Überprüfung des DNA Center Inventory Service und allgemeiner Probleme

Inhalt

Einleitung

In diesem Dokument werden die grundlegenden Konzepte des Cisco DNA Center Inventory Service sowie häufig auftretende Probleme in der Produktion beschrieben.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Details zum Bestandsdienst

Der Cisco DNA Center Inventory Service basiert auf einem Kubernetes (K8s) Pod, der im Namespace "fusion" mit dem Namen "apic-em-Inventory-Manager-Service-<id>" als Bereitstellungsumgebungstyp ausgeführt wird.

Im K8s Pod befindet sich ein Docker Container namens "apic-em-Inventory-Manager-Service".

Die Hauptaufgaben des POD-Pods "apic-em-Inventory-Manager-service" sind die

Geräteerkennung und das Lifecycle-Management von Geräten.

Dadurch wird sichergestellt, dass Gerätedaten in Postgres SQL (von Fusion Services genutzte Datenbank) verfügbar sind.

Der "Fusion"-Namespace (Appstack), auch Network Controller Platform (NCP) genannt, stellt die Service Provisioning Framework (SPF)-Services für alle Anforderungen an die Netzwerkautomatisierung bereit.

Dazu gehören Erkennung, Inventarisierung, Topologie, Richtlinie, Software Image Management (SWIM), Konfigurationsarchiv, Netzwerkprogrammierer, Standorte, Gruppierung, Telemetrie, Tesseract-Integration, Vorlagenprogrammierer, Karten, IPAM, Sensoren, Orchestrierung/Workflow/Planung, ISE-Integration und Ähnliches.

Der Status des Inventar-POD kann mithilfe des folgenden Befehls überprüft werden:

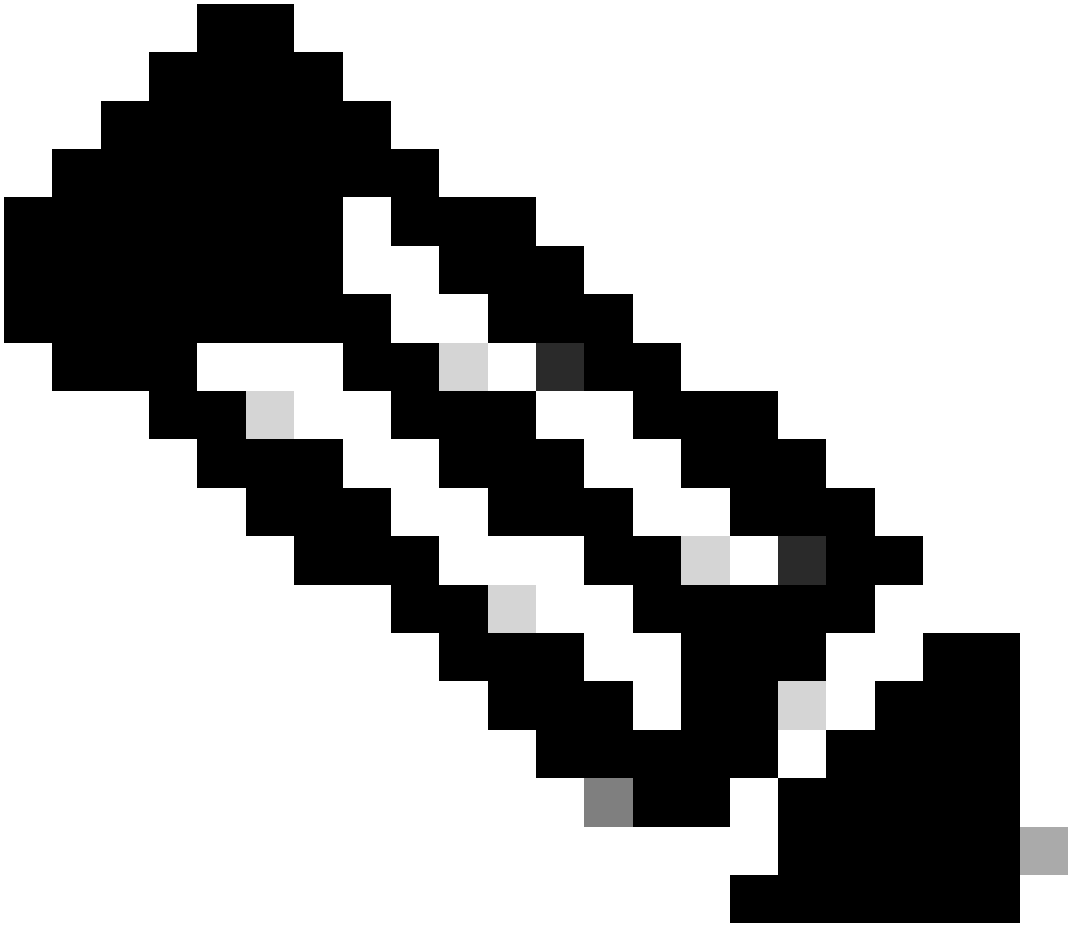
```
$ magctl appstack status | grep inventory
```

Der Bestandsdienststatus kann mit dem folgenden Befehl überprüft werden:

```
$ magctl service status
```

Die Inventardienstprotokolle können mit dem folgenden Befehl überprüft werden:

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



Anmerkung: Der Inventardienst kann auch aus zwei laufenden PODs bestehen. Sie müssen also einen einzelnen POD in den Befehlen angeben, indem Sie den vollständigen Inventarpodennamen einschließlich der POD-ID verwenden.

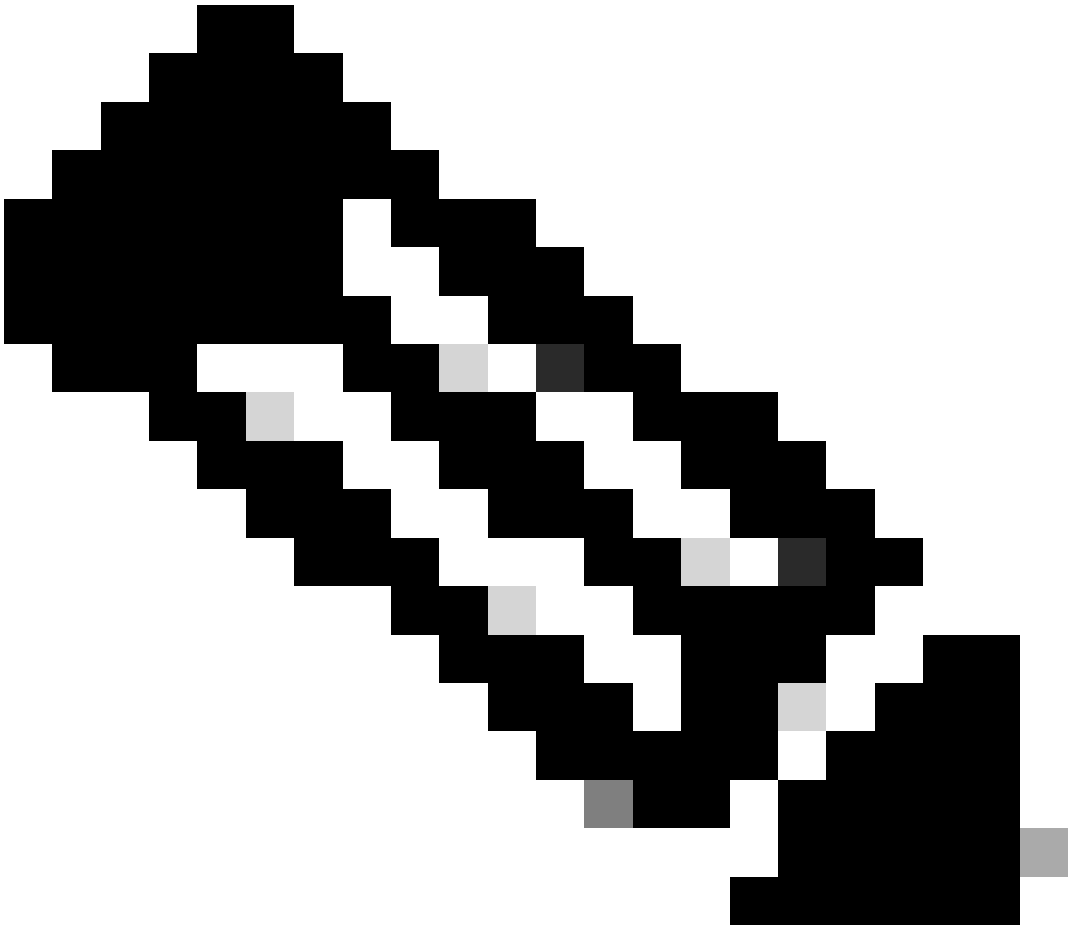
In diesem Dokument können wir uns auf die Bestandsgeräte-Verwaltbarkeit und den Status der letzten Synchronisierung konzentrieren, um häufige Probleme zu überprüfen:

Verwaltungsstatus

- Verwaltet mit grünem Häkchen: Gerät ist erreichbar und wird vollständig verwaltet.
- Orangefarbenes Fehlersymbol: Das Gerät wird mit einigen Fehlern verwaltet, z. B. "unreachable" (nicht erreichbar), "authentication failure" (Authentifizierungsfehler), "missing Netconf ports" (fehlende Netconf-Ports), "internal error" (Interner Fehler) usw. Bewegen Sie den Mauszeiger über die Fehlermeldung, um weitere Details zum Fehler und den betroffenen Anwendungen anzuzeigen.
- Nicht verwaltet: Das Gerät kann nicht erreicht werden, und aufgrund von Geräteverbindungsproblemen wurden keine Bestandsinformationen gesammelt.

