Utilice la API de Umbrella Reporting mediante Postman

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Overview

Procedimiento general

Procedimiento de cartero

Respuestas

Introducción

Este documento describe cómo utilizar la API de Cisco Umbrella Reporting en Postman.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

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.

Overview

La API de Umbrella se publicó en septiembre de 2022, y proporciona una plataforma segura y fácil de usar que permite a los usuarios crear, ampliar e integrar con Umbrella.

Los terminales de la API Umbrella se alojan en api.umbrella.com, con rutas agrupadas por caso práctico. Las claves de API se pueden administrar tanto en el panel de Umbrella, en Admin > API keys, como mediante programación con la API KeyAdmin. Cada clave se puede configurar de

forma granular con varios ámbitos agrupados en cinco casos prácticos principales:

- Los terminales de la API de administración le permiten aprovisionar y administrar claves y usuarios de la API de Umbrella, ver roles y administrar clientes para proveedores y proveedores administrados.
- Los terminales de la API de autenticación permiten autorizar integraciones de otros servicios con la plataforma Umbrella.
- Las implementaciones de terminales API le permiten aprovisionar, supervisar y gestionar redes y otras entidades diferentes, así como protegerlas configurándolas en las políticas de Umbrella existentes.
- Políticas Los terminales API le permiten aprovisionar y administrar listas de destinos y los destinos por lista.
- Los terminales de la API de Reports permiten leer y auditar información de seguridad en tiempo real sobre las implementaciones. La API Umbrella App Discovery proporciona información sobre las aplicaciones basadas en la nube.

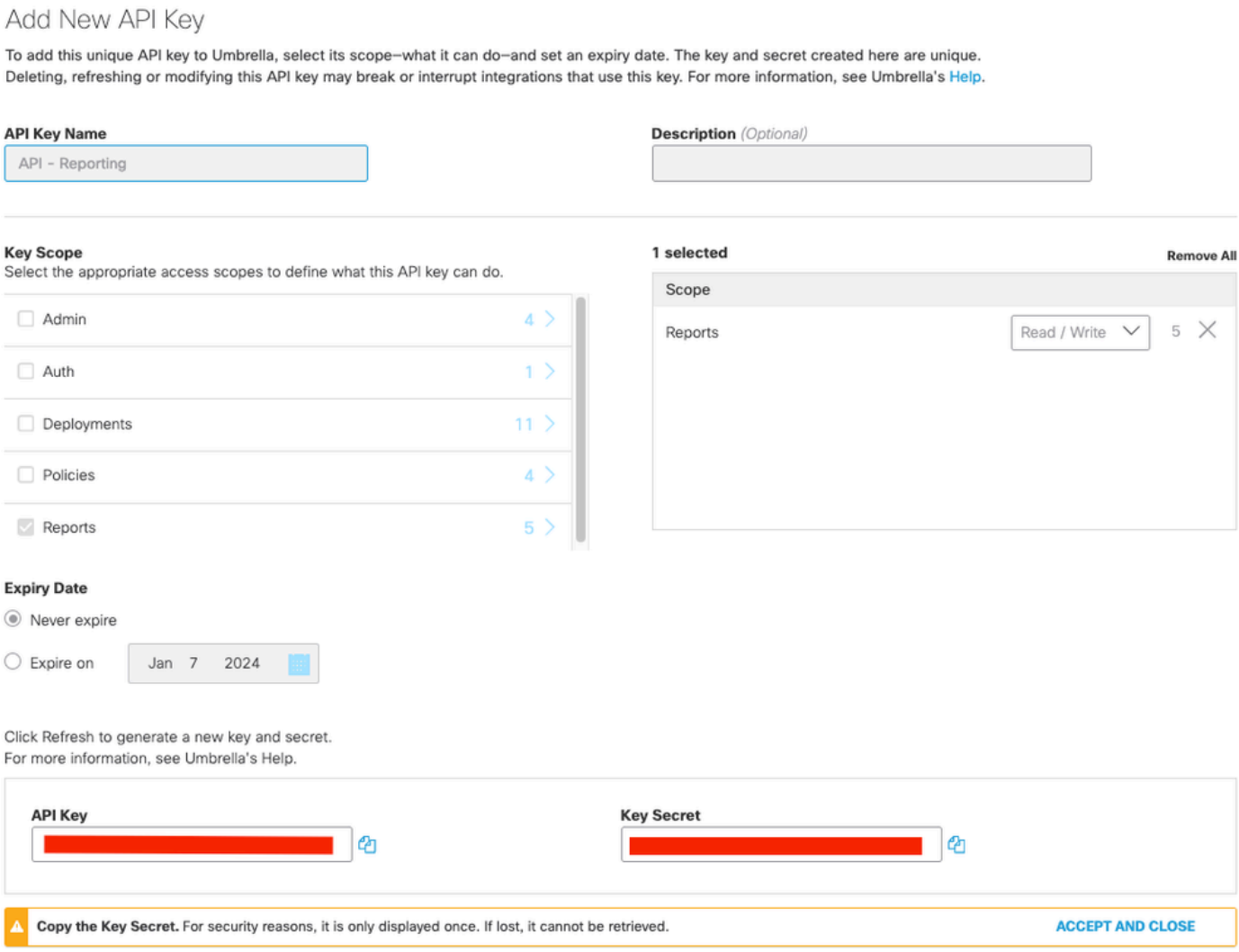
En este artículo se muestra cómo recopilar informes de búsqueda de actividades a través de la API.

