination y puede añadir una política de recursos al destino mediante el API PutDestination. En el siguiente ejemplo se permite otroAWSCuenta con el ID de cuenta 111122223333 para suscribir sus grupos de registro al destino`arn:aws:logs:us-east-1:123456789012:destination:testDestination`.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "111122223333"
      },
      "Action" : "logs:PutSubscriptionFilter",
      "Resource" : "arn:aws:logs:us-east-1:123456789012:destination:testDestination"
    }
  ]
}
```

## Especificar elementos de la política: Acciones, efectos y entidades principales

Para cada recurso de CloudWatch Logs, el servicio define un conjunto de operaciones de API. Para conceder permisos a estas operaciones de la API, CloudWatch Logs define un conjunto de acciones que puede especificar en una política. Algunas operaciones de API pueden requerir permisos para más de una acción para poder realizar la operación de API. Para obtener más información sobre los recursos y las operaciones de API, consulte CloudWatch Logs recursos y operaciones (p. 143) y Referencia de permisos CloudWatch Logs (p. 151).

A continuación, se indican los elementos básicos de la política:

- Recurso: use un Nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte CloudWatch Logs recursos y operaciones (p. 143) .
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `logs.DescribeLogGroups` concede permiso a los usuarios para realizar la operación `DescribeLogGroups`.
- Efecto: especifique el efecto (permitir o denegar) cuando el usuario solicite la acción específica. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Los registros de CloudWatch Logs admiten políticas basadas en recursos para destinos.

Para obtener más información acerca de la sintaxis y descripciones de las políticas de IAM, consulteAWSReferencia de la política de IAMen laIAM User Guide.

Para ver una tabla con todas las acciones de API de CloudWatch Logs y los recursos a los que se aplican, consulteReferencia de permisos CloudWatch Logs (p. 151).

## Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. Para obtener una lista de claves de contexto admitidas por cadaAWSy una lista deAWSclaves de directiva de gran alcance, consulteAcciones, recursos y claves de condiciones paraAWSServicios deyAWSClaves de contexto de condición globales de.

> **Note**
>
> CloudWatch Logs no admite directivas de IAM que impidan que los usuarios asignen etiquetas especificadas a grupos de registro mediante el`aws:Resource/key-name`o`aws:TagKeys`Claves de condición. Además, no puede controlar el acceso a la`DescribeLogGroups`mediante el uso de la función`aws:ResourceTag/key-name`Clave de condición Otras acciones de CloudWatch Logs sí admiten el uso de`aws:ResourceTag/key-name`clave de condición para controlar el acceso. Para obtener más información acerca del uso de etiquetas de para controlar el acceso, consulteControl de acceso a los recursos de Amazon Web Services mediante etiquetas.

# Usar políticas basadas en identidad (políticas de IAM) para CloudWatch Logs

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

> **Important**
>
> Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos

de CloudWatch Logs. Para obtener más información, consulte Información general sobre la administración de permisos de acceso a los recursos de CloudWatch Logs (p. 142) .

Note

CloudWatch Logs no admite directivas de IAM que impidan que los usuarios asignen etiquetas especificadas a grupos de registro mediante el`aws:Resource/key-name`o`aws:TagKeys`Claves de condición. Además, no puede controlar el acceso a la`DescribeLogGroups`mediante el uso de la función`aws:ResourceTag/key-name`Clave de condición Otras acciones de CloudWatch Logs sí admiten el uso de`aws:ResourceTag/key-name`clave de condición para controlar el acceso. Para obtener más información acerca del uso de etiquetas de para controlar el acceso, consulteControl de acceso a los recursos de Amazon Web Services mediante etiquetas.

Este tema cubre lo siguiente:

- Permisos necesarios para usar la consola de CloudWatch (p. 147)
- AWSPolíticas administradas (predefinidas) para CloudWatch Logs (p. 149)
- Ejemplos de políticas administradas por el cliente (p. 149)

A continuación se muestra un ejemplo de una política de permisos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
    ],
      "Resource": [
        "arn:aws:logs:*:*:*"
    ]
  }
 ]
}
```

Esta política tiene una declaración que concede permisos para crear grupos de registros y flujos de registro para cargar eventos de registro a flujos de registro y para mostrar un listado de detalles acerca de los flujos de registro.

El carácter comodín (*) que aparece al final del valor `Resource` significa que la declaración concede permiso para las acciones `logs:CreateLogGroup`, `logs:CreateLogStream`, `logs:PutLogEvents` y `logs:DescribeLogStreams` en cualquier grupo de registros. Para limitar este permiso a un grupo de registros específico, sustituya el carácter comodín (*) en el ARN del recurso con el ARN de grupo de registros específico. Para obtener más información acerca de las secciones de una instrucción de política de IAM, consulteReferencia de elementos de la política de IAMinIAM User Guide. Para ver una lista de todas las acciones de CloudWatch Logs, consulteReferencia de permisos CloudWatch Logs (p. 151).

## Permisos necesarios para usar la consola de CloudWatch

Para que un usuario pueda trabajar con registros de CloudWatch en la consola de CloudWatch, debe tener un conjunto mínimo de permisos que le permitan describir otrosAWSrecursos en suAWSaccount. Para poder usar CloudWatch Logs en la consola de CloudWatch, debe tener permisos de los siguientes servicios:

- CloudWatch
- Registros de CloudWatch
- Amazon ES
- IAM
- Kinesis
- Lambda
- Amazon S3

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para los usuarios con esa política de IAM. Para asegurarse de que esos usuarios puedan seguir utilizando la consola de CloudWatch, asocie también el`CloudWatchReadOnlyAccess`Política administrada al usuario, como se describe enAWSPolíticas administradas (predefinidas) para CloudWatch Logs (p. 149).

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a laAWS CLIo la API de CloudWatch Logs.

A continuación, se enumera el conjunto completo de permisos necesarios para un usuario que no utilice la consola de CloudWatch para administrar suscripciones de registro:

- cloudwatch:getMetricData
- cloudwatch:listMetrics
- logs:cancelExportTask
- logs:createExportTask
- logs:createLogGroup
- logs:createLogStream
- logs:deleteLogGroup
- logs:deleteLogStream
- logs:deleteMetricFilter
- logs:deleteQueryDefinition
- logs:deleteRetentionPolicy
- logs:deleteSubscriptionFilter
- logs:describeExportTasks
- logs:describeLogGroups
- logs:describeLogStreams
- logs:describeMetricFilters
- logs:describeQueryDefinitions
- logs:describeSubscriptionFilters
- logs:filterLogEvents
- logs:getLogEvents
- logs:putMetricFilter
- logs:putQueryDefinition
- logs:putRetentionPolicy
- logs:putSubscriptionFilter
- logs:testMetricFilter

Para un usuario que también utilice la consola para administrar las suscripciones de registro, los siguientes permisos son igualmente necesarios:

- es:describeElasticsearchDomain
- es:listDomainNames
- iam:attachRolePolicy
- iam:createRole
- iam:getPolicy
- iam:getPolicyVersion
- iam:getRole
- iam:listAttachedRolePolicies
- iam:listRoles
- kinesis:describeStreams
- kinesis:listStreams
- lambda:addPermission
- lambda:createFunction
- lambda:getFunctionConfiguration
- lambda:listAliases
- lambda:listFunctions
- lambda:listVersionsByFunction
- lambda:removePermission
- s3:listBuckets

## AWSPolíticas administradas (predefinidas) para CloudWatch Logs

AWS aborda muchos casos de uso comunes proporcionando políticas de IAM independientes creadas y administradas por AWS. Las políticas administradas por AWS conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los siguientes ejemplos deAWSLas políticas administradas por, que puede asociar a los usuarios de su cuenta de, son específicas de CloudWatch Logs:

- CloudWatchLogsFullAccess: concede acceso completo a CloudWatch Logs.
- CloudWatchLogsReadOnlyAccess: concede acceso de solo lectura a CloudWatch Logs.

> **Note**
>
> Para consultar estas políticas de permisos, inicie sesión en la consola de IAM y busque las políticas específicas.

También puede crear sus propias políticas de IAM personalizadas para conceder permisos a las acciones y recursos de CloudWatch Logs. Puede asociar estas políticas personalizadas a los usuarios o grupos de IAM que requieran esos permisos.

## Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que conceden permisos para varias acciones de CloudWatch Logs. Estas políticas funcionan cuando se utiliza la API de registros de CloudWatch Logs,AWSSDK, o elAWS CLI.

Ejemplos



## Ejemplo 1: Permitir acceso completo a CloudWatch Logs

La siguiente política permite a un usuario acceder a todas las acciones de CloudWatch Logs.

