Configuración de registros de flujo de AWS VPC para entrada CTB

Contenido

Introducción

Este documento describe cómo configurar los registros de flujo de VPC como entrada para Cisco Telemetry Broker (CTB).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios web de Amazon (AWS)
- Administración de CTB.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CTB (v2.2.1+)
- AWS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

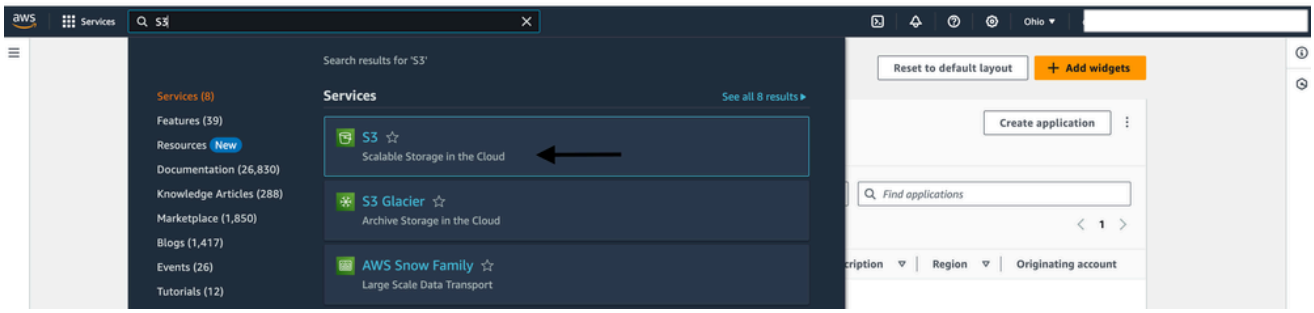
Configuration Steps

Paso 1. Configure el Bucket S3 en AWS

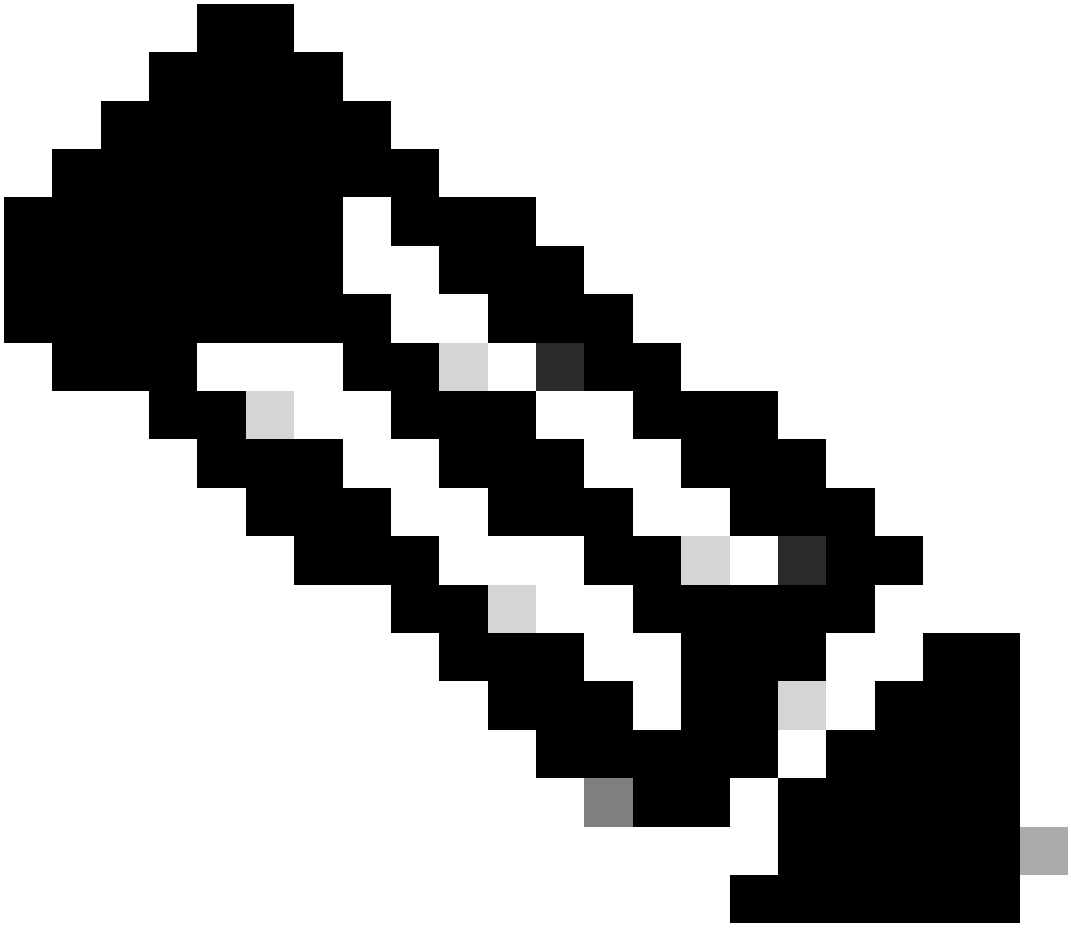
1: Inicie sesión en la consola de administración de AWS con nombre de usuario y contraseña.

2: Asegúrese de iniciar sesión en la región adecuada.

3: Vaya a la barra de búsqueda y escriba S3.

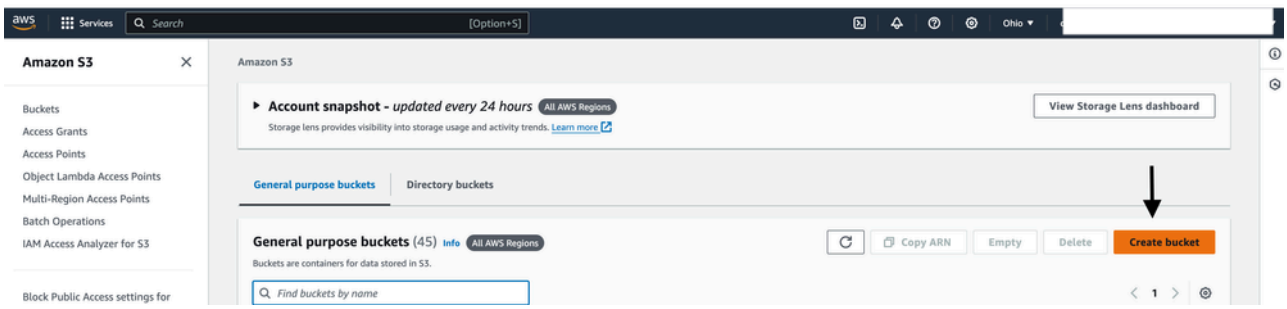


AWS-Dashboard



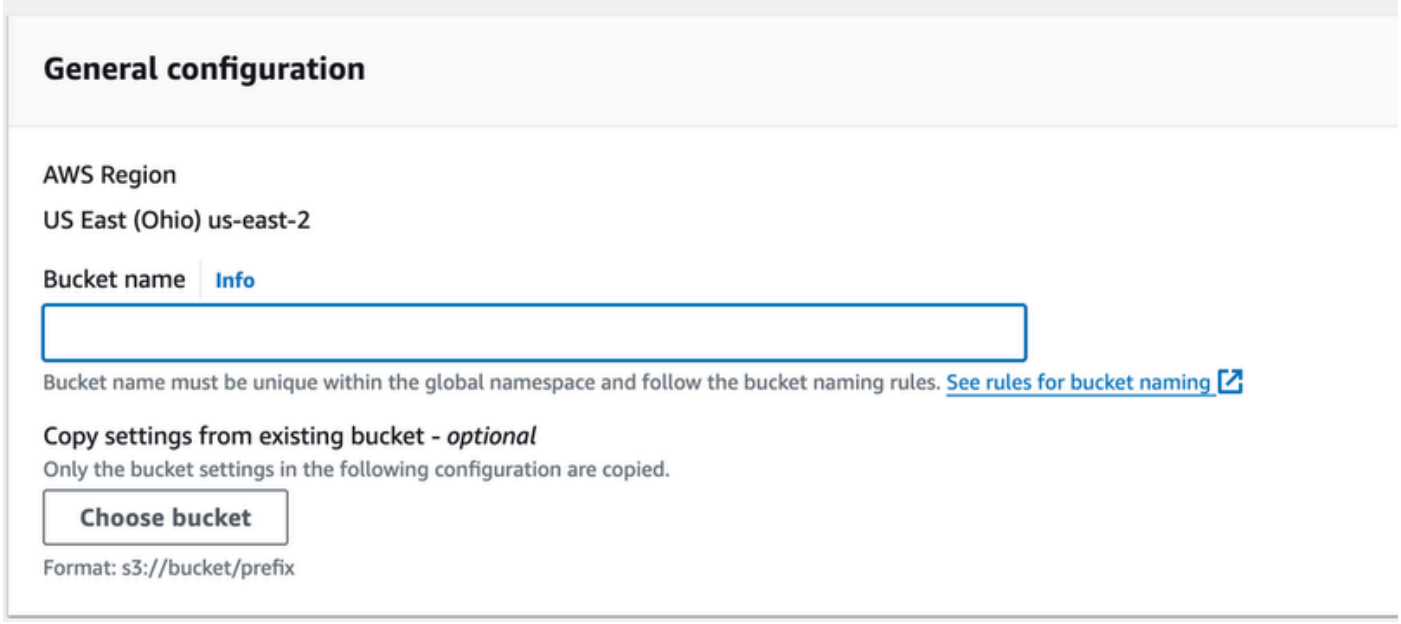
Nota: En la demostración, ha seleccionado la región de Ohio con la zona de disponibilidad us-east-2, que es visible justo al lado del icono del engranaje.

4: Haga clic en crear depósito.