Procedimiento general

1. Desde el panel de Umbrella, navegue hasta Admin > API Keys.

2. Seleccione Claves API > Agregar.

3. En Key Scope, seleccione Reports y, a continuación, Create Key.



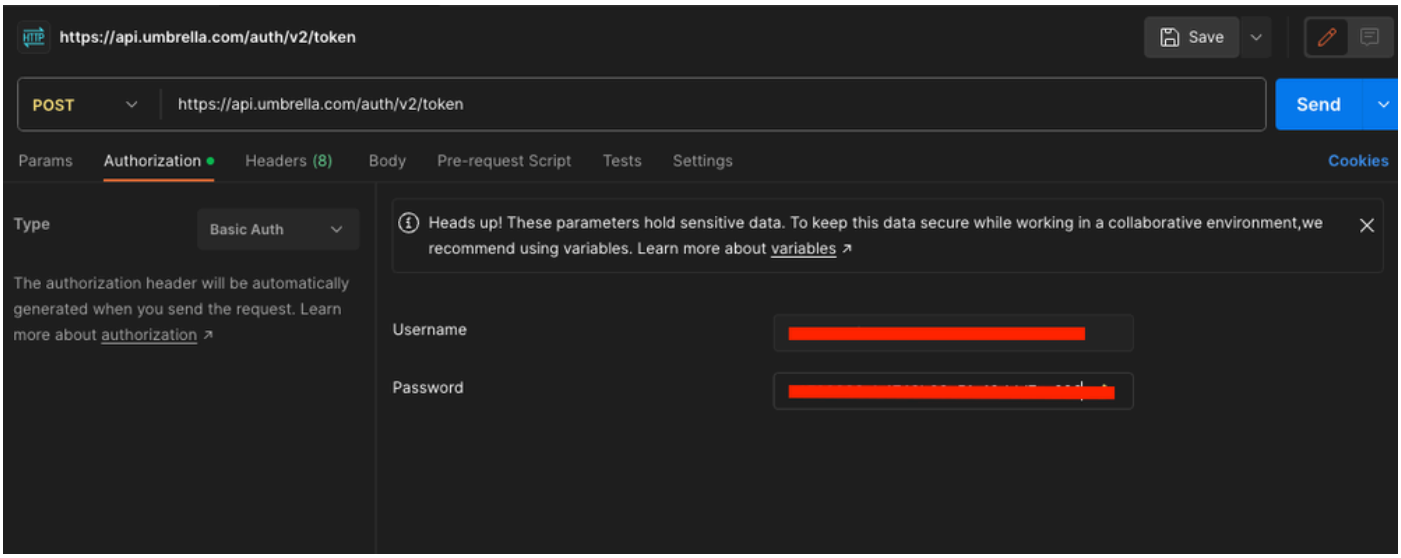
21495050167956

Los administradores pueden ajustar el nivel de acceso por ámbito entre lectura/escritura y solo lectura, en función del uso esperado de cada clave de API, mientras que las claves de API se pueden configurar para que caduquen en una fecha predefinida. Es necesario que recopile la clave/secreto de la API en este paso, ya que están visibles actualmente y no pueden aparecer después.

