檢查DNA中心庫存服務和常見問題

目錄

簡介

本文檔介紹Cisco DNA Center Inventory服務基本概念和在生產中發現的常見問題。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

庫存服務詳細資訊

Cisco DNA Center Inventory服務基於Kubernetes(K8s)Pod，您可以在名為「apic-em-inventory-manager-service-<id>」的名稱空間「fusion」中發現該服務正在運行作為部署環境型別。

在K8s艙內，您可以找到一個Docker容器，稱為「apic-em-inventory-manager-service」。

「apic-em-inventory-manager-service」Pod的主要任務包括：裝置發現和裝置生命週期管理。

這可確保裝置資料在Postgres SQL（fusion services使用的資料庫）中可用。

「fusion」命名空間(Appstack)也稱為網路控制器平台(NCP)，為所有網路自動化要求提供服務調配框架(SPF)服務。

其中包括發現、清單、拓撲、策略、軟體映像管理(SWIM)、配置存檔、網路程式設計師、站點、分組、遙測、Tesseract整合、模板程式設計師、對映、IPAM、感測器、協調/工作流/排程、ISE整合等。

inventory pod status可通過運行以下命令來檢查：

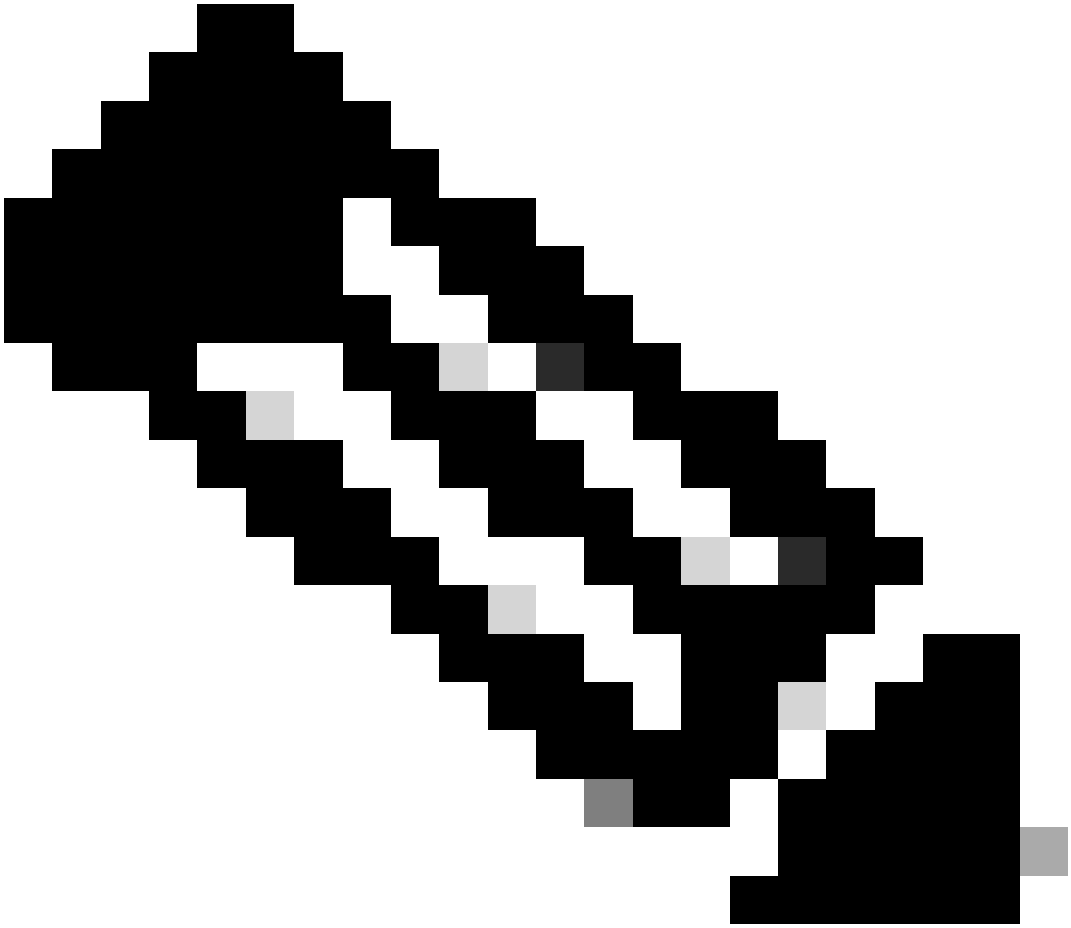
```
$ magctl appstack status | grep inventory
```

可以使用以下命令檢查清單服務狀態:

```
$ magctl service status
```

可以使用以下命令檢查清單服務日誌:

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



附註：清單服務也可以由兩個正在運行的pod組成，因此您需要通過使用完整的清單pod名

稱（包括pod id）在命令中指定單個pod。

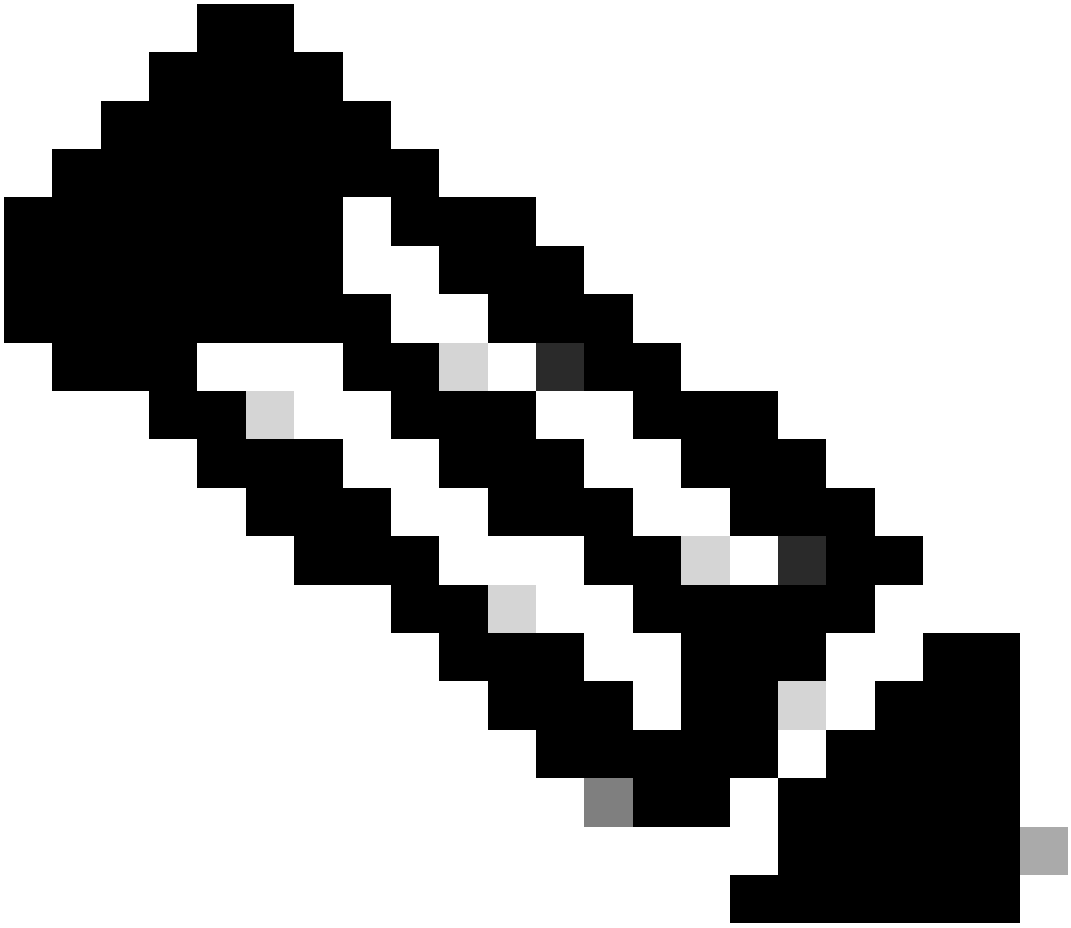
在本文檔中，我們可以重點檢視清單裝置可管理性和上次同步狀態，以檢視常見問題：

可管理性狀態

- 使用綠色勾選圖示管理:裝置可訪問且完全受管理。
- 使用橙色錯誤圖示進行管理:裝置管理存在一些錯誤，例如無法訪問、身份驗證失敗、缺少Netconf埠、內部錯誤等。您可以將游標懸停在錯誤消息上，以檢視有關錯誤和受影響的應用程式的更多詳細資訊。
- 非託管:由於裝置連線問題，無法訪問裝置，並且未收集任何清單資訊。