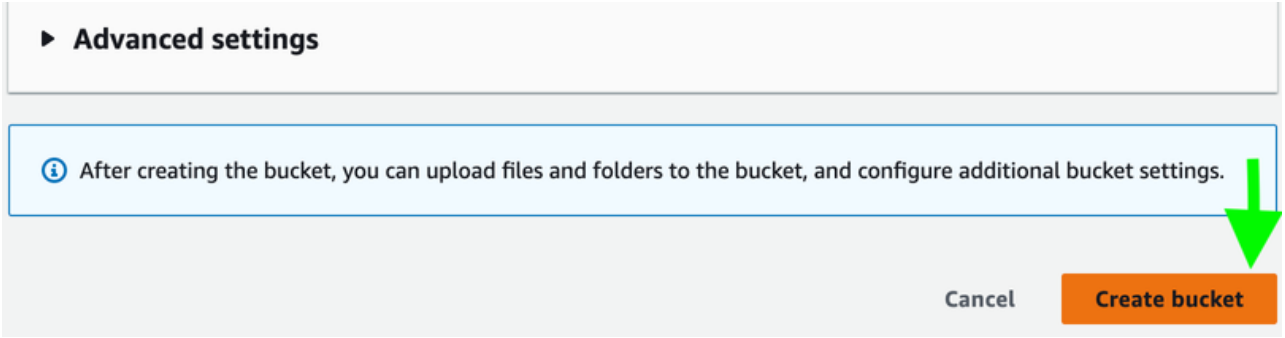


AWS-S3

5: Dé un nombre a bucket y deje cada opción tal cual y haga clic en create.

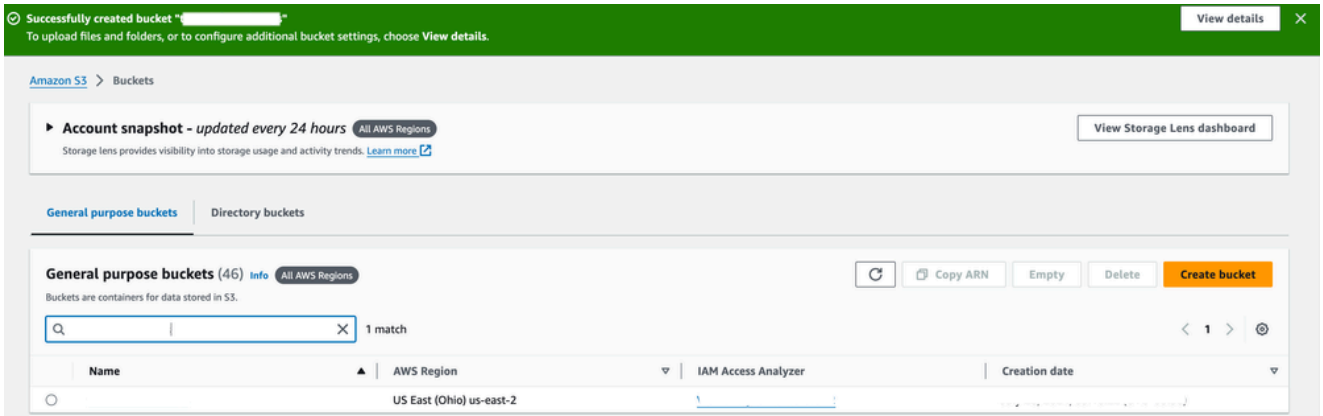


AWS-S3

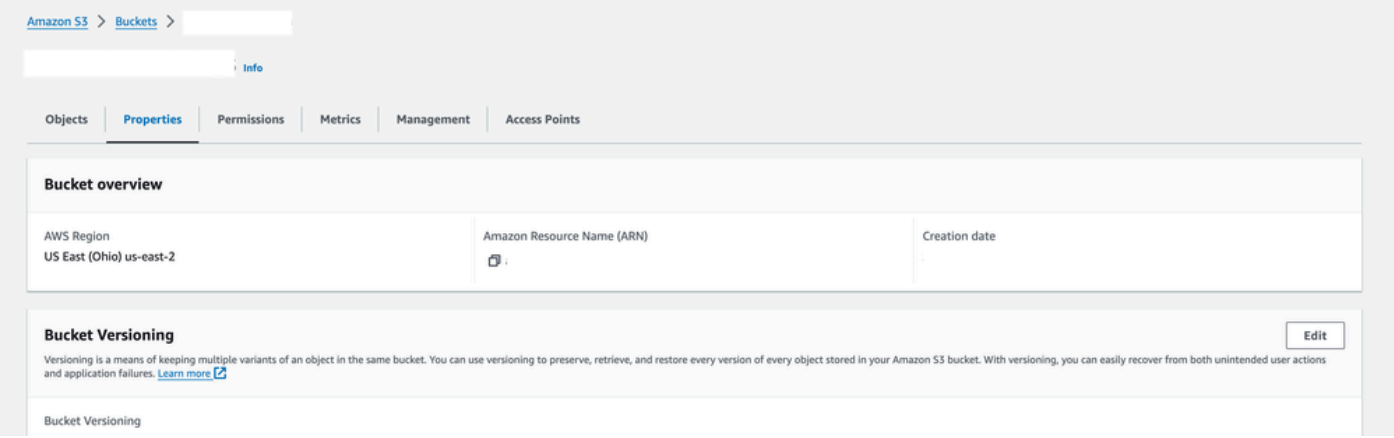


AWS-S3

6: Una vez que la cubeta se haya creado correctamente, guarde el ARN de la cubeta que se utilizará más adelante durante la configuración.



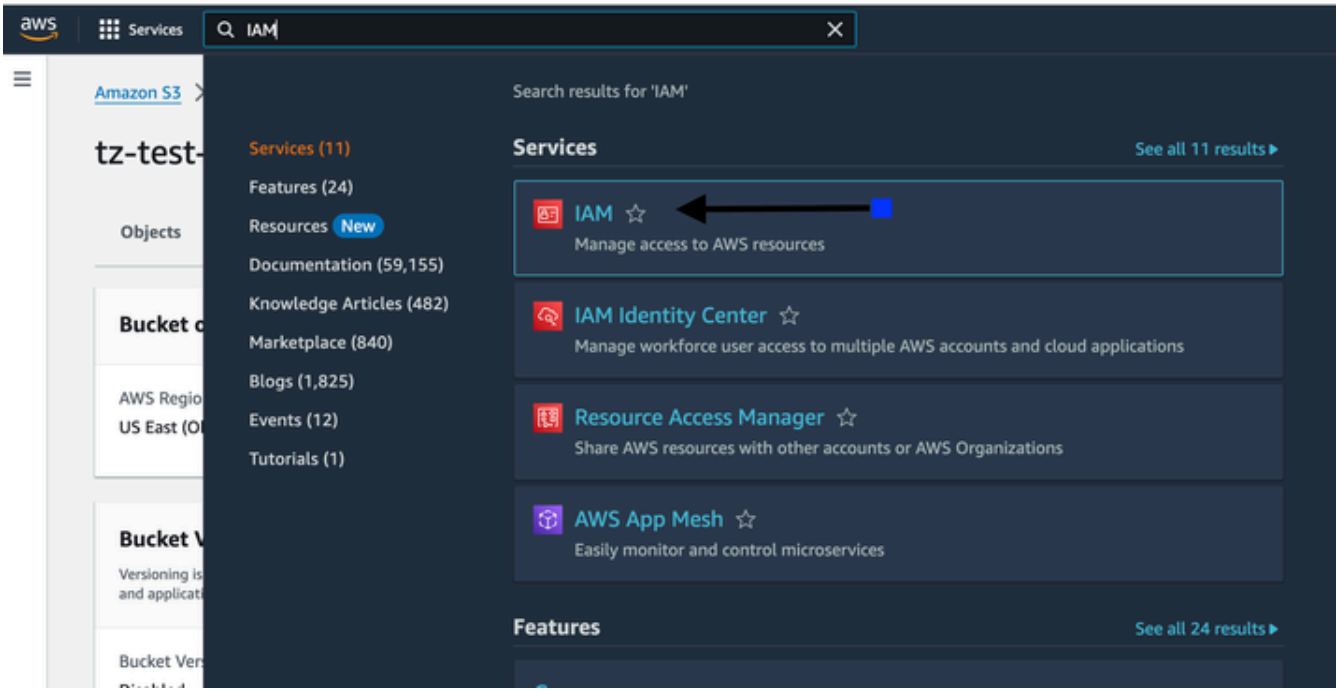
AWS-S3



AWS-S3

Paso 2. Crear usuario IAM con clave de acceso y Adjuntar política de depósito S3

1: Inicie el IAM desde la barra de búsqueda de AWS.



AWS-IAM

2: Desplácese hasta usuarios.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

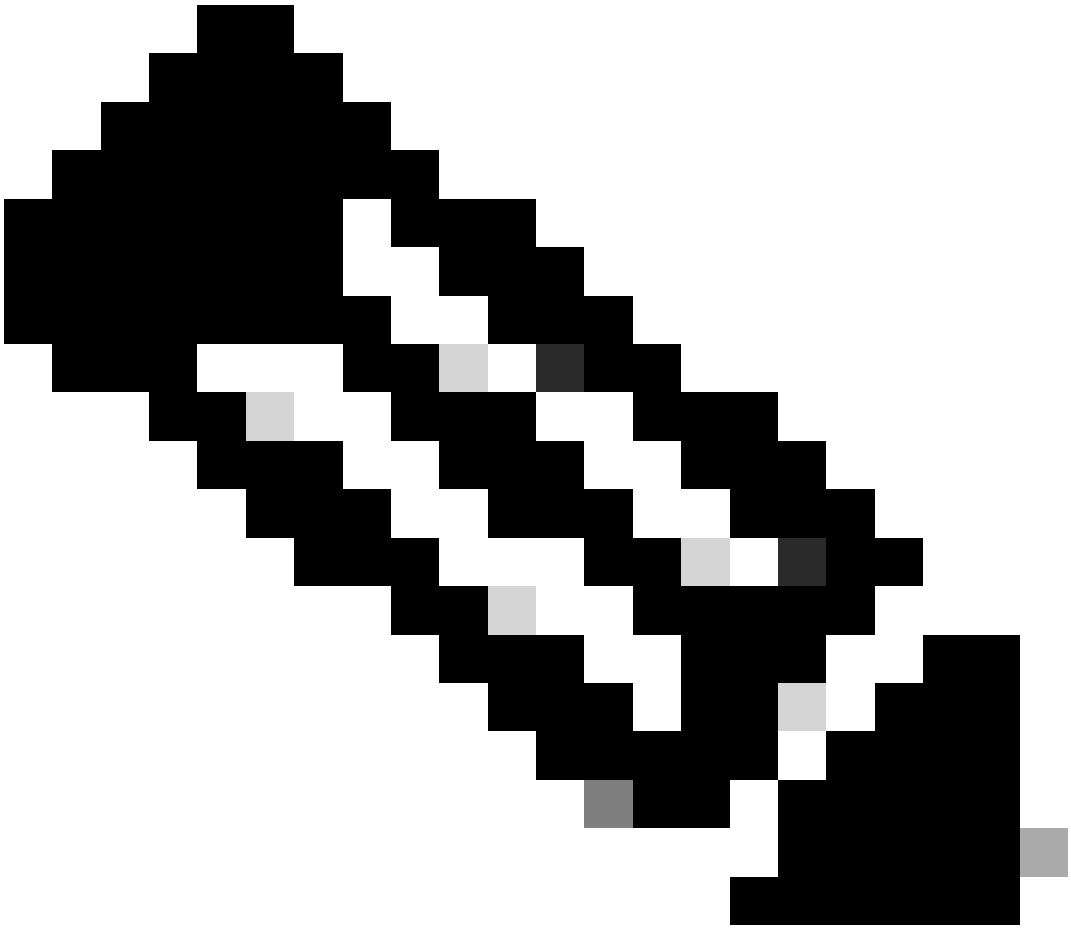
Users

Roles

Policies

Al desactivar la casilla de acceso de la consola de administración de AWS, evita que el usuario inicie sesión en la cuenta de AWS mediante la interfaz de usuario web.