Las credenciales de la API generan tokens de acceso a la API válidos durante 60 minutos. Este procedimiento admite el flujo de credenciales del cliente OAuth 2.0. En los entornos de proveedores de servicios o multiorganización de Umbrella, las credenciales de la API de organización principal se pueden utilizar para generar tokens de acceso con los mismos ámbitos para una organización secundaria especificada durante el proceso de autorización.

Procedimiento de cartero

En primer lugar, debe crear un token de acceso de OAuth 2.0. Las rutas de autenticación de la API Umbrella comienzan con https://api.umbrella.com/auth/v2. Al enviar una consulta POST y una clave de la API de usuario como nombre de usuario y contraseña de la API como contraseña, se genera un token de acceso.

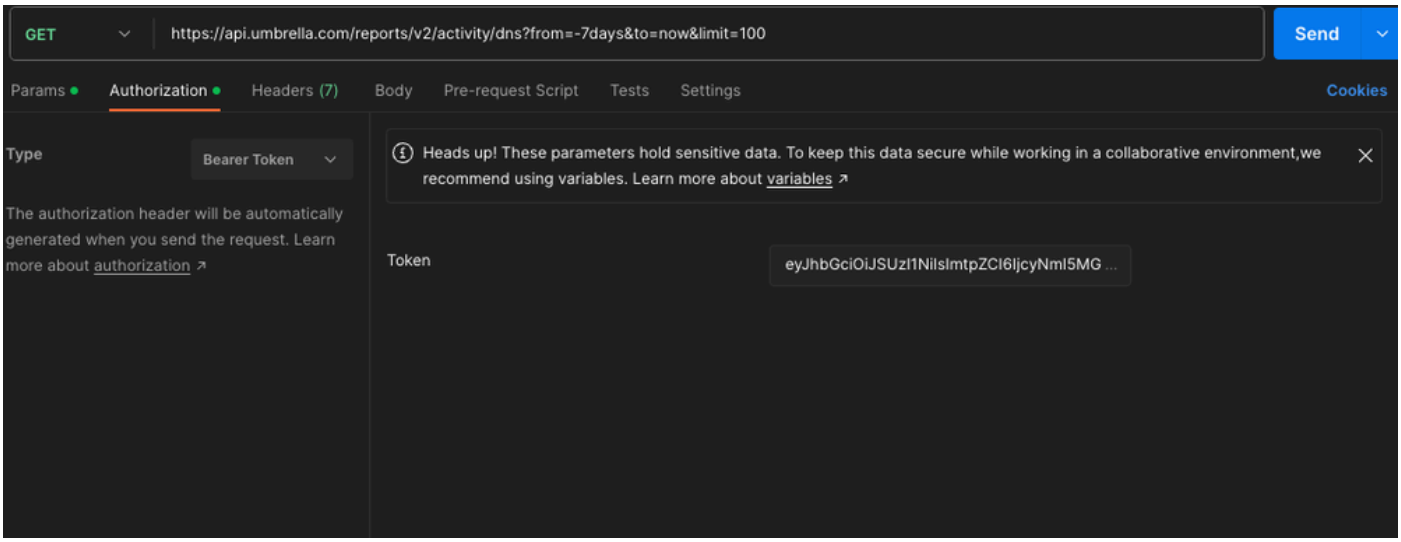


21606708808468

21607051456276

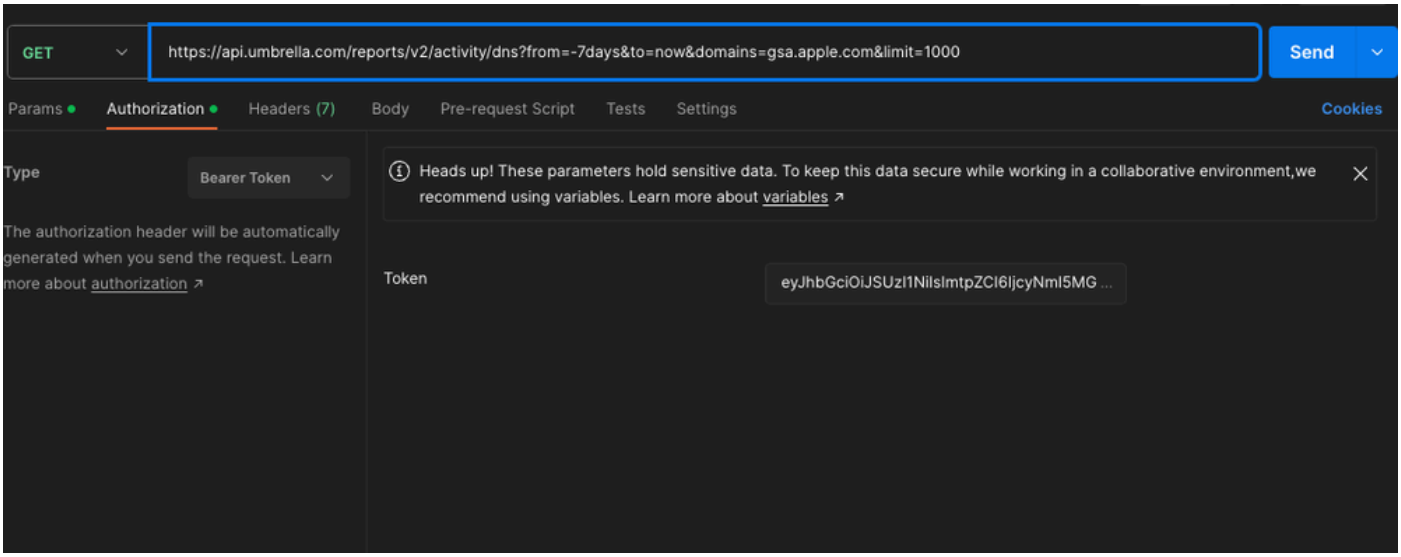
En este paso, se le solicita que recopile el token de acceso. Ahora puede recuperar información con el token de acceso.

Debe seleccionar el método GET e introducir la ruta de la API (incluido el parámetro que necesita) y el token de acceso. En este ejemplo, puede recuperar 100 informes de la búsqueda de actividad exclusivamente para tráfico DNS de los últimos 7 días.



