

Actualice el gateway de defensa de varias nubes desde el controlador de defensa de varias nubes

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Actualización de Multicloud Defense Gateway](#)

[Verificación](#)

[Supervise el proceso de actualización desde la lista de gateways.](#)

[Supervise el proceso de la puerta de enlace desde los registros del sistema.](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de actualización de Multicloud Defense Gateway desde Multicloud Defense Controller.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de defensa multicloud
- Multicloud Defense Gateway

Componentes Utilizados

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

- Multicloud Defense Gateway, versión 23.08-14.

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.

Antecedentes

El proceso de actualización no tiene impacto operativo ni tiempo de inactividad. Multicloud Defense Controller crea un nuevo conjunto de instancias con la nueva versión de la imagen. Una vez que las nuevas instancias están disponibles, el gateway comienza a procesar el tráfico. Una vez que se vacía el tráfico de las instancias antiguas, se eliminan las instancias antiguas.

Configurar

Actualización de Multicloud Defense Gateway

Estas imágenes muestran el proceso de actualización de la puerta de enlace de defensa de varias nubes. Los procesos de actualización del gateway de entrada y salida son los mismos.

1. En primer lugar, inicie sesión en el controlador de defensa de la nube múltiple y navegue hasta **Manage > Gateways**.

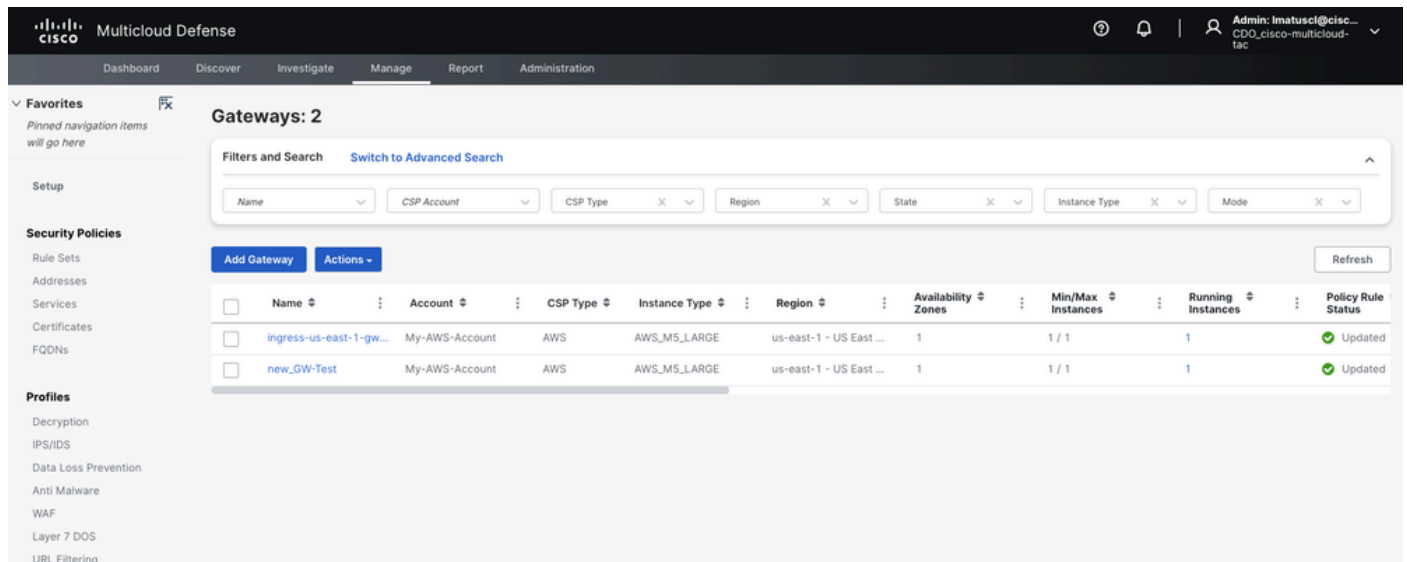


Imagen 1. Lista de gateway.