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

## Ejemplo 2: Permitir acceso de solo lectura a CloudWatch Logs

AWSproporciona unCloudWatchLogsReadOnlyAccessque permite el acceso de solo lectura a los datos de CloudWatch Logs. Esta política incluye los siguientes permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs:Describe*",
                "logs:Get*",
                "logs:List*",
                "logs:StartQuery",
                "logs:StopQuery",
                "logs:TestMetricFilter",
                "logs:FilterLogEvents"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

## Ejemplo 3: Permitir el acceso a un grupo de registros

La siguiente política permite a un usuario leer y escribir eventos de registro en un grupo de registros especificado.

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

```
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:us-west-2:123456789012:log-group:SampleLogGroupName:*"
      }
   ]
}
```

## Usar directivas de IAM y etiquetado para el control en el nivel de grupo de registros

Puede conceder a los usuarios acceso a determinados grupos de registros al mismo tiempo que les impide tener acceso a otros grupos de registros. Para ello, etiquete sus grupos de registros y utilice políticas de IAM que hagan referencia a esas etiquetas.

Para obtener más información sobre el etiquetado de grupos de registros, consulte EtiquetarlOGgGrupos en Amazon CloudWatch Logs (p. 63).

Al etiquetar grupos de registros, puede conceder una política de IAM a un usuario para permitirle el acceso únicamente a los grupos de registros con una etiqueta determinada. Por ejemplo, la siguiente instrucción de política concede acceso únicamente a los grupos de registros que tienen el valor `Team` para la clave de etiqueta `Green`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs:*"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "logs:ResourceTag/Team": "Green"
                }
            }
        }
    ]
}
```

Para obtener más información acerca del uso de las instrucciones de política de IAM, consulteControl del acceso mediante políticasen laIAM User Guide.

# Referencia de permisos CloudWatch Logs

Puede usar la siguiente tabla como referencia cuando configure Control de acceso (p. 142) y escriba políticas de permisos que vaya a asociar a una identidad de IAM (políticas basadas en identidad). En la tabla figuran las operaciones de las API de CloudWatch Logs y las acciones correspondientes para las que puede conceder permisos para realizar la acción. Las acciones se especifican en el campo `Action` de la política. Para el registro`Resource`, puede especificar el ARN de un grupo de registros o flujo de registros, o especificar`*`para representar todos los recursos de CloudWatch Logs.

Puede utilizarAWSEn sus políticas de CloudWatch Logs para expresar condiciones. Para obtener una lista completa deAWSteclas anchas, consulteAWSClaves de contexto de condición de IAM y globalesen laIAM User Guide.

Note

Para especificar una acción, use el prefijo `logs:` seguido del nombre de operación de API. Por ejemplo:`logs:CreateLogGroup`,`logs:CreateLogStream`, o bien`logs:*`(para todas las acciones de CloudWatch Logs).

Operaciones de la API de CloudWatch Logs y permisos necesarios para las acciones

| Operaciones de la API de CloudWatch Logs | Permisos necesarios (acciones de API) |
|---|---|
| CancelExportTask | `logs:CancelExportTask`<br><br>Necesario para cancelar una tarea de exportación en ejecución o pendiente. |
| CreateExportTask | `logs:CreateExportTask`<br><br>Necesario para exportar datos desde un grupo de registros a un bucket de Amazon S3. |
| CreateLogGroup | `logs:CreateLogGroup`<br><br>Necesario para crear un nuevo grupo de registros. |
| CreateLogStream | `logs:CreateLogStream`<br><br>Necesario para crear un nuevo flujo de registros en un grupo de registros. |
| DeleteDestination | `logs:DeleteDestination`<br><br>Necesario para eliminar un destino de registro y deshabilita los filtros de suscripción al mismo. |
| DeleteLogGroup | `logs:DeleteLogGroup`<br><br>Necesario para eliminar un grupo de registros y todos los eventos de registro asociados. |
| DeleteLogStream | `logs:DeleteLogStream`<br><br>Necesario para eliminar un flujo de registros y todos los eventos de registro asociados. |
| DeleteMetricFilter | `logs:DeleteMetricFilter`<br><br>Necesario para eliminar un filtro de métricas asociado con un grupo de registros. |
| DeleteQueryDefinition | `logs:DeleteQueryDefinition`<br><br>Necesario para eliminar una definición de consulta guardada en CloudWatch Logs Insights. |
| DeleteResourcePolicy | `logs:DeleteResourcePolicy`<br><br>Necesario para eliminar una política de recursos de CloudWatch Logs. |
| DeleteRetentionPolicy | `logs:DeleteRetentionPolicy` |

| Operaciones de la API de CloudWatch Logs | Permisos necesarios (acciones de API) |
|---|---|
| | Necesario para eliminar la política de retención de un grupo de registros. |
| DeleteSubscriptionFilter | `logs:DeleteSubscriptionFilter`<br><br>Necesario para eliminar el filtro de suscripción asociado a un grupo de registros. |
| DescribeDestinations | `logs:DescribeDestinations`<br><br>Necesario para ver todos los destinos asociados a la cuenta. |
| DescribeExportTasks | `logs:DescribeExportTasks`<br><br>Necesario para ver todas las tareas de exportación asociadas a la cuenta. |
| DescribeLogGroups | `logs:DescribeLogGroups`<br><br>Necesario para ver todos los grupos de registro asociados a la cuenta. |
| DescribeLogStreams | `logs:DescribeLogStreams`<br><br>Necesario para ver todos los flujos de registro asociados a un grupo de registros. |
| DescribeMetricFilters | `logs:DescribeMetricFilters`<br><br>Necesario para ver todas las métricas asociadas a un grupo de registros. |
| DescribeQueryDefinitions | `logs:DescribeQueryDefinitions`<br><br>Necesario para ver la lista de definiciones de consulta guardadas en CloudWatch Logs Insights. |
| DescribeQueries | `logs:DescribeQueries`<br><br>Necesario para ver la lista de consultas de CloudWatch Logs Insights programadas, en proceso de ejecución o ejecutadas recientemente. |
| DescribeResourcePolicies | `logs:DescribeResourcePolicies`<br><br>Necesario para ver una lista de políticas de recursos de CloudWatch Logs. |
| DescribeSubscriptionFilters | `logs:DescribeSubscriptionFilters`<br><br>Necesario para ver todos los filtros de suscripción asociados con un grupo de registros. |
| FilterLogEvents | `logs:FilterLogEvents`<br><br>Necesario para ordenar los eventos de registros por patrón de filtro de grupo de registros. |

| Operaciones de la API de CloudWatch Logs | Permisos necesarios (acciones de API) |
|---|---|
| GetLogEvents | `logs:GetLogEvents`<br><br>Necesario para recuperar eventos de registro de un flujo de registros. |
| GetLogGroupFields | `logs:GetLogGroupFields`<br><br>Necesario para recuperar la lista de campos que se incluyen en los eventos de registro de un grupo de registros. |
| GetLogRecord | `logs:GetLogRecord`<br><br>Necesario para recuperar los detalles de un único evento de registro. |
| GetQueryResults | `logs:GetQueryResults`<br><br>Necesario para recuperar los resultados de las consultas de CloudWatch Logs Insights. |
| ListTagsLogGroup | `logs:ListTagsLogGroup`<br><br>Necesario para ver las etiquetas asociadas a un grupo de registros. |
| PutDestination | `logs:PutDestination`<br><br>Necesario para crear o actualizar un flujo de registros de destino (como, por ejemplo, un flujo de Kinesis). |
| PutDestinationPolicy | `logs:PutDestinationPolicy`<br><br>Necesario para crear o actualizar una política de acceso asociada a un destino de registro existente. |
| PutLogEvents | `logs:PutLogEvents`<br><br>Necesario para cargar un lote de eventos de registro en un flujo de registros. |
| PutMetricFilter | `logs:PutMetricFilter`<br><br>Necesario para crear o actualizar un filtro de métricas y asociarlo a un grupo de registros. |
| PutQueryDefinition | `logs:PutQueryDefinition`<br><br>Necesario para guardar una consulta en CloudWatch Logs Insights. |
| PutResourcePolicy | `logs:PutResourcePolicy`<br><br>Necesario para crear una política de recursos de CloudWatch Logs. |

| Operaciones de la API de CloudWatch Logs | Permisos necesarios (acciones de API) |
|---|---|
| PutRetentionPolicy | `logs:PutRetentionPolicy`<br><br>Necesario para establecer el número de días que conservar los eventos de registro (retención) en un grupo de registros. |
| PutSubscriptionFilter | `logs:PutSubscriptionFilter`<br><br>Necesario para crear o actualizar un filtro de suscripción y asociarlo a un grupo de registros. |
| StartQuery | `logs:StartQuery`<br><br>Necesario para iniciar consultas de CloudWatch Logs Insights |
| StopQuery | `logs:StopQuery`<br><br>Necesario para detener una consulta de CloudWatch Logs Insights en curso. |
| TagLogGroup | `logs:TagLogGroup`<br><br>Necesario para añadir o actualizar etiquetas de grupo de registro. |
| TestMetricFilter | `logs:TestMetricFilter`<br><br>Necesario para probar un patrón de filtro frente a una muestra de mensajes de evento de registro. |