上次同步狀態

- 託管:裝置處於完全託管狀態。
- 部分收集失敗:裝置處於部分收集狀態，並且尚未收集所有清單資訊。將游標懸停在資訊(i)圖示上，以顯示有關故障的其他資訊。
- 無法連線：由於裝置連線問題，無法訪問裝置，並且未收集任何清單資訊。發生定期收集時會發生此情況。
- 憑證錯誤:如果在將裝置新增到清單後更改了裝置憑證，則會記錄此情況。
- In progress:正在進行庫存收集。



附註：有關Cisco DNA Center中庫存功能的詳細資訊，請參閱2.3.5.x版官方指南：管理庫存

問題

內部錯誤

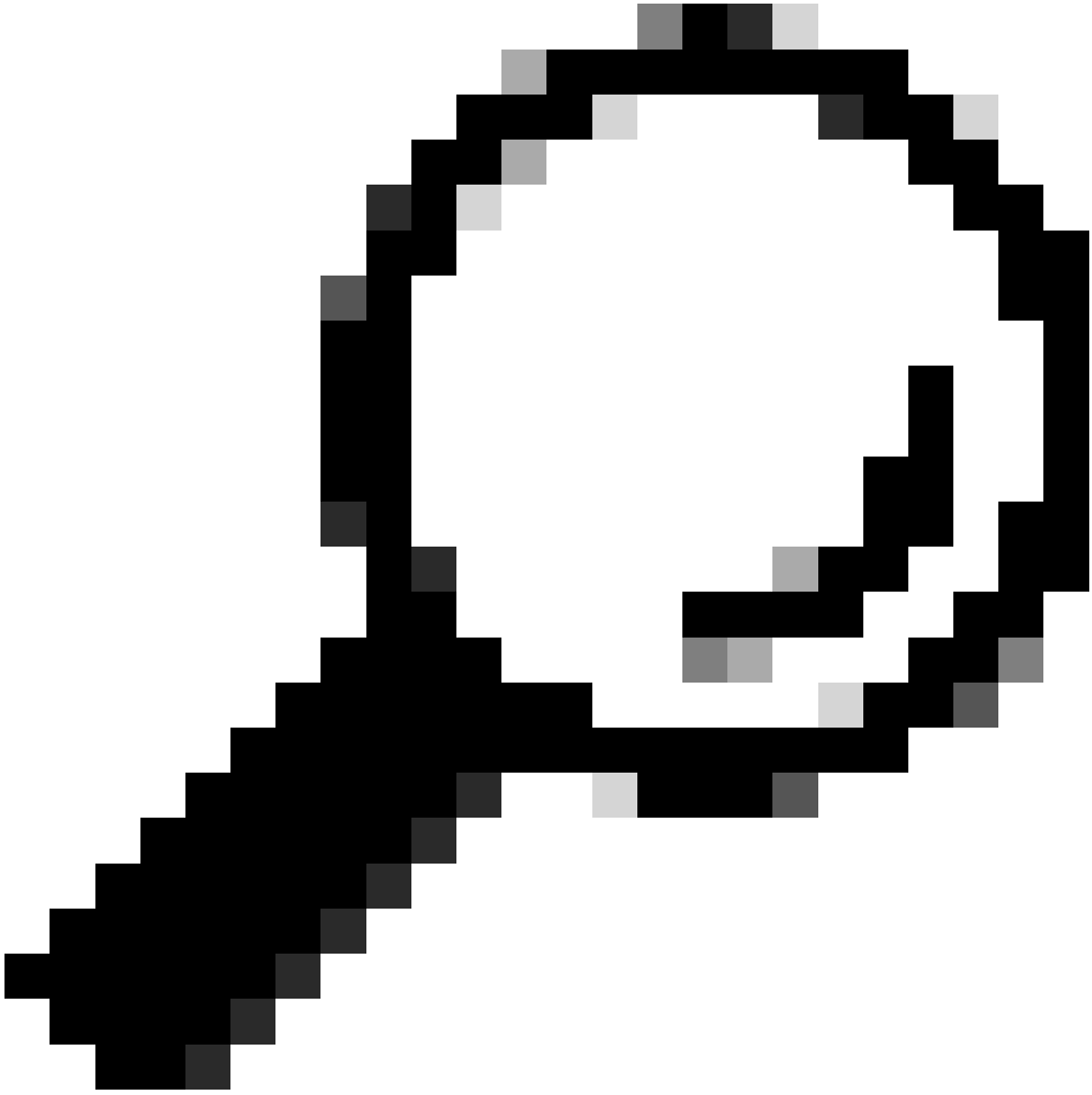
Cisco DNA Center Inventory（Cisco DNA Center庫存）頁面可以在裝置的可管理性狀態中顯示警告消息，這些裝置存在某種衝突以防止資料收集：

"內部錯誤: NCIM12024:無法成功收集裝置中的所有資訊，或者此裝置的資產收集尚未啟動。它可能是一個臨時問題，可以自動解決。重新同步裝置，如果無法解決問題，請聯絡Cisco TAC。」