2. Identifique y seleccione la puerta de enlace que desea actualizar. Solo puede realizar una selección en este momento.

The screenshot shows the Cisco Multicloud Defense interface. On the left, there's a sidebar with navigation options like Setup, Security Policies, and Profiles. The main area is titled 'Gateways: 2' and contains a table of gateways. One gateway, 'ingress-us-east-1-gw-01', is highlighted with a red box. To the right, the 'Details' panel for this gateway is shown, with the 'Upgrade' button highlighted with a red box. The gateway details include Name, State (ACTIVE), Description, Instance Type (AWS_MS_LARGE), Min/Max Instances (1 / 1), Mode (HUB / Ingress), Policy Rule Set (cisco-cd-sample-ingress-policy-ruleset), Gateway Endpoint, Image, Packet Capture Profile, Log Profile, Metrics Profile, NTP Profile, and BGP Profile.

Imagen 2. Detalles del gateway.

3.a. Selecciónelo en la ventana **Upgrade** de detalles de la puerta de enlace.

This screenshot is identical to the previous one, showing the details of the 'ingress-us-east-1-gw-01' gateway. The 'Upgrade' button in the top right of the details panel is highlighted with a red box, indicating the next step in the process.

Imagen 3. Puede actualizar la puerta de enlace desde la ficha de detalles.

3.b. También puede seleccionar **Actions > Upgrade**.

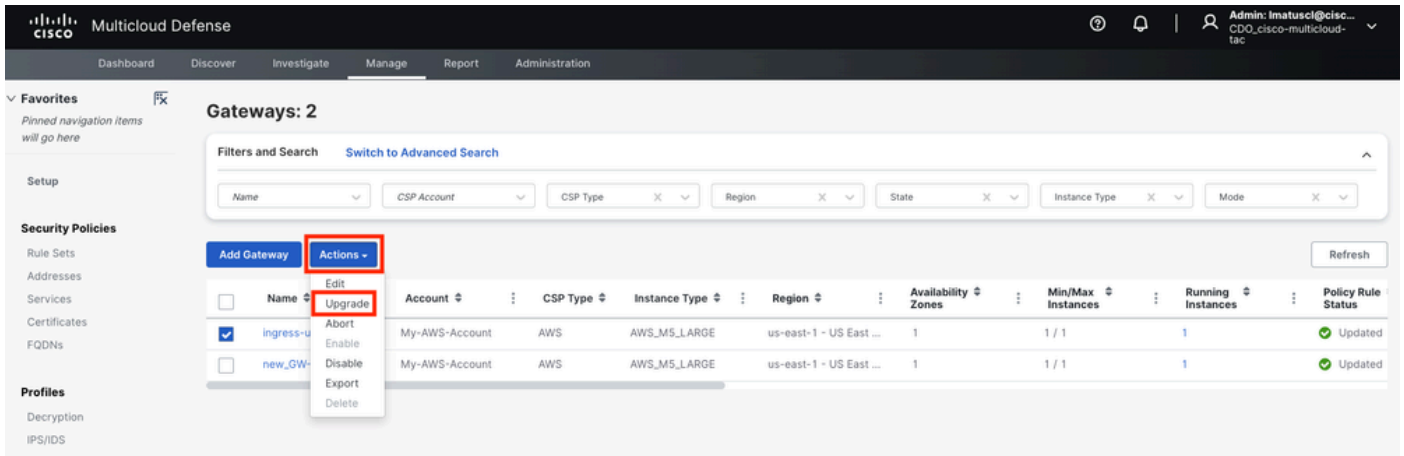


Imagen 4. Puede actualizar la puerta de enlace desde el botón Acción.

4. Seleccione el menú desplegable para mostrar las versiones de gateway disponibles. A continuación, seleccione la versión de destino y guarde los cambios.