# Uso de roles vinculados a servicios para CloudWatch Logs

Amazon CloudWatch LogsAWS Identity and Access Management(IAM)Roles vinculados a servicios. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a CloudWatch Logs. Los roles vinculados a servicios están predefinidos por CloudWatch Logs e incluyen todos los permisos que el servicio requiere para llamar a otrosAWSServicios de en su nombre.

Un rol vinculado a un servicio simplifica la configuración de registros de CloudWatch Logs de porque ya no tendrá que agregar manualmente los permisos necesarios. CloudWatch Logs define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo CloudWatch Logs puede asumir esos roles. Los permisos definidos incluyen la política de confianza y la política de permisos. Esa política de permisos no se puede asociar a ninguna otra entidad de IAM.

Para obtener más información acerca de otros servicios que admiten los roles vinculados a un servicio, consulteAWSServicios que funcionan con IAM. Busque los servicios para los que se indique Sí en la columna Roles vinculados a servicios. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Permisos de roles vinculados a servicios para CloudWatch Logs

usa la función vinculada a servicios denominadaAWSServiceRoleForLogDelivery. CloudWatch Logs utiliza este rol vinculado a servicios para escribir registros directamente en Kinesis Data Firehose. Para obtener más información, consulte Habilitación de registros desdeAWSServicios de (p. 121) .

LaAWSServiceRoleForLogDeliveryLa función vinculada al servicio confía en que los siguientes servicios asuman el rol:

- `CloudWatch Logs`

La política de permisos del rol permite que CloudWatch Logs realice las siguientes acciones en los recursos especificados:

- Acción:`firehose:PutRecord`y`firehose:PutRecordBatch`en todas las transmisiones de Kinesis Data Firehose que tienen una etiqueta con un`LogDeliveryEnabled`con un valor de`True`. Esta etiqueta se adjunta automáticamente a una transmisión de Kinesis Data Firehose cuando crea una suscripción para entregar los registros a Kinesis Data Firehose.

Debe configurar permisos para permitir a una entidad de IAM crear, editar o eliminar la descripción de un rol vinculado a un servicio. Esta entidad puede ser un usuario, un grupo o un rol. Para obtener más información, consulte Permisos de roles vinculados a servicios en la guía del usuario de IAM.

## Creación de un rol vinculado a un servicio de CloudWatch Logs

No es necesario crear manualmente un rol vinculado a un servicio de. Cuando configure los registros para que se envíen directamente a una transmisión de Kinesis Data Firehose en elAWS Management Console, elAWS CLI, o elAWSAPI de, CloudWatch Logs crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando vuelva a configurar registros para que se envíen directamente a un flujo de Kinesis Data Firehose, CloudWatch Logs crea de nuevo el rol vinculado al servicio.

## Edición de un rol vinculado a un servicio para CloudWatch Logs

CloudWatch Logs no le permite editarAWSServiceRoleForLogDelivery, o cualquier otro rol vinculado al servicio, después de crearlo. No puede cambiar el nombre de la función porque varias entidades pueden hacer referencia a ella. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

## Eliminación de un rol vinculado a servicios para CloudWatch Logs

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio CloudWatch Logs utiliza el rol cuando intenta eliminar los recursos, es posible que no se pueda borrar. En tal caso, espere unos minutos e intente de nuevo la operación.

### Para eliminar los recursos de CloudWatch Logs utilizados por elAWSServiceRoleForLogDeliveryRol vinculado al servicio de

- Deje de enviar registros directamente a los flujos de Kinesis Data Firehose.

### Para eliminar manualmente el rol vinculado a un servicio mediante IAM

Utilice la consola de IAM, elAWS CLI, o elAWSAPI para eliminar laAWSServiceRoleForLogDeliveryRol vinculado a servicios. Para obtener más información, consulteEliminar un rol vinculado a un servicio

### Regiones admitidas para los roles vinculados a servicios de CloudWatch Logs

CloudWatch Logs admite el uso de roles vinculados a servicios en todas las instancias deAWSRegiones en las que el servicio está disponible. Para obtener más información, consulteCloudWatch Logs regiones y puntos finales.

# Conformidadvalidación de Amazon CloudWatch Logs

Auditores externos evalúan la seguridad y la conformidad de Amazon CloudWatch LogsAWSProgramas de conformidad. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de los servicios de AWS en el ámbito de programas de conformidad específicos, consulte AWS Services in Scope by Compliance Program (Servicios en el ámbito de programas de conformidad). Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad en relación con la conformidad al utilizar Amazon CloudWatch Logs depende de la confidencialidad de los datos, los objetivos de conformidad de su empresa y de la legislación y los reglamentos aplicables.AWSproporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA : en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglasen la AWS Config Guía para desarrolladores–AWS Config; evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

# Resiliencia de Amazon CloudWatch Logs

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

# Información de infraestructurasSeguridad en Amazon CloudWatch Logs

Como servicio gestionado, Amazon CloudWatch Logs está protegido por laAWSSeguridad de red globales de que se describen en la sección deAmazon Web Services: Información general sobre procesos de seguridadDocumento técnico.

UtilizaAWSpara obtener acceso a Amazon CloudWatch Logs a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Le recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Uso de CloudWatch LogsiVPCendpoints

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar suAWS, puede establecer una conexión privada entre su VPC y CloudWatch Logs. Puede utilizar esta conexión para enviar registros a CloudWatch Logs sin enviarlos a través de Internet.

Amazon VPC es unAWSServicio de que se puede utilizar para lanzarAWSen una red virtual que haya definido. 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 Logs, debe definir unapunto de enlace de la VPC de la interfazpara CloudWatch Logs 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 Logs 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, consulteQué es Amazon VPCen laGuía 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, consulteNuevo — AWS PrivateLink : paraAWSServicios.

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 Logs actualmente admite puntos de enlace de la VPC en las regiones siguientes:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Hong Kong)
- 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)
- AWSGovCloud (EE. UU. Este)
- AWSGovCloud (EE. UU. Oeste)

# Creación de una VPCendpoint para CloudWatch Logs

Para comenzar a utilizar CloudWatch Logs con su VPC, cree un punto de enlace de la VPC de tipo interfaz para CloudWatch Logs. El servicio que debe elegir es com.amazonaws.*región*.logs. No es necesario cambiar ninguna configuración de CloudWatch Logs. Para obtener más información, consulte Creación de un punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

# ProbarconnecciónbetweenyNuestros VPC y CloudWatch Logs

Una vez creado el punto de enlace, puede probar la conexión.

Para probar la conexión entre la VPC y el punto de enlace de CloudWatch Logs

1. Connect a una instancia de Amazon EC2 que resida en su VPC. Para obtener información acerca de las conexiones, consulteConexión con la instancia de LinuxorConexión con la instancia de Windowsen la documentación de Amazon EC2.
2. Desde la instancia, utilice la AWS CLI para crear una entrada de registro en uno de sus grupos de registros existentes.

   En primer lugar, cree un archivo JSON con un evento de registro. La marca temporal se debe especificar como el número de milisegundos después del 1 de enero de 1970 00:00:00 UTC.

   ```
   [
     {
       "timestamp": 1533854071310,
       "message": "VPC Connection Test"
     }
   ]
   ```

   A continuación, utilice el comando `put-log-events` para crear la entrada de registro:

   ```
   aws logs put-log-events --log-group-name LogGroupName --log-stream-name LogStreamName
    --log-events file://JSONFileName
   ```

   Si la respuesta al comando incluye `nextSequenceToken`, el comando se ha realizado correctamente y el punto de enlace de la VPC funciona.

# Controlaccess ayNuestra VPC de CloudWatch Logsendpoint

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 las políticas de usuario de IAM ni 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 Logs. Esta política permite los usuarios que se conectan a CloudWatch Logs a través de la VPC crear flujos de registro y enviar registros a CloudWatch Logs, y les impide realizar otras acciones de CloudWatch Logs.

```
{
  "Statement": [
    {
      "Sid": "PutOnly",
      "Principal": "*",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

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

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 Logs, elijaCreación de un punto de enlace. A continuación, seleccione com.amazonaws.***región***.logs y elija Create endpoint (Crear punto de enlace).
4. Seleccione el punto de enlace com.amazonaws.***región***.logs 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.