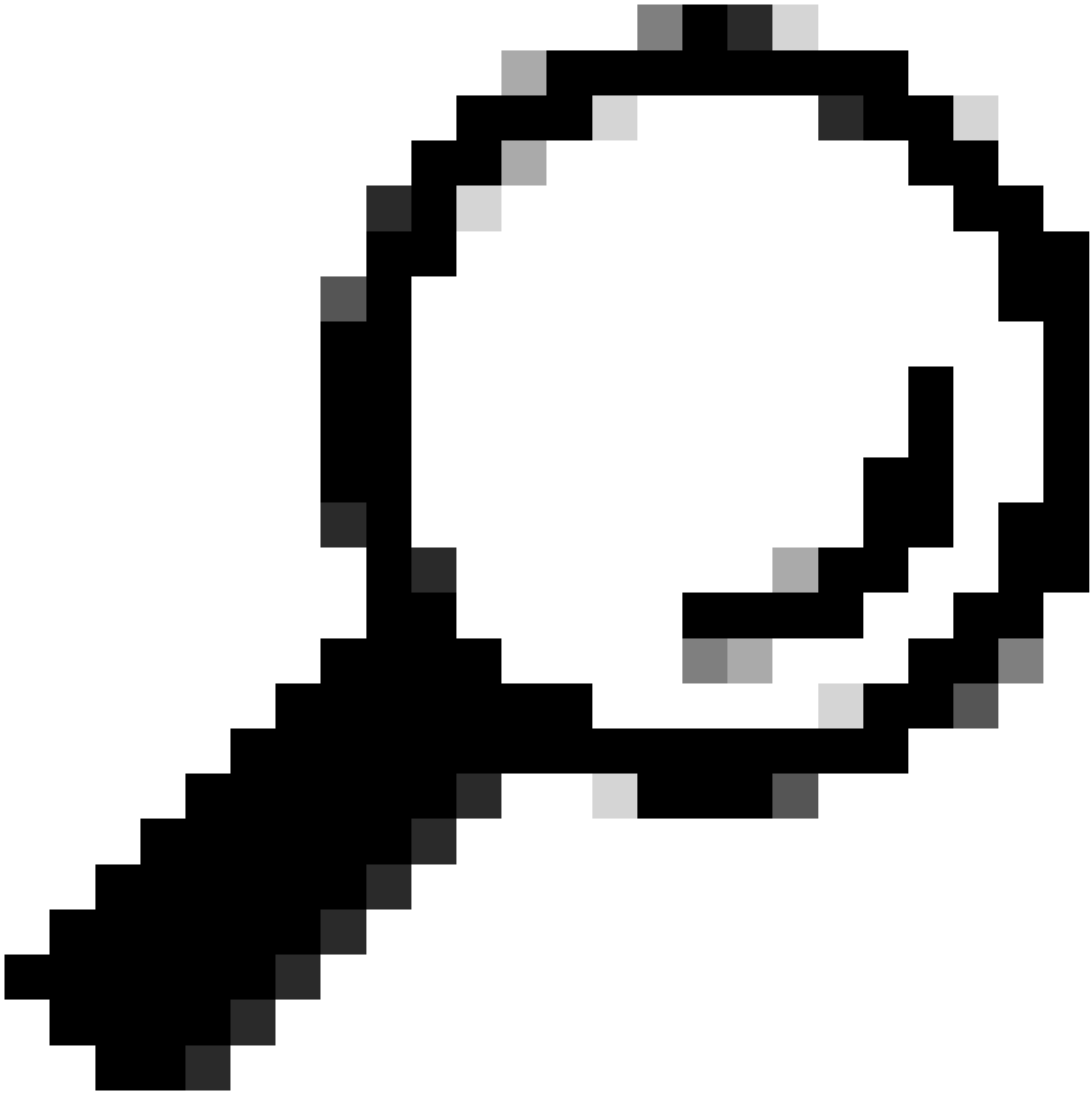
如果錯誤不能自動解決或在裝置重新同步後解決，我們可以從初始故障排除開始。該錯誤可能是由於多種原因，但此處我們僅列出一些最常見的原因：

- SNMP、SSH和Netconf的裝置憑證不正確。

- 與SNMP、SSH和Netconf相關的網路連線問題。
- 裝置中的Netconf配置問題導致Netconf無法正常工作。
- 在裝置同步正在進行時觸發裝置重新同步。
- 從裝置接收到多個陷阱，在短時間內導致多個重新同步觸發器。
- 與裝置相關的多個表中的清單資料庫條目存在後端問題。



提示：刪除網路裝置並使用正確的CLI、SNMP和NETCONF憑證重新發現該裝置有助於刪除可能導致內部錯誤的過時資料庫條目。



提示：檢視清單服務日誌並按裝置IP或主機名進行過濾有助於確定內部錯誤根本原因。

裝置憑證

要檢視裝置憑證，請導航到Cisco DNA Center Menu -> Provision -> Inventory -> Select Device -> Actions -> Inventory -> Edit Device，然後點選「Validate」 ，確認強制憑證（CLI和SNMP）通過綠色勾選驗證（如果適用，包括netconf）。

如果驗證失敗，請檢視Cisco DNA Center用於管理網路裝置的使用者名稱和密碼是否直接在裝置命令列中有效。

如果已在本地配置或已在AAA伺服器（TACACS或RADIUS）中配置，請驗證使用者名稱和密碼是否在AAA伺服器中配置正確。

還要檢查使用者名稱許可權是否要求在Cisco DNA C的「裝置憑證設定」中設定「啟用」密碼輸入庫存。

CLI憑據中的錯誤可能導致清單中出現可管理性錯誤消息：CLI驗證失敗。

Netconf

Netconf是一種通過遠端過程呼叫(RPC)遠端管理相容網路裝置的協定。

Cisco DNA Center使用Netconf功能來推送或刪除網路裝置上的配置，以啟用通過保證進行監控等功能。

Cisco DNA Center Inventory還可以驗證Netconf要求是否正確，其中包括：

- Netconf預設埠830是開放的，在網路中可以正常工作。
- 具有許可權15的使用者，通過SSH訪問網路裝置（本地或配置了AAA）。
- 在網路裝置上啟用Netconf:

```
<#root>

(config)#

netconf-yang
```

- 如果啟用aaa new-model，則還需要配置AAA默認設定要求：

```
<#root>

(config)#

aaa authorization exec default
```

```
(config)#

aaa authentication login default
```

Netconf憑證中的錯誤可能導致清單中的可管理性錯誤消息：Netconf連線失敗。

網路檢查

我們還可以根據版本驗證網路連線和協定設定（如SNMP設定）。

例如，我們可以根據SNMP版本來仔細檢查社群、使用者、組、引擎ID、身份驗證和加密設定等。

我們還可以在裝置命令列中使用ping和traceroute命令，在防火牆、代理或訪問清單中使用SSH(22)和SNMP（161和162）埠來檢查SSH和SNMP連線。

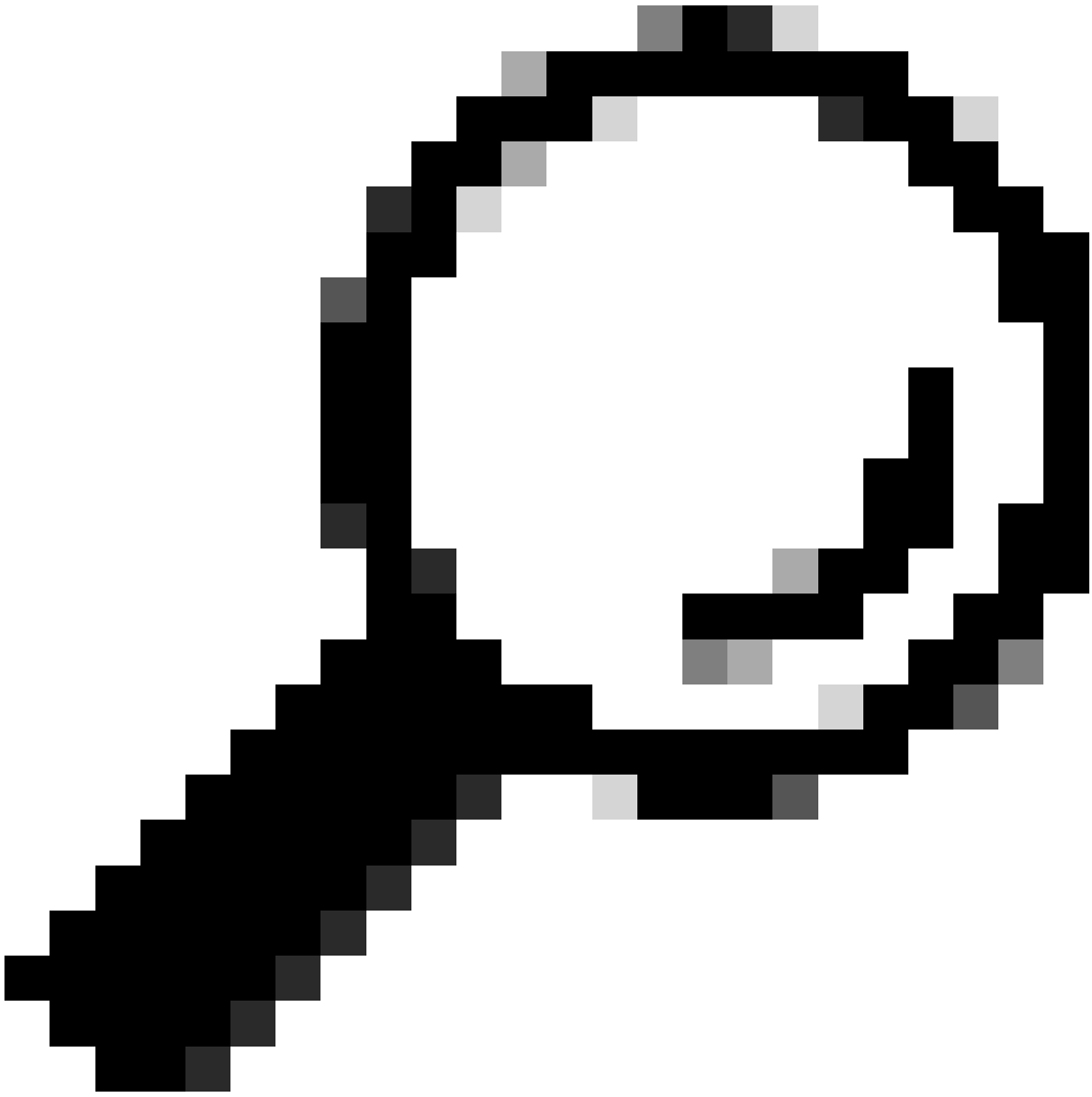
在Cisco DNA Center中，磁懸浮式CLI使用ip route命令驗證與網路裝置的連線。