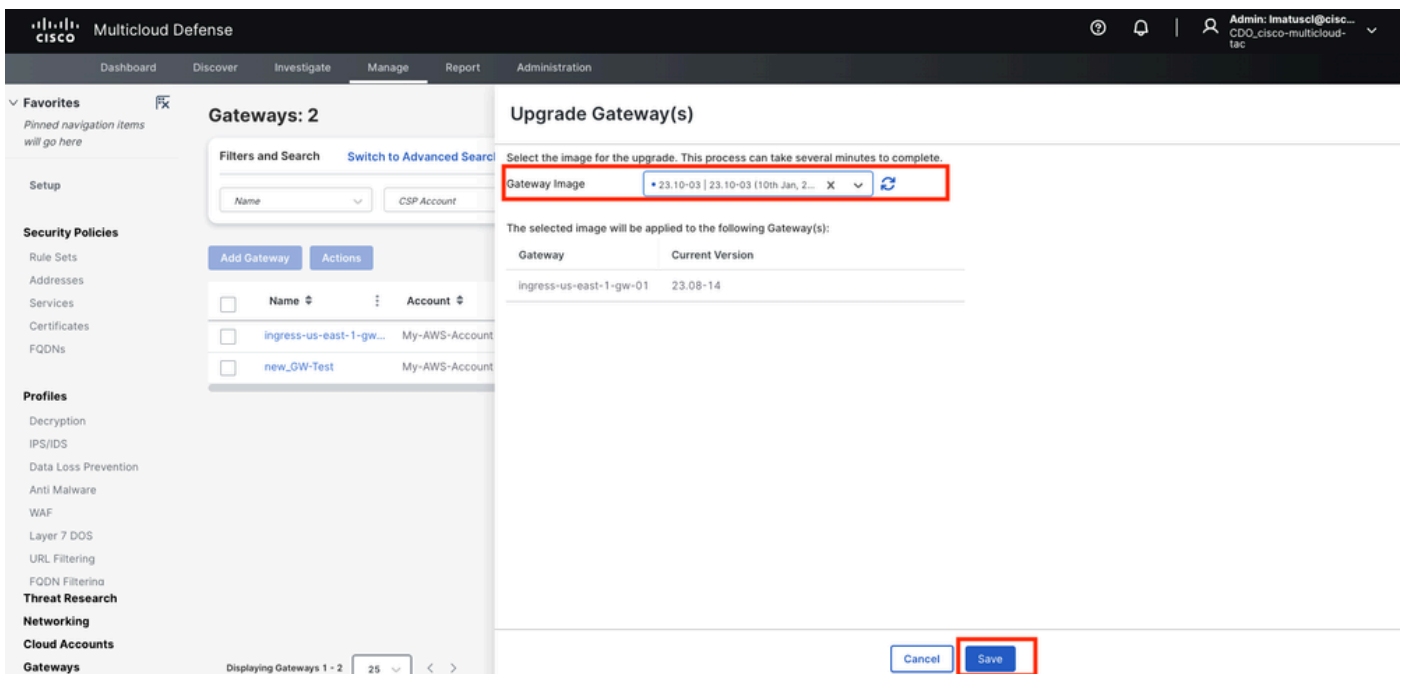


Imagen 5. Versiones de gateway disponibles.

Confirme la asignación de recursos del proveedor de servicios en la nube necesaria para la actualización.

6. Seleccione esta opción **Yes** si la asignación de recursos es suficiente. Haga clic en **No** si la asignación de recursos es insuficiente, aumente la asignación de recursos en el proveedor de servicios en la nube y vuelva para continuar la actualización.

