Examine el servicio de inventario del centro DNA y los problemas comunes

Contenido

Introducción

Este documento describe los conceptos básicos del servicio de inventario de Cisco DNA Center y los problemas comunes encontrados en la producción.

Componentes Utilizados

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.

Detalles del servicio de inventario

El servicio de inventario de Cisco DNA Center se basa en un POD de Kubernetes (K8s) que puede encontrar en ejecución en el espacio de nombres "fusión" con el nombre "apic-em-Inventory-manager-service-<id>" como tipo de entorno de implementación.

Dentro de la vaina K8s, puede encontrar un contenedor Docker llamado "apic-em-Inventory-manager-service".

Las tareas principales del grupo de dispositivos "apic-em-Inventory-manager-service" son: detección de dispositivos y gestión del ciclo de vida de los dispositivos.

Esto garantiza que los datos del dispositivo estén disponibles en Postgres SQL (base de datos utilizada por los servicios de fusión).

El espacio de nombres "fusión" (Appstack) también conocido como plataforma de controlador de red (NCP), proporciona los servicios de Service Provisioning Framework (SPF) para todos los requisitos de automatización de la red.

Entre estas se incluyen detección, inventario, topología, política, gestión de imágenes de software (SWIM), archivo de configuración, programador de red, sitios, agrupación, telemetría, integración de Tesseract, programador de plantillas, mapas, IPAM, sensores, orquestación/flujo de trabajo/programación, integración con ISE y similares.

El estado del grupo de dispositivos del inventario se puede verificar ejecutando el comando:

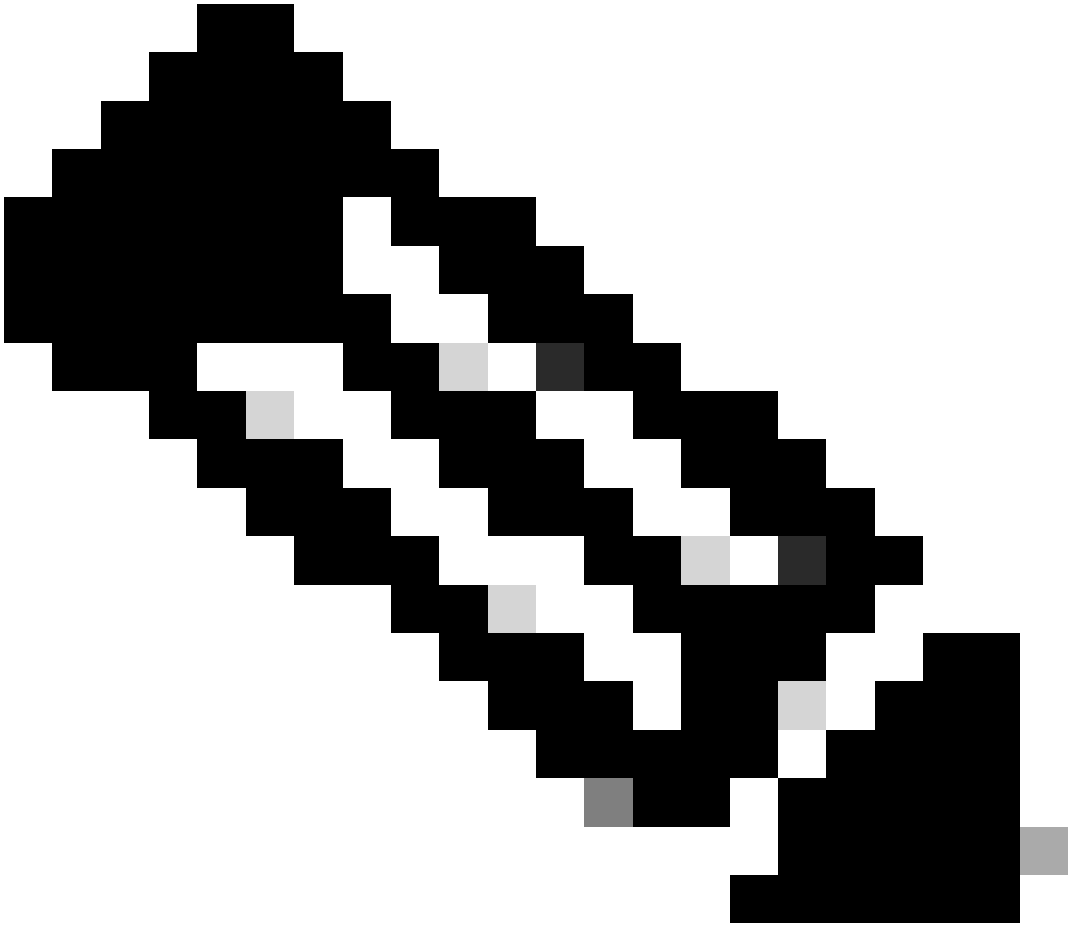
```
$ magctl appstack status | grep inventory
```

El estado del servicio de inventario se puede verificar con el comando:

```
$ magctl service status
```

Los registros de servicio de inventario se pueden verificar con el comando:

```
$ magctl service logs -r
```



Nota: El servicio de inventario también puede constar de dos grupos de dispositivos en ejecución, por lo que debe especificar un único grupo de dispositivos en los comandos mediante el nombre completo del grupo de dispositivos de inventario, incluido el grupo de dispositivos ID.

En este documento, podemos centrarnos en la capacidad de administración de dispositivos del inventario y el estado de la última sincronización para revisar los problemas comunes:

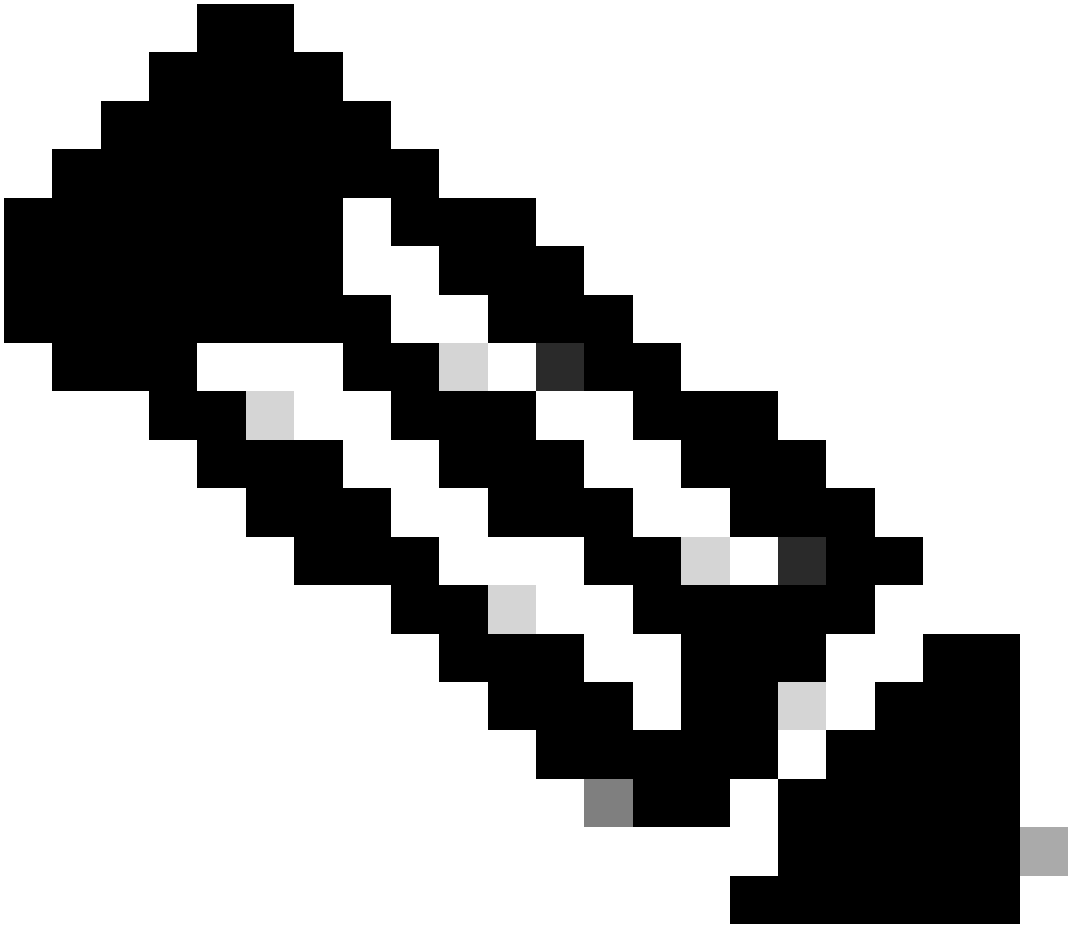
Estado de capacidad de gestión

- Gestionado con icono de marca de verificación verde: El dispositivo es accesible y está totalmente gestionado.
- Gestionado con icono de error naranja: El dispositivo se gestiona con algunos errores como inalcanzable, fallo de autenticación, puertos Netconf faltantes, error interno, etc. Coloque el cursor sobre el mensaje de error para ver más detalles sobre el error y las aplicaciones afectadas.
- No gestionado: No se puede alcanzar el dispositivo y no se recopiló información de

inventario debido a problemas de conectividad del dispositivo.