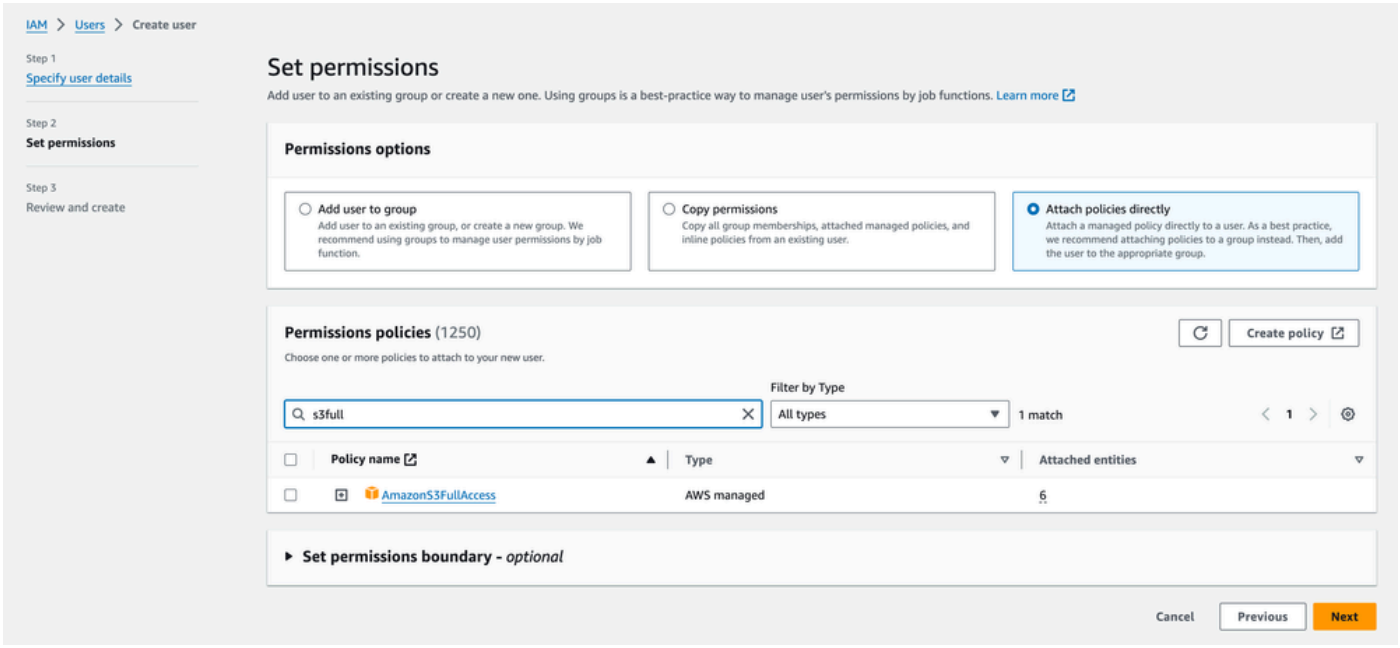
6: Asigne la política al usuario, asociándola directamente a un grupo o configurándola en línea.



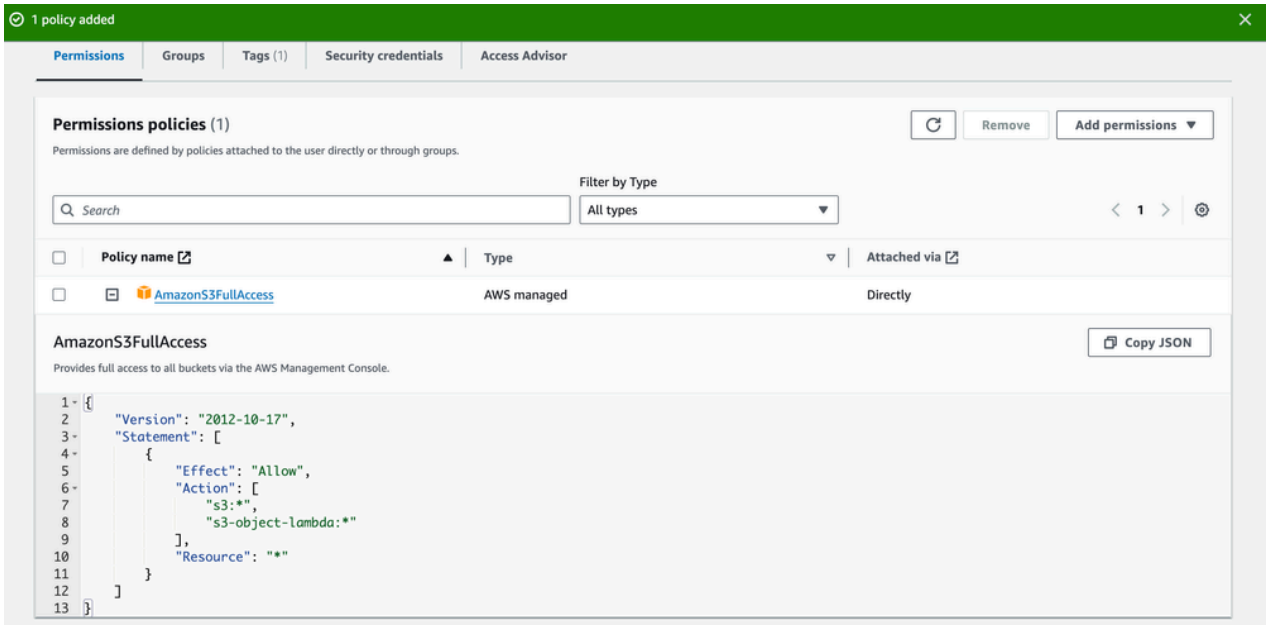
Nota: Para ver una demostración, puede asignar directamente una directiva al usuario. Para obtener más información: administración de políticas de AWS

7: Busque S3 full access y seleccione AmazonS3full access, que permite al usuario tener acceso completo para cada cubeta S3 creada en su cuenta AWS correspondiente.

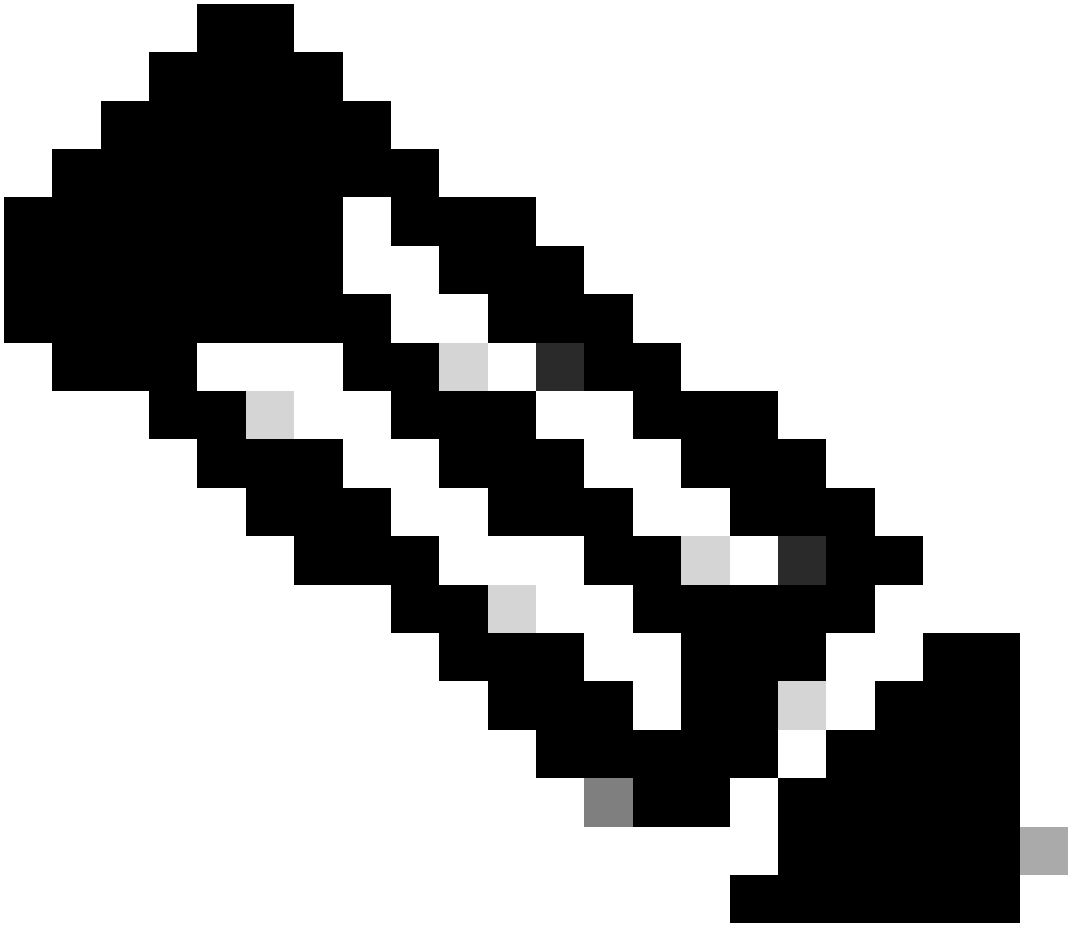
8: Marque la casilla con el nombre de la política AmazonS3FullAccess y haga clic en Next.