Letzter Synchronisierungsstatus

- Verwaltet: Das Gerät befindet sich in einem vollständig verwalteten Zustand.
- Teilweise Erfassung fehlgeschlagen: Das Gerät befindet sich in einem teilweise erfassten Zustand, und nicht alle Inventarinformationen wurden erfasst. Bewegen Sie den Mauszeiger über das Informationssymbol (i), um zusätzliche Informationen zu dem Fehler anzuzeigen.
- Nicht erreichbar: Das Gerät kann nicht erreicht werden, und aufgrund von Geräteverbindungsproblemen wurden keine Bestandsinformationen gesammelt. Diese Bedingung tritt auf, wenn eine periodische Sammlung stattfindet.
- Falsche Anmeldeinformationen: Wenn die Geräteanmeldedaten geändert werden, nachdem das Gerät dem Bestand hinzugefügt wurde, wird dieser Zustand festgestellt.
- In progress: Die Bestandserfassung wird durchgeführt.



Anmerkung: Weitere Informationen zu den Bestandsfunktionen in Cisco DNA Center

---

finden Sie im offiziellen Leitfaden für Version 2.3.5.x: Bestandsverwaltung.

Probleme

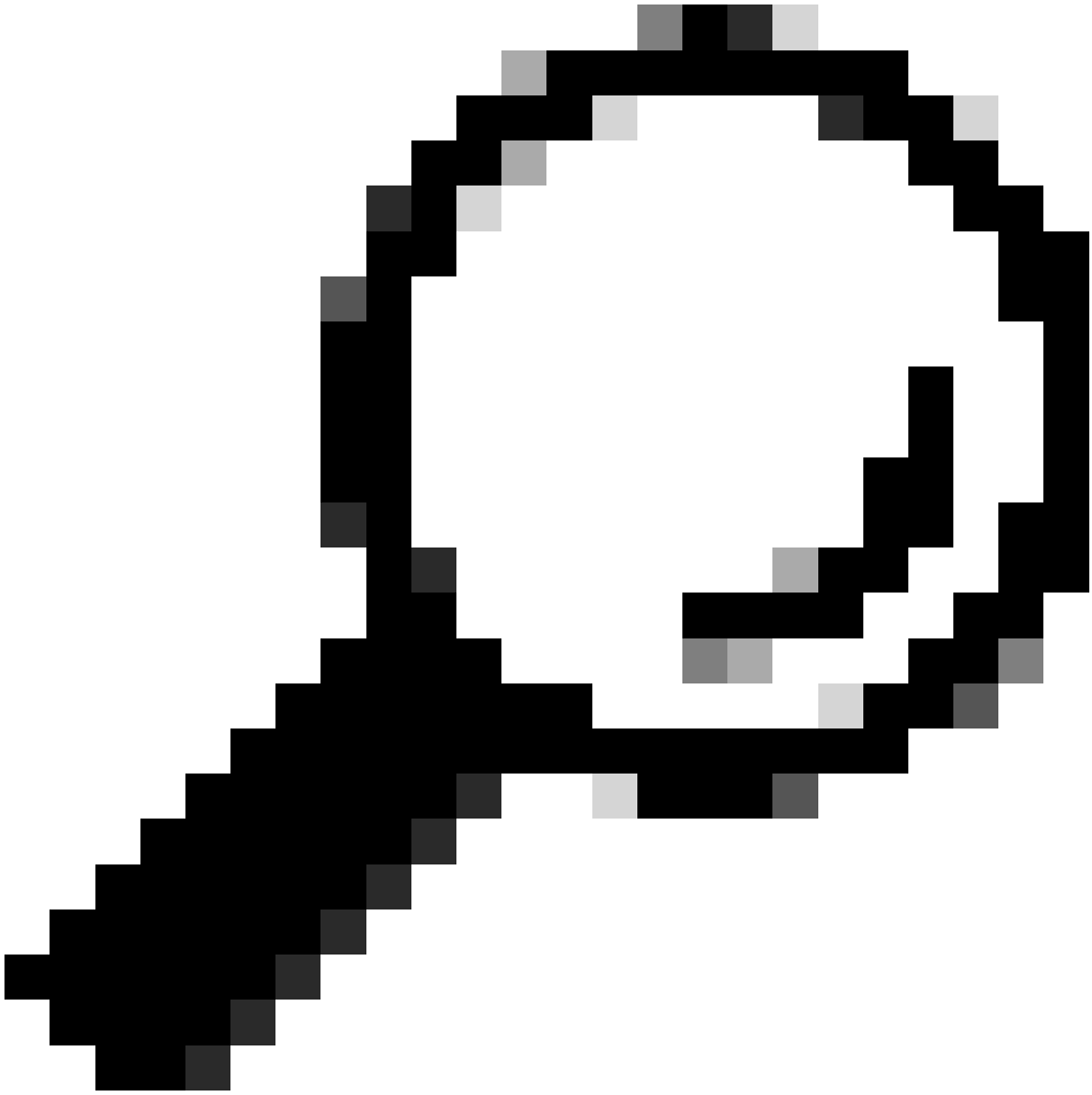
Internal error

Auf der Inventarseite von Cisco DNA Center kann eine Warnmeldung im Verwaltbarkeitsstatus für Geräte angezeigt werden, bei denen ein Konflikt bei der Datenerfassung aufgetreten ist:

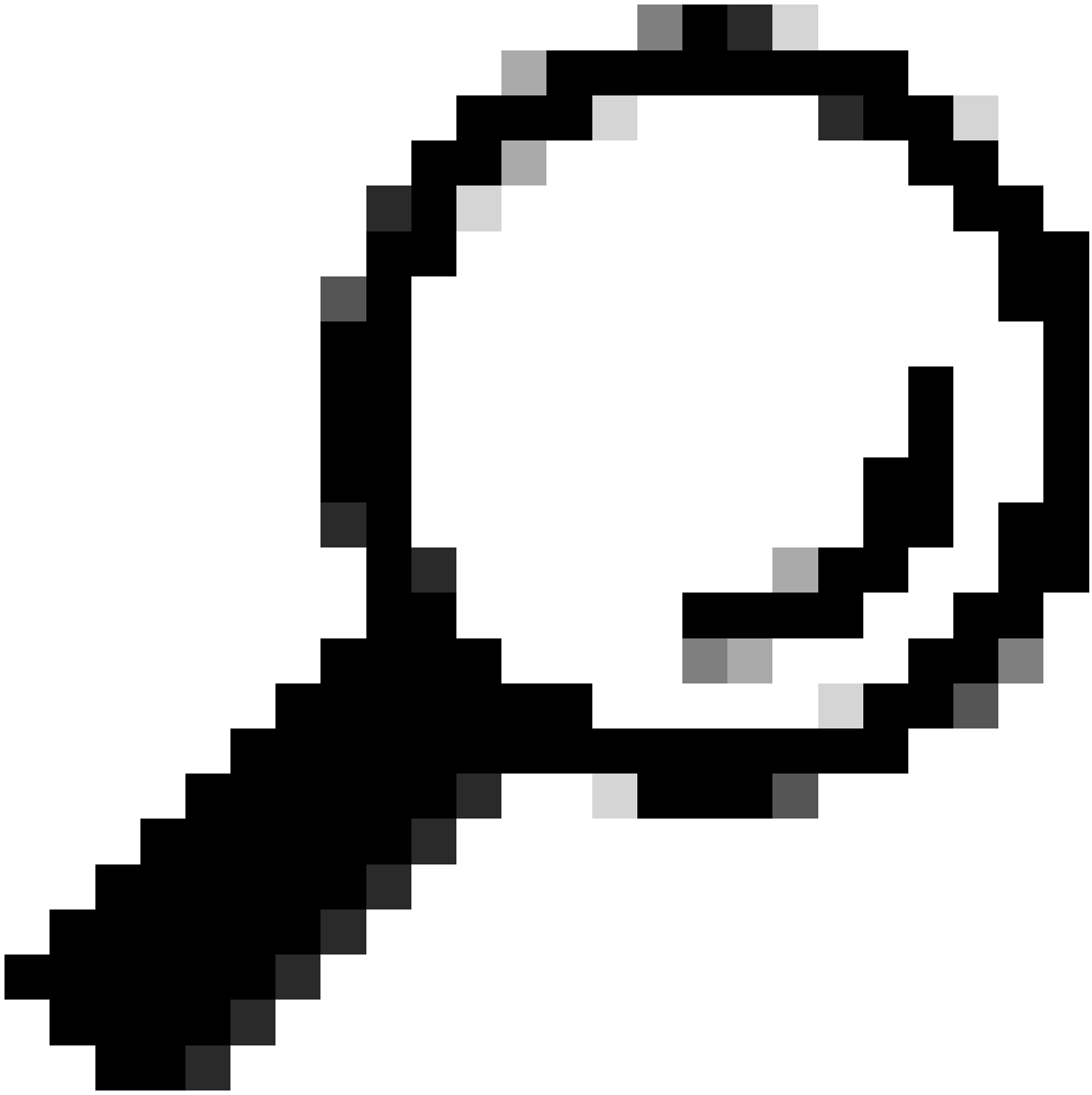
"Interner Fehler: NCIM12024: Alle Informationen vom Gerät konnten nicht erfolgreich gesammelt werden, oder die Bestandserfassung für dieses Gerät wurde noch nicht gestartet. Es kann sich um ein vorübergehendes Problem handeln, das sich automatisch beheben lässt. Synchronisieren Sie das Gerät neu. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an das Cisco TAC."

Wenn sich der Fehler nicht automatisch löst oder das Gerät neu synchronisiert wurde, können wir mit der ersten Fehlerbehebung beginnen. Dieser Fehler kann auf mehrere Gründe zurückzuführen sein, aber hier listen wir nur einige der häufigsten:

- Die Geräteanmeldedaten für SNMP, SSH und Netconf sind falsch.
- Netzwerkverbindungsprobleme im Zusammenhang mit SNMP, SSH und Netconf.
- Probleme mit der Netconf-Konfiguration im Gerät führen dazu, dass Netconf nicht richtig funktioniert.
- Die Geräte-Resynchronisierung wird ausgelöst, während die Geräte-Synchronisierung bereits läuft.
- Mehrere Traps wurden vom Gerät empfangen, was mehrere Resynchronisierungsauslöser innerhalb kurzer Zeit verursachte.
- Backend-Probleme mit Bestandsdatenbankeinträgen in mehreren Tabellen für das Gerät.



Tipp: Wenn Sie das Netzwerkgerät entfernen und es mithilfe der richtigen CLI-, SNMP- und NETCONF-Anmeldeinformationen erneut erkennen, können Sie veraltete Datenbankeinträge entfernen, die den internen Fehler verursachen könnten.



Tipp: Die Überprüfung der Inventardienstprotokolle und die Filterung nach Geräte-IP oder Hostname können hilfreich sein, um die Ursache des internen Fehlers zu identifizieren.

Geräteanmeldedaten

Um die Geräteanmeldedaten zu überprüfen, navigieren Sie zum Cisco DNA Center-Menü -> Provisioning -> Inventory -> Select Device -> Actions -> Inventory -> Edit Device, und klicken Sie auf "Validate" (Validieren). Bestätigen Sie, dass die erforderlichen Anmeldedaten (CLI und SNMP) die Validierung mit einem grünen Häkchen bestehen (ggf. auch "netconf").

Wenn die Validierung fehlschlägt, überprüfen Sie bitte, ob Benutzername und Kennwort, die Cisco DNA Center zur Verwaltung des Netzwerkgeräts verwendet, direkt in der Befehlszeile des Geräts gültig sind.

Wenn sie lokal oder auf einem AAA-Server (TACACS oder RADIUS) konfiguriert sind, stellen Sie sicher, dass Benutzername und Kennwort auf dem AAA-Server korrekt konfiguriert sind.

Überprüfen Sie außerdem, ob für die Berechtigung "Benutzername" das Kennwort "Enable" (Aktivieren) in den Einstellungen für Geräteanmeldedaten in Cisco DNA C eingerichtet werden muss.Bestand eingeben.

Fehler in CLI-Anmeldeinformationen können eine Verwaltbarkeitsfehlermeldung in Inventory auslösen: CLI-Authentifizierungsfehler.

Netconf

Netconf ist ein Protokoll zur Remoteverwaltung eines kompatiblen Netzwerkgeräts über Remote Procedure Calls (RPC).

Cisco DNA Center nutzt Netconf-Funktionen, um Konfigurationen auf Netzwerkgeräten bereitzustellen oder zu entfernen und so Funktionen wie die Überwachung über Assurance zu ermöglichen.

Cisco DNA Center Inventory kann außerdem die Richtigkeit der Netconf-Anforderungen überprüfen. Dazu gehören:

- Der Netconf-Standardport 830 ist im Netzwerk offen und funktionsfähig.
- Benutzer mit der Berechtigung 15 mit SSH-Zugriff auf das Netzwerkgerät (lokal oder AAA konfiguriert).
- Aktivieren Sie Netconf im Netzwerkgerät:

<#root>

(config)#

netconf-yang

- Wenn aaa new-model aktiviert ist, müssen Sie auch die AAA-Standardeinstellungen konfigurieren:

<#root>

(config)#

aaa authorization exec default

(config)#

aaa authentication login default

Fehler in den NetConf-Anmeldeinformationen können eine Verwaltbarkeitsfehlermeldung in Inventory verursachen: Fehler bei der NetConf-Verbindung.

Netzwerkprüfungen

Abhängig von der Version können wir auch die Netzwerkverbindungen und Protokolleinstellungen wie SNMP validieren.

Wir können beispielsweise je nach SNMP-Version Community, Benutzer, Gruppe, Engine-ID, Authentifizierungs- und Verschlüsselungseinstellungen usw. überprüfen.

Wir können auch die SSH- und SNMP-Verbindungen überprüfen, indem wir Ping- und Traceroute-Befehle in der Befehlszeile des Geräts und Ports für SSH (22) und SNMP (161 und 162) in der Firewall, dem Proxy oder den Zugriffslisten verwenden.