Estado de última sincronización

- Gestionado: El dispositivo se encuentra en un estado completamente administrado.
- Falla de recolección parcial: El dispositivo se encuentra en un estado de recopilación parcial y no se ha recopilado toda la información de inventario. Sitúe el cursor sobre el icono Información (i) para mostrar información adicional sobre el fallo.
- Inalcanzable: No se puede alcanzar el dispositivo y no se recopiló información de inventario debido a problemas de conectividad del dispositivo. Esta condición ocurre cuando se realiza una recolección periódica.
- Credenciales Erróneas: Si se cambian las credenciales del dispositivo después de agregar el dispositivo al inventario, se toma nota de esta condición.
- En curso: Se está recopilando el inventario.



Nota: Para obtener más información sobre las funciones de inventario de Cisco DNA Center, consulte la guía oficial de la versión 2.3.5.x: Administración del inventario

Problemas

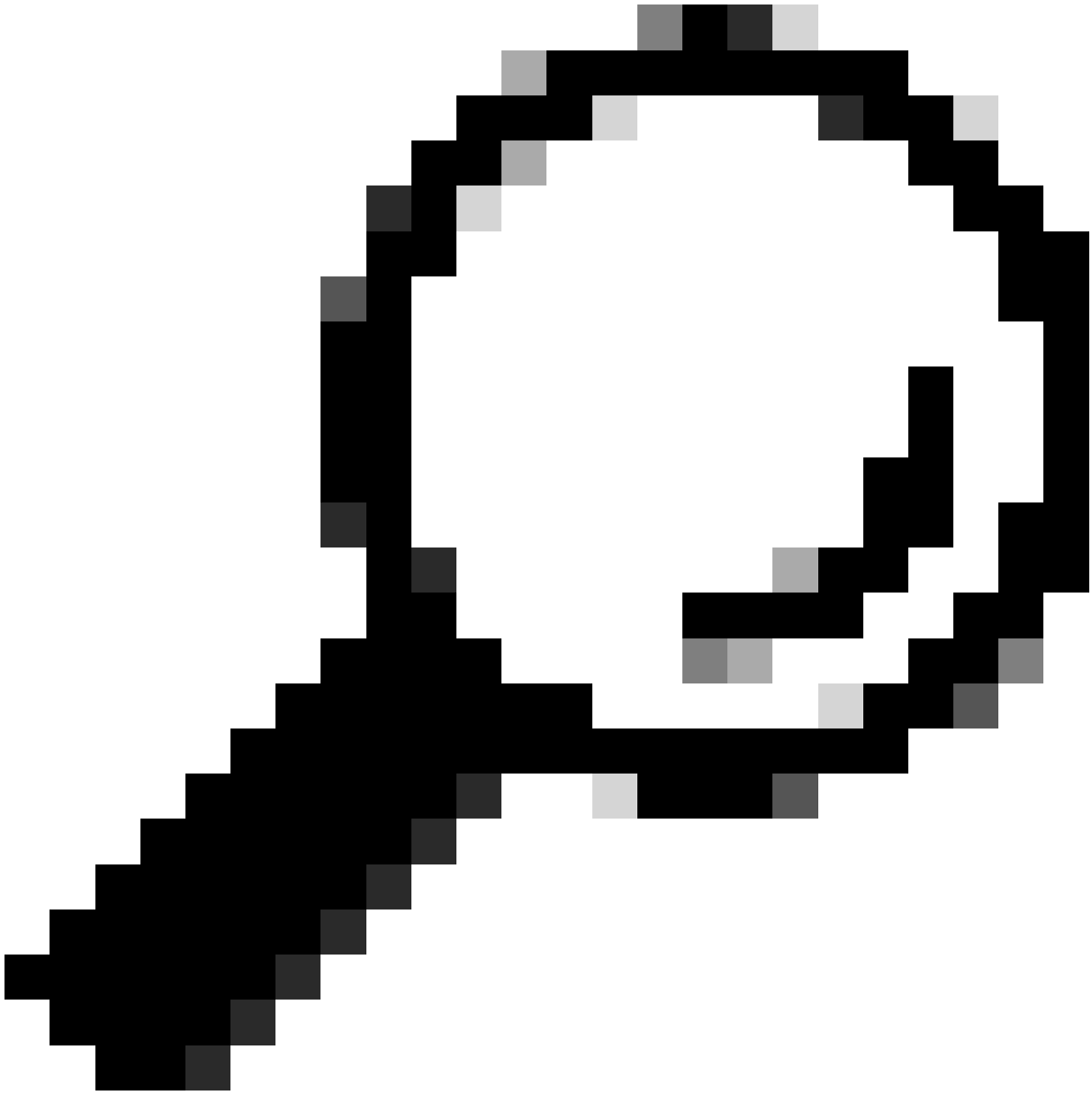
Internal Error

La página Cisco DNA Center Inventory puede mostrar un mensaje de advertencia en el estado Manageability para los dispositivos con algún tipo de conflicto que impide la recopilación de datos:

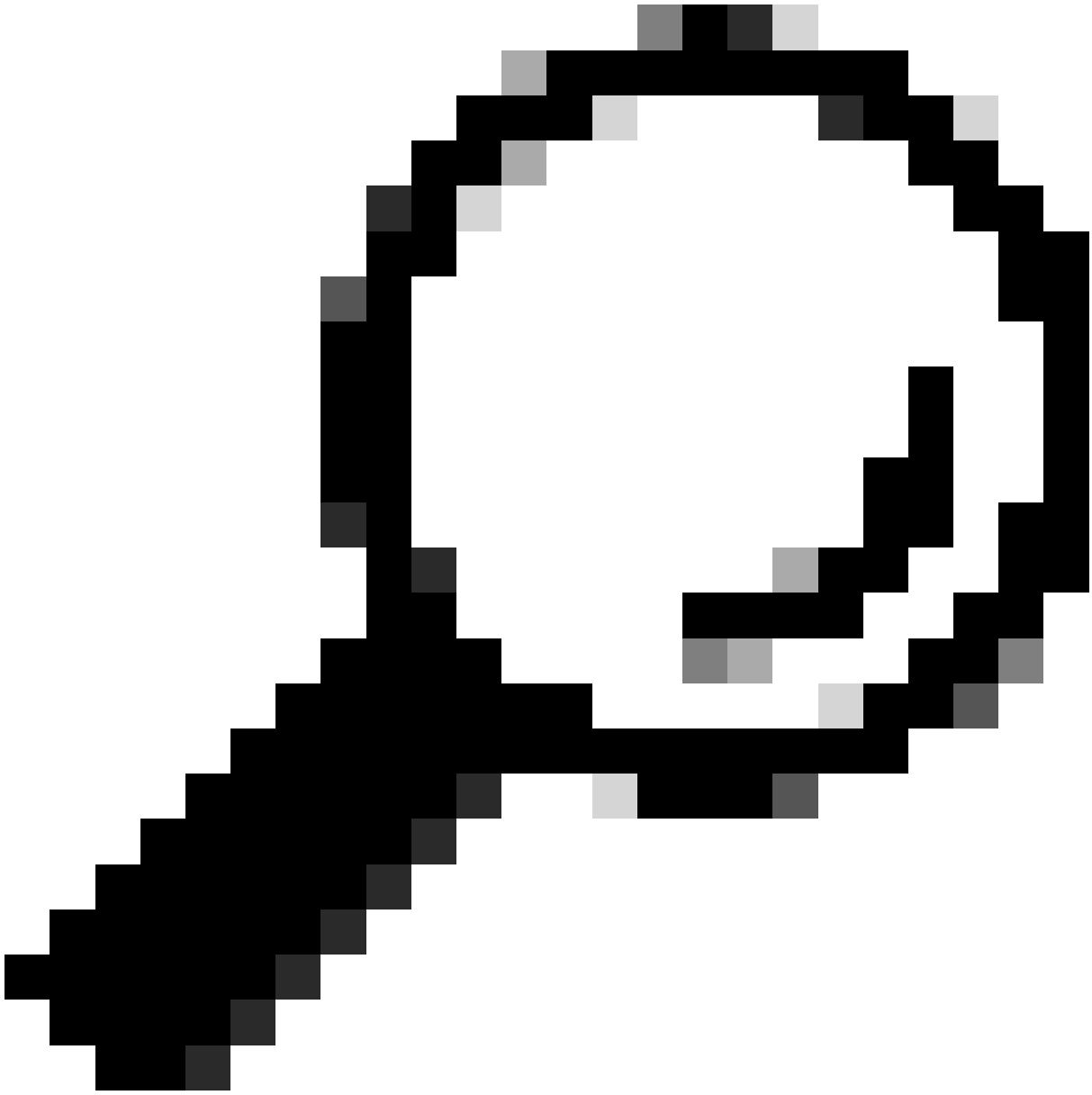
Error interno: NCIM12024: No se pudo recopilar correctamente toda la información del dispositivo o la recopilación de inventario para este dispositivo aún no se ha iniciado. Puede ser un problema temporal que se puede resolver automáticamente. Resincronice el dispositivo; si esto no resuelve el problema, póngase en contacto con el TAC de Cisco."