AWS-IAM

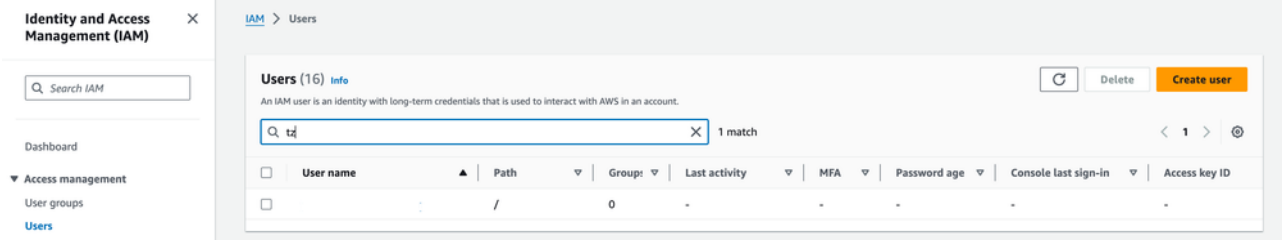


AWS-IAM

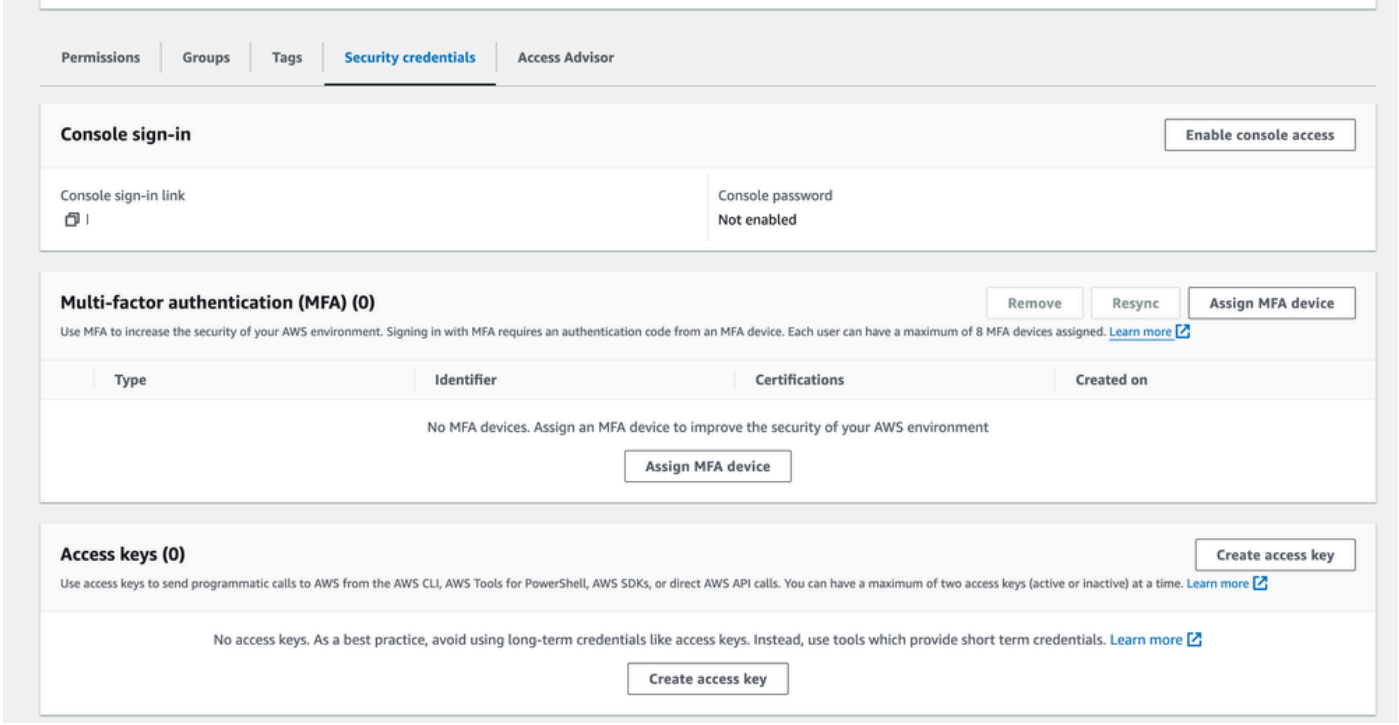


Nota: Puede crear una política más granular permitiendo solo un depósito específico también. Navegue hasta Creación de política para crear su política de depósito S3 en formato json.

9: Una vez creado el usuario, enumere el usuario y navegue hasta la ficha credencial de seguridad y haga clic en crear clave de acceso.