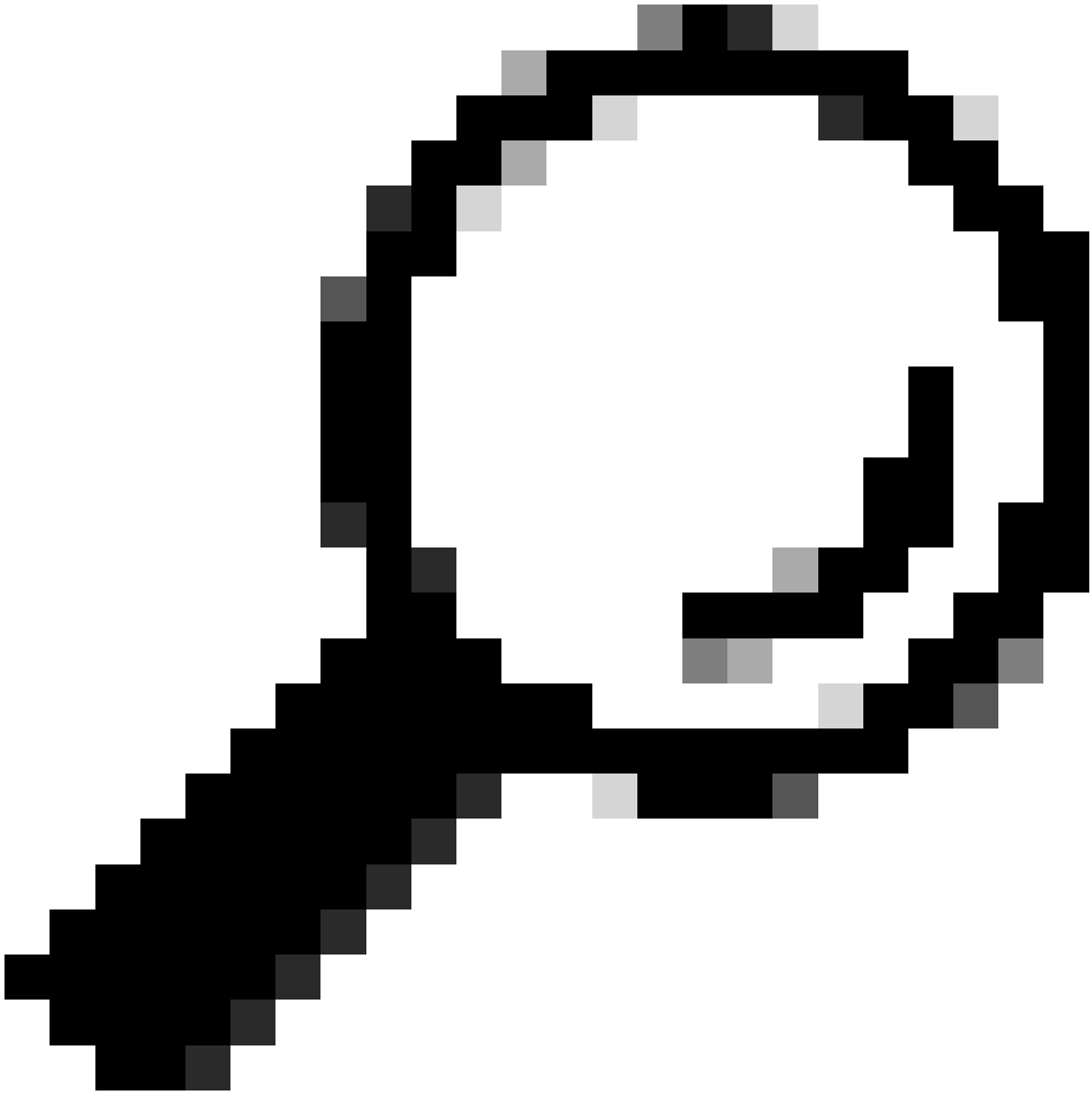
Von Cisco DNA Center, maglev CLI, verwenden wir die IP-Route-Befehle, um die Verbindung zum Netzwerkgerät zu validieren.

SNMP-Schritte können ebenfalls zur Fehlerbehebung verwendet werden.

Fehler in SNMP-Anmeldeinformationen können eine Verwaltbarkeitsfehlermeldung in Inventory verursachen: SNMP-Authentifizierungsfehler oder Gerät nicht erreichbar.

Datenbanktabellen

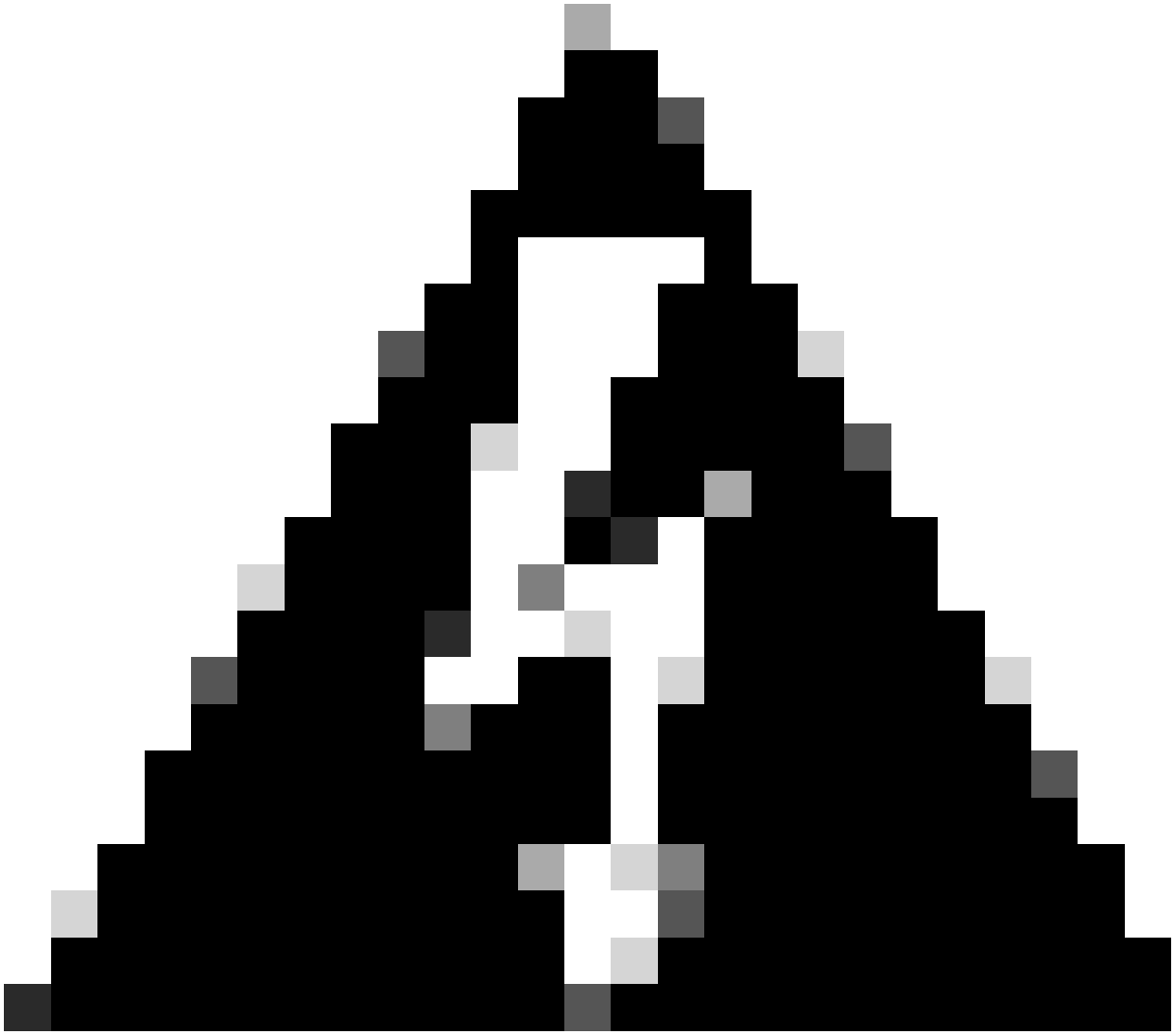
Als Endbenutzer können Sie die Cisco DNA Center-GUI mit Grafana verwenden, um SQL-Abfragen auszuführen, sodass Sie nicht über die maglev CLI auf die Postgres-Shell zugreifen müssen.