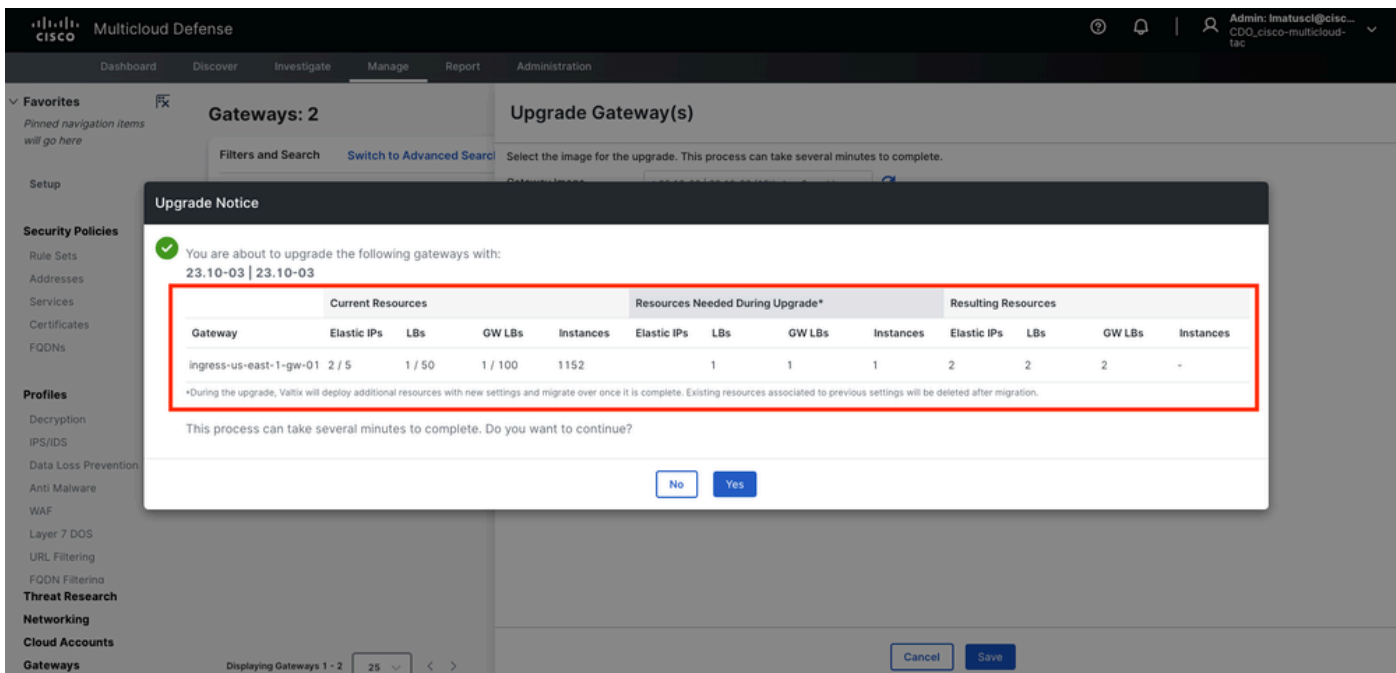


Imagen 6. Asignación de recursos en el proveedor de servicios en la nube.

Verificación

Supervise el proceso de actualización desde la lista de gateways.

El proceso puede tardar varios minutos en completarse. Puede supervisar el proceso desde la página de lista de puertas de enlace.

Desplácese hasta Manage > Gateways.