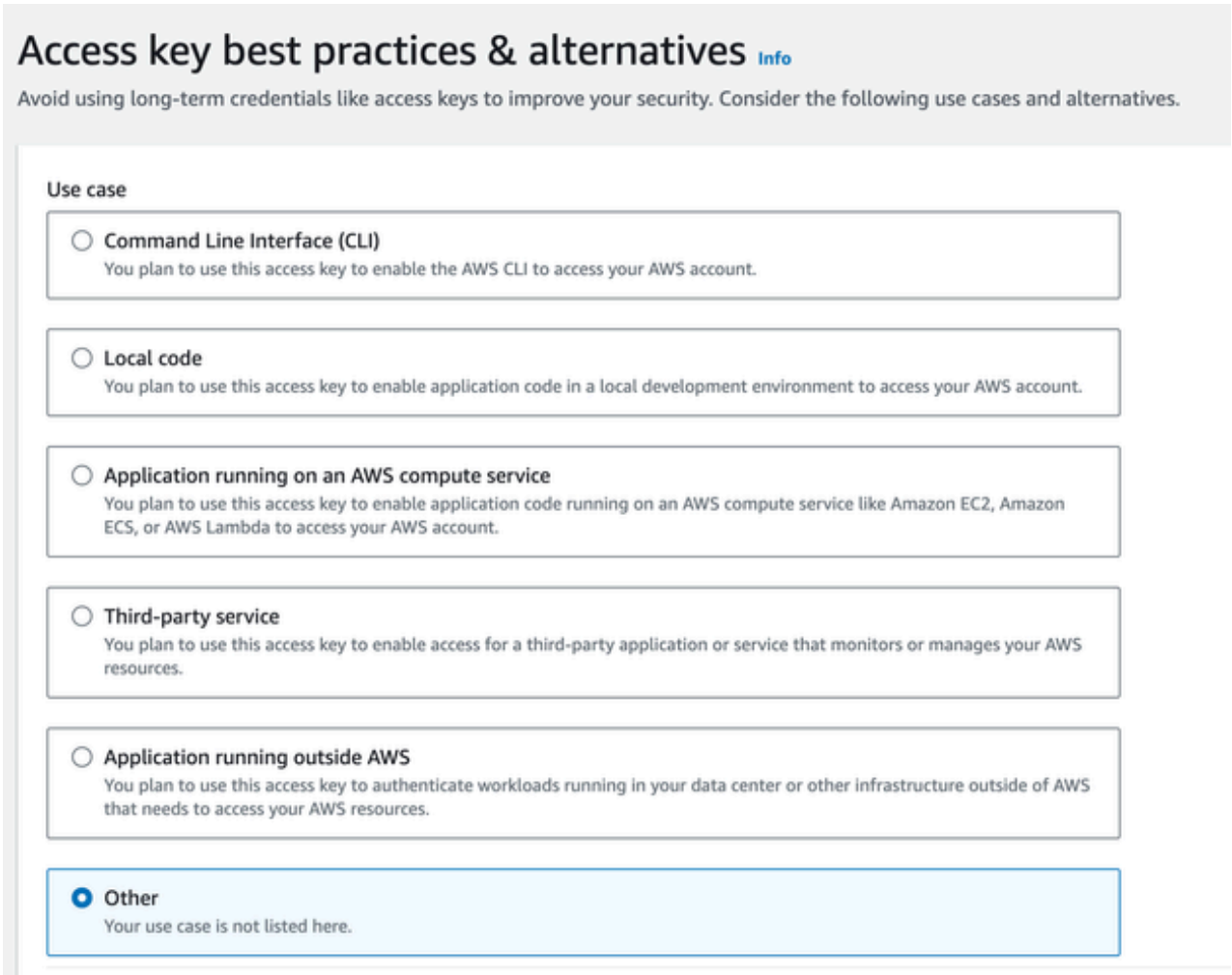


AWS-IAM

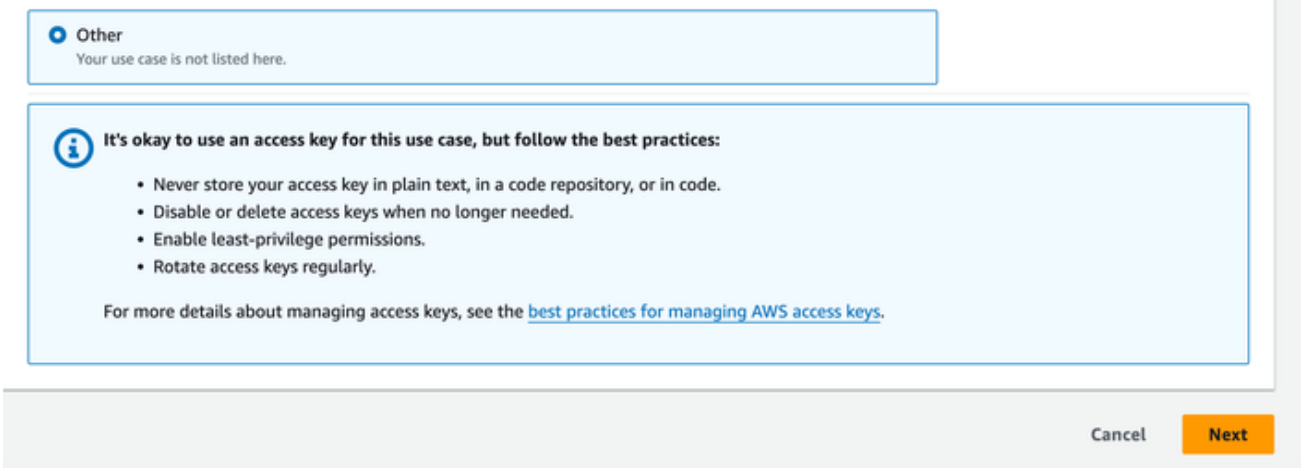


AWS-IAM

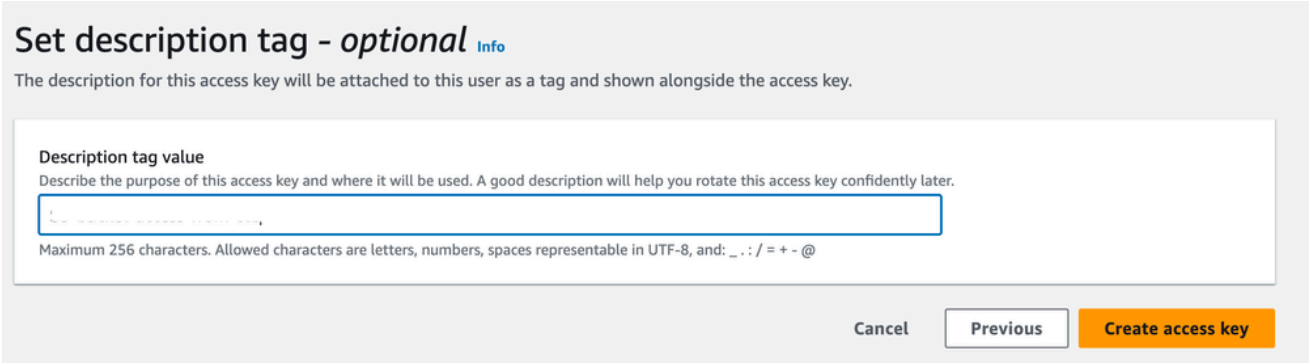
10: Seleccione el otro botón de opción y, opcionalmente, agregue una etiqueta.



AWS-IAM

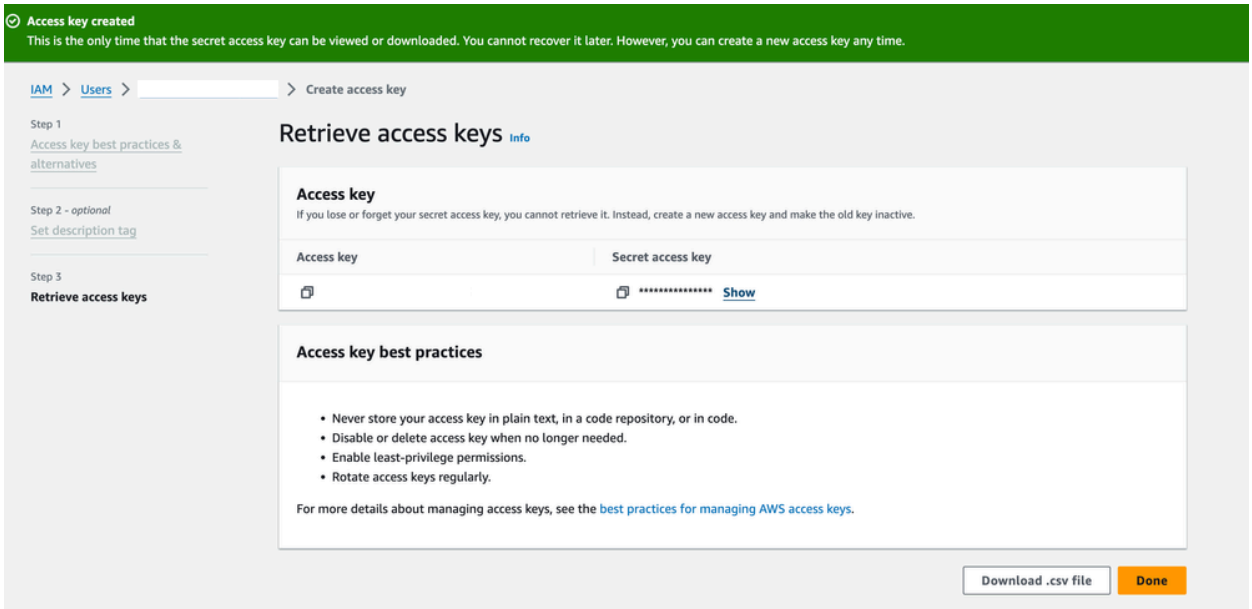


AWS-IAM



AWS-IAM

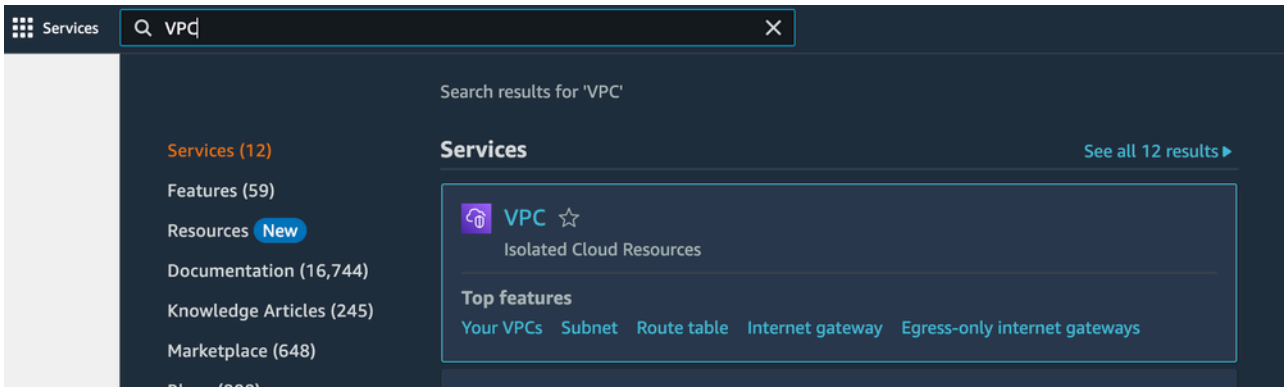
11: Haga clic en Descargar archivo .csv. Esta es la clave de acceso de un archivo csv y ya no está disponible para descargar o ver una vez que se desplace fuera de esta página.



AWS-IAM

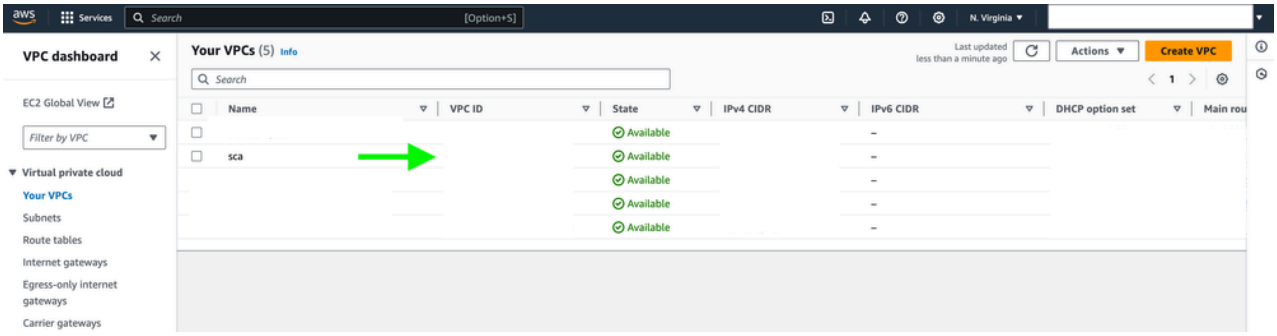
Paso 3. Configuración de los registros de flujo de VPC

1: Inicie el VPC en la región deseada y navegue hasta la opción Your VPC.

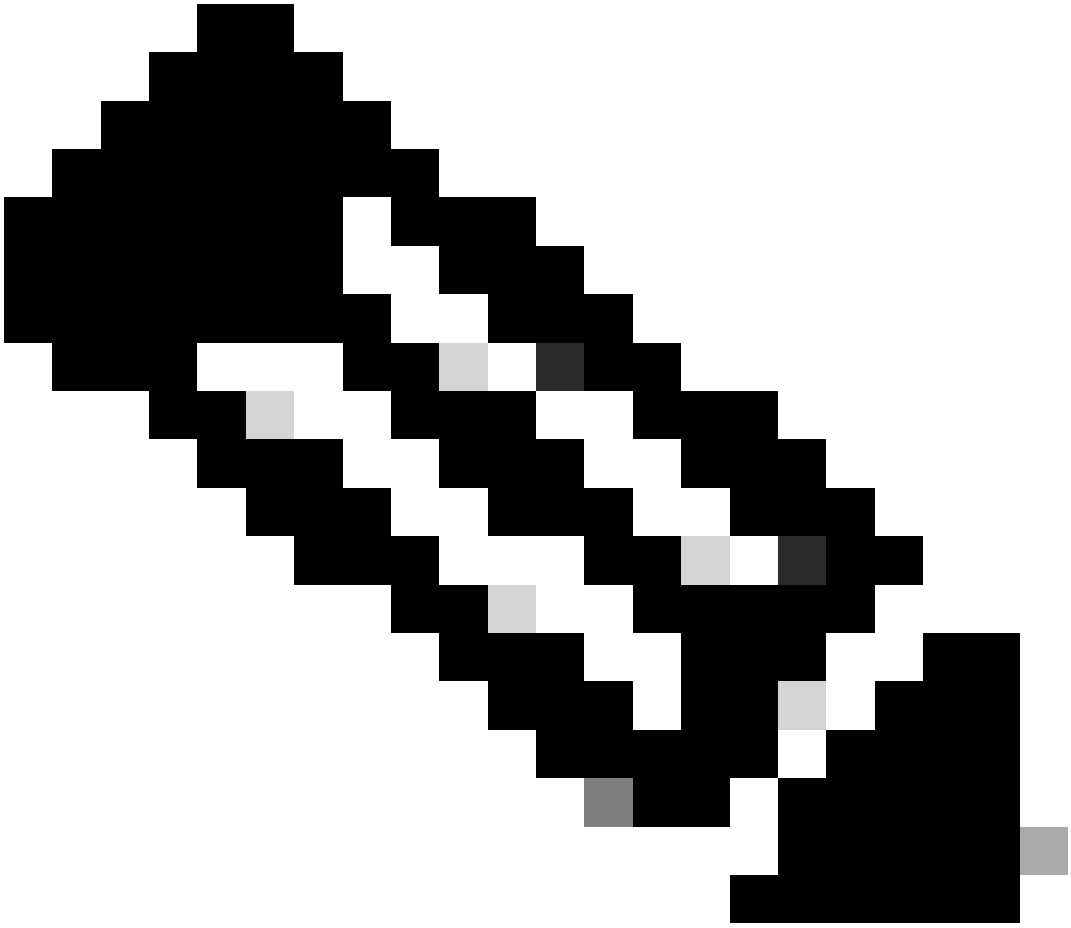


AWS-Flow-Logs

2: Seleccione el VPC en la lista que aparece en la pantalla.