# Support con VPCcontextkeys

Los CloudWatch Logs`aws:SourceVpc`y`aws:SourceVpce`que pueden limitar el acceso a VPC específicas o puntos de enlace de la VPC específicos. Estas claves funcionan solo cuando el usuario utiliza puntos de enlace de la VPC. Para obtener más información, consulteClaves disponibles para algunos serviciosen laGuía del usuario de IAM.

# API de registro de Amazon CloudWatch LogscALL ENAWS CloudTrail

Amazon CloudWatch Logs se integra conAWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un usuario deAWSen CloudWatch Logs. CloudTrail captura las llamadas a la API realizadas por o en nombre de suAWSaccount. 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 Logs. 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 los registros 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 Logs, 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 laAWS CloudTrailGuía del usuario.

Temas



## Registros de CloudWatchinformation en CloudTrail

CloudTrail está habilitado en suAWSal crearla. Cuando se produce una actividad de eventos compatible en CloudWatch Logs, dicha actividad se registra en un evento de CloudTrail junto con otros eventos deAWSeventos de servicios enHistorial 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 laAWS, incluidos los eventos de CloudWatch Logs, 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 laAWSy entrega los archivos log al bucket de Amazon S3 que se especifique. Además, puede configurar otrosAWSPara analizar 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

Mediante los registros de CloudWatch Logs admite el registro de las siguientes acciones como eventos en los archivos de log de Cloud

- CancelExportTask
- CreateExportTask
- CreateLogGroup
- CreateLogStream
- DeleteDestination
- DeleteLogGroup
- DeleteLogStream
- DeleteMetricFilter
- DeleteRetentionPolicy
- DeleteSubscriptionFilter
- PutDestination
- PutDestinationPolicy
- PutMetricFilter
- PutResourcePolicy
- PutRetentionPolicy
- PutSubscriptionFilter
- StartQuery
- StopQuery
- TestMetricFilter

Solo los elementos de solicitud se registran en CloudTrail para estas acciones de la API de CloudWatch Logs:

- DescribeDestinations
- DescribeExportTasks
- DescribeLogGroups
- DescribeLogStreams
- DescribeMetricFilters
- DescribeQueries
- DescribeResourcePolicies
- DescribeSubscriptionFilters
- GetLogGroupFields
- GetLogRecord

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.

# Descripción delOGfileentries

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 muestra un usuario que ha llamado a los registros de CloudWatch LogsCreateExportTaskaction.

```
{
        "eventVersion": "1.03",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/someuser",
            "accountId": "123456789012",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "someuser"
        },
        "eventTime": "2016-02-08T06:35:14Z",
        "eventSource": "logs.amazonaws.com",
        "eventName": "CreateExportTask",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "aws-sdk-ruby2/2.0.0.rc4 ruby/1.9.3 x86_64-linux Seahorse/0.1.0",
        "requestParameters": {
            "destination": "yourdestination",
            "logGroupName": "yourloggroup",
            "to": 123456789012,
            "from": 0,
            "taskName": "yourtask"
        },
        "responseElements": {
            "taskId": "15e5e534-9548-44ab-a221-64d9d2b27b9b"
        },
        "requestID": "1cd74c1c-ce2e-12e6-99a9-8dbb26bd06c9",
        "eventID": "fd072859-bd7c-4865-9e76-8e364e89307c",
        "eventType": "AwsApiCall",
        "apiVersion": "20140328",
        "recipientAccountId": "123456789012"
}
```

# Registros de CloudWatchacaballeroreference

> **Important**
>
> Esta referencia es para el agente de CloudWatch Logs anterior, que se encuentra en vías de ser declarado obsoleto. Le recomendamos que, en su lugar, utilice el agente de CloudWatch unificado. Para obtener más información acerca de ese agente de, consulteRecopilación de métricas y registros de instancias de Amazon EC2 y servidores locales con el agente de CloudWatch.

El agente de CloudWatch Logs proporciona una forma automatizada de enviar datos de registro a CloudWatch Logs desde instancias Amazon EC2. El agente incluye los componentes siguientes:

- Un complemento a laAWS CLIque envía los datos de registro a CloudWatch Logs.
- Un script (demonio) que inicia el proceso para enviar datos a CloudWatch Logs.
- Un trabajo cron que garantiza que el demonio esté siempre en ejecución.

## Agenteconfiguraciónfile

El archivo de configuración del agente de CloudWatch Logs describe la información que necesita dicho agente de CloudWatch Logs. La sección [general] del archivo de configuración del agente define las configuraciones comunes que se aplican a todos los flujos de registro. La sección [logstream] define la información necesaria para enviar un archivo local a un flujo de registros remoto. Puede tener más de una sección [logstream], pero cada una debe tener un nombre único en el archivo de configuración, por ejemplo, [logstream1], [logstream2], etc. El valor [logstream] junto con la primera línea de datos en el archivo de registro define la identidad del archivo de registro.

```
[general]
state_file = value
logging_config_file = value
use_gzip_http_content_encoding = [true | false]

[logstream1]
log_group_name = value
log_stream_name = value
datetime_format = value
time_zone = [LOCAL|UTC]
file = value
file_fingerprint_lines = integer | integer-integer
multi_line_start_pattern = regex | {datetime_format}
initial_position = [start_of_file | end_of_file]
encoding = [ascii|utf_8|..]
buffer_duration = integer
batch_count = integer
batch_size = integer

[logstream2]
...
```

state_file

Especifica dónde se almacena el archivo de estado.

logging_config_file

(Opcional) Especifica la ubicación del archivo de configuración de registro del agente. Si no especifica aquí un archivo de configuración de registro de agente, se utiliza el archivo de configuración. La ubicación predeterminada del archivo es `/var/awslogs/etc/awslogs.conf` si instaló el agente con un script y es `/etc/awslogs/awslogs.conf` si instaló el agente con rpm. El archivo se encuentra en formato de archivo de configuración de Python (https://docs.python.org/2/library/logging.config.html#logging-config-fileformat). Las funciones de registro con los nombres siguientes se pueden personalizar.

```
cwlogs.push
cwlogs.push.reader
cwlogs.push.publisher
cwlogs.push.event
cwlogs.push.batch
cwlogs.push.stream
cwlogs.push.watcher
```

El ejemplo siguiente cambia el nivel de lector y editor a WARNING mientras el valor por defecto es INFO.

```
[loggers]
keys=root,cwlogs,reader,publisher

[handlers]
keys=consoleHandler

[formatters]
keys=simpleFormatter

[logger_root]
level=INFO
handlers=consoleHandler

[logger_cwlogs]
level=INFO
handlers=consoleHandler
qualname=cwlogs.push
propagate=0

[logger_reader]
level=WARNING
handlers=consoleHandler
qualname=cwlogs.push.reader
propagate=0

[logger_publisher]
level=WARNING
handlers=consoleHandler
qualname=cwlogs.push.publisher
propagate=0

[handler_consoleHandler]
class=logging.StreamHandler
level=INFO
formatter=simpleFormatter
args=(sys.stderr,)

[formatter_simpleFormatter]
```

```
format=%(asctime)s - %(name)s - %(levelname)s - %(process)d - %(threadName)s -
 %(message)s
```

use_gzip_http_content_encoding

Cuando se establece en true (predeterminado), permite la codificación de contenido gzip http para enviar cargas comprimidas a CloudWatch Logs. Esto reduce la utilización de la CPU, reduce NetworkOut y reduce la latencia de Put. Para deshabilitar esta característica, agregueuse_gzip_http_content_encoding = falsea la[general de]del archivo de configuración del agente de CloudWatch Logs y, a continuación, reinicie el agente.

> **Note**
>
> Esta configuración solo está disponible en la versión 1.3.3 o posterior de awscli-cwlogs.

log_group_name

Especifica el grupo de registro de destino. Un grupo de registro se crea automáticamente si no existe todavía. Los nombres de grupo de registros puede tener de 1 a 512 caracteres de longitud. Entre los caracteres permitidos se incluyen a-z, A-Z, 0-9, "_" (carácter de subrayado), "-" (guion), "/" (barra diagonal) y "." (punto).

log_stream_name

Especifica el flujo de registro de destino. Puede usar una cadena literal, variables predefinidas ({instance_id}, {hostname} y {ip_address}), o una combinación de ellas para definir el nombre del flujo de registro. Un flujo de registro se crea automáticamente si no existe todavía.

datetime_format

Especifica cómo se extrae la marca temporal de los registros. La marca temporal se utiliza para recuperar eventos de registro y generar métricas. Se utiliza la hora actual para cada evento de registro si no se proporciona datetime_format. Si el valor de datetime_format proporcionado no es válido para un mensaje de registro determinado, se utiliza la marca temporal (analizada correctamente) del último evento de registro. Si no existen eventos de registro anteriores, se utiliza la hora actual.