SNMP walk也可用於進行故障排除。

SNMP憑證中的錯誤可能導致清單中的可管理性錯誤消息：SNMP身份驗證失敗或設備無法訪問。

資料庫表

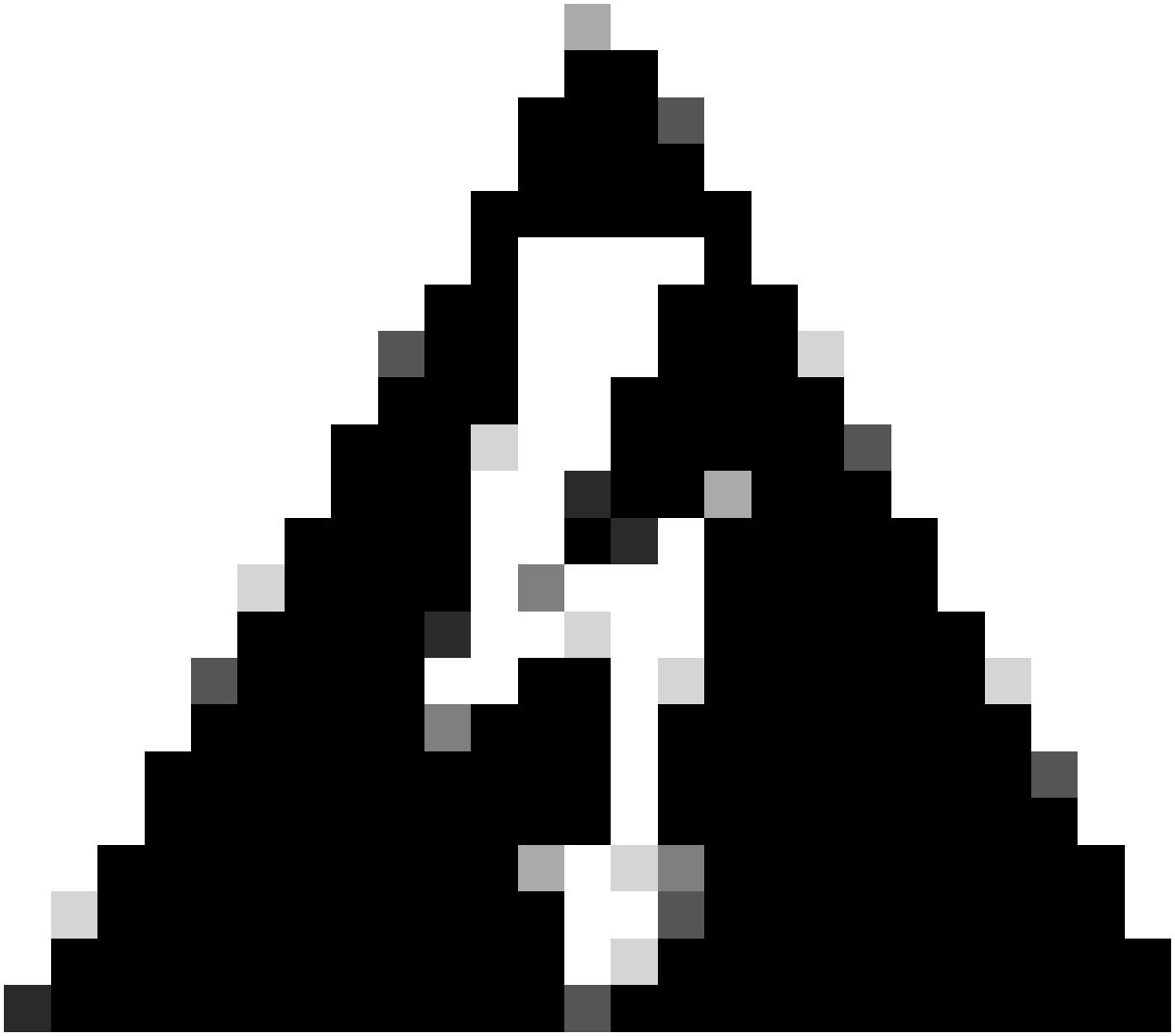
作為終端使用者，您可以使用帶有Grafana的Cisco DNA Center GUI來執行SQL查詢，因此您無需通過磁懸浮命令列介面訪問Postgres外殼。



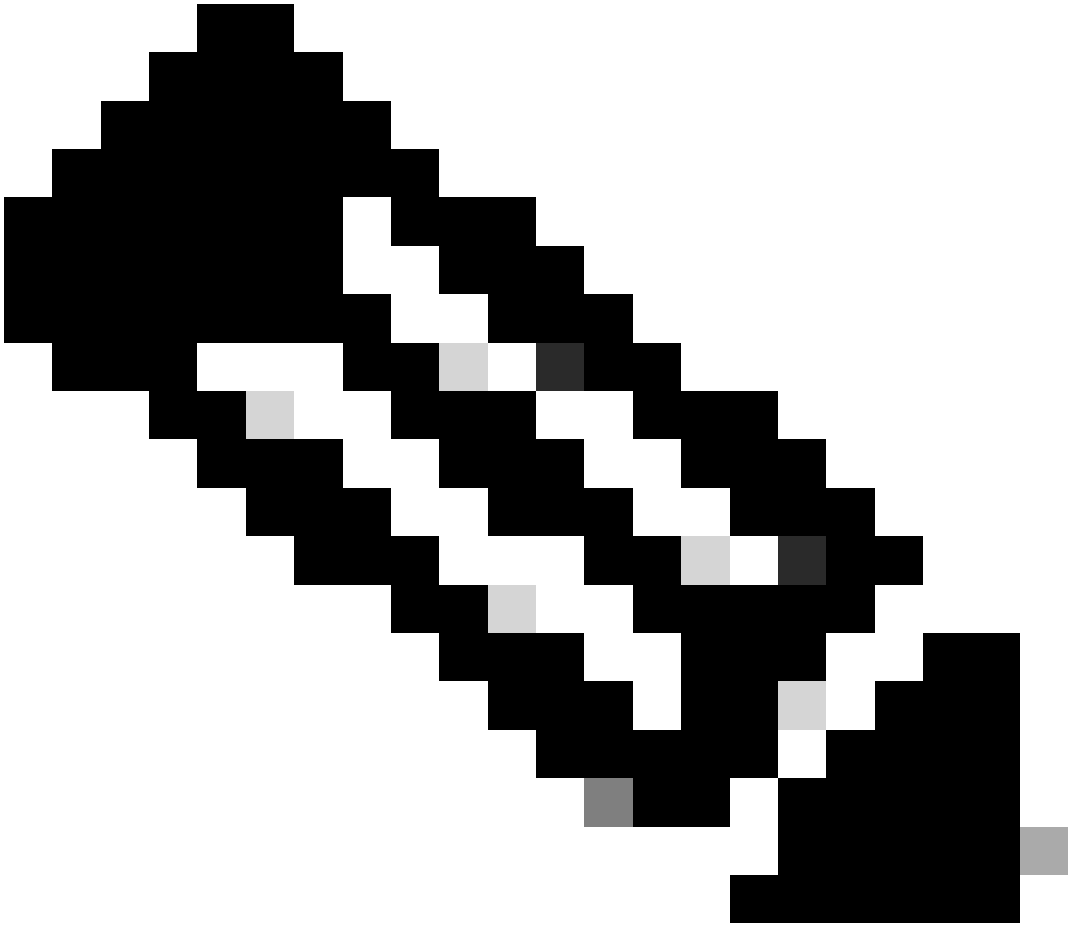
提示：如果您想瞭解如何使用Grafana，請檢視官方指南：在Cisco DNA Center GUI中執行Postgres查詢