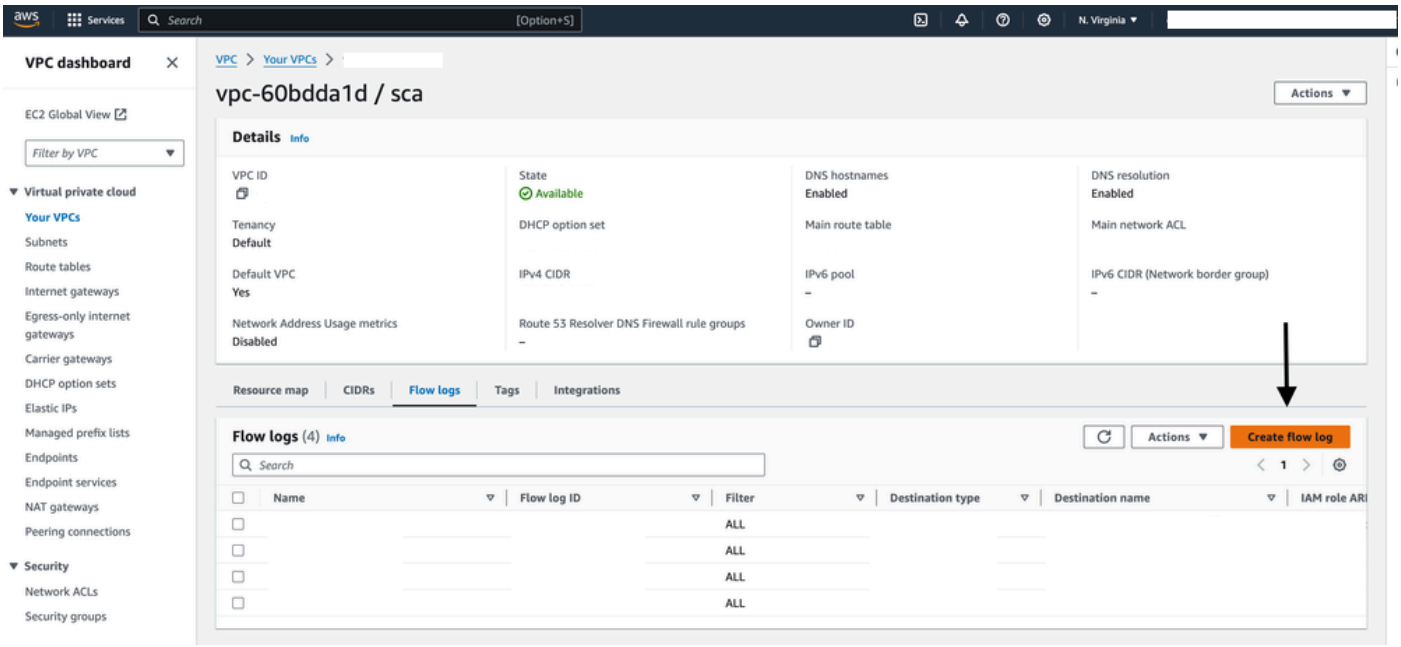


AWS-Flow-Logs



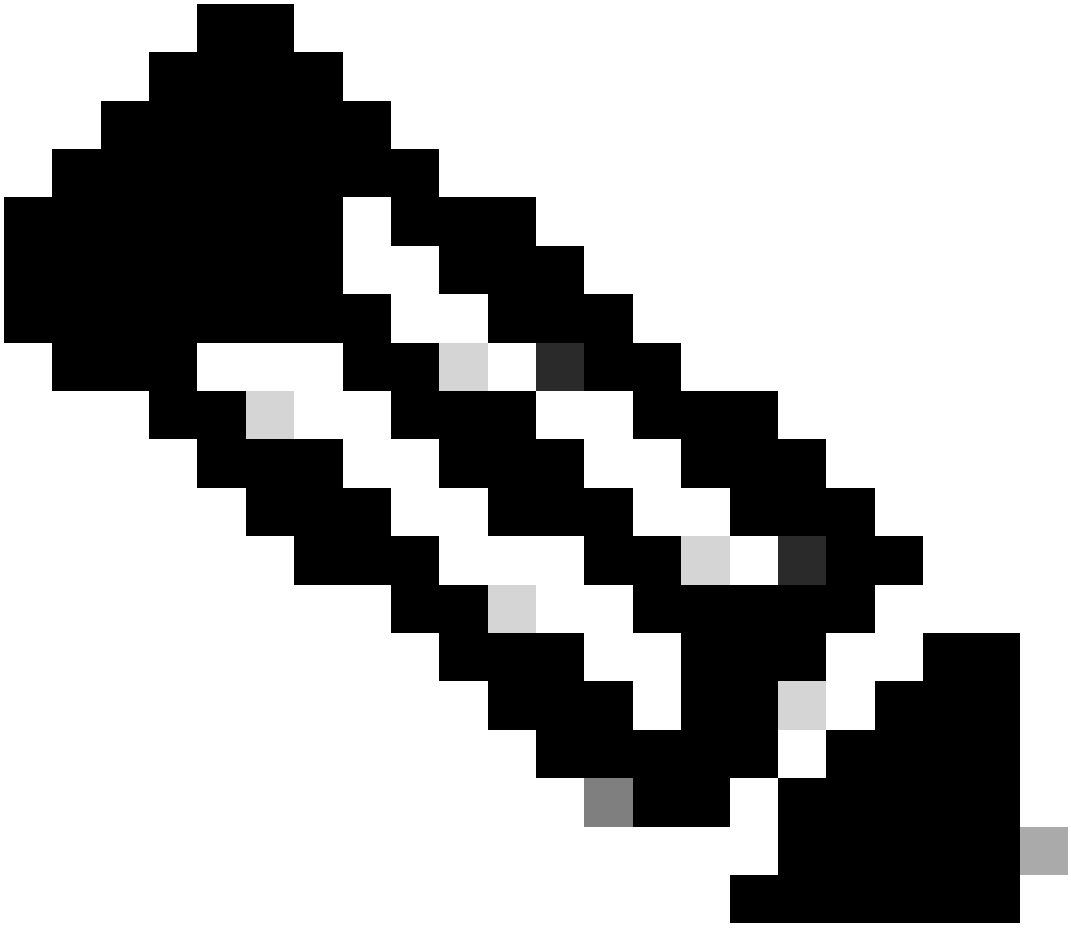
Nota: Ha seleccionado el nombre VPC SCA en esta demostración.

3: Navegue hasta Sus VPC en Nube privada virtual, cambie a la pestaña Registros de flujo y haga clic en Crear registros de flujo.



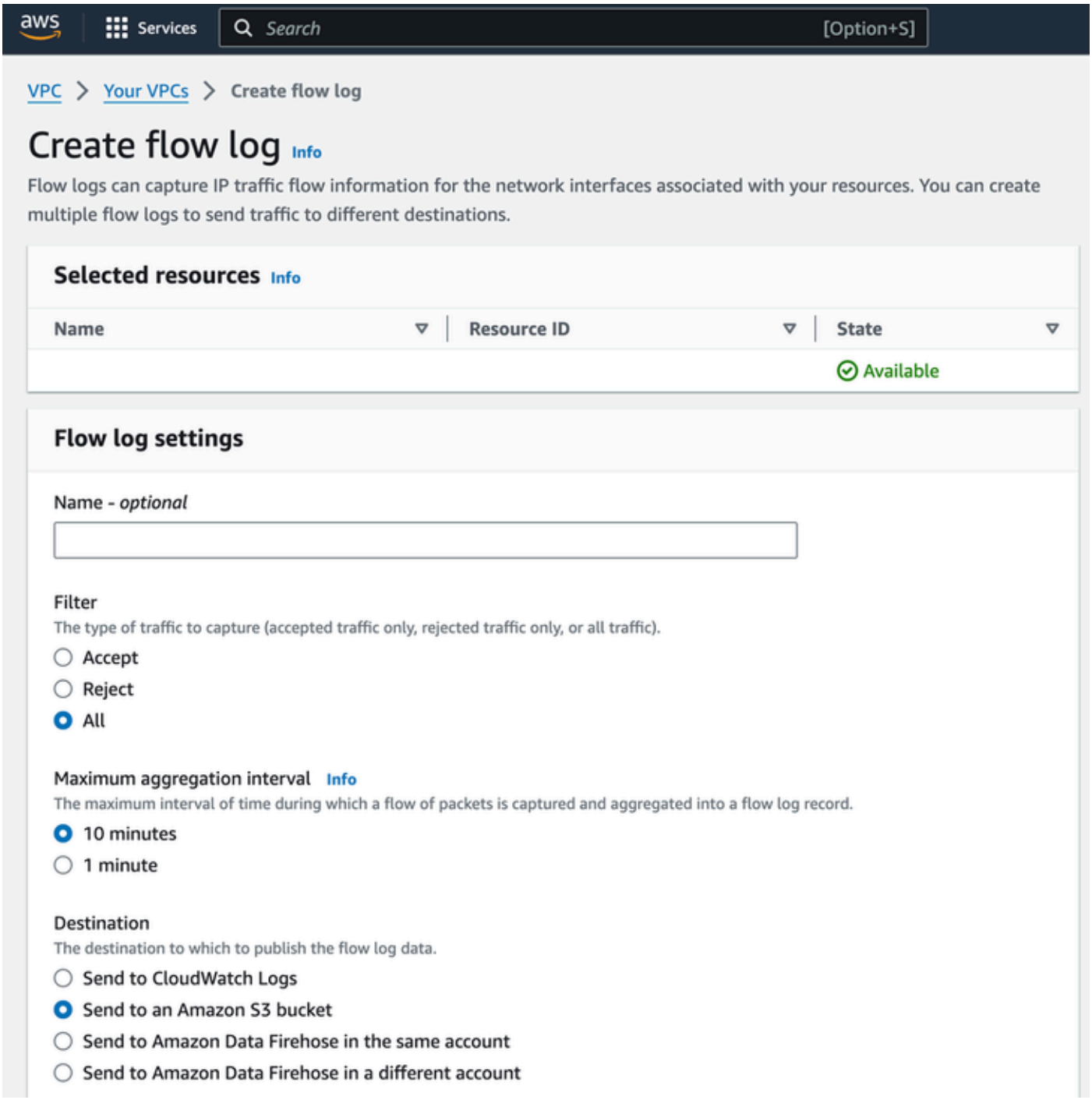
AWS-Flow-Logs

4: Dé un nombre a sus registros de flujo y comparta el ARN de cubeta S3 creado anteriormente.