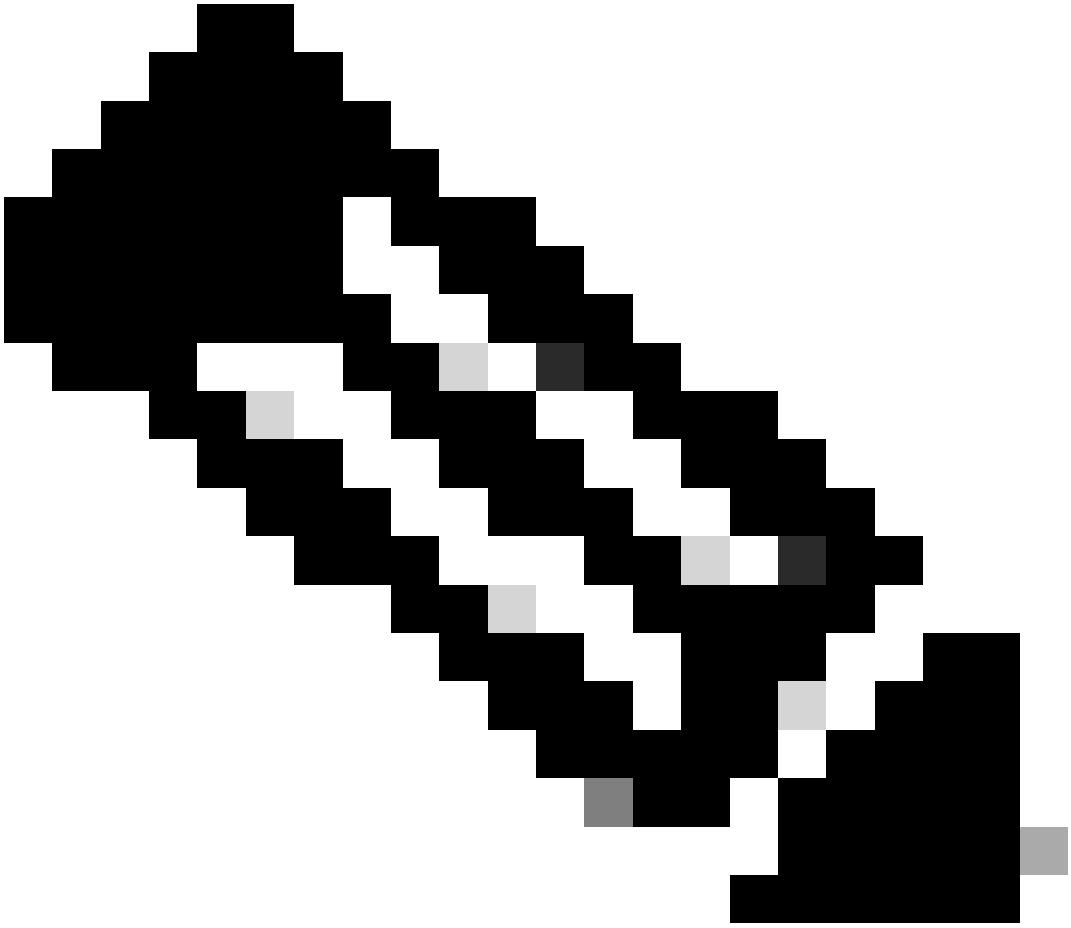
Tipp: Wenn Sie erfahren möchten, wie Sie Grafana verwenden, lesen Sie bitte den offiziellen Leitfaden: Ausführen von Postgre-Abfragen in der Cisco DNA Center GUI

Einige der folgenden Datenbanktabellen werden angezeigt, wenn Probleme mit Netzwerkgeräten im Bestand auftreten:

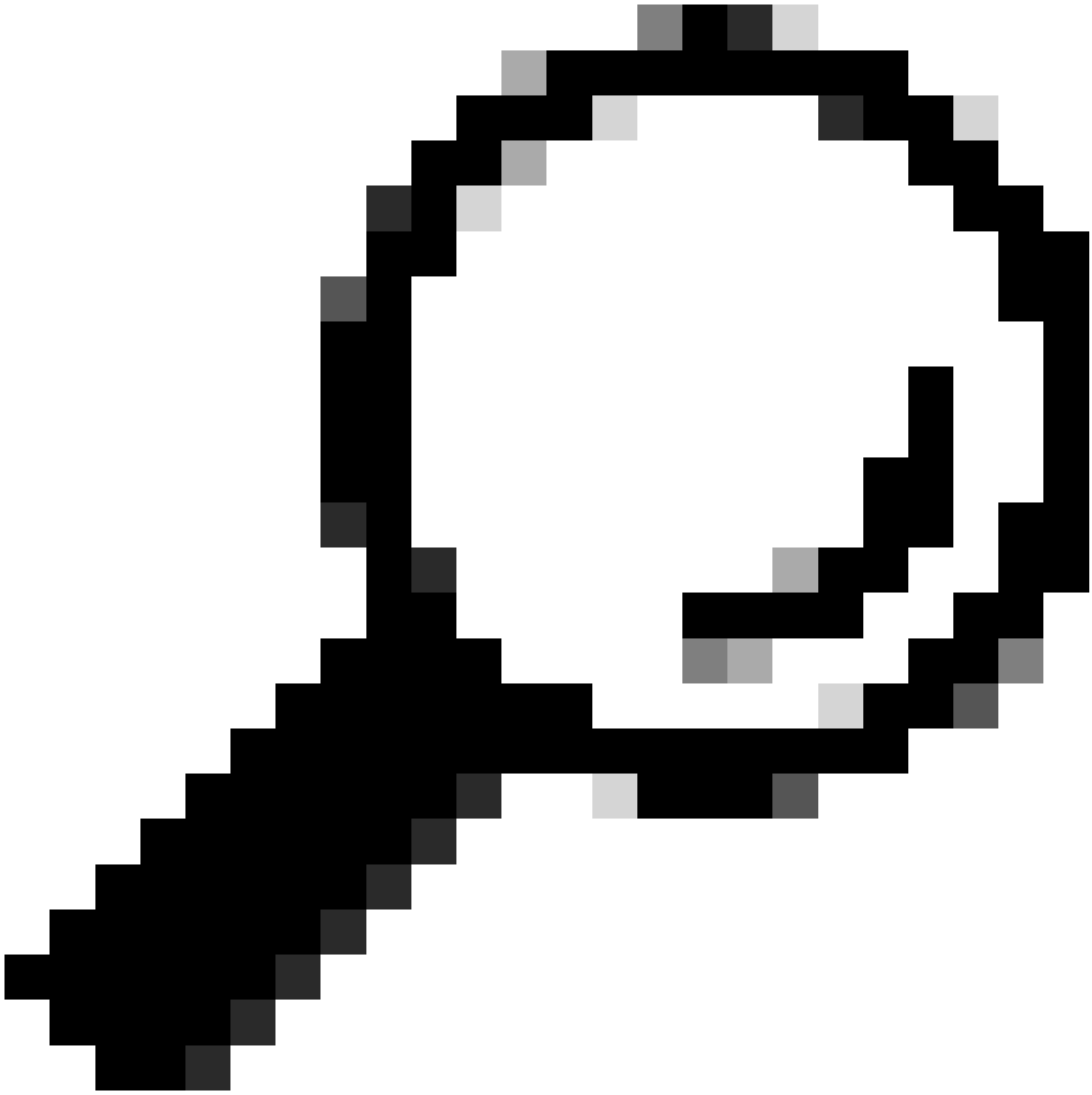
- Netzwerkgerät
- ManagementSchnittstelle
- Netzwerkelement
- NetzwerkQuelle
- deviceif
- Ipaddress



Warnung: Nur das Cisco TAC ist zum Ausführen von Anzeigeabfragen in der Postgres-Shell berechtigt, und nur BU/DE-Teams sind zum Ändern von DB-Tabellen berechtigt.



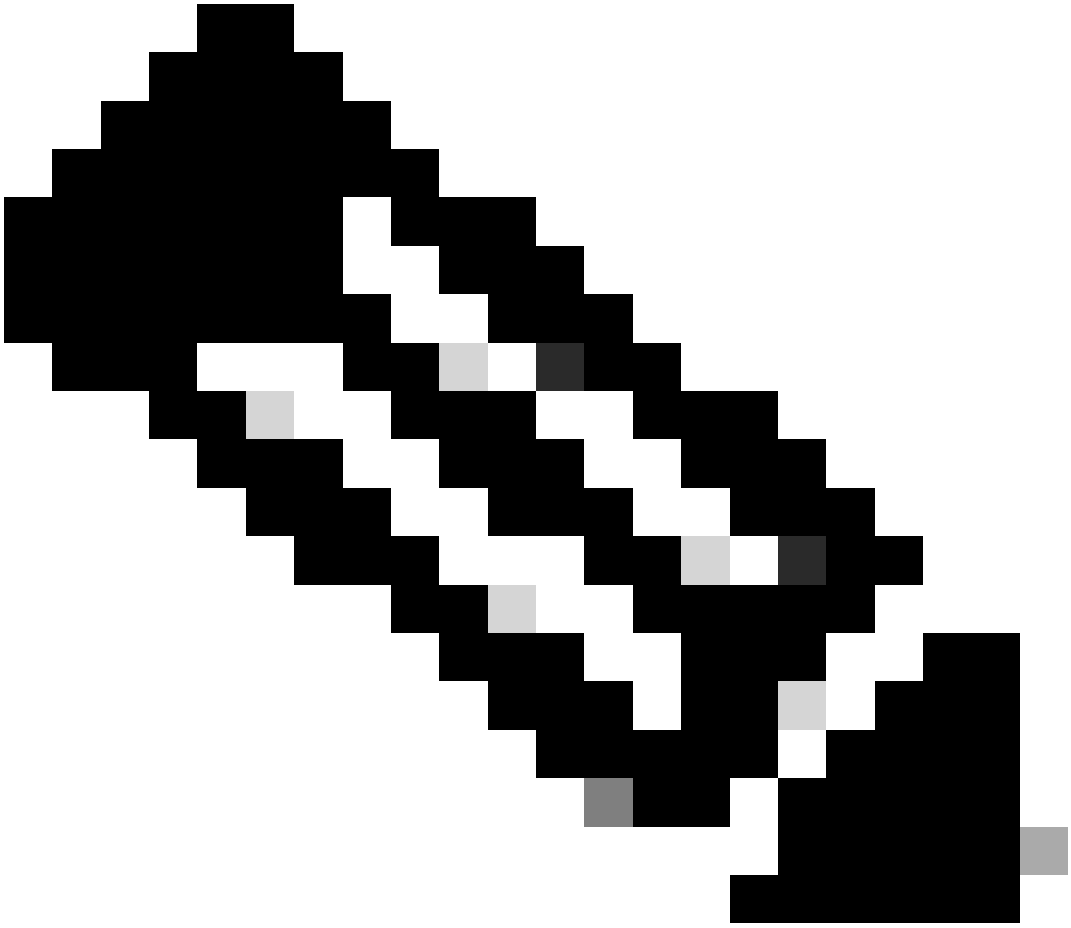
Anmerkung: Datenbankprobleme können auch die interne Fehlermeldung für Geräte verursachen, wodurch die Datenerfassung und die Gerätebereitstellung verhindert werden können.