當清單中的網路裝置有問題時，需要檢視的一些postgres資料庫表包括：

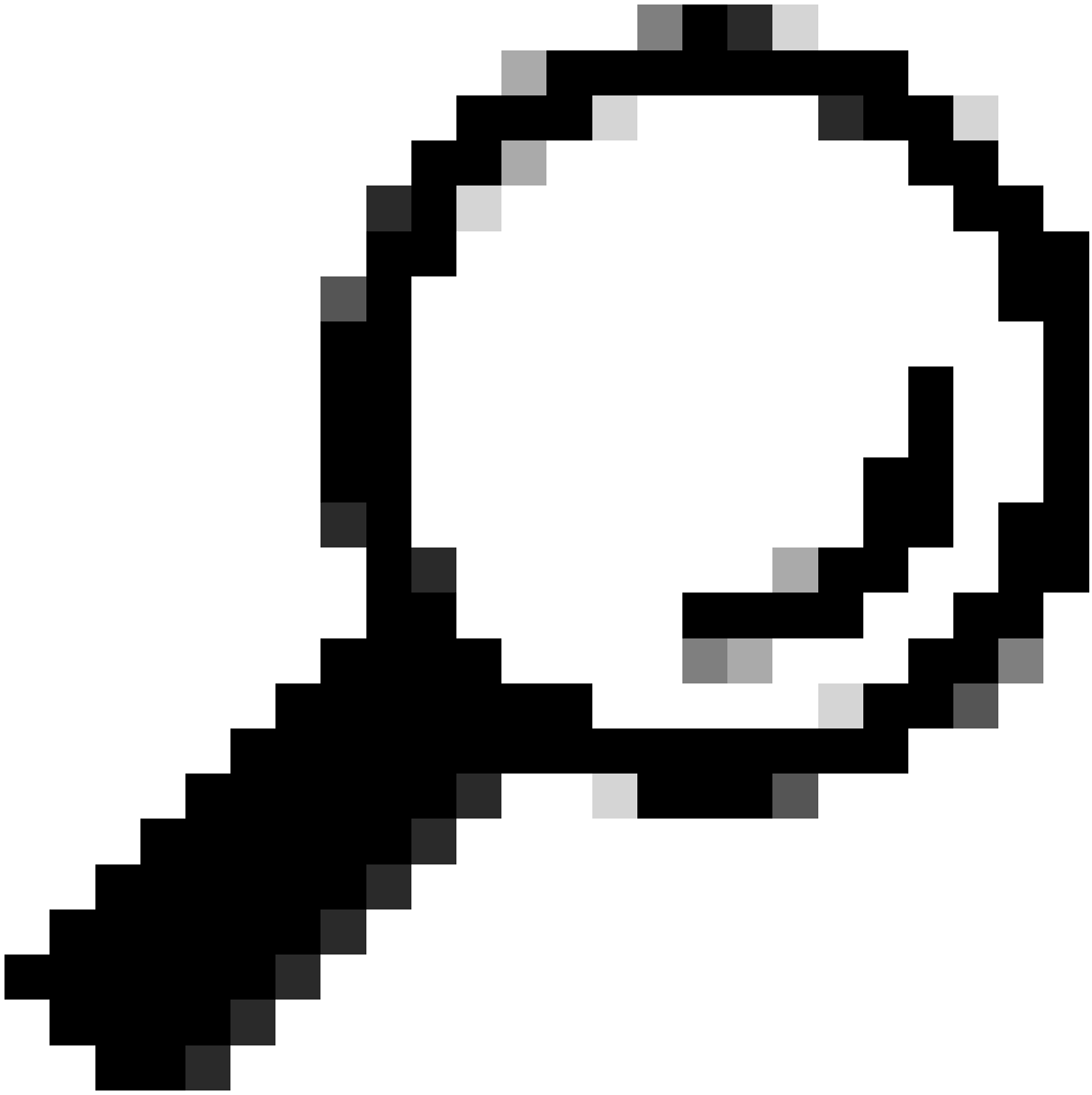
- 網路裝置
- managedelementinterface
- 網路元素
- 網路資源
- 裝置if
- IP地址