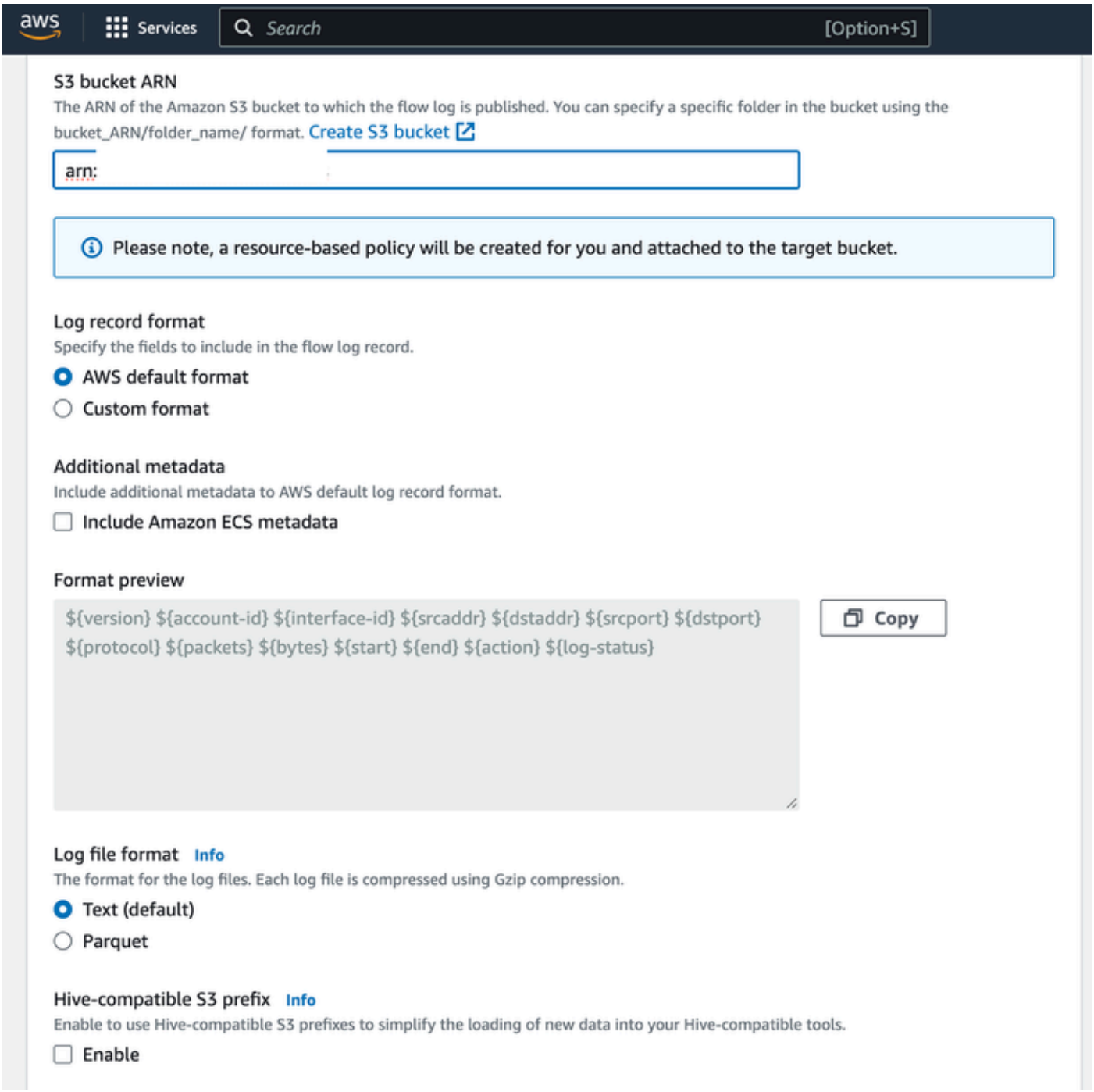


Nota: Para ARN, consulte Configure S3 bucket - Step 6

5: Tiene la opción de utilizar el formato de registro predeterminado de AWS o crear un formato de registro personalizado en caso de que se necesiten más campos.