Los códigos datetime_format comunes se enumeran a continuación. También puede utilizar cualquier código datetime_format que admita Python, datetime.strptime (). El desfase de la zona horaria (%z) también se admite aunque no se ha admitido hasta python 3.2, [+ -] HHMM sin dos puntos (:). Para obtener más información, consulte strftime() and strptime() Behavior.

%y: Año sin siglo como un número decimal rellenado con ceros. 00, 01, ..., 99

%Y: Año con siglo como número decimal. 1970, 1988, 2001, 2013

%b: : mes como nombre abreviado de configuración regional. Ene, Feb, ..., Dic (es_ES);

%B: : mes como nombre completo de configuración regional. enero, febrero,..., diciembre (es_ES);

%m: mes como número decimal relleno con ceros. 01, 02, ..., 12

%d: : día del mes como número decimal relleno con ceros. 01, 02, ..., 31

%H: Hora (formato de 24 horas) como número decimal rellenado con ceros. 00, 01, ..., 23

%I: Hora (formato de 12 horas) como número decimal rellenado con ceros. 01, 02, ..., 12

%p: Equivalente de la configuración regional a AM o PM.

%M: : minutos como número decimal relleno con ceros. 00, 01, ..., 59

%S: : segundos como número decimal relleno con ceros. 00, 01, ..., 59

%f: : microsegundos como número decimal, rellenos con ceros a la izquierda. 000000, ..., 999999

%z: Desfase respecto a UTC en la forma +HHMM o -HHMM. +0000, -0400, +1030

Formatos de ejemplo:

```
Syslog: '%b %d %H:%M:%S', e.g. Jan 23 20:59:29

Log4j: '%d %b %Y %H:%M:%S', e.g. 24 Jan 2014 05:00:00

ISO8601: '%Y-%m-%dT%H:%M:%S%z', e.g. 2014-02-20T05:20:20+0000
```

time_zone

Especifica la zona horaria de la marca temporal de evento de registro. Los dos valores admitidos son UTC y LOCAL. El valor predeterminado es LOCAL, que se utiliza en caso de que la zona horaria no se pueda determinar a partir de datetime_format.

file

Especifica los archivos de registro que desea enviar a CloudWatch Logs. File puede apuntar a un archivo específico o a varios archivos (utilizando comodines como /var/log/system.log*). Solo se envía el último archivo a CloudWatch Logs en función de la hora de modificación del archivo. Le recomendamos que utilice comodines para especificar una serie de archivos del mismo tipo, como access_log.2014-06-01-01, access_log.2014-06-01-02, etc., pero no varios tipos de archivos, como por ejemplo access_log_80 y access_log_443. Para especificar varios tipos de archivos, agregue otra entrada de flujo de registro al archivo de configuración para que cada tipo de archivo de registro vaya a un flujo de registros distinto. Los archivos comprimidos no son compatibles.

file_fingerprint_lines

Especifica el intervalo de líneas para identificar un archivo. Los valores admitidos son un número o dos números delimitados por guion, como, por ejemplo, "1", "2-5". El valor predeterminado es "1" de modo que se utiliza la primera línea para calcular la huella. Las líneas de huella no se envían a CloudWatch Logs, a menos que todas las líneas especificadas estén disponibles.

multi_line_start_pattern

Especifica el patrón para identificar el inicio de un mensaje de registro. Un mensaje de registro consta de una línea que coincide con el patrón y de líneas siguientes que no coinciden con el patrón. Los valores válidos son expresiones regulares o {datetime_format}. Cuando se utiliza {datetime_format}, se debe especifica la opción datetime_format. El valor predeterminado es "^[^\s]" de modo que cualquier línea que comience con un carácter sin espacios en blanco cierra el mensaje de registro anterior y comienza un nuevo mensaje de registro.

initial_position

Especifica dónde empezar a leer datos (start_of_file o end_of_file). El valor predeterminado es start_of_file. Se utiliza únicamente si no se almacena de forma persistente ningún estado para dicho flujo de registro.

encoding

Especifica la codificación del archivo de registro, de modo que el archivo se pueda leer correctamente. El valor predeterminado es utf_8. Se pueden utilizar aquí las codificaciones compatibles con Python codecs.decode().

> Warning
>
> La especificación de una codificación incorrecta podría provocar pérdida de datos porque los caracteres que no se pueden descodificar se sustituirán por otro carácter.

A continuación se muestran las codificaciones comunes:

```
ascii, big5, big5hkscs, cp037, cp424, cp437, cp500, cp720, cp737, cp775,
cp850, cp852, cp855, cp856, cp857, cp858, cp860, cp861, cp862, cp863, cp864,
```

```
cp865, cp866, cp869, cp874, cp875, cp932, cp949, cp950, cp1006, cp1026,
cp1140, cp1250, cp1251, cp1252, cp1253, cp1254, cp1255, cp1256, cp1257,
cp1258, euc_jp, euc_jis_2004, euc_jisx0213, euc_kr, gb2312, gbk, gb18030,
hz, iso2022_jp, iso2022_jp_1, iso2022_jp_2, iso2022_jp_2004, iso2022_jp_3,
iso2022_jp_ext, iso2022_kr, latin_1, iso8859_2, iso8859_3, iso8859_4,
iso8859_5, iso8859_6, iso8859_7, iso8859_8, iso8859_9, iso8859_10,
iso8859_13, iso8859_14, iso8859_15, iso8859_16, johab, koi8_r, koi8_u,
mac_cyrillic, mac_greek, mac_iceland, mac_latin2, mac_roman, mac_turkish,
ptcp154, shift_jis, shift_jis_2004, shift_jisx0213, utf_32, utf_32_be,
utf_32_le, utf_16, utf_16_be, utf_16_le, utf_7, utf_8, utf_8_sig
```

buffer_duration

Especifica la duración para agrupar en lotes eventos de registro. El valor mínimo es 5000ms y valor predeterminado es 5000ms.

batch_count

Especifica el número máximo de eventos de registro en un lote, hasta 10 000. El valor predeterminado es 10 000.

batch_size

Especifica el tamaño máximo de eventos de registro en un lote, en bytes, hasta 1 048 576 bytes. El valor predeterminado es de 1 048 576 bytes. Este tamaño se calcula como la suma de todos los mensajes de eventos en UTF-8, más 26 bytes para cada evento de registro.

# Uso de CloudWatch Logsagente con HTTPproxies

Puede utilizar el agente de CloudWatch Logs con servidores proxy HTTP.

Note

Los servidores proxy HTTP se admiten en awslogs-agent-setup.py versión 1.3.8 o posterior.

Para utilizar el agente de CloudWatch Logs con servidores proxy HTTP

1. Aplique alguna de las siguientes acciones:

   a. Para una nueva instalación del agente de CloudWatch Logs, ejecute los siguientes comandos:

   ```
   curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-
   setup.py -O
   ```

   ```
   sudo python awslogs-agent-setup.py --region us-east-1 --http-proxy http://your/
   proxy --https-proxy http://your/proxy --no-proxy 169.254.169.254
   ```

   Para mantener el acceso al servicio de metadatos de Amazon EC2 en instancias EC2, utilice—no-proxy 169.254.169.254(recomendado). Para obtener más información, consulte el tema Metadatos de instancia y datos de usuario en la Guía del usuario de instancias de Linux de Amazon EC2.

   En el valor de `http-proxy` y `https-proxy`, especifique la URL completa.

   b. Para una instalación existente del agente de CloudWatch Logs, edite /var/awslogs/etc/proxy.conf, y agregue sus servidores proxy:

   ```
   HTTP_PROXY=
   HTTPS_PROXY=
   ```

```
NO_PROXY=
```

2. Reinicie el agente para que los cambios surtan efecto:

```
sudo service awslogs restart
```

Si está utilizando Amazon Linux 2, utilice el comando siguiente para reiniciar el agente:

```
sudo service awslogsd restart
```

# Compartimentación de CloudWatch Logsacaballeroconfiguraciónfiles

Si utiliza la versión 1.3.8 o posterior de awslogs-agent-setup.py con awscli-cwlogs 1.3.3 o una versión posterior, puede importar diferentes configuraciones de flujo para diversos componentes de forma independiente entre sí mediante la creación de archivos de configuración adicionales en el directorio /var/awslogs/etc/config/. Cuando se inicia el agente de CloudWatch Logs, se incluye cualquier configuración de flujo en estos archivos de configuración adicionales. Las propiedades de configuración en la sección [general] deben definirse en el archivo de configuración principal (/var/awslogs/etc/awslogs.conf) y se omiten en los archivos de configuración adicionales que se encuentran en /var/awslogs/etc/config/.

Si no dispone de un directorio /var/awslogs/etc/config/ dado que ha instalado el agente con rpm, puede utilizar en su lugar el directorio /etc/awslogs/config/.