Si el error no se resuelve automáticamente o después de la sincronización de un dispositivo, podemos comenzar con la resolución de problemas inicial. Ese error puede deberse a múltiples razones, pero aquí, enumeramos solo algunas de las más comunes:

- Credenciales de dispositivo incorrectas para SNMP, SSH y Netconf.
- Problemas de conectividad de red relacionados con SNMP, SSH y Netconf.
- Los problemas de configuración de Netconf en el dispositivo hacen que Netconf no funcione correctamente.
- Desencadenar una sincronización de dispositivo mientras la sincronización de un dispositivo ya está en curso.
- Se han recibido varias trampas desde el dispositivo, lo que ha provocado varios desencadenadores de sincronización en un breve período de tiempo.
- Problemas de administración con entradas de bases de datos de inventario en varias tablas relacionadas con el dispositivo.



Consejo: La eliminación del dispositivo de red y su redetección mediante las credenciales CLI, SNMP y NETCONF correctas pueden ayudar a eliminar las entradas de base de datos obsoletas que podrían estar causando el error interno.



Consejo: La revisión de los registros del servicio de inventario y el filtrado por IP de dispositivo o nombre de host pueden ser útiles para identificar la causa raíz del error interno.

Credenciales del dispositivo

Para revisar las credenciales del dispositivo, navegue hasta el Menú del Cisco DNA Center -> Provisión -> Inventario -> Seleccionar dispositivo -> Acciones -> Inventario -> Editar dispositivo y haga clic en "Validar" y confirme que las credenciales obligatorias (CLI y SNMP) están pasando la validación con una marca verde (incluido netconf si se aplica).

Si la validación falla, revise que el nombre de usuario y la contraseña que Cisco DNA Center utiliza para administrar el dispositivo de red sean válidos directamente en la línea de comandos del dispositivo.

Si están configurados localmente o si están configurados en un servidor AAA (TACACS o RADIUS), valide que el nombre de usuario y la contraseña están configurados correctamente en el servidor AAA.

También verifique si el privilegio de nombre de usuario requiere tener la configuración de la contraseña "Enable" en la Configuración de credenciales de dispositivo en Cisco DNA Cintroduzca Inventario.

Los errores en las credenciales CLI pueden causar un mensaje de error de capacidad de administración en el inventario: Falla de autenticación CLI.

Netconf

Netconf es un protocolo para administrar de forma remota un dispositivo de red compatible a través de llamadas a procedimiento remoto (RPC).

Cisco DNA Center utiliza las funciones de Netconf para introducir o eliminar la configuración de los dispositivos de red con el fin de habilitar funciones como la supervisión a través de Assurance.

El inventario de Cisco DNA Center también puede validar que los requisitos de Netconf son correctos, lo que incluye:

- El puerto predeterminado Netconf 830 debe estar abierto y funcionar en la red.
- Usuario con privilegio 15 con acceso SSH al dispositivo de red (configurado localmente o AAA).
- Active Netconf en el dispositivo de red:

<#root>

(config)#

netconf-yang

- Si aaa new-model está habilitado, también debe configurar los requisitos de configuración predeterminada de AAA:

<#root>

(config)#

aaa authorization exec default

(config)#

aaa authentication login default

Los errores en las credenciales de Netconf pueden causar un mensaje de error de manejabilidad en Inventory: Error De Conexión Netconf.

Comprobaciones de red

También podemos validar la conectividad de red y la configuración de protocolos, como la configuración SNMP, según la versión.

Por ejemplo, podemos verificar la configuración de comunidad, usuario, grupo, engineID, autenticación y cifrado, etc. dependiendo de la versión de SNMP.

También podemos revisar la conectividad SSH y SNMP usando los comandos ping y traceroute en la línea de comandos del dispositivo y los puertos para SSH (22) y SNMP (161 y 162) en el firewall, proxy o listas de acceso.

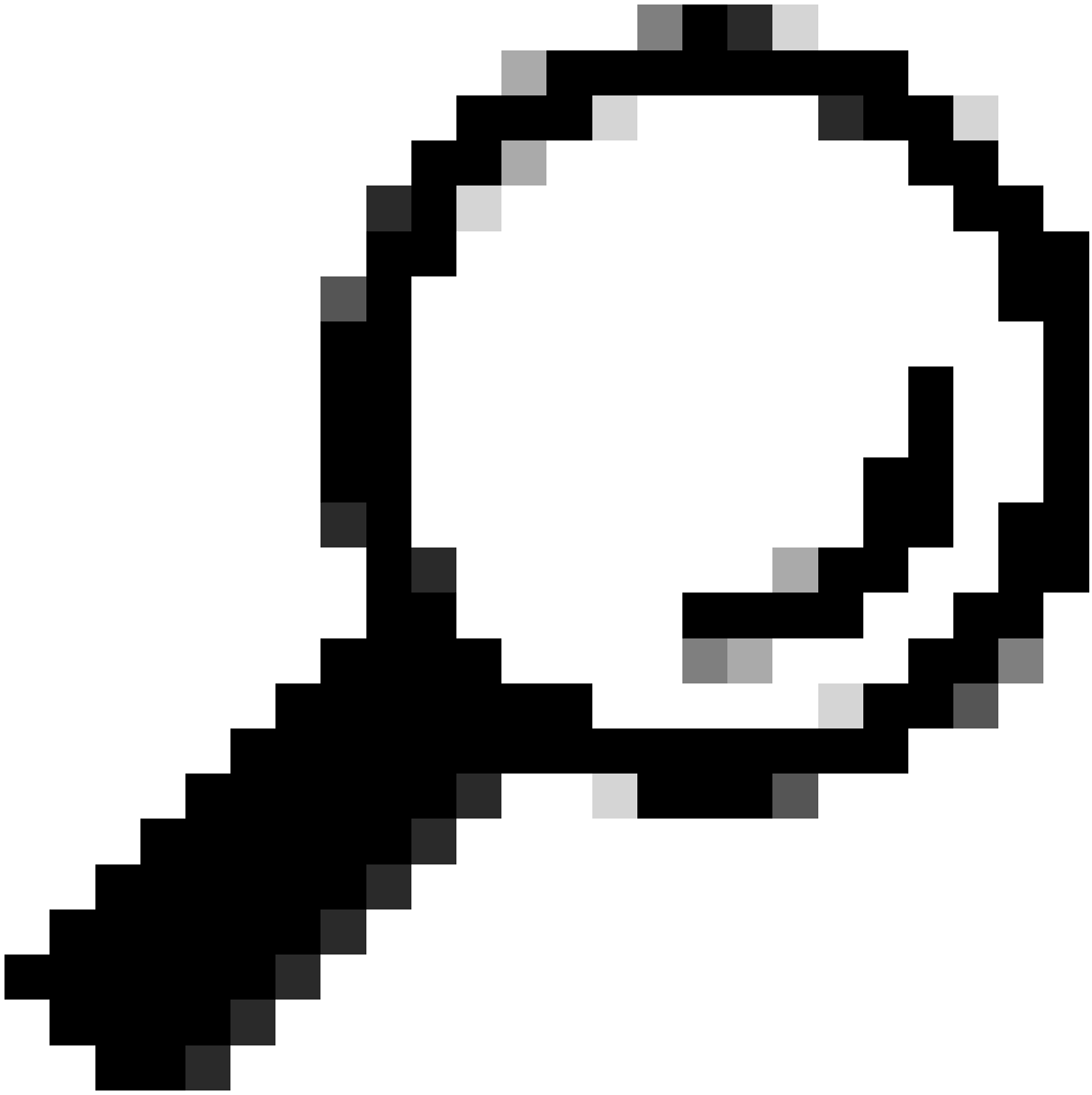
Desde Cisco DNA Center, maglev CLI, utilizamos los comandos ip route para validar la conectividad con el dispositivo de red.