Tipp: Sie können die Postgres-Protokolle mithilfe von Kibana auf der Seite Cisco DNA Center System 360 überprüfen und nach Einschränkungsverletzungen suchen, wenn der Inventardienst versucht, Einträge in Postgres-Datenbanktabellen zu speichern oder zu aktualisieren.

Schleife und Traps synchronisieren

Cisco DNA Center ist so konzipiert, dass jedes Mal, wenn ein Trap vom Gerät empfangen wird, eine erneute Geräteerkennung ausgeführt wird, nachdem eine größere Änderung am Gerät selbst durchgeführt wurde, um das Cisco DNA Center-Inventar auf dem neuesten Stand zu halten. Manchmal behält die Cisco DNA Center-Inventarseite Ihre Netzwerkgeräte für einen langen Zeitraum oder für immer im Abschnitt Verwaltbarkeit im Status "Synchronisierung".



Anmerkung: Diese Art von Synchronisierungsschleifen aufgrund massiver Traps kann dazu führen, dass sich Cisco DNA Center innerhalb kurzer Zeit mehrmals bei Geräten authentifiziert, die die Traps aufgrund erkannter Änderungen senden.

API zur Erzwingung der Gerätesynchronisierung

Wenn Ihr Netzwerkgerät zu lange oder sogar Tage im Synchronisierungsstatus bleibt, überprüfen Sie zuerst die grundlegenden Prüfungen auf Erreichbarkeit und Konnektivität. Dann erzwingen Sie die Geräte-Resynchronisierung per API-Aufruf:

1.- Öffnen Sie die Cisco DNA Center maglev CLI-Sitzung.

2.- Rufen Sie das Cisco DNA Center-Authentifizierungstoken über die API ab:

<#root>

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

3.- Verwenden Sie das Token aus dem vorherigen Schritt, um die API auszuführen und die Gerätesynchronisierung zu erzwingen:

<#root>

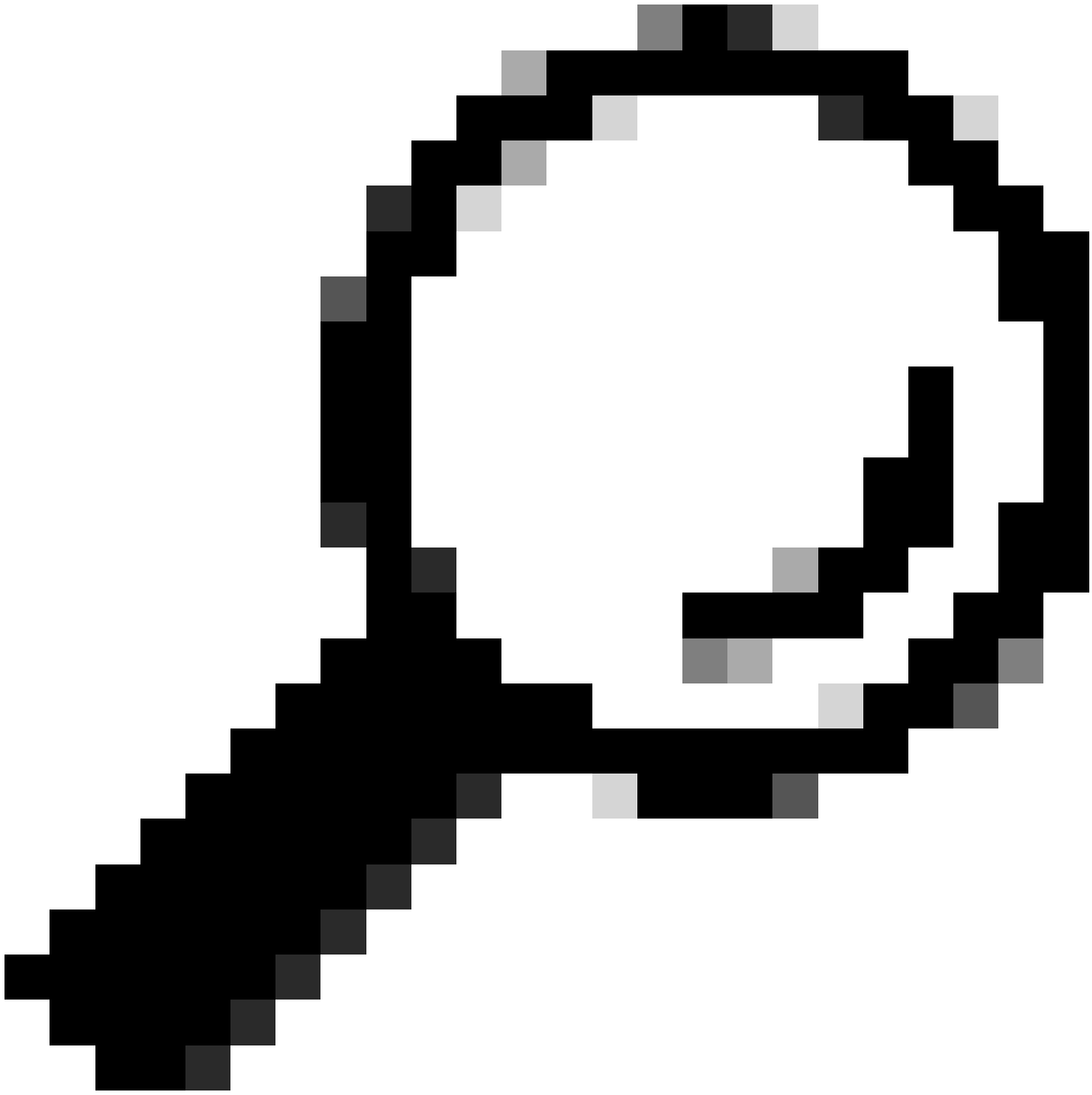
curl -X PUT -H "X-AUTH-TOKEN:

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

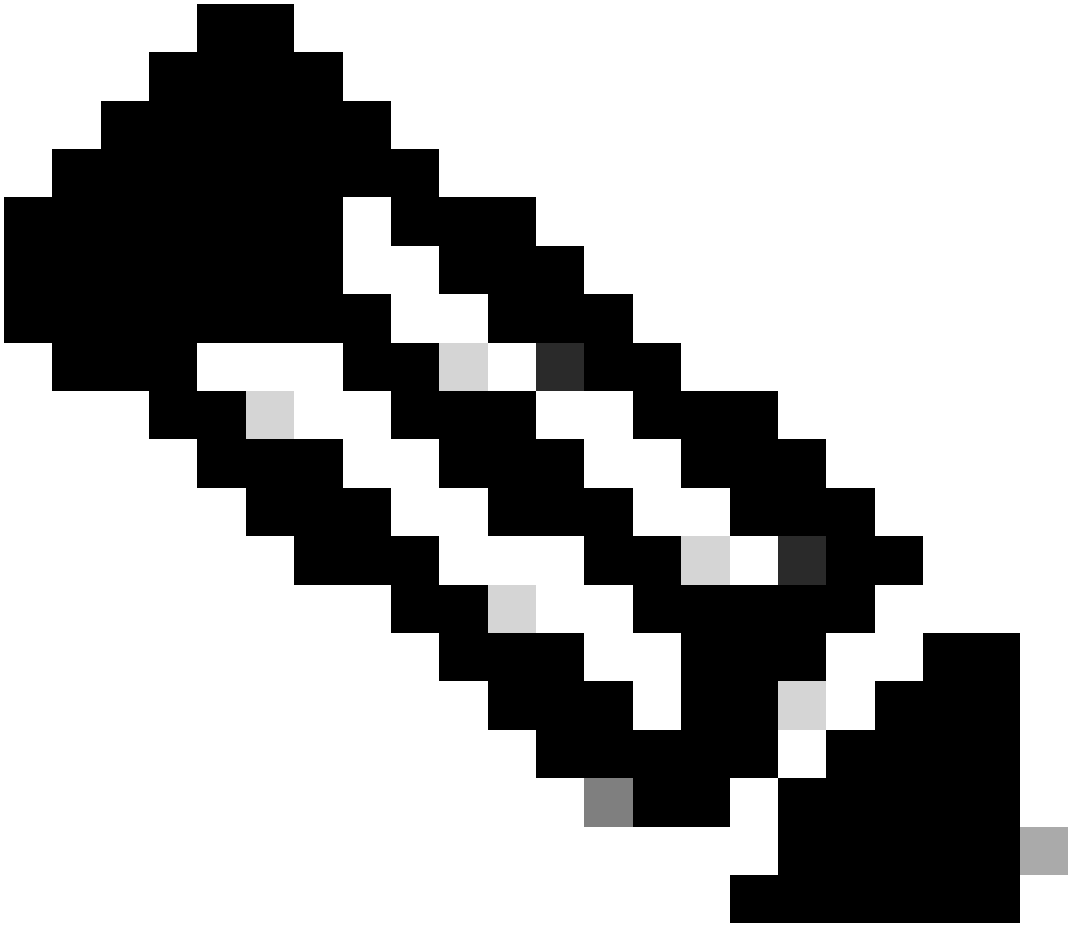
' https://

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

4.- Sie können das Gerät in der Synchronisierung wieder sehen, aber diesmal mit einer Force Sync-Option über API.



Tipp: Sie können die Geräte-UUID von der Browser-URL (device-id oder id) auf der Seite Cisco DNA Center Inventory Device Details (Inventar - Gerätedetails) oder Device View 360 (Geräteansicht) abrufen.



Anmerkung: Weitere Informationen zu APIs im Cisco DNA Center finden Sie im Cisco DevNet API Guide.

Traps überprüfen

Wenn das Problem weiterhin besteht, nachdem die Synchronisierungsaufgabe im Gerät erzwungen wurde, können wir überprüfen, ob der Cisco DNA Center-"Ereignisdienst" zu viele Traps empfängt, und die Art der Traps überprüfen, indem wir die Ereignisdienstprotokolle lesen:

1.- Bevor wir die Protokolle lesen, können wir einfach die Gesamtzahl der Traps mit dem Befehl überprüfen:

<#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.- Dann werden wir an den Event-Service-Container anhängen:

<#root>

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

3.- Sobald Sie in den Ereignisdienstcontainer eingedrungen sind, wechseln Sie in das Verzeichnis logs:

<#root>

$ cd /opt/CSCOlumos/logs/

4.- Wenn Sie die Dateien innerhalb des Verzeichnisses überprüfen, können Sie einige Protokolldateien sehen, deren Name mit "ncs" beginnt.

Beispiel:

<#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.- Diese "ncs"-Dateien sind die, die wir analysieren müssen, welche Art von Traps wir empfangen und wie viele. Wir können die Protokolldateien nach dem Hostnamen des Geräts oder dem Schlüsselwort "trapType" filtern:

<#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

Es gibt zu viele Arten von Traps, von denen einige eine Resynchronisierung des Geräts auslösen können. Wenn sie zu häufig auftreten, können sie die Synchronisierungsschleife verursachen.

Durch die Analyse der Traps können wir die Ursache identifizieren und Traps erstellen, die gestoppt werden sollen, z. B. ein AP in einem Neustart-Zyklus.

Sie können die Traps-Ausgabe in einer Datei speichern und sie ggf. an das Eskalationsteam weitergeben.

Absturzstatus des Diensts

Wenn Sie vermuten, dass der Inventar-Pod bei der Verwaltung von Netzwerkgeräten aufgrund eines ungeraden Verhaltens auf der Inventarseite des Cisco DNA Center abstürzt, können Sie den Pod-Status zuerst überprüfen:

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

Überprüfen der Ausgabe des POD-Status, wenn Sie eine hohe Anzahl von Neustarts oder einen Fehlerstatus sehen, dann können Sie an den Bestandscontainer anhängen und die Heapdump-Datei sammeln, die die Daten haben kann, die Eskalationsteam helfen können, die Ursache des

Absturzes zu analysieren und zu definieren:

<#root>

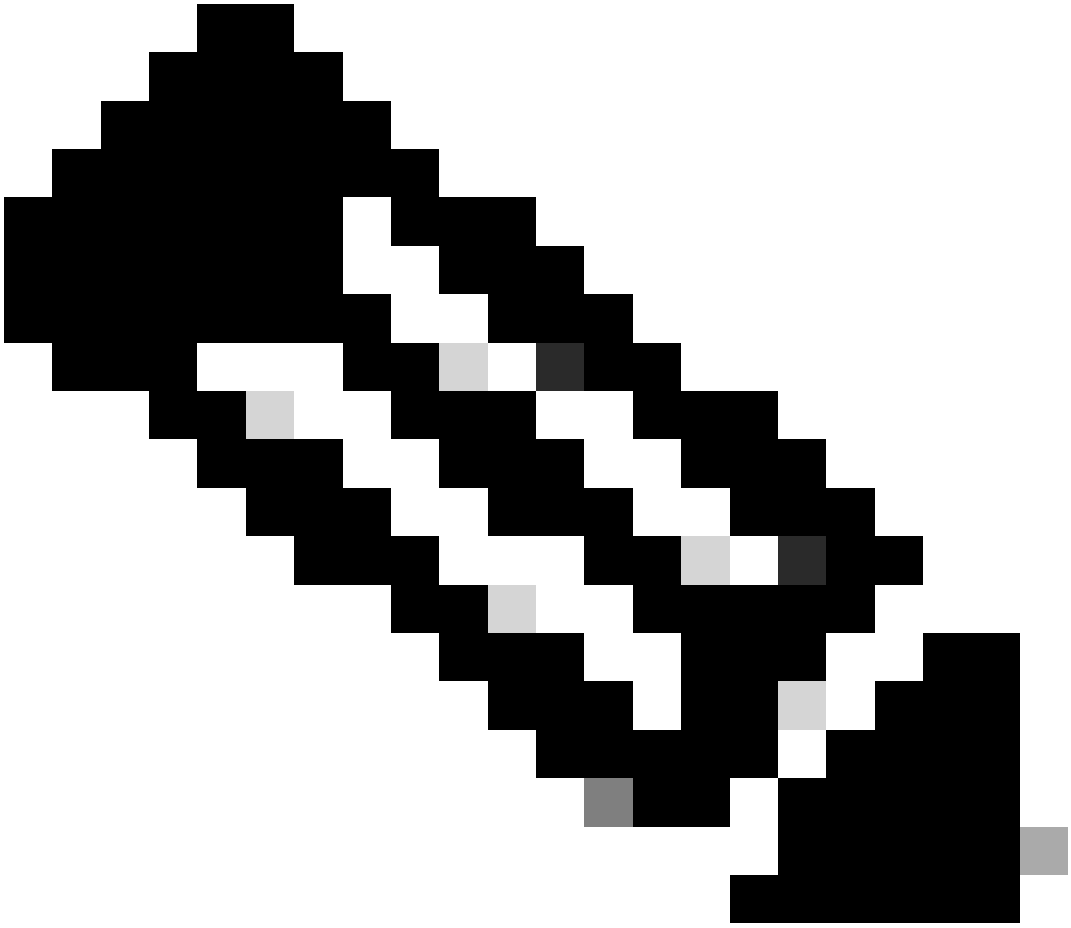
$ magctl service attach -D

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



Anmerkung: Wenn keine Heapdump-Datei im Containerverzeichnis gefunden wurde, war kein Absturzstatus im Container vorhanden.

Gerät kann nicht gelöscht werden

In einigen Fällen kann Cisco DNA Center ein Netzwerkgerät aufgrund eines Backend-Problems nicht aus der Benutzeroberfläche des Inventars löschen.