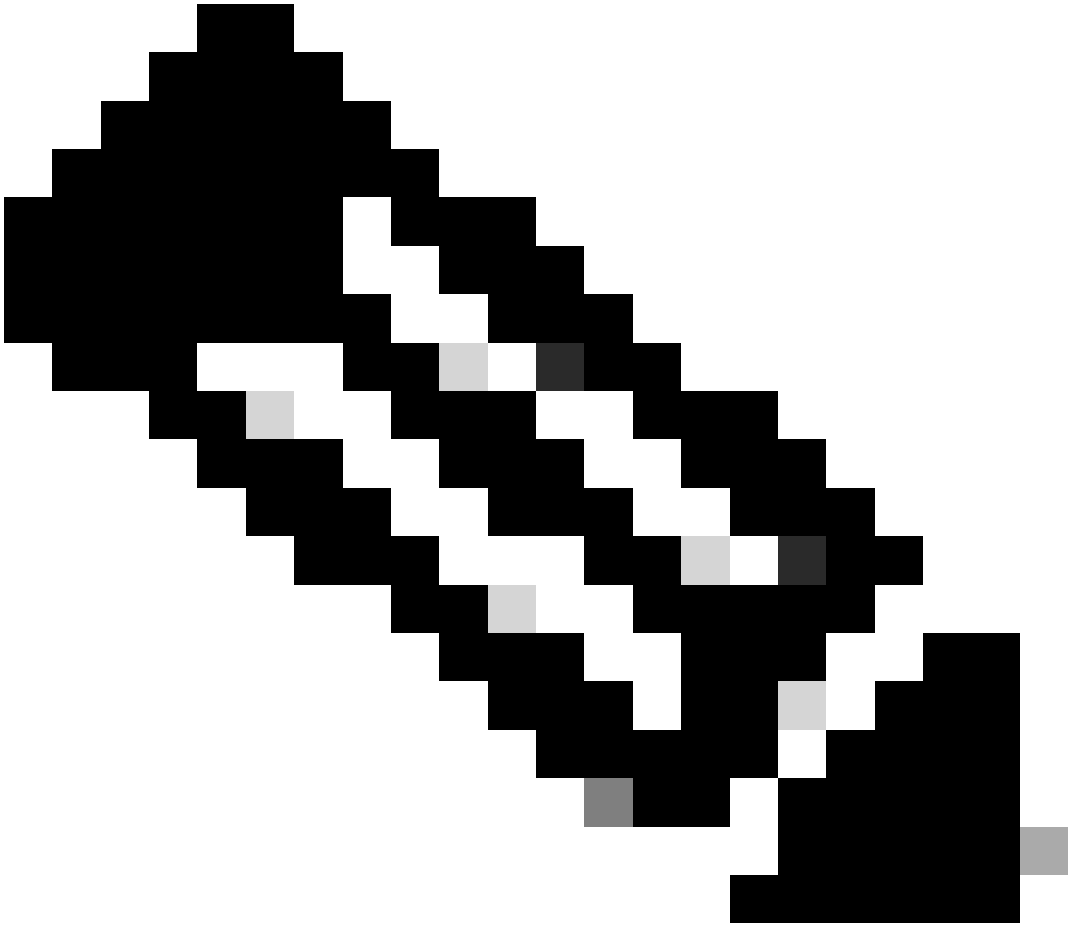
21607952074772

En otro ejemplo, puede intentar extraer 1000 informes de la búsqueda de actividad, exclusivamente para tráfico DNS durante los últimos 7 días, específicamente para el dominio "gsa.apple.com".



21607927544468

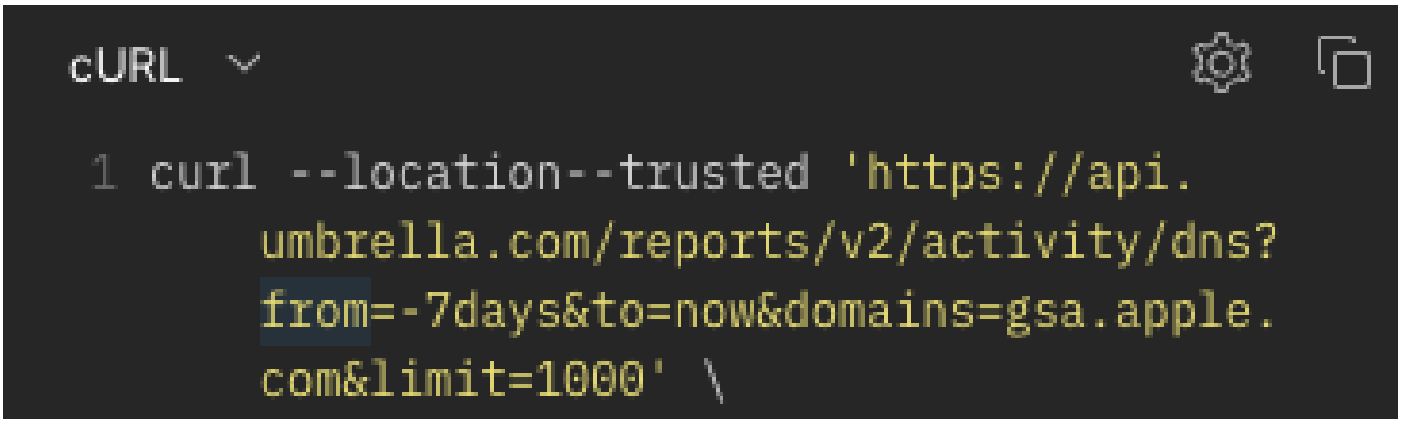
Puede consultar Request Query Parameters para descubrir parámetros adicionales que puede utilizar en su consulta de API.