警告：僅允許Cisco TAC在Postgres Shell中運行show查詢，並且僅允許BU/DE團隊修改資料庫表。



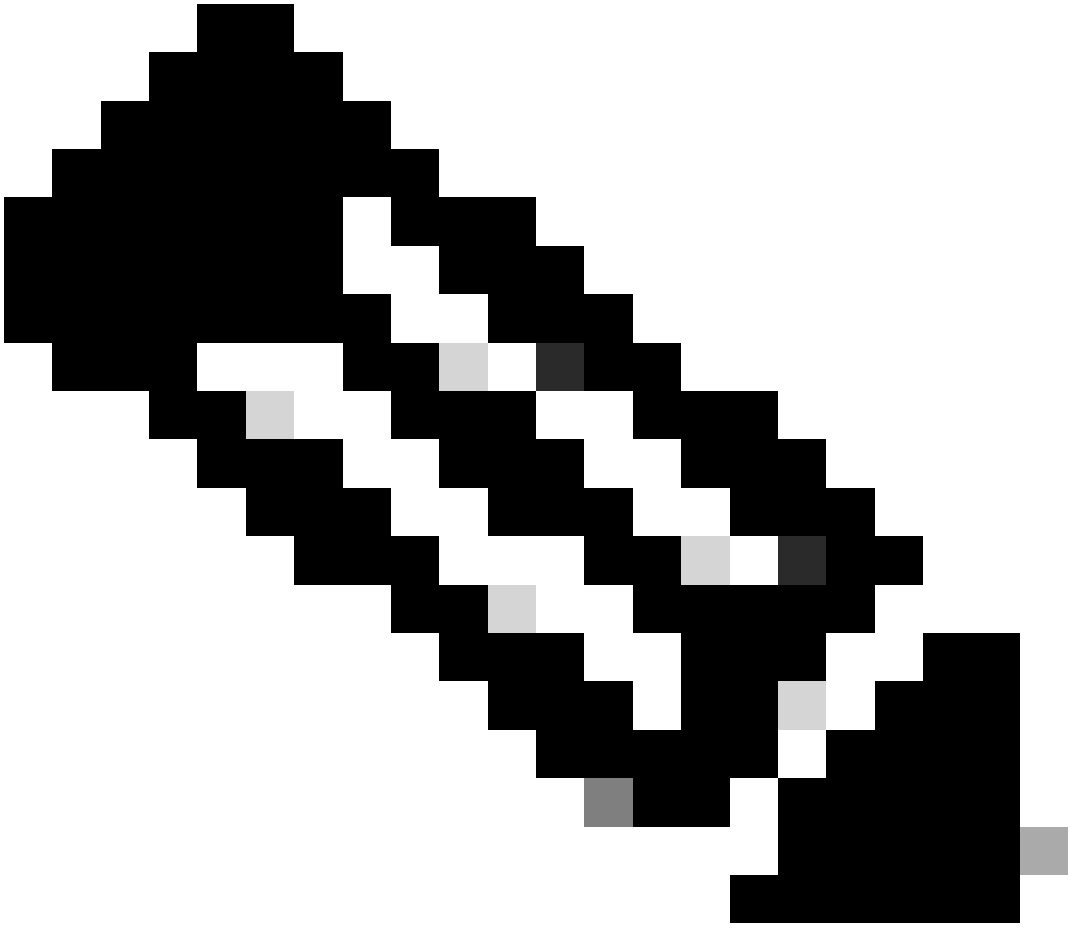
附註：資料庫問題還可能導致裝置出現內部錯誤消息，從而阻止資料收集和裝置調配。



提示：在Cisco DNA Center System 360頁面中，可以使用Kibana檢視Postgres日誌，並在Inventory服務嘗試儲存或更新日誌資料庫表中的條目時查詢約束衝突。

同步循環和陷阱

Cisco DNA Center設計為在裝置本身執行重大更改後，每次收到來自裝置的陷阱時執行裝置重新同步，以保持更新Cisco DNA Center清單。有時，Cisco DNA Center清單頁面會在可管理性部分將網路裝置長期或永久保持為「同步」狀態。



附註：由於存在大量陷阱，這些型別的同步環路會導致Cisco DNA Center在短時間內多次向因檢測到更改而傳送陷阱的裝置進行身份驗證。

用於強制裝置同步的API

如果您的網路裝置保持同步狀態的時間過長（甚至過天），請先檢查基本檢查連通性和連通性。然後通過API呼叫強制裝置重新同步：

1. — 開啟Cisco DNA Center maglev CLI會話。

2. — 通過API獲取Cisco DNA Center身份驗證令牌：

<#root>

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

3. — 使用上一步中的令牌運行API以強制裝置同步：

<#root>

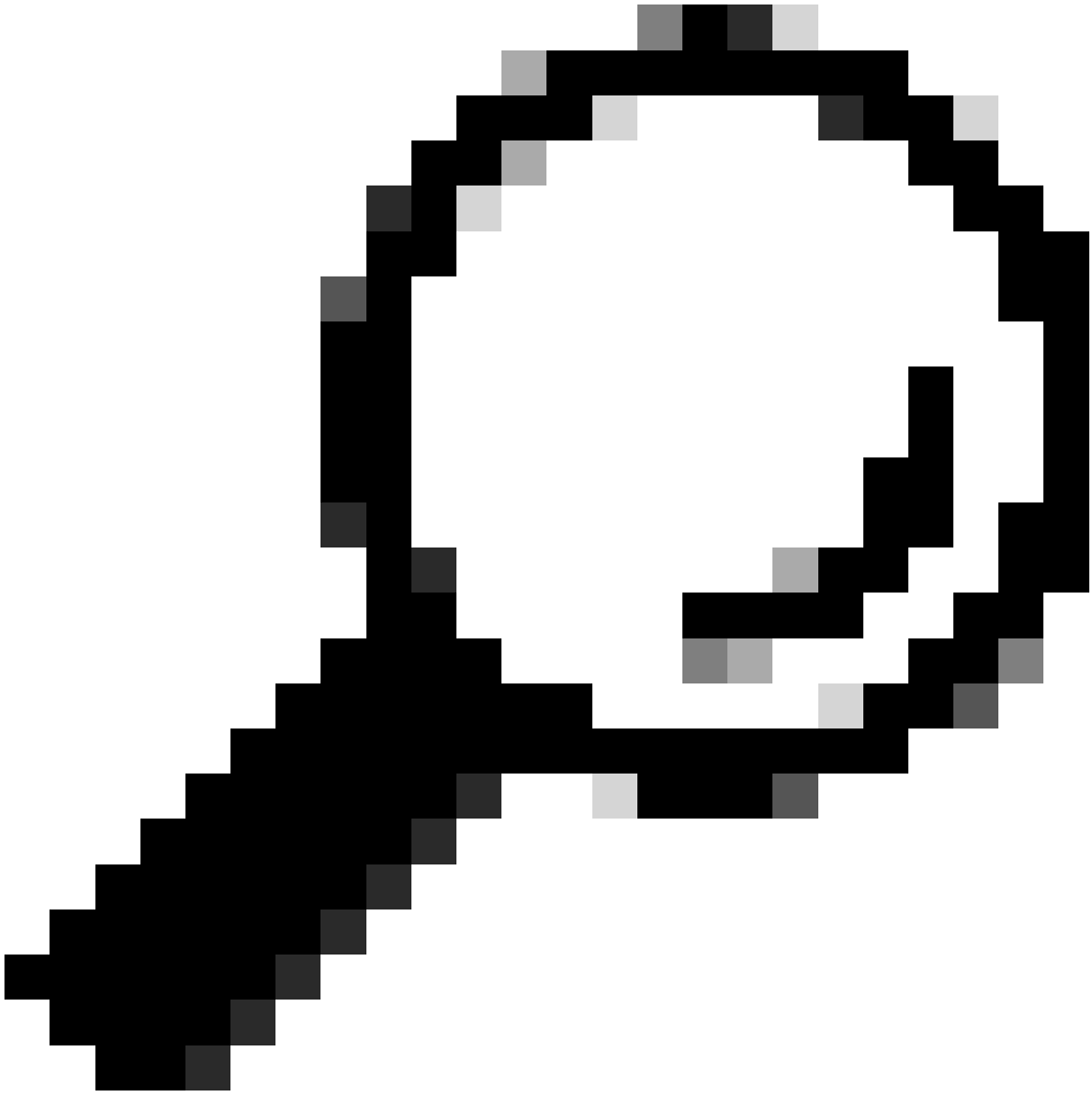
curl -X PUT -H "X-AUTH-TOKEN:

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

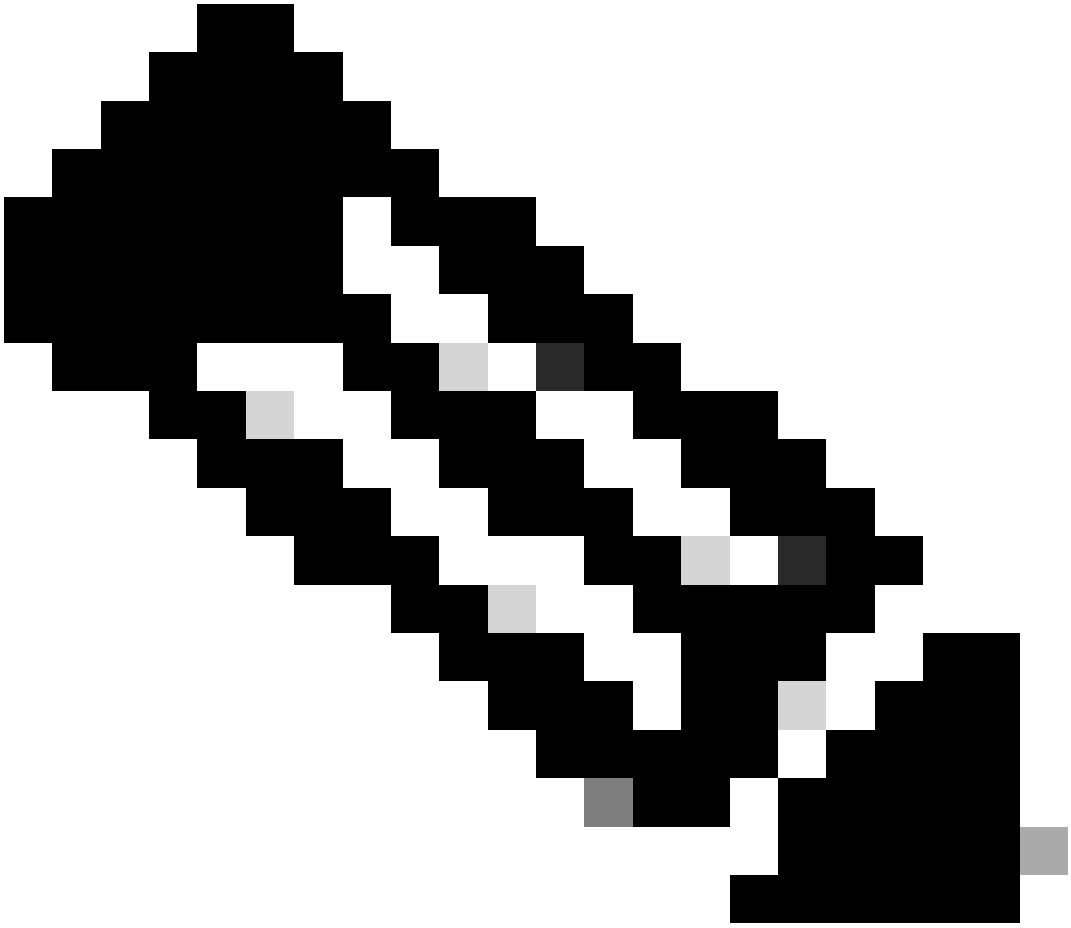
' https://

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

4. — 您可以再次看到正在同步的裝置，但這次通過API使用強制同步選項。



提示：您可以從瀏覽器URL（裝置ID或ID）中從Cisco DNA Center Inventory Device Details頁面或Device View 360頁面獲取裝置UUID。



附註：有關Cisco DNA Center中API的詳細資訊，請參閱Cisco DevNet API指南

檢視陷阱

如果在強制在裝置中執行同步任務後問題仍然存在，我們可以檢查Cisco DNA Center 「event-service」是否接收了過多的陷阱，並通過讀取事件服務日誌來檢查陷阱的類型：

1. — 在讀取日誌之前，我們只需使用以下命令檢查陷阱總數：

<#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. — 然後我們附加至事件服務容器：

<#root>

$ magctl service attach -D event-service

3. — 進入事件服務容器後，將目錄更改為日誌資料夾：

<#root>

$ cd /opt/CSCOlumos/logs/

4. — 如果檢視目錄中的檔案，您可以看到一些名稱以「ncs」開頭的日誌檔案。

範例：

<#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. — 這些「ncs」檔案是我們需要分析接收的陷阱型別和數量的檔案。我們可以檢視按裝置主機名或關鍵字「trapType」過濾這些日誌檔案的日誌檔案：

<#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

陷阱的型別過多，有些陷阱會觸發裝置重新同步，如果它們過於頻繁，則可能會導致Sync循環。

通過分析陷阱，我們可以確定根本原因並使陷阱停止，例如重新啟動週期中的AP。

您可以將陷阱輸出儲存到檔案中，並在需要時與升級團隊共用這些輸出。

服務崩潰狀態

如果您懷疑庫存Pod由於管理網路裝置時Cisco DNA Center庫存頁面中的異常行為而崩潰，則可以首先驗證Pod狀態：

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

檢視Pod狀態的輸出（如果您看到大量重新啟動或錯誤狀態），則您可以連線到庫存容器並收集堆轉儲檔案，該檔案可以包含有助於上報團隊分析和定義崩潰狀態的根本原因的資料：