Reinicie el agente para que los cambios surtan efecto:

```
sudo service awslogs restart
```

Si está utilizando Amazon Linux 2, utilice el comando siguiente para reiniciar el agente:

```
sudo service awslogsd restart
```

# Registros de CloudWatchaPreguntas frecuentes sobre gent

¿Qué tipo de rotaciones de archivo se admiten?

Se admiten los siguientes mecanismos de rotación de archivos:

- Cambiar el nombre de los archivos de registro existentes por un sufijo numérico y, a continuación, volver a crear el archivo de registro vacío original. Por ejemplo, el nombre de /var/log/syslog.log se cambia a /var/log/syslog.log.1. Si ya existe /var/log/syslog.log.1 de una rotación anterior, se cambia el nombre a /var/log/syslog.log.2.
- Truncar el archivo de registro original en vigor después de crear una copia. Por ejemplo, /var/log/syslog.log se copia a /var/log/syslog.log.1 y /var/log/syslog.log se trunca. Podría haber pérdida de datos en este caso, por tanto tenga cuidado a la hora de utilizar este mecanismo de rotación de archivo.
- Creación de un nuevo archivo con un patrón común como el antiguo. Por ejemplo, se mantiene /var/log/syslog.log.2014-01-01 y se crea /var/log/syslog.log.2014-01-02.

La huella (ID de origen) del archivo se calcula mediante el hash de la clave del flujo de registro y la primera línea de contenido del archivo. Para omitir este comportamiento, se puede utilizar la opción file_fingerprint_lines. Cuando se produce la rotación de archivos, el nuevo archivo se supone que tiene nuevo contenido y el archivo antiguo no se supone que tenga contenido añadido; el agente envía el nuevo archivo una vez que termine la lectura del antiguo.

¿Cómo puedo determinar la versión del agente que estoy utilizando?

Si utilizó un script de configuración para instalar el agente de CloudWatch Logs, puede utilizar/var/awslogs/bin/awslogs-version.shPara comprobar la versión del agente que utiliza. Imprime la versión del agente y sus dependencias principales. Si utilizó yum para instalar el agente de CloudWatch Logs, puede utilizar«yum info awslogs»y«yum info aws-cli-plugin-cloudwatch-logs»para comprobar la versión del agente y el complemento CloudWatch Logs.

¿Cómo se convierten las entradas de registro a eventos de registro?

Los eventos de registro contienen dos propiedades: la marca temporal de cuando se produjo el evento y el mensaje de registro sin procesar. De forma predeterminada, cualquier línea que comience con un carácter sin espacios en blanco cierra el mensaje de registro anterior si lo hay y comienza un nuevo mensaje de registro. Para anular este comportamiento, se puede usar multi_line_start_pattern y todas las líneas que coincidan con el patrón inician un nuevo mensaje de registro. El patrón podría ser cualquier regex o "{datetime_format}". Por ejemplo, si la primera línea de cada mensaje de registro contiene una marca de tiempo como '2014-01-02T 13:13:01 Z', entonces elmulti_line_start_patternse puede establecer en '\ d {4} -\ d {2} -\ d {2} T\ d {2}:\ d {2}:\ d {2} Z'. Para simplificar la configuración, la variable "{datetime_format}" variable se puede utilizar si se especifica datetime_format option. Para el mismo ejemplo, si datetime_format se establece en "%Y-%m-%dT%H:%M:%S%z", entonces el patrón multi_line_start_pattern podría ser sencillamente "{datetime_format}".

Se utiliza la hora actual para cada evento de registro si no se proporciona datetime_format. Si el valor de datetime_format proporcionado no es válido para un mensaje de registro determinado, se utiliza la marca temporal (analizada correctamente) del último evento de registro. Si no existen eventos de registro anteriores, se utiliza la hora actual. Se registra un mensaje de advertencia cuando un evento de registro utiliza la hora actual o la hora del evento de registro anterior.

Las marcas temporales se utilizan para recuperar eventos de registro y generar métricas, por lo que si especifica el formato equivocado, los eventos de registro no podrían recuperarse y podrían generar métricas erróneas.

¿Cómo se agrupan en lotes los eventos de registro?

Un lote se completa y se publica cuando cumple alguna de las siguientes condiciones:

1. La cantidad de tiempo de buffer_duration que ha transcurrido desde que se agregó el primer evento de registro.
2. Se ha acumulado un valor inferior a batch_size para eventos de registro, pero al agregar el nuevo evento de registro se supera el valor de batch_size.
3. El número de eventos de registro ha alcanzado el valor batch_count.
4. Los eventos de registro del lote no abarcan más de 24 horas, pero al añadir el nuevo evento de registro se supera la restricción de 24 horas.

¿Qué provocaría la omisión o el truncamiento de las entradas de registro, los eventos de registro o los lotes?

Para seguir la restricción de la operación `PutLogEvents`, los siguientes problemas podrían provocar la omisión de un evento de registro o lote.

> Note
>
> El agente de CloudWatch Logs escribe una advertencia en su registro cuando se omiten datos.

1. Si el tamaño de un evento de registro es superior a 256 KB, el evento de registro se omitirá por completo.

2. Si la marca temporal del evento de registro es de más de 2 horas en el futuro, se omitirá el evento de registro.
3. Si la marca temporal del evento de registro es de más de 14 días en el pasado, se omitirá el evento de registro.
4. Si cualquier evento de registro es más antiguo que el periodo de retención del grupo de registro, se omitirá todo el lote.
5. Si el lote de eventos de registro en una solicitud `PutLogEvents` única abarca más de 24 horas, la operación `PutLogEvents` falla.

¿Provoca la parada del agente la pérdida de datos/duplicados?

No siempre y cuando el archivo de estado esté disponible y no se haya producido la rotación de ningún archivo desde la última ejecución. El agente de CloudWatch Logs puede iniciarse desde donde se paró y continuar enviando los datos de registro.

¿Puedo señalar a diferentes archivos de registro desde el mismo host o diferentes al mismo flujo de registro?

No se admite configurar varias fuentes de registro para enviar datos a un único flujo de registro.

¿Qué llamadas al API realiza el agente (o qué acciones debo añadir a mi política de IAM)?