Nota: Si una solicitud de cliente HTTP no se origina en el mismo continente que la ubicación del almacén de datos de Umbrella, el servidor de Umbrella responde con 302 Found. Para redirigir automáticamente las solicitudes HTTP y conservar el encabezado de autorización HTTP, puede establecer indicadores adicionales o habilitar una configuración de redirección.

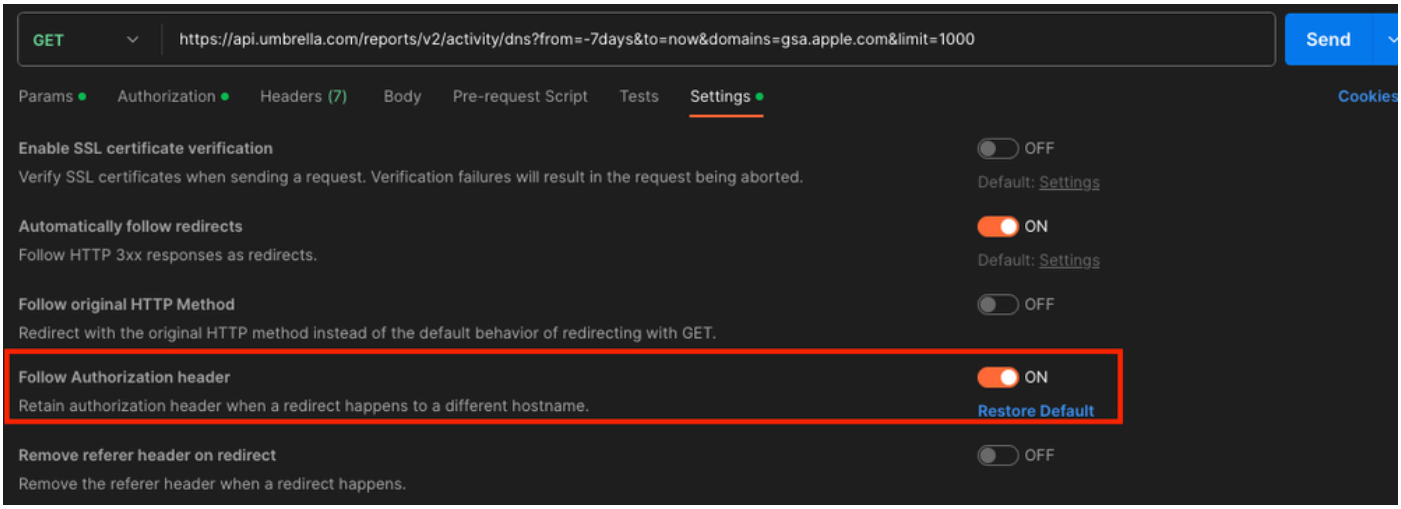
---

rizo: Debe pasar los indicadores -L o —location y —location-trusted para redirigir la solicitud HTTP curl y conservar el encabezado de autorización.



21608126036628

POSTMAN: En el entorno Postman, desplácese hasta una API y seleccione un método GET. Navegue hasta Configuraciones > Habilitar encabezado Seguir autorización para conservar el encabezado Autorización para las solicitudes de redireccionamiento.



21608126042388

Respuestas

Después de enviar la acción GET a la URL, puede recibir varios códigos de estado:

- Estado:200: La solicitud tomó correctamente la información que solicitó.
- Estado: 400: solicitud no válida. Puede estar relacionado con la URL que ha enviado a la consulta. Uno o más parámetros no son correctos.
- Estado: 401: No autorizado. Falta el encabezado de autorización o el token no está autorizado.
- Estado:403: Prohibido. El token no es válido.

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).