<#root>

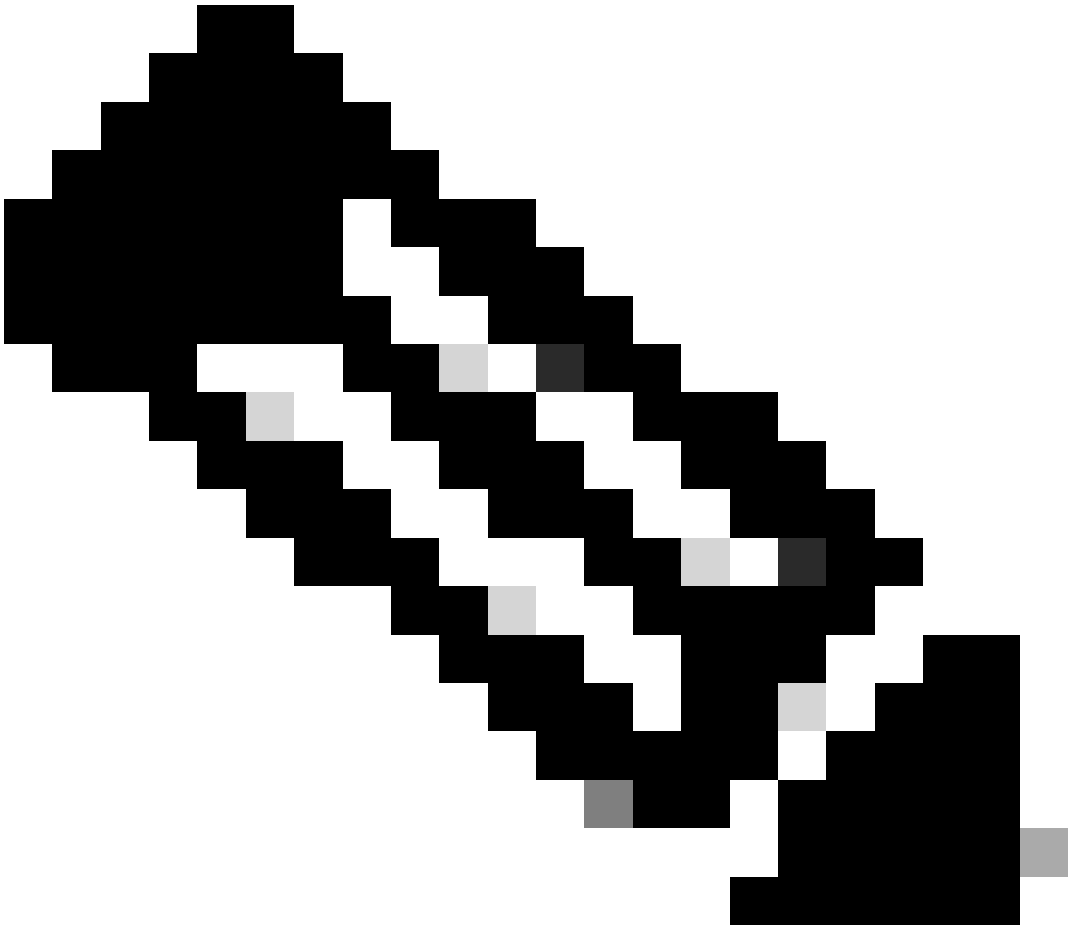
$ magctl service attach -D

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



附註：如果在容器目錄中找不到heapdump檔案，則容器中不存在崩潰狀態。

無法刪除裝置

在某些情況下，由於後端問題，Cisco DNA Center無法從清單使用者介面中刪除網路裝置。

強制裝置刪除的API

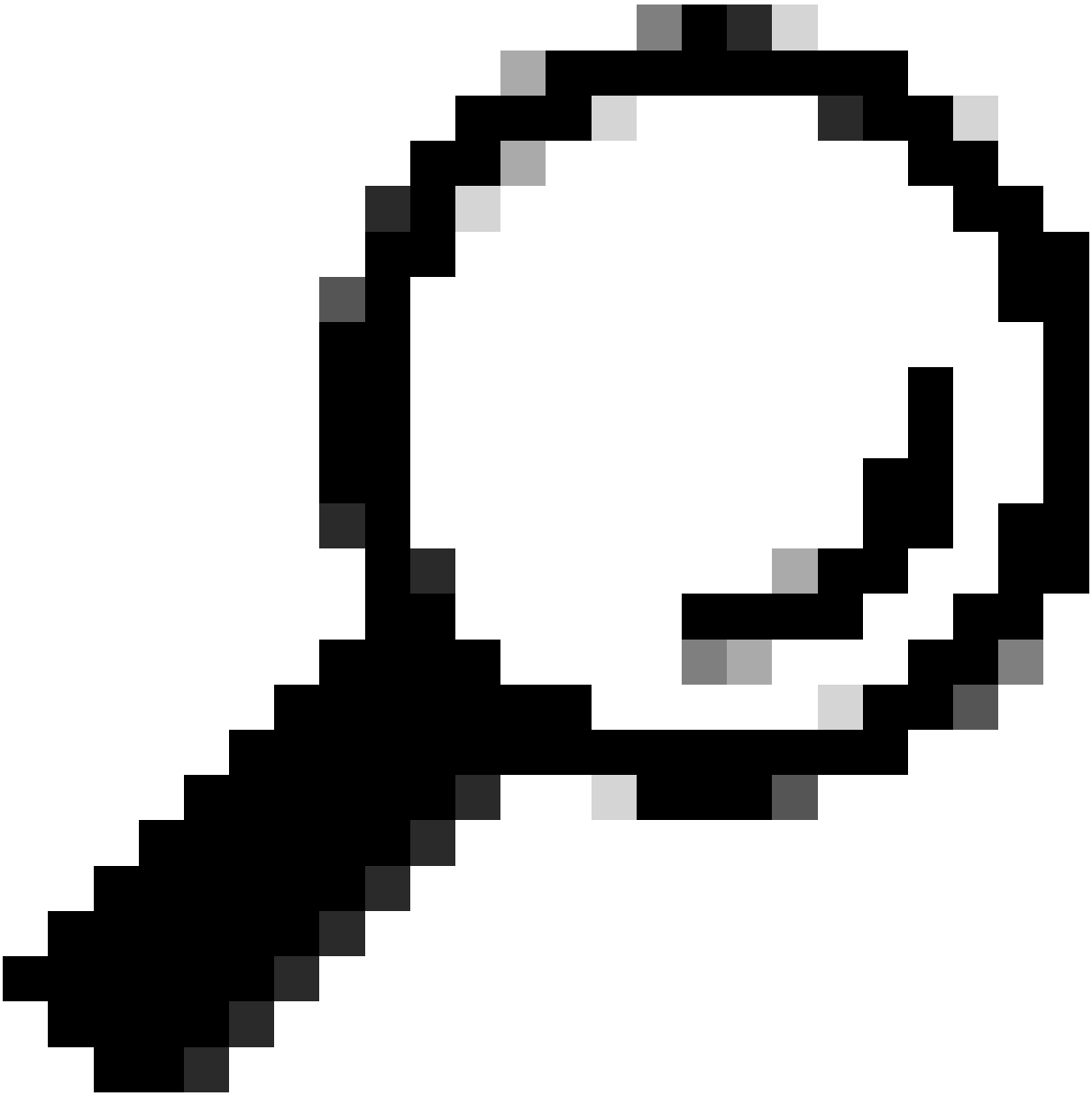
如果您無法使用Cisco DNA Center GUI從清單中刪除裝置，則可以使用API按ID刪除裝置：

1. — 導航至Cisco DNA Center Menu -> Platform -> Developer Toolkit -> APIs Tab，並在搜尋欄中搜尋Devices，在結果中按一下Know your network部分中的Devices，然後搜尋DELETE by Device

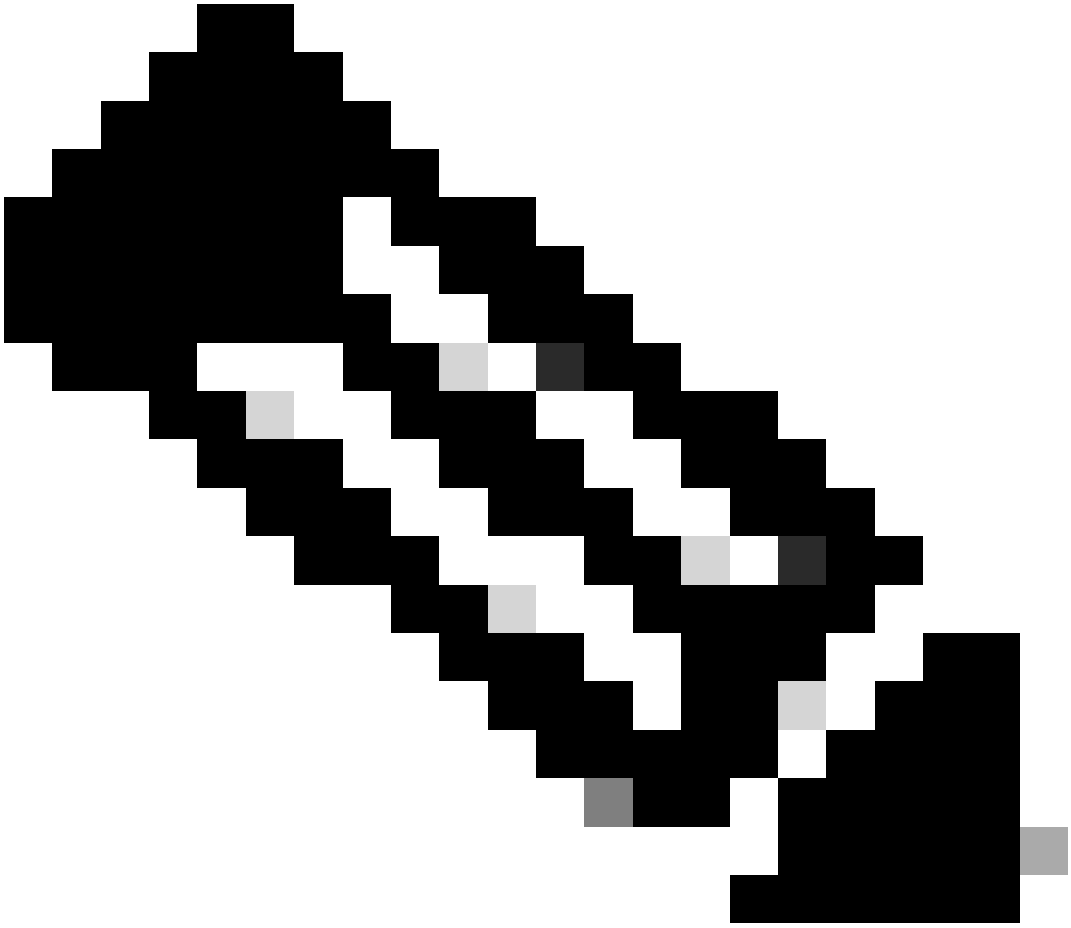
IdAPI。

2. — 在DELETE by Device Id API中按一下，在Try中按一下，然後提供要從清單中刪除的所需裝置的裝置ID。

3. — 等待API運行並獲得200 OK響應，然後確認網路裝置不再存在於清單頁面中。



提示：您可以從瀏覽器URL（裝置ID或ID）中從Cisco DNA Center Inventory Device Details頁面或Device View 360頁面獲取裝置UUID。



附註：有關Cisco DNA Center中API的詳細資訊，請參閱Cisco DevNet API指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。