SNMP walk también se puede utilizar para resolver problemas.

Los errores en las credenciales SNMP pueden causar un mensaje de error de manejabilidad en Inventory: Error de autenticación SNMP o Dispositivo inalcanzable.

Tablas de base de datos

Como usuario final, puede utilizar la GUI de Cisco DNA Center con Grafana para ejecutar consultas SQL para no tener que acceder al shell de Postgres a través de la CLI de maglev.

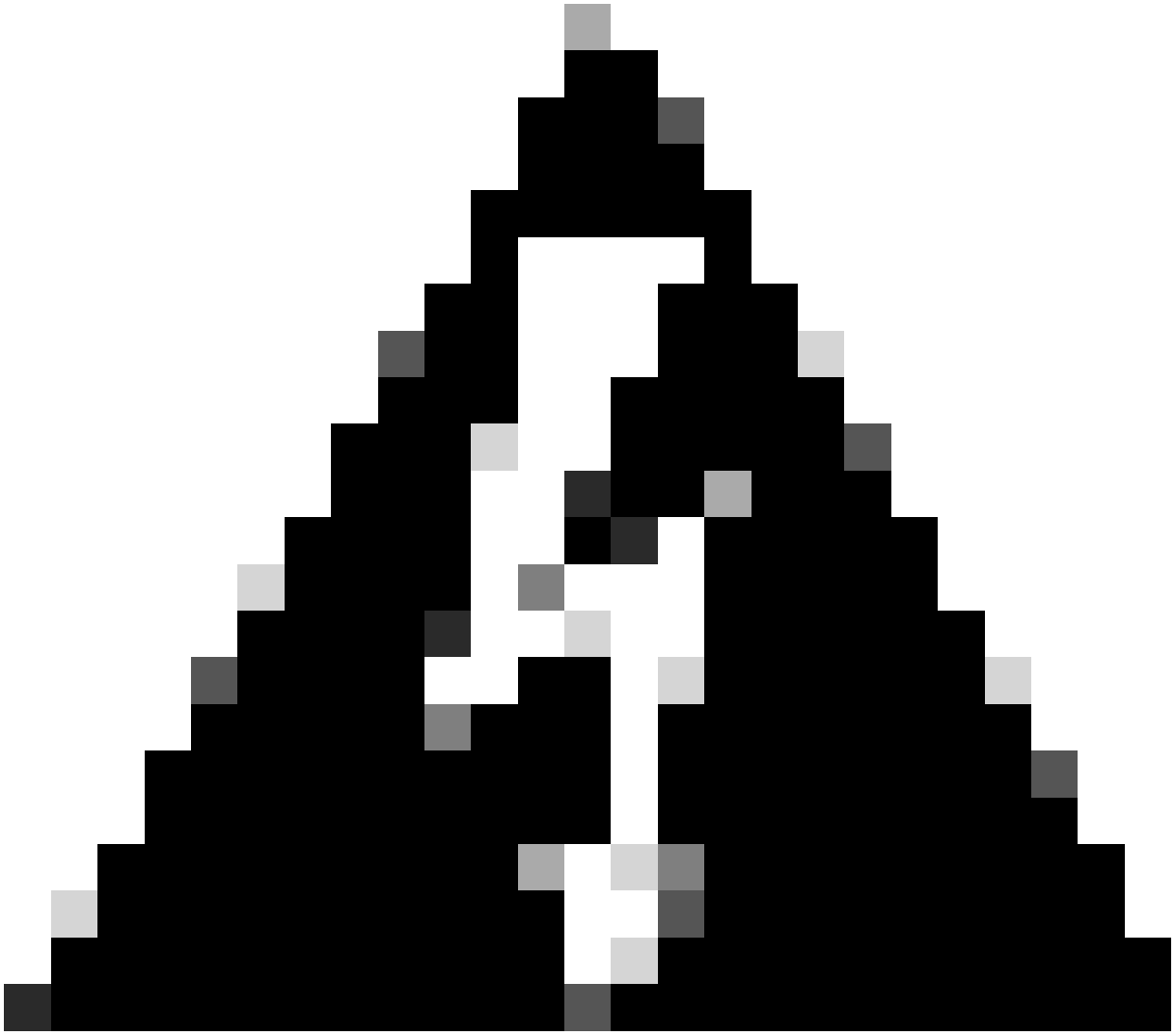


Consejo: Si desea aprender a utilizar Grafana, consulte la guía oficial: Ejecución de consultas Postgres en la GUI del Cisco DNA Center

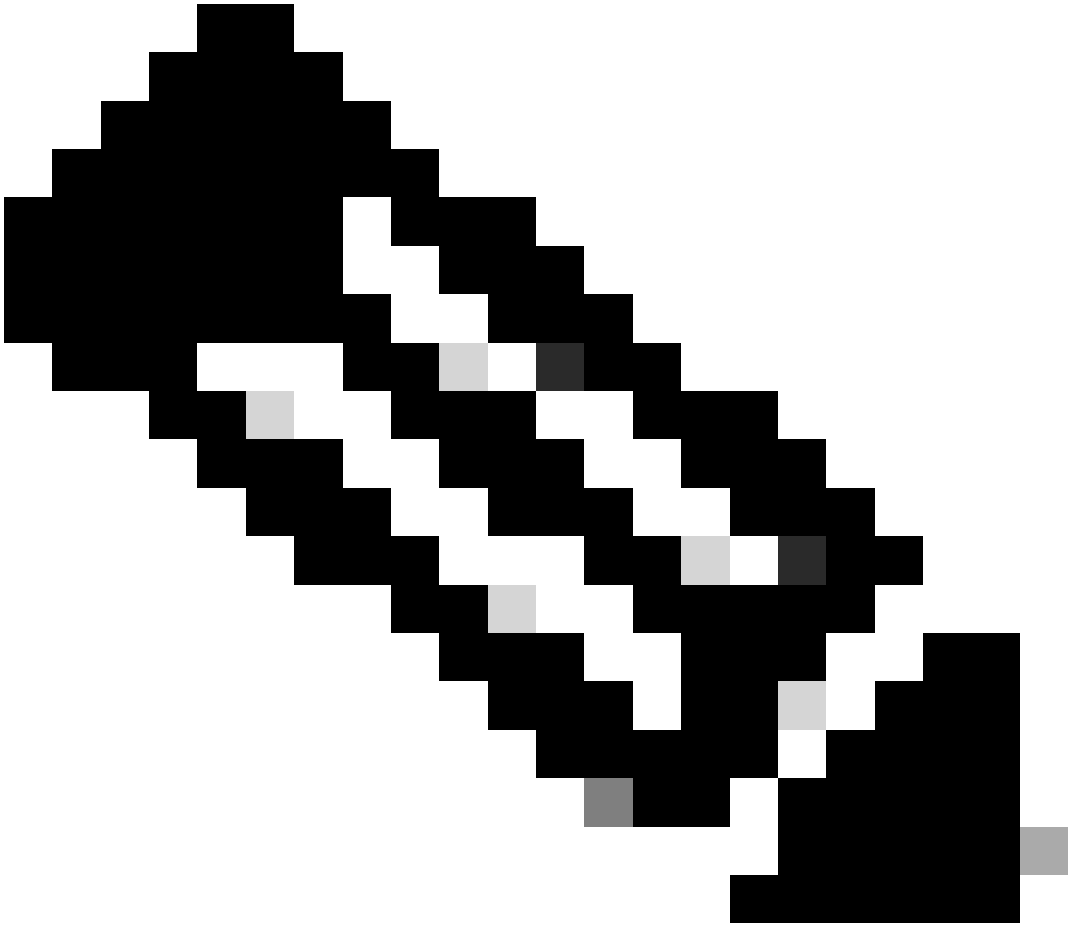
---

Algunas tablas de bases de datos postgres para revisar cuando se tienen problemas con los dispositivos de red en Inventory son:

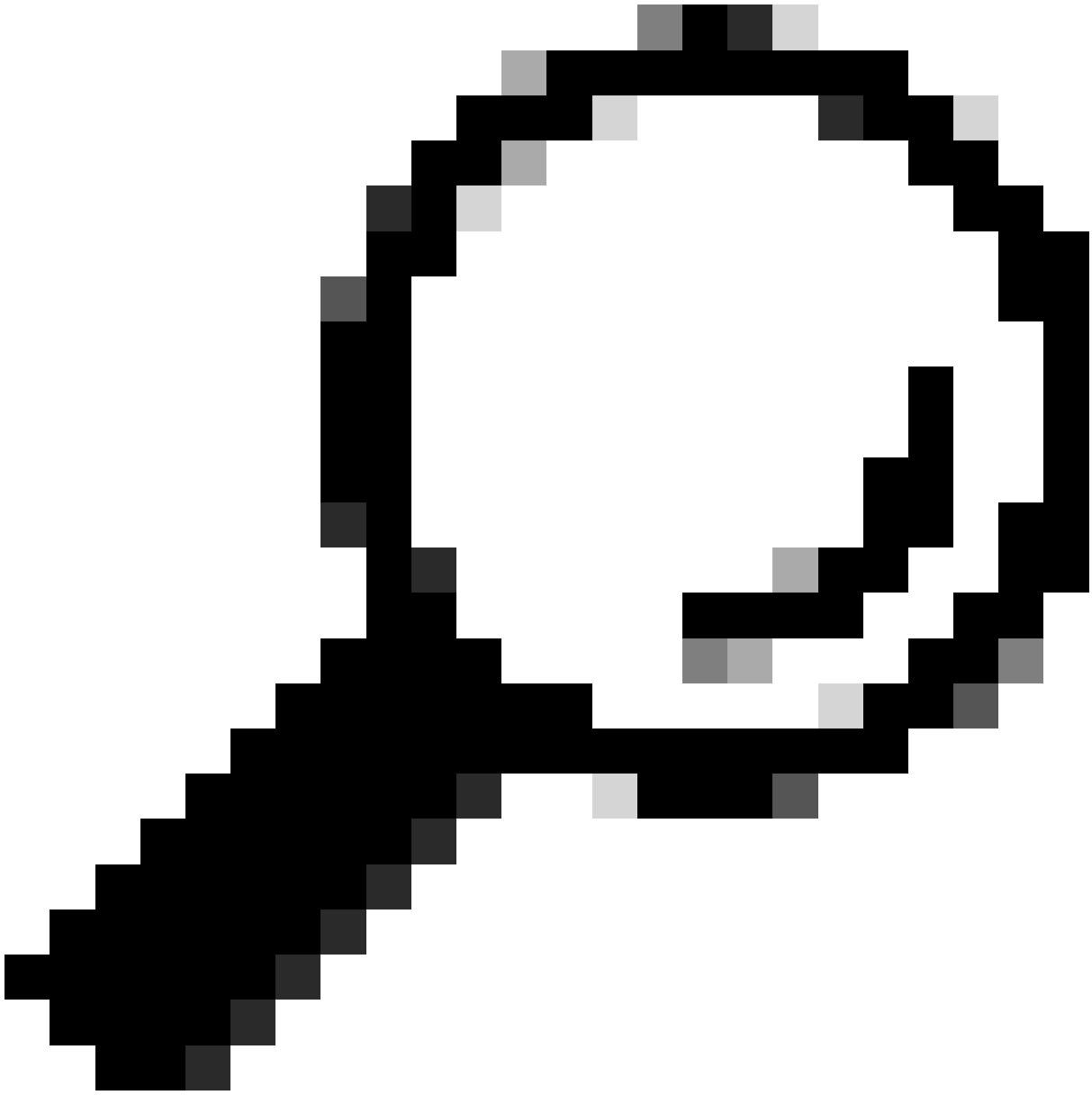
- dispositivo de red
- interfazDeGestión
- elemento de red
- recurso de red
- dispositivo si
- dirección IP



Advertencia: Solo Cisco TAC puede ejecutar show queries en el Shell de Postgres y solo los equipos BU/DE pueden hacer modificaciones en las tablas DB.



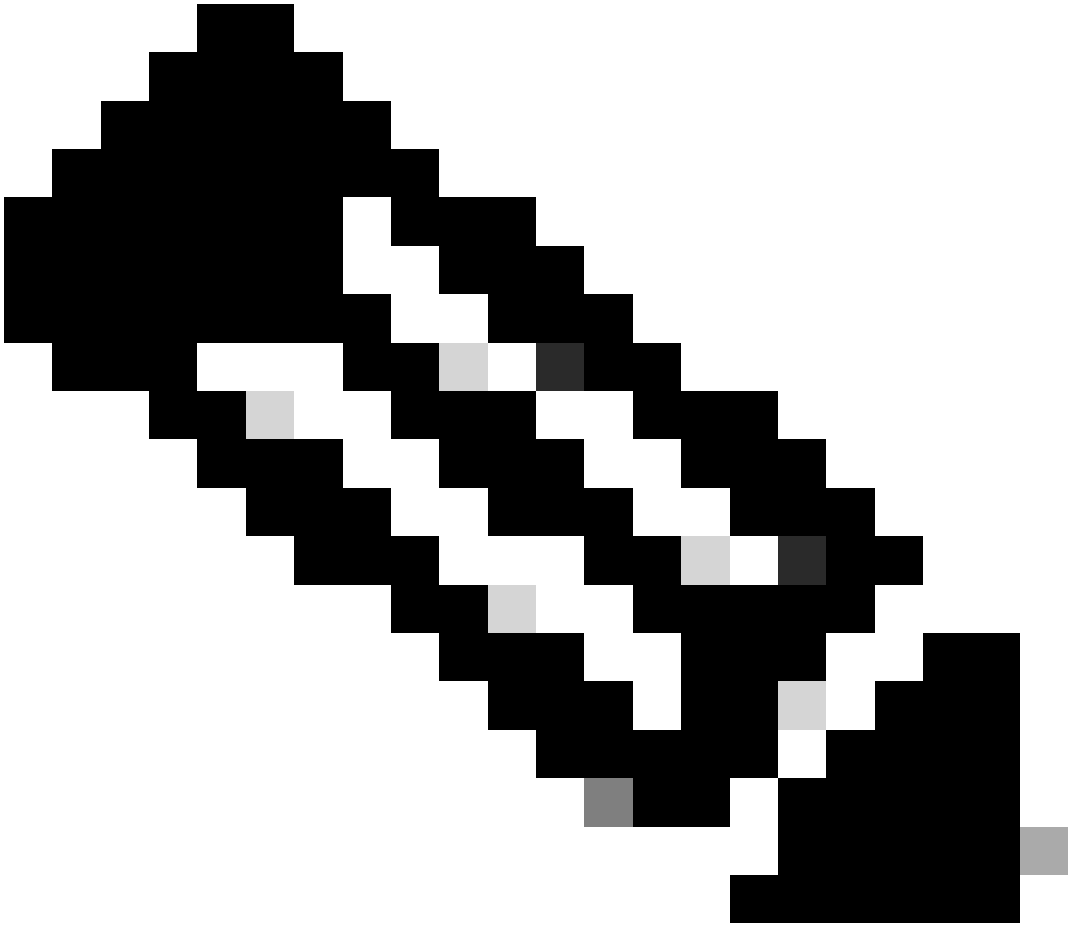
Nota: Los problemas de la base de datos también pueden causar el mensaje de error interno para los dispositivos que pueden impedir la recopilación de datos y el aprovisionamiento de dispositivos.