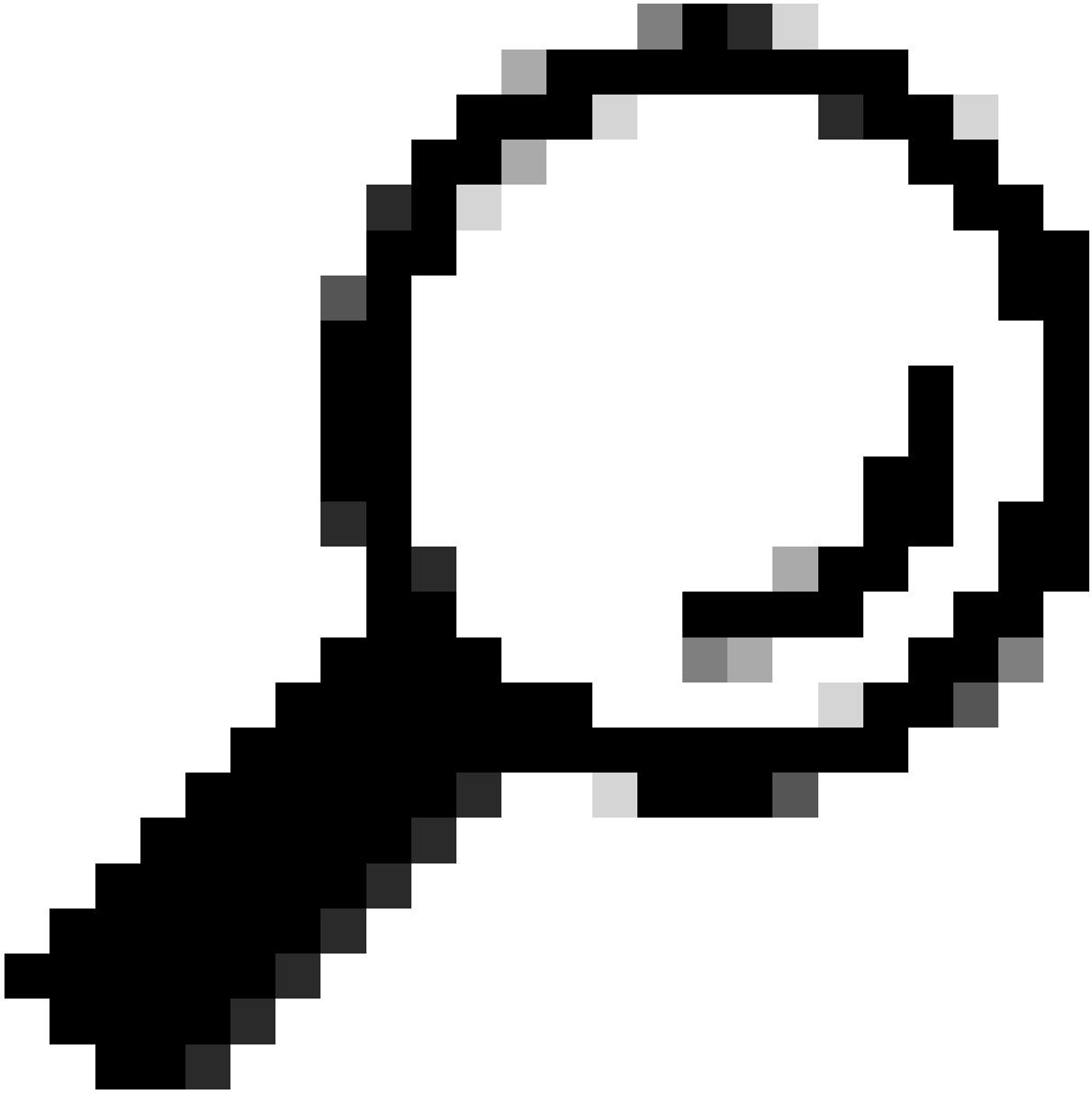
API zum Erzwingen des Löschens von Geräten

Wenn Sie das Gerät nicht über die Cisco DNA Center-GUI aus dem Inventar löschen können, können Sie es über die API unter folgender ID löschen:

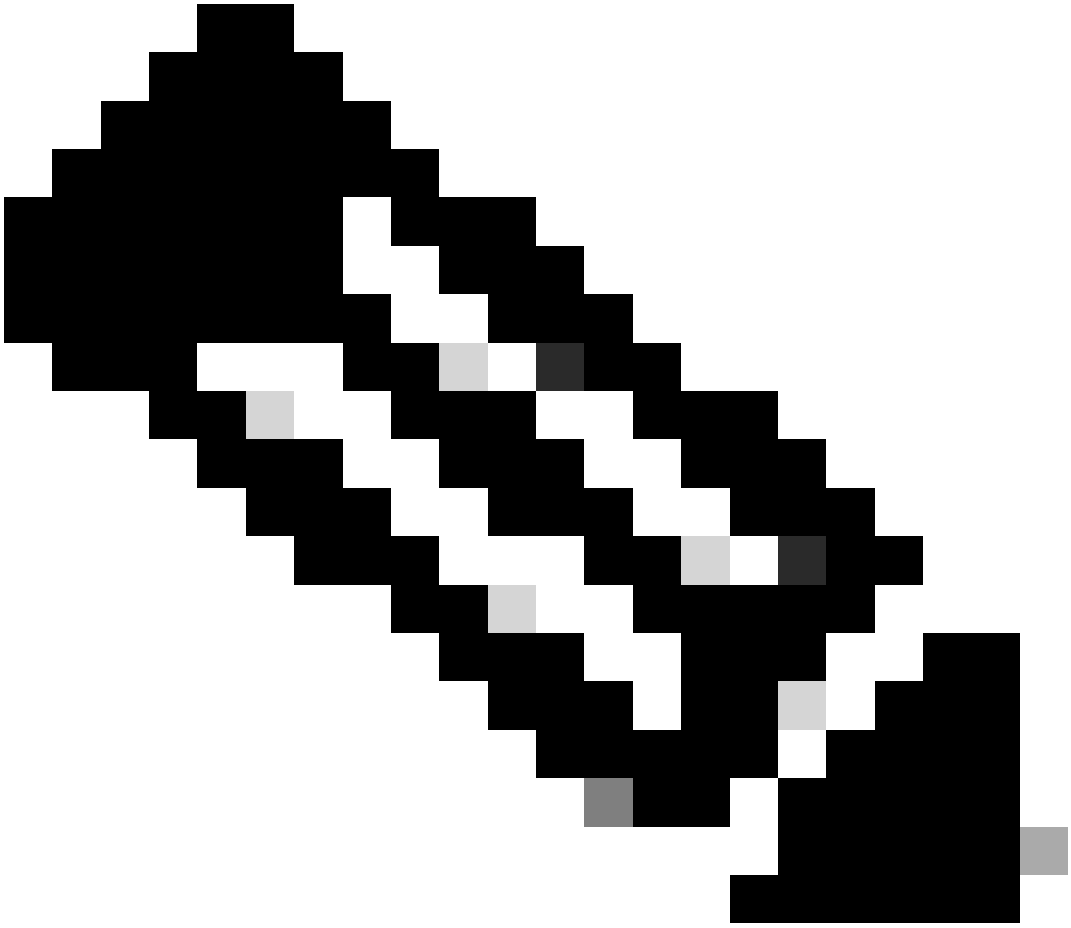
1.- Navigieren Sie zum Cisco DNA Center-Menü -> Plattform -> Developer Toolkit -> APIs Registerkarte und suchen Sie in der Suchleiste nach Geräten, klicken Sie in den Ergebnissen auf Geräte im Abschnitt Kennen Sie Ihr Netzwerk und suchen Sie nach der API DELETE by Device Id.

2.- Klicken Sie in die DELETE by Device Id-API, klicken Sie auf Try, und geben Sie die Geräte-ID des gewünschten Geräts an, das aus dem Inventar entfernt werden soll.

3.- Warten Sie, bis die API ausgeführt wird und erhalten Sie eine 200 OK-Antwort, dann bestätigen Sie, dass das Netzwerkgerät nicht mehr in der Inventarseite vorhanden ist.



Tipp: Sie können die Geräte-UUID von der Browser-URL (device-id oder id) auf der Seite Cisco DNA Center Inventory Device Details (Inventar - Gerätedetails) oder Device View 360 (Geräteansicht) abrufen.



Anmerkung: Weitere Informationen zu APIs im Cisco DNA Center finden Sie im Cisco DevNet API Guide.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.