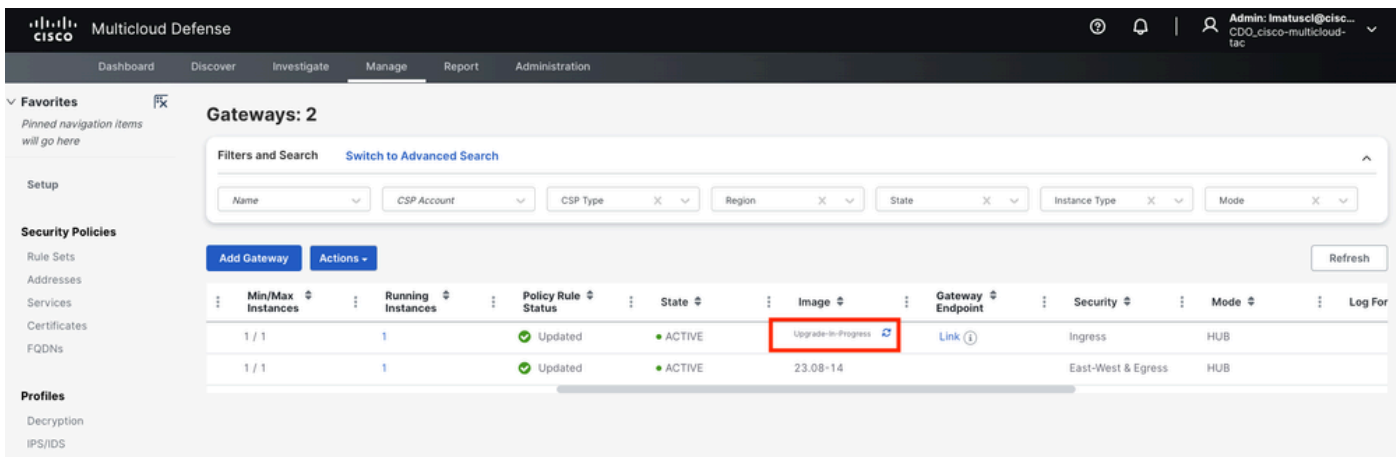


Imagen 7. Actualizar para supervisar el proceso de actualización.

Una vez finalizado el proceso de actualización, la puerta de enlace muestra la nueva versión.

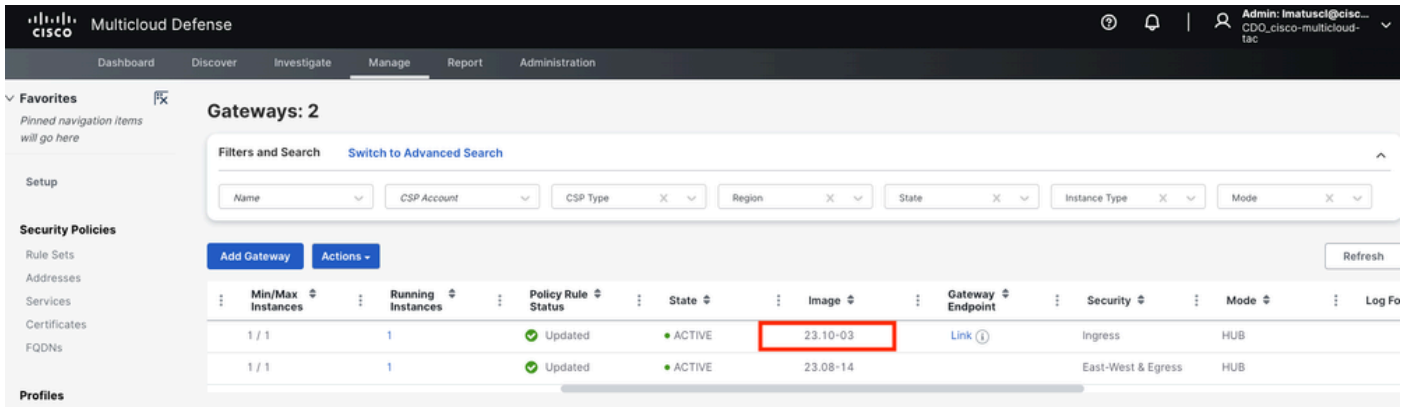


Imagen 8. Proceso de actualización finalizado.

Supervise el proceso de la puerta de enlace desde los registros del sistema.

Desplácese hasta Investigate > System Logs.

Puede ver la fecha y la hora en que se inicia y finaliza el proceso de actualización.

Seleccione **more** para mostrar más información sobre los registros del sistema.