Consejo: Puede revisar los registros de Postgres mediante Kibana en la página Cisco DNA Center System 360 y buscar infracciones de restricciones cuando el servicio de inventario intente guardar o actualizar entradas en las tablas de la base de datos de Postgres.

Bucle de sincronización y desvíos

Cisco DNA Center está diseñado para ejecutar un resync de dispositivo cada vez que recibe una trampa del dispositivo después de que se realice un cambio importante en el propio dispositivo con el fin de mantener actualizado el inventario de Cisco DNA Center. A veces, la página de inventario de Cisco DNA Center mantiene los dispositivos de red en el estado "Sincronización" en la sección Capacidad de gestión durante un largo período de tiempo o para siempre.



Nota: Este tipo de loops de sincronización debido a trampas masivas puede hacer que Cisco DNA Center autentique varias veces en un corto período de tiempo a los dispositivos que están enviando las trampas debido a los cambios detectados.

API para forzar la sincronización de dispositivos

Si el dispositivo de red permanece en estado Sincronización durante demasiado tiempo, incluso días, revise primero las comprobaciones básicas de disponibilidad y conectividad. A continuación, fuerce la sincronización del dispositivo a través de una llamada API:

1.- Abra la sesión de Cisco DNA Center maglev CLI.

2.- Obtenga el token de autenticación del Cisco DNA Center a través de la API:

<#root>

curl -s -X POST -u admin https://kong-frontend.maglev-system.svc.cluster.local/api/system/v1/identitymg

3.- Utilice el token del paso anterior para ejecutar la API para forzar la sincronización del dispositivo:

<#root>

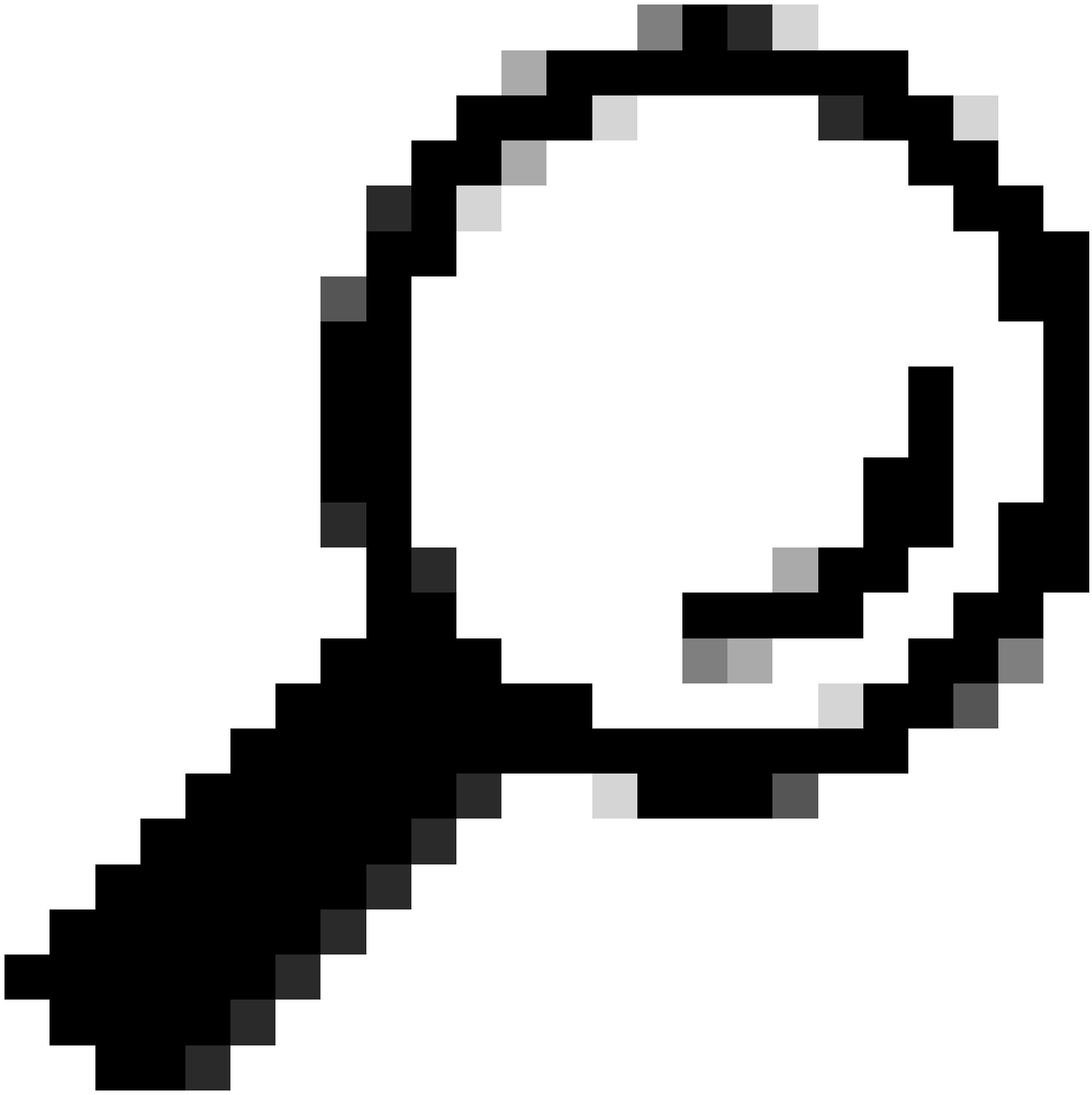
curl -X PUT -H "X-AUTH-TOKEN:

" -H "content-type: application/json" -d '

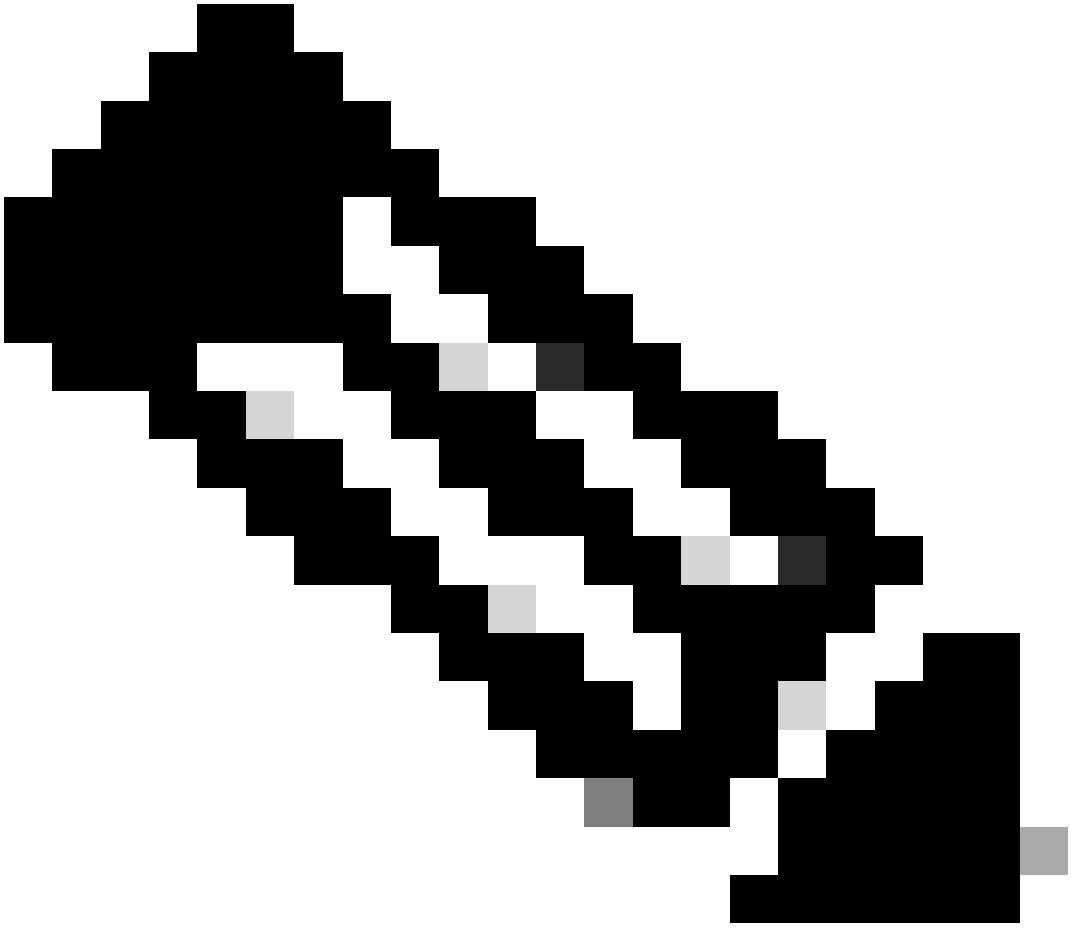
' https://

/api/v1/network-device/sync-with-cleanup?forceSync=true --insecure

4.- Puedes ver el dispositivo en Sincronización una vez más, pero esta vez con una opción de Force Sync a través de API.