El agente CloudWatch Logs requiere`CreateLogGroup`,`CreateLogStream`,`DescribeLogStreams`, y`PutLogEvents`operaciones. Si está utilizando el último agente, no es necesario `DescribeLogStreams`. Consulte la política de IAM de ejemplo a continuación.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource": [
      "arn:aws:logs:*:*:*"
    ]
  }
 ]
}
```

No deseo que el agente de CloudWatch Logs cree grupos de registro o flujos de registro de forma automática. ¿Cómo puedo evitar que el agente vuelva a crear grupos de registro y flujos de registro?

En la política de IAM, puede limitar el agente únicamente a las siguientes operaciones:`DescribeLogStreams`,`PutLogEvents`.

Antes de revocar los permisos `CreateLogStream` y `CreateLogGroup` del agente, asegúrese de crear los grupos de registro y las secuencias de registro que desee que utilice el agente. El agente de registros no puede crear secuencias de registro en un grupo de registros que haya creado a menos que tenga los permisos `CreateLogStream` y `CreateLogGroup`.

¿Qué registros debería examinar durante la resolución de problemas?

El registro del agente de instalación se encuentra en `/var/log/awslogs-agent-setup.log` y el registro del agente, en `/var/log/awslogs.log`.

# Monitoreo con métricas de CloudWatch

CloudWatch Logs envía métricas a Amazon CloudWatch cada minuto.

## Métricas de CloudWatch Logs

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

| Métrica | Descripción |
| --- | --- |
| `CallCount` | El número de operaciones especificadas de API realizadas en su cuenta.<br><br>`CallCount`es una métrica de uso del servicio CloudWatch Logs. Para obtener más información, consulte Métricas de uso del servicio CloudWatch Logs (p. 174) .<br><br>Dimensiones válidas: Clase, Recurso, Servicio, Tipo<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |
| `DeliveryErrors` | El número de eventos de registro para los que CloudWatch Logs ha recibido un error al reenviar los datos al destino de la suscripción.<br><br>Dimensiones válidas: LogGroupName, DestinationType, FilterName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |
| `DeliveryThrottling` | El número de eventos de registro a los que ha aplicado una limitación de CloudWatch Logs al reenviar los datos al destino de la suscripción.<br><br>Dimensiones válidas: LogGroupName, DestinationType, FilterName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |
| `ErrorCount` | El número de operaciones de API realizadas en su cuenta que han producido errores.<br><br>`ErrorCount`es una métrica de uso del servicio CloudWatch Logs. Para obtener más información, consulte Métricas de uso del servicio CloudWatch Logs (p. 174) .<br><br>Dimensiones válidas: Clase, Recurso, Servicio, Tipo<br><br>Estadísticas válidas: Sum |

| Métrica | Descripción |
| --- | --- |
| | Unidades: Ninguno |
| `ForwardedBytes` | El nombre de eventos de registro en bytes comprimidos reenviados al destino de la suscripción.<br><br>Dimensiones válidas: LogGroupName, DestinationType, FilterName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Bytes |
| `ForwardedLogEvents` | El número de eventos de registro en bytes comprimidos reenviados al destino de la suscripción.<br><br>Dimensiones válidas: LogGroupName, DestinationType, FilterName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |
| `IncomingBytes` | El volumen de eventos de registro en bytes descomprimidos cargados en CloudWatch Logs. Cuando se usa con la dimensión `LogGroupName`, es el volumen de eventos de registro en bytes descomprimidos cargados en el grupo de registros.<br><br>Dimensiones válidas: LogGroupName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Bytes |
| `IncomingLogEvents` | El número de eventos de registro cargados en CloudWatch Logs. Cuando se usa con la dimensión `LogGroupName`, es el número de eventos de registro cargados en el grupo de registros.<br><br>Dimensiones válidas: LogGroupName<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |
| `ThrottleCount` | El número de operaciones de API realizadas en su cuenta que se han limitado debido a las cuotas de uso.<br><br>`ThrottleCount`es una métrica de uso del servicio CloudWatch Logs. Para obtener más información, consulte Métricas de uso del servicio CloudWatch Logs (p. 174) .<br><br>Dimensiones válidas: Clase, Recurso, Servicio, Tipo<br><br>Estadísticas válidas: Sum<br><br>Unidades: Ninguno |

# Dimensiones de las métricas de CloudWatch Logs

Las dimensiones que puede utilizar con las métricas de CloudWatch Logs se indican a continuación.

| Dimensión | Descripción |
|---|---|
| `LogGroupName` | El nombre del grupo de registros de CloudWatch Logs para el que se muestran métricas. |
| `DestinationType` | El destino de la suscripción para los datos de CloudWatch Logs, que puedeAWS Lambda, Amazon Kinesis Data Streams o Amazon Kinesis Data Firehose. |
| `FilterName` | El nombre del filtro de suscripción que reenvía datos desde el grupo de logs al destino. convierte automáticamente el nombre del filtro de suscripción a ASCII y todos los caracteres no admitidos se reemplazan por un signo de interrogación (?). |

# Métricas de uso del servicio CloudWatch Logs

CloudWatch Logs envía métricas a CloudWatch que rastrean el uso de las operaciones de la API CloudWatch Logs. Estas métricas corresponden a las cuotas de servicio de AWS. El seguimiento de estas métricas puede ayudarle a administrar sus cuotas de forma proactiva. Para obtener más información, consulteMétricas de integración y uso de cuotas de servicio.

Por ejemplo, puede realizar un seguimiento de`ThrottleCounto` establezca una alarma en esa métrica. Si el valor de esta métrica aumenta, debe considerar la posibilidad de solicitar un aumento de cuota para la operación API que se está limitando. Para obtener más información acerca de las cuotas de servicio de CloudWatch Logs, consulteCuotas de CloudWatch Logs (p. 176).

CloudWatch Logs publica métricas de uso de cuotas de servicio cada minuto en el`AWS/Usage`y`AWS/Logs`Espacios de nombres.

En la siguiente tabla se muestran las métricas de uso de servicios publicadas por CloudWatch Logs. Estas métricas no tienen una unidad especificada. La estadística más útil para estas métricas es`SUM`, que representa el recuento total de operaciones para el periodo de 1 minuto.

Cada una de estas métricas se publica con valores para todos los`Service`,`Class`,`Type`, y`Resource`Dimensiones válidas. También se publican con una sola dimensión llamada`Account Metrics`. Usar`Account Metrics`para ver la suma de métricas para todas las operaciones de API de su cuenta. Utilice las otras dimensiones y especifique el nombre de una operación de API para el`Resource`para encontrar las métricas de esa API en particular.

Métricas

| Métrica | Descripción |
|---|---|
| `CallCount` | El número de operaciones especificadas realizadas en su cuenta.<br><br>`CallCount`se publica tanto en el`AWS/Usage`y`AWS/Logs`Espacios de nombres. |
| `ErrorCount` | El número de operaciones de API realizadas en su cuenta que han producido errores.<br><br>`ErrorCount`se publica solo en el`AWS/Logs`. |
| `ThrottleCount` | El número de operaciones de API realizadas en su cuenta que se han limitado debido a las cuotas de uso.<br><br>`ThrottleCount`se publica solo en el`AWS/Logs`. |

Dimensiones

| Dimensión | Descripción |
| --- | --- |
| `Account metrics` | Utilice esta dimensión para obtener una suma de la métrica en todas las API de CloudWatch Logs.<br><br>Si desea ver las métricas de una API en particular, utilice las otras dimensiones enumeradas en esta tabla y especifique el nombre de la API como el valor de`Resource`. |
| `Service` | El nombre del servicio de AWS que contiene el recurso. Para las métricas de uso de CloudWatch Logs, el valor de esta dimensión es`Logs`. |
| `Class` | La clase de recurso del que se realiza el seguimiento. Las métricas de uso de la API de CloudWatch Logs utilizan esta dimensión con un valor de`None`. |
| `Type` | El tipo de recurso del que se realiza el seguimiento. Actualmente, cuando la dimensión de `Service` es `Logs`, el único valor válido para `Type` es `API`. |
| `Resource` | El nombre de la operación de la API. Los valores válidos incluyen todos los nombres de operaciones de API que se enumeran enActions. Por ejemplo, `PutLogEvents` |

# Cuotas de CloudWatch Logs

En las siguientes tablas se proporcionan las cuotas de servicio predeterminados, las que también se conocen como límites, para CloudWatch Logs para unaAWSaccount. La mayoría de estas cuotas de servicio, pero no todas, se enumeran en el espacio de nombres de Amazon CloudWatch Logs en la consola de Service Quotas. Para solicitar un aumento de cuota para esas cuotas, consulte el procedimiento más adelante en esta sección.

| Recurso | Cuota predeterminada |
|---|---|
| Tamaño del lote | 1 MB (máximo). Esta cuota no se puede cambiar. |
| Archivado de datos | Hasta 5 GB de archivado de datos de forma gratuita. Esta cuota no se puede cambiar. |
| CreateLogGroup | 5 transacciones por segundo (TPS/cuenta/región), después de lo cual se limitarán las transacciones. Puede solicitar un aumento de cuota. |
| CreateLogStream | 50 transacciones por segundo (TPS/cuenta/región), después de lo cual se limitarán las transacciones. Puede solicitar un aumento de cuota. |
| DeleteLogGroup | 5 transacciones por segundo (TPS/cuenta/región), después de lo cual se limitarán las transacciones. Puede solicitar un aumento de cuota. |
| DescribeLogGroups | 5 transacciones por segundo (TPS/cuenta/región). Puede solicitar un aumento de cuota. |
| DescribeLogStreams | 5 transacciones por segundo (TPS/cuenta/región). Puede solicitar un aumento de cuota. |
| Campos de registro detectados | CloudWatch Logs Insights puede descubrir un máximo de 1000 campos de eventos de registro en un grupo de registros. Esta cuota no se puede cambiar.<br><br>Para obtener más información, consulte Registros admitidos y campos descubiertos (p. 36). |
| Campos de registro extraídos en registros JSON | CloudWatch Logs Insights puede extraer un máximo de 100 campos de eventos de registro de un registro JSON. Esta cuota no se puede cambiar.<br><br>Para obtener más información, consulte Registros admitidos y campos descubiertos (p. 36). |
| Tamaño de eventos | 256 KB (máximo). Esta cuota no se puede cambiar. |
| Exportar tarea | Una tarea de exportación (activa o pendiente) a la vez, por cuenta. Esta cuota no se puede cambiar. |
| FilterLogEvents | 5 transacciones por segundo (TPS)/cuenta/Región. Esta cuota no se puede cambiar. |
| GetLogEvents | 10 solicitudes por segundo, cuenta y región. Esta cuota no se puede cambiar. |

| Recurso | Cuota predeterminada |
| --- | --- |
| | Recomendamos las suscripciones si continuamente está procesando datos nuevos. Si necesita datos históricos, recomendamos exportarlos a Amazon S3. |
| Datos de entrada | Hasta 5 GB de datos de entrada de forma gratuita. Esta cuota no se puede cambiar. |
| Grupos de registros | 1 000 000 de grupos de registros por cuenta y región. Puede solicitar un aumento de cuota.<br><br>No hay cuotas en el número de flujos de registro que pueden pertenecer a un grupo de registros. |
| Filtros de métricas | 100 por grupo de registros. Esta cuota no se puede cambiar. |
| Métricas de formato métrico integradas | 100 métricas por evento de registro y 9 dimensiones por métrica. Para obtener más información sobre el formato de métrica integrado, consulteEspecificación: Formato de métricas integradasen la guía del usuario de Amazon CloudWatch. |
| PutLogEvents | 5 solicitudes por segundo por flujo de registros. Las solicitudes adicionales se limitan. Esta cuota no se puede cambiar.<br><br>El tamaño de lote máximo de una solicitud PutLogEvents es de 1 MB.<br><br>800 transacciones por segundo por cuenta y región, excepto para las siguientes regiones donde la cuota es de 1500 transacciones por segundo por cuenta y por región: EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Oregón) y Europa (Irlanda). Puede solicitar un aumento de cuota. |
| Tiempo de espera de ejecución de la consulta | Se agota el tiempo de espera de los registros de CloudWatch después de 15 minutos. Este límite de tiempo no se puede cambiar. |
| Grupos de registros consultados | Se puede consultar un máximo de 20 grupos de registros en una única consulta de CloudWatch Logs Insights. Esta cuota no se puede cambiar. |
| Simultaneidad de consultas | Se permite un máximo de 10 consultas de CloudWatch Logs Insights simultáneas, incluidas las que se han añadido a paneles. Esta cuota no se administra a través Service Quotas. Puede solicitar un aumento de cuotaCreación de un caso de soporte. |
| Disponibilidad de los resultados de la consulta | Los resultados de una consulta se pueden recuperar durante 7 días. Este tiempo de disponibilidad no se puede cambiar. |
| Resultados de consultas mostrados en la consola | De forma predeterminada, el número máximo de filas que aparecen en los resultados de la consulta de la consola es 1000. Puede utilizar el comando **`limit`** de una consulta para aumentar este valor hasta las 10 000 filas. Para obtener más información, consulte Sintaxis de consulta CloudWatch Logs Insights (p. 41). |

| Recurso | Cuota predeterminada |
| --- | --- |
| Políticas de recursos | Hasta 10 políticas de recursos de CloudWatch Logs por región y cuenta. Esta cuota no se puede cambiar. |
| Consultas guardadas | Puede guardar hasta 1000 consultas de CloudWatch Logs Insights, por región y cuenta. Esta cuota no se puede cambiar. |
| Filtros de suscripción | 2 por grupo de registros. Esta cuota no se puede cambiar. |

# Administración de las cuotas de servicio de CloudWatch Logs

CloudWatch Logs se ha integrado con Service Quotas, unAWSque le permite ver y administrar sus cuotas desde una ubicación central. Para obtener más información, consulte¿Qué son las Service Quotas?en laGuía del usuario de cuotas de servicio.

Service Quotas facilita la búsqueda del valor de sus cuotas de servicio de CloudWatch Logs.

AWS Management Console

Para ver las cuotas de servicio de CloudWatch Logs mediante la consola

1. Abra la consola de Service Quotas enhttps://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, elija serviciosAWS.
3. Desde laAWSservices, busque y seleccioneAmazon CloudWatch Logs.

   En la lista Service quotas (Cuotas de servicio), puede ver el nombre de cuota de servicio, el valor aplicado (si está disponible), la cuota predeterminada de AWS y si el valor de cuota es ajustable.
4. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.
5. (Opcional) Para solicitar un aumento de cuota, seleccione la cuota que desea aumentar, seleccione Request quota increase (Solicitar aumento de cuota), escriba o seleccione la información necesaria y seleccione Request (Solicitar).

Para trabajar más con cuotas de servicio mediante la consola, consulte laGuía del usuario de cuotas de servicio. Para solicitar un aumento de cuota, consulteSolicitud de aumento de cuotaen laGuía del usuario de cuotas de servicio.

AWS CLI

Para ver las cuotas de servicio de CloudWatch Logs mediante laAWS CLI

Ejecute el siguiente comando para ver las cuotas predeterminadas de CloudWatch Logs.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code logs \
    --output table
```