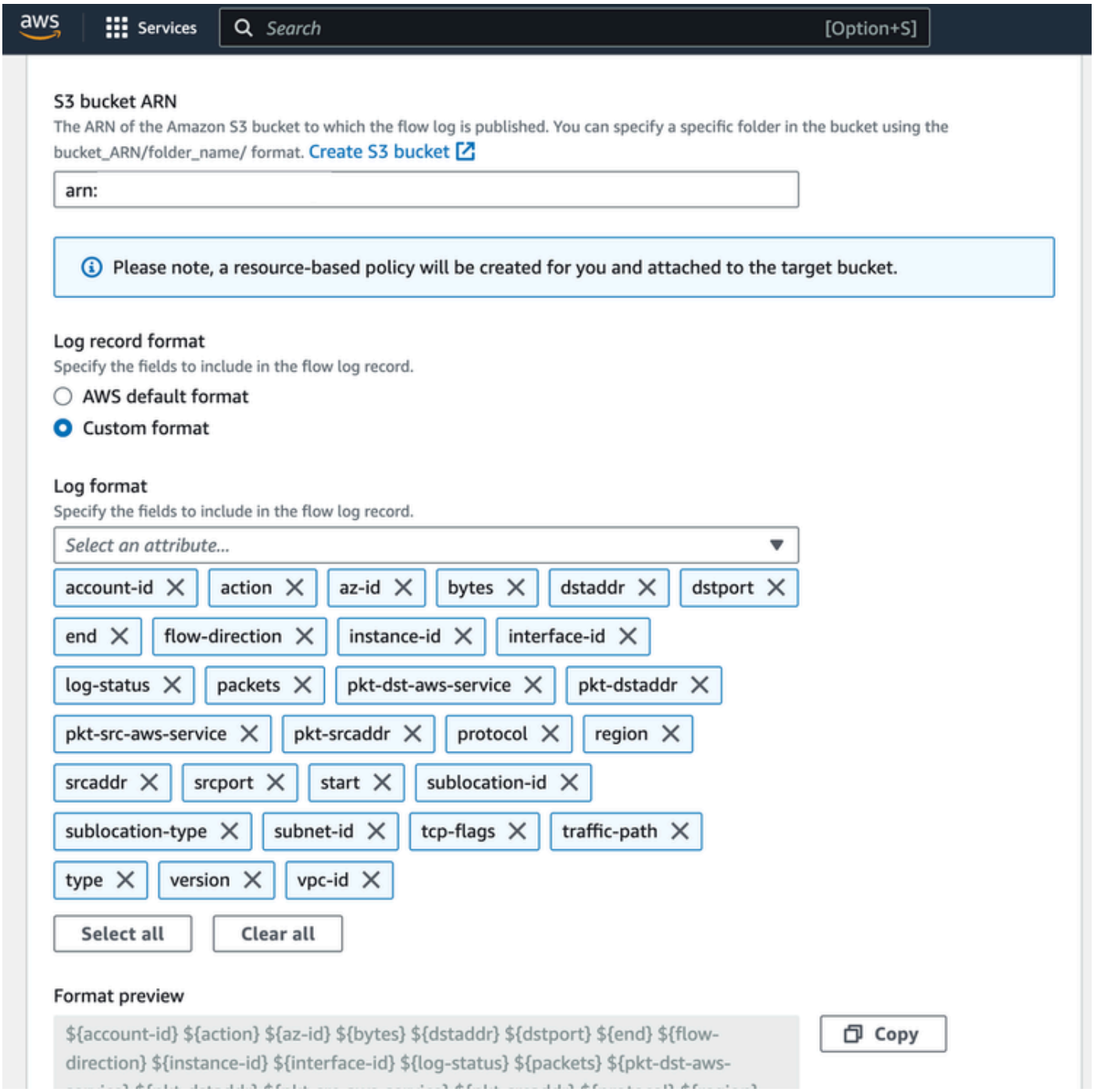


AWS-Flow-Logs

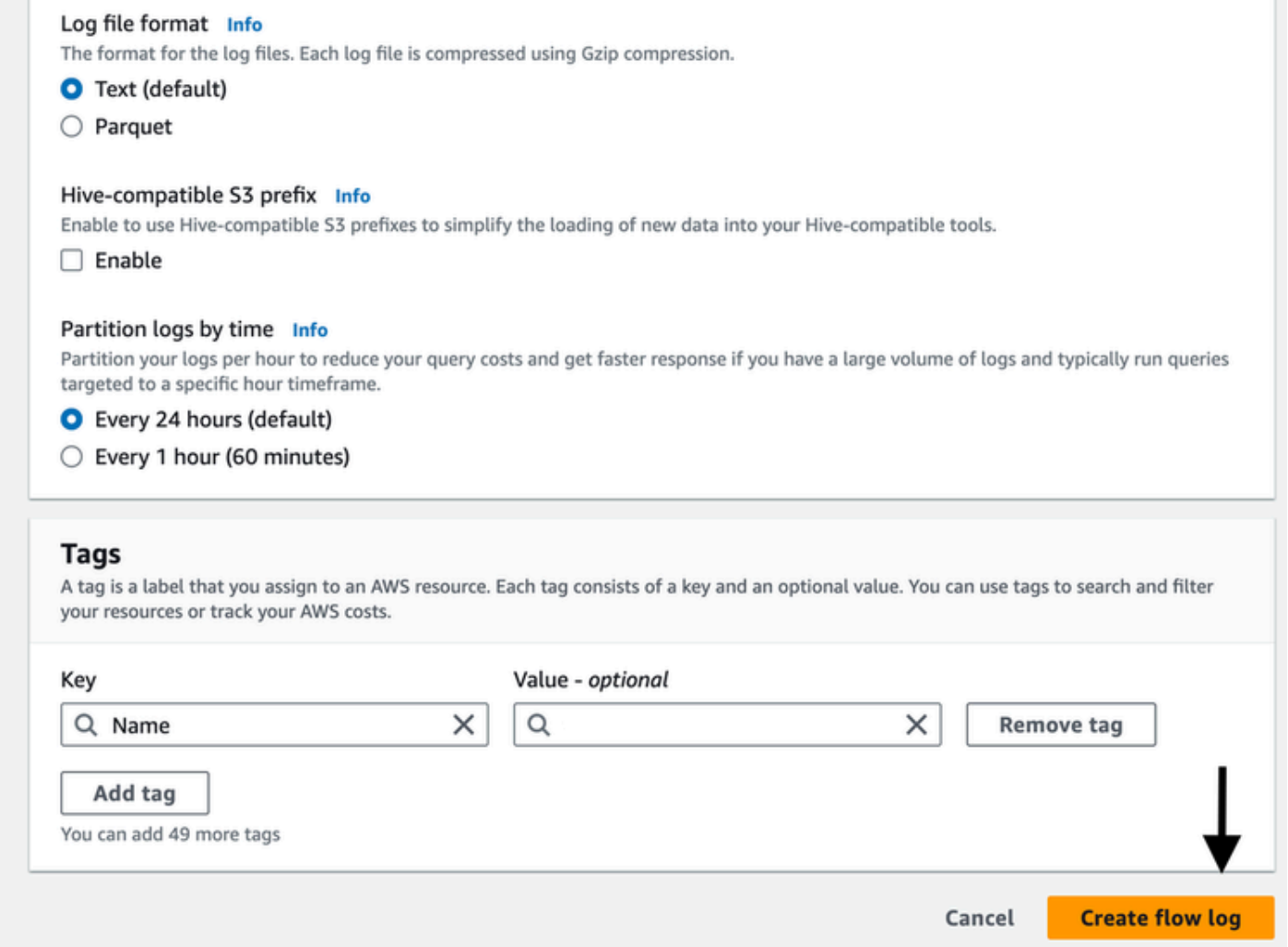


AWS-Flow-Logs

7: Haga clic en Create flow logs.



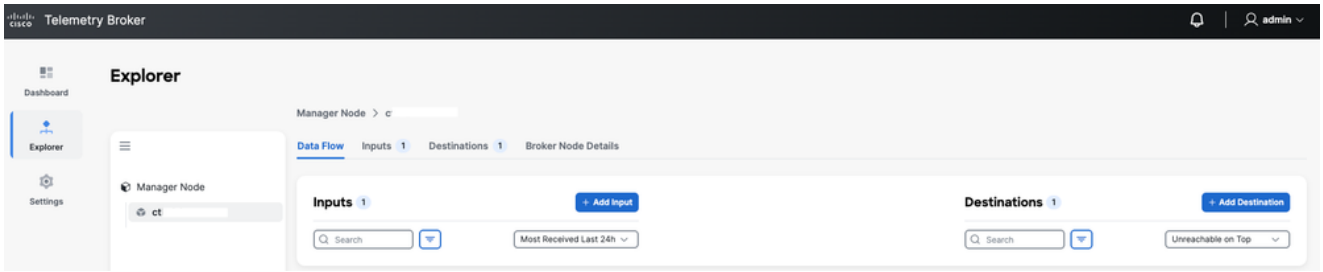
AWS-Flow-Logs



AWS-Flow-Logs

Paso 4. Configuración de la entrada VPC en CTB

1: Acceda a la interfaz de usuario web de CTB, navegue hasta Explorador> ficha Nodo de Broker > haga clic en Abrir nodo de broker >ficha Flujo de datos > Haga clic en Agregar entrada.



CTB-Input-UI

2: Seleccione Input type as AWS VPC Flow log y haga clic en next.

Add Input

Select Input type

Type or Select Input

UDP Input

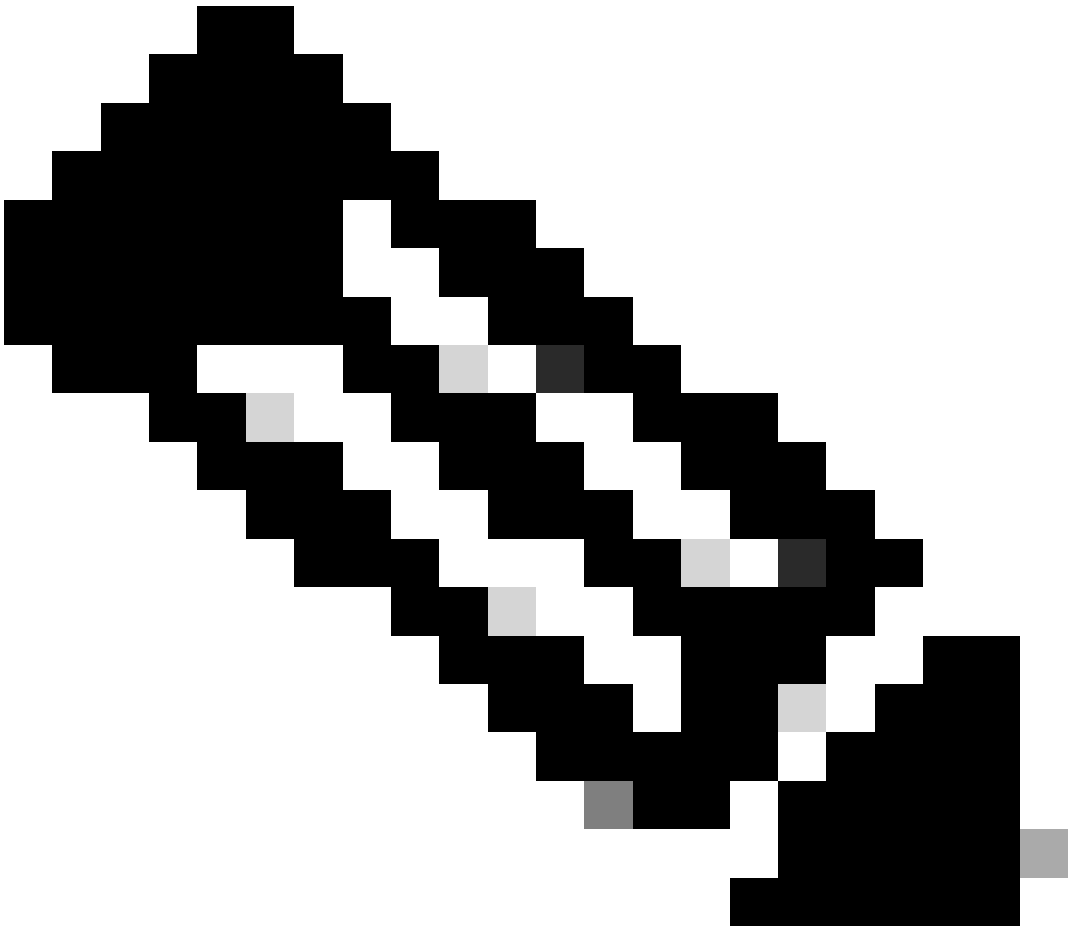
AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

Flow Generator Input

: Cualquier dirección IP configurada como dirección IP de entrada (IP única no compartida por ningún otro exportador) se notifica como el exportador para los datos de NetFlow transformados.



Nota: Para el ID de clave de acceso de AWS, consulte Configuración del usuario IAM para la clave de acceso con la política de acceso S3, paso 9

Verificación

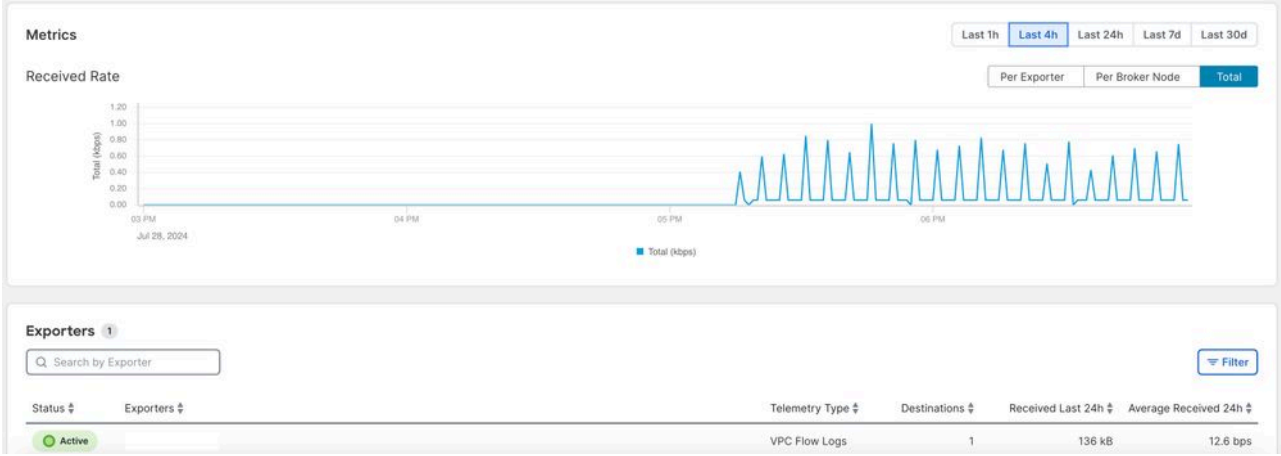
Después de unos minutos de configurar la entrada AWS VPC, la columna de estado se activa si la cubeta AWS S3 tiene datos.

Verifique el estado de la entrada AWS VPC mediante estos pasos.

1: Inicie sesión en la interfaz de usuario de CTB y navegue hastaExplorador> ficha Nodo de Broker > haga clic en nodo de OpenBroker >cambie a Entrada >Haga clic en Abrir entrada de

AWS.

2: Verifique que los logs de aws-flow configurados tengan el estado activo y que la métrica recibida tenga un gráfico ascendente.



CTB-Input-UI

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).