Consejo: Puede obtener el uuid del dispositivo desde la URL del navegador (id o id del dispositivo) desde la página Cisco DNA Center Inventory Device Details o la página Device View 360.



Nota: Para obtener más información sobre las API de Cisco DNA Center, consulte la Guía de API de Cisco DevNet

---

Revisar desvíos

Si el problema persiste después de forzar la tarea de sincronización en el dispositivo, podemos revisar si el "servicio de eventos" de Cisco DNA Center está recibiendo demasiadas trampas y revisar qué tipo de trampas leyendo los registros del servicio de eventos:

1.- Antes de leer los registros podemos simplemente comprobar el total de trampas con el comando:

<#root>

$ echo;echo;eventsId=$(docker ps | awk '/k8s_apic-em-event/ {print $1}'); docker cp $eventsId:/opt/CSCOlumos/logs/ /tmp/;for ip in $(awk -F\: '/ipAddres

2.- Luego adjuntamos al contenedor de servicios de eventos:

<#root>

```
$ magctl service attach -D event-service
```

3.- Una vez que se encuentre dentro del contenedor de servicios de eventos, cambie el directorio a la carpeta logs:

<#root>

```
$ cd /opt/CSCOlumos/logs/
```

4.- Si revisas los archivos dentro del directorio podrás ver algunos archivos de logs cuyo nombre empieza por "ncs".

Ejemplo:

<#root>

```
root@apic-em-event-service-586df7d4b8-f9c74:/opt/CSCOlumos/logs#

ls -l

total 90852
drwxr-xr-x 1 maglev maglev     4096 May  9 21:33 ./
drwxr-xr-x 1 maglev maglev     4096 Apr 29 17:56 ../

-rw-r--r-- 1 root root 2937478 May 9 21:37 ncs-0-0.log -rw-r--r-- 1 root root 0 Apr 29 23:59 ncs-0-0.log

-rw-r--r-- 1 root   root        424 Apr 30 00:01 nms_launchout.log
-rw-r--r-- 1 root   root        104 Apr 30 00:01 serverStatus.log
```

5.- Esos archivos "ncs" son los que necesitamos para analizar qué tipo de trampas estamos recibiendo y cuántas. Podemos revisar los archivos de registro filtrándolos por nombre de host del dispositivo o la palabra clave "trapType":

<#root>

```
root@apic-em-event-service-586df7d4b8-f9c74:/opt/CSCOlumos/logs#

grep trapType ncs*.log

root@apic-em-event-service-586df7d4b8-f9c74:/opt/CSCOlumos/logs#

grep
```

ncs*.log

Hay demasiados tipos de trampas, algunas de ellas pueden activar la resincronización del dispositivo y si vienen con demasiada frecuencia pueden causar el loop de sincronización.

Al analizar las trampas podemos identificar la causa raíz y hacer que las trampas se detengan, por ejemplo, un AP en un ciclo de reinicio.

Puede guardar la salida de las trampas en un archivo y compartirlas con el equipo de escalado si es necesario.

Estado de caída del servicio

Si sospecha que el grupo de dispositivos del inventario está fallando debido a un comportamiento extraño en la página Cisco DNA Center Inventory mientras administra los dispositivos de red, puede validar primero el estado del grupo de dispositivos:

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

Al revisar la salida del estado del grupo de dispositivos, si observa un gran número de reinicios o un estado de error, puede adjuntar al contenedor de inventario y recopilar el archivo de volcado de memoria que puede tener los datos que pueden ayudar al equipo de escalado a analizar y

definir la causa raíz del estado de bloqueo:

<#root>

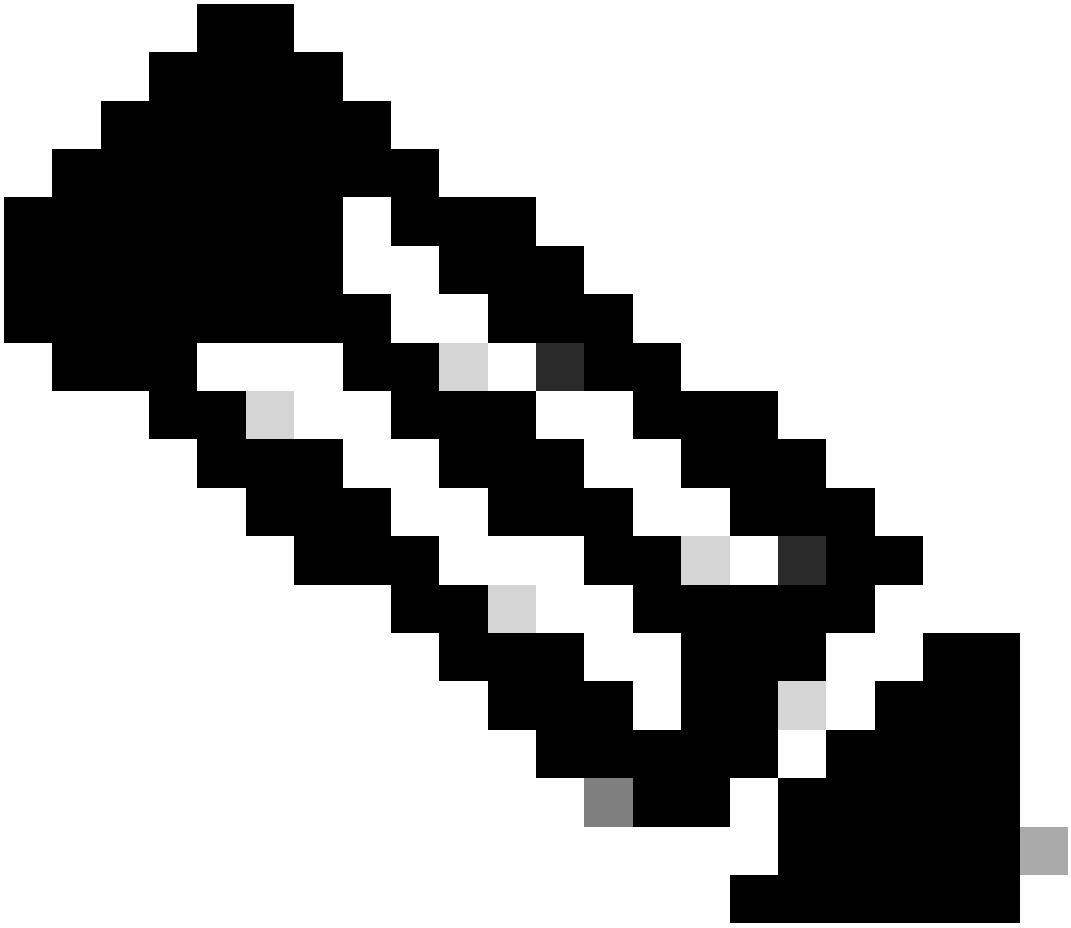
$ magctl service attach -D

root@apic-em-inventory-manager-service-76f7f8d7f5-427m5:/#

ll /opt/maglev/srv/diagnostics/ | grep heapdump

-rw-r--r-- 1 root root 1804109 Jul 20 21:16

apic-em-inventory-manager-service-76f7f8d7f5-427m5.heapdump



Nota: Si no se encontró ningún archivo heapdump en el directorio contenedor, no había ningún estado de bloqueo en el contenedor.

No se puede eliminar un dispositivo

En algunas situaciones, Cisco DNA Center puede no poder eliminar un dispositivo de red de la interfaz de usuario del inventario debido a un problema de backend.