Para trabajar más con cuotas de servicio mediante laAWS CLI, consulte laCuotas de servicioAWS CLIReferencia de los comandos de la. Para solicitar un aumento de cuota, consulte el `request-service-quota-increase` comando en la Referencia de comandos de la AWS CLI.

# Documentohistory

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del usuario de CloudWatch Logs 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 |
| --- | --- | --- |
| CloudWatch Logs Insights (p. 179) | Puede utilizar CloudWatch Logs Insights para buscar y analizar de forma interactiva sus datos de registro. Para obtener más información, consulteAnalizar datos de registro con CloudWatch Logs Insightsen laGuía de usuario de Amazon CloudWatch Logs | 27 de noviembre de 2018 |
| Compatibilidad con los puntos de enlace de la VPC de Amazon (p. 179) | Ahora puede establecer una conexión privada entre su VPC y CloudWatch Logs. Para obtener más información, consulteUso de CloudWatch Logs con los puntos de enlace de la VPCen laGuía de usuario de Amazon CloudWatch Logs. | 28 de junio de 2018 |

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

| Cambio | Descripción | Liberar eldcomió |
| --- | --- | --- |
| Puntos de conexión de la VPC de tipo interfaz | En algunas regiones puede utilizar un punto de conexión de la VPC de tipo interfaz para evitar que el tráfico entre la VPC de Amazon y CloudWatch Logs abandone la red de Amazon. Para obtener más información, consulteUso de CloudWatch LogsiVPCendpoints (p. 158). | 7 de marzo de 2018 |
| Registros de consultas DNS de Route 53 | Puede utilizar CloudWatch Logs para almacenar registros sobre las consultas de DNS recibidas por Route 53. Para obtener más información, consulteQué esi¿Qué es Amazon CloudWatch Logs? (p. 1)orConsultas de DNS de registroen la Guía para desarrolladores de Amazon Route 53. | 7 de septiembre de 2017 |
| Etiquetar grupos de registros | Puede utilizar las etiquetas para categorizar los grupos de registros. Para obtener más información, consulte EtiquetarlOGgGrupos en Amazon CloudWatch Logs (p. 63) . | 13 de diciembre de 2016 |

| Cambio | Descripción | Liberar eldcomió |
| --- | --- | --- |
| Mejoras en la consola | Puede navegar desde los gráficos de métricas a los grupos de registros asociados. Para obtener más información, consulte Tabla dinámica desdemmétricas alogs (p. 62) . | 7 de noviembre de 2016 |
| Mejoras de uso de la consola | Mejora de la experiencia para facilitar la búsqueda, el filtrado y la resolución de problemas. Por ejemplo, ahora puede filtrar los datos de registro en un intervalo de fecha y hora. Para obtener más información, consulte VistalOGdatasen CloudWatch Logs (p. 60) . | 29 de agosto de 2016 |
| Se ha añadidoAWS CloudTrailCompatibilidad con Amazon CloudWatch Logs y nuevas métricas de CloudWatch Logs | Se ha añadidoAWS CloudTrailCompatibilidad con CloudWatch Logs. Para obtener más información, consulte API de registro de Amazon CloudWatch LogscALL ENAWS CloudTrail (p. 161) . | 10 de marzo de 2016 |
| Añadido soporte para la exportación de CloudWatch Logs a Amazon S3 | Se ha agregado compatibilidad para exportar datos de CloudWatch Logs a Amazon S3. Para obtener más información, consulte Exporting (Exportando)lOGdATA a Amazon S3 (p. 128) . | 7 de diciembre de 2015 |
| Se ha agregado compatibilidad paraAWS CloudTrailRegistros de eventos registrados en Amazon CloudWatch Logs | Puede crear alarmas en CloudWatch y recibir notificaciones de la actividad del API particular registrada por CloudTrail y utilizar la notificación para llevar a cabo la resolución de problemas. | 10 de noviembre de 2014 |
| Se ha agregado compatibilidad para Amazon CloudWatch Logs | Puede utilizar Amazon CloudWatch Logs para monitorizar, almacenar y obtener acceso a los archivos de registro del sistema, aplicación y personalizados desde instancias de Amazon Elastic Compute Cloud (Amazon EC2), u otros orígenes. A continuación, puede recuperar los datos de registro asociados desde CloudWatch Logs mediante la consola de Amazon CloudWatch, los comandos de CloudWatch Logs en laAWS CLIo el SDK de CloudWatch Logs. Para obtener más información, consulte Qué esi¿Qué es Amazon CloudWatch Logs? (p. 1) . | 10 de julio de 2014 |

# AWSGlosario

Contiene la más recienteAWSterminología, consulte laAWSGlosarioen laAWSReferencia general de.

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