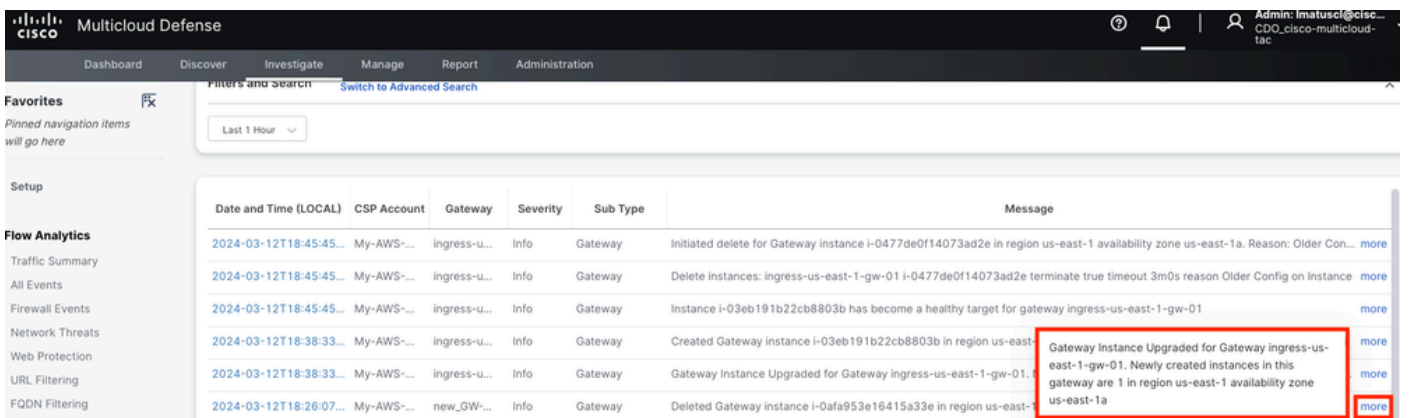


Imagen 9. Archivos de registro del sistema.

Esta imagen muestra cómo el registro del sistema muestra la creación de la nueva instancia de gateway y la eliminación de la anterior una vez que la nueva esté en buen estado y lista.

Date and Time (LOCAL)	CSP Account	Gateway	Severity	Sub Type	Message	
2024-03-12T18:48:51...	My-AWS-...	ingress-u...	Info	Gateway	Upgrade to DP Image Version 23.10-03 and CSP image ID ami-03ce47873675045eb is complete	more
2024-03-12T18:48:47...	My-AWS-...	ingress-u...	Info	Gateway	Deleted Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a	more
2024-03-12T18:45:45...	My-AWS-...	ingress-u...	Info	Gateway	Initiated delete for Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a. R...	more
2024-03-12T18:45:45...	My-AWS-...	ingress-u...	Info	Gateway	Delete instances: ingress-us-east-1-gw-01 i-0477de0f14073ad2e terminate true timeout 3m0s reason Older ...	more
2024-03-12T18:45:45...	My-AWS-...	ingress-u...	Info	Gateway	Instance i-03eb191b22cb8803b has become a healthy target for gateway ingress-us-east-1-gw-01	more
2024-03-12T18:38:33...	My-AWS-...	ingress-u...	Info	Gateway	Created Gateway instance i-03eb191b22cb8803b in region us-east-1 availability zone us-east-1a. Gateway In...	more
2024-03-12T18:38:33...	My-AWS-...	ingress-u...	Info	Gateway	Gateway Instance Upgraded for Gateway ingress-us-east-1-gw-01. Newly created instances in this gateway ar...	more

Imagen 10. Creación y eliminación de la instancia anterior y la nueva.

Esta imagen muestra todos los registros del sistema relacionados con el proceso de actualización de la puerta de enlace.

System Logs

Filters and Search [Switch to Advanced Search](#)

Last 1 Hour

Date and Time (LOCAL)	CSP Account	Gateway	Severity	Sub Type	Message
2024-03-12T18:48:51...	My-AWS...	ingress-u...	Info	Gateway	Upgrade to DP Image Version 23.10-03 and CSP image ID ami-03ce47873675045eb is complete
2024-03-12T18:48:47...	My-AWS...	ingress-u...	Info	Gateway	Deleted Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Initiated delete for Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a. Reason: Older Config on Insta...
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Delete instances: ingress-us-east-1-gw-01 i-0477de0f14073ad2e terminate true timeout 3m0s reason Older Config on Instance
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Instance i-03eb191b22cb8803b has become a healthy target for gateway ingress-us-east-1-gw-01
2024-03-12T18:38:33...	My-AWS...	ingress-u...	Info	Gateway	Created Gateway instance i-03eb191b22cb8803b in region us-east-1 availability zone us-east-1a. Gateway Instance Upgraded
2024-03-12T18:38:33...	My-AWS...	ingress-u...	Info	Gateway	Gateway Instance Upgraded for Gateway ingress-us-east-1-gw-01. Newly created instances in this gateway are 1 in region us-east-1 avail...

Imagen 1. Registros del sistema relacionados con el proceso de actualización del gateway.

Información Relacionada

- [Guía del usuario de Cisco Multicloud Defense](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

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).