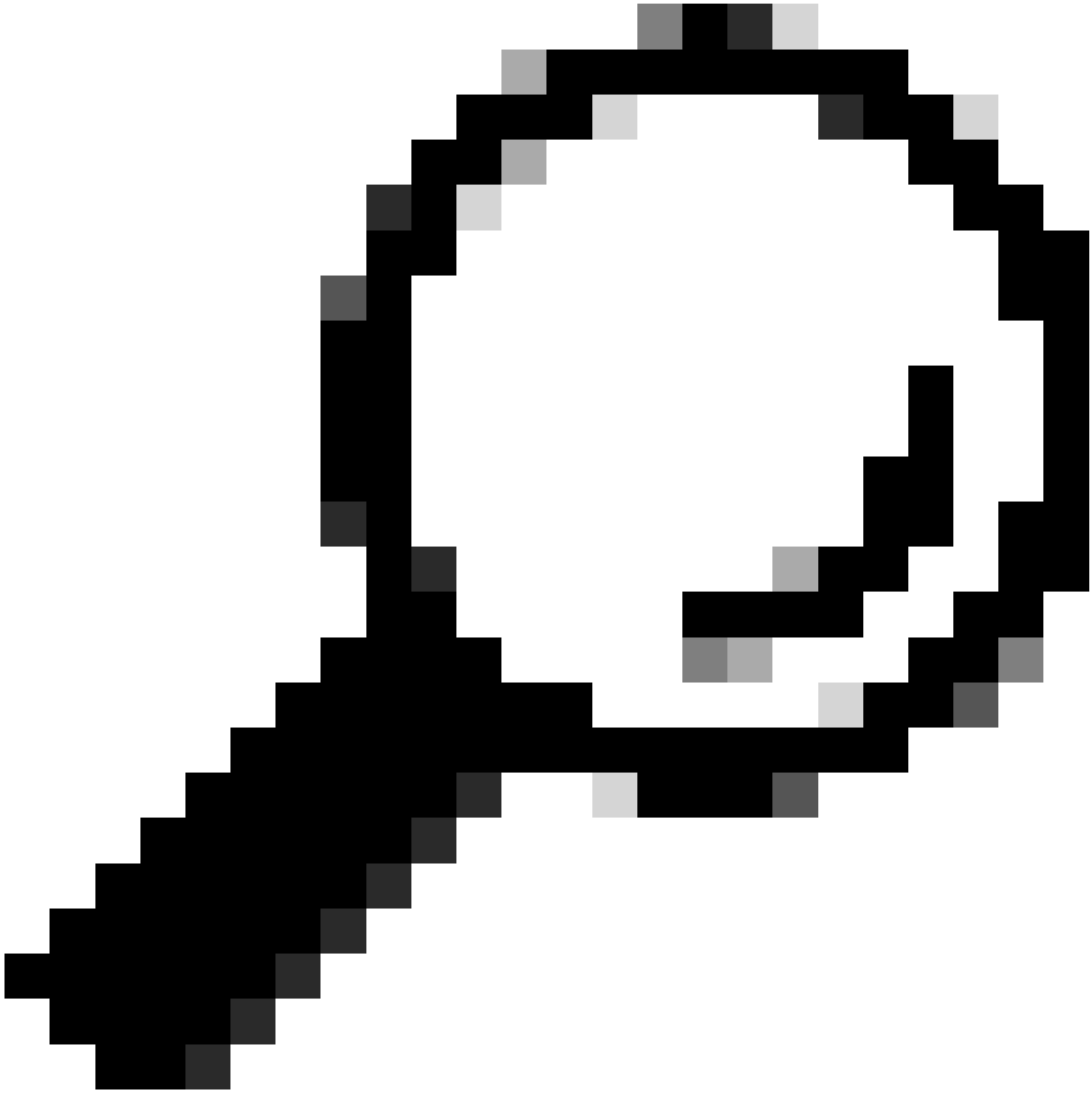
API para forzar la eliminación de dispositivos

Si no puede eliminar el dispositivo del inventario mediante la GUI de Cisco DNA Center, puede utilizar la API para eliminar el dispositivo por ID:

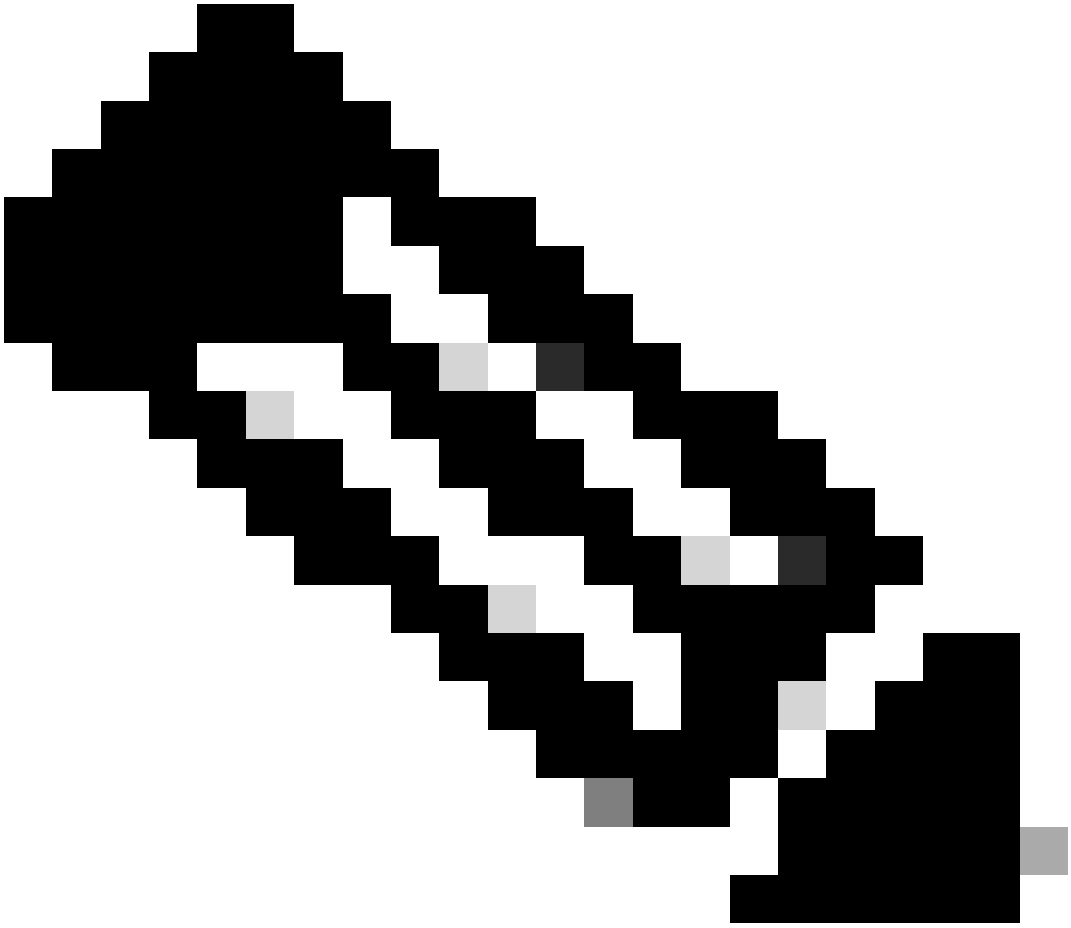
1.- Navegue hasta el Menú de Cisco DNA Center -> Plataforma -> Kit de herramientas del desarrollador -> Ficha APIs y busque Dispositivos en la barra de búsqueda, en los resultados haga clic en Dispositivos de la sección Conozca su red y busque la API DELETE by Device Id.

2.- Haga clic en la API DELETE by Device Id, haga clic en Try y proporcione la ID del dispositivo deseado para eliminarlo del inventario.

3.- Espere a que la API se ejecute y obtenga una respuesta 200 OK, luego confirme que el dispositivo de red ya no está presente en la página de Inventario.



Consejo: Puede obtener el uuid del dispositivo desde la URL del navegador (id o id del dispositivo) desde la página Cisco DNA Center Inventory Device Details o la página Device View 360.



Nota: Para obtener más información sobre las API de Cisco DNA Center, consulte la Guía de API de Cisco DevNet

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).