DNA Center Inventory Service 및 Common Issues 검토

목차

소개

이 문서에서는 Cisco DNA Center Inventory 서비스의 기본 개념 및 프로덕션에서 발견되는 일반적인 문제에 대해 설명합니다.

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

인벤토리 서비스 세부 정보

Cisco DNA Center Inventory 서비스는 Kubernetes(K8s) Pod에 기반하며, 이 Pod는 이름 "apic-em-inventory-manager-service-<id>"를 구축 환경 유형으로 사용하여 "fusion" 네임스페이스에서 실행할 수 있습니다.

K8s 포드 내에서는 "apic-em-inventory-manager-service"라는 Docker 컨테이너를 찾을 수 있습니다.

"apic-em-inventory-manager-service" Pod 주요 작업은 디바이스 검색 및 디바이스 라이프사이클

관리입니다.

이렇게 하면 Postgres SQL(Fusion Services에서 사용하는 데이터베이스)에서 디바이스 데이터를 사용할 수 있습니다.

NCP(Network Controller Platform)라고도 하는 "fusion" 네임스페이스(Appstack)는 모든 네트워크 자동화 요구 사항에 대해 SPF(Service Provisioning Framework) 서비스를 제공합니다.

여기에는 검색, 인벤토리, 토폴로지, 정책, SWIM(Software Image Management), 컨피그레이션 아카이브, 네트워크 프로그래머, 사이트, 그룹화, 텔레메트리, Tesseract 통합, 템플릿 프로그래머, 맵, IPAM, 센서, 오케스트레이션/워크플로/스케줄링, ISE 통합 등이 포함됩니다.

인벤토리 포드 상태는 다음 명령을 실행하여 확인할 수 있습니다.

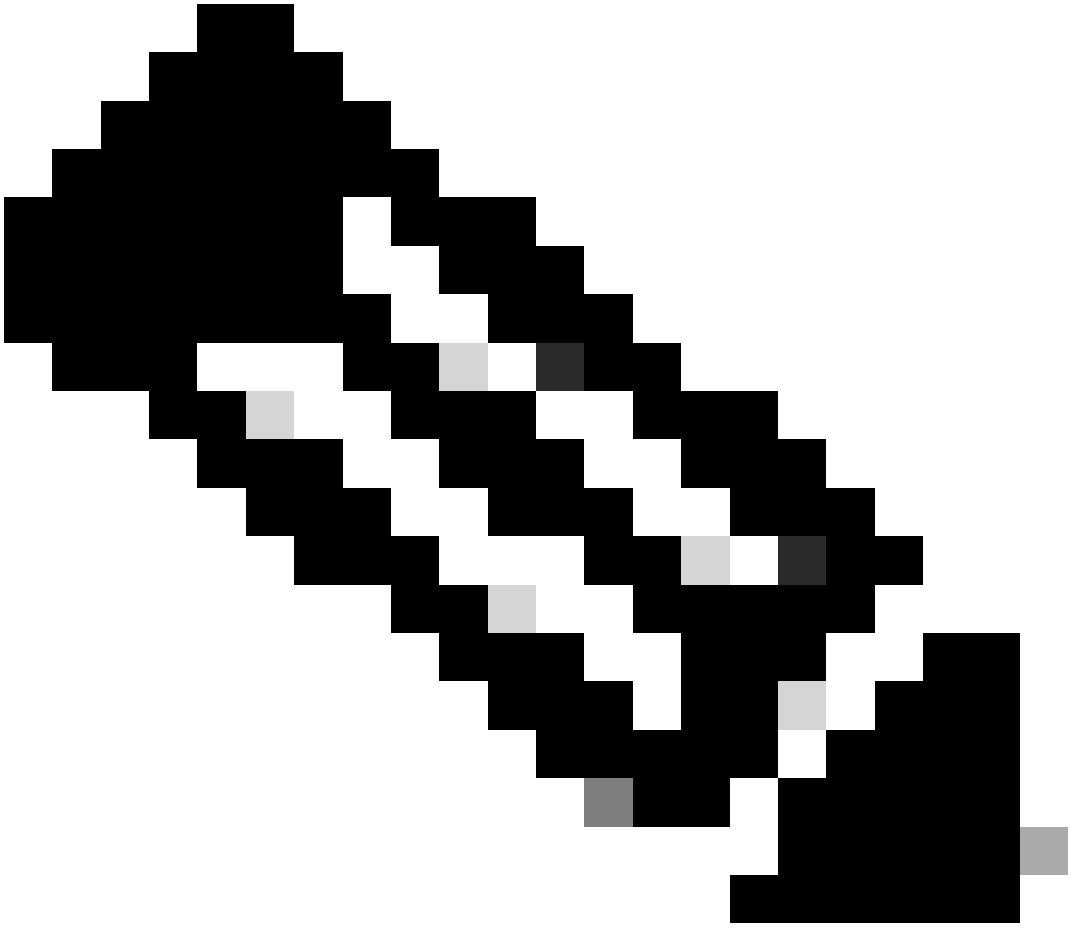
```
$ magctl appstack status | grep inventory
```

인벤토리 서비스 상태는 다음 명령을 사용하여 확인할 수 있습니다.

```
$ magctl service status
```

인벤토리 서비스 로그는 다음 명령을 사용하여 확인할 수 있습니다.

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



참고: 인벤토리 서비스는 실행 중인 2개의 포드로 구성될 수도 있으므로 포드 ID를 비롯한 전체 인벤토리 포드 이름을 사용하여 명령에서 단일 포드를 지정해야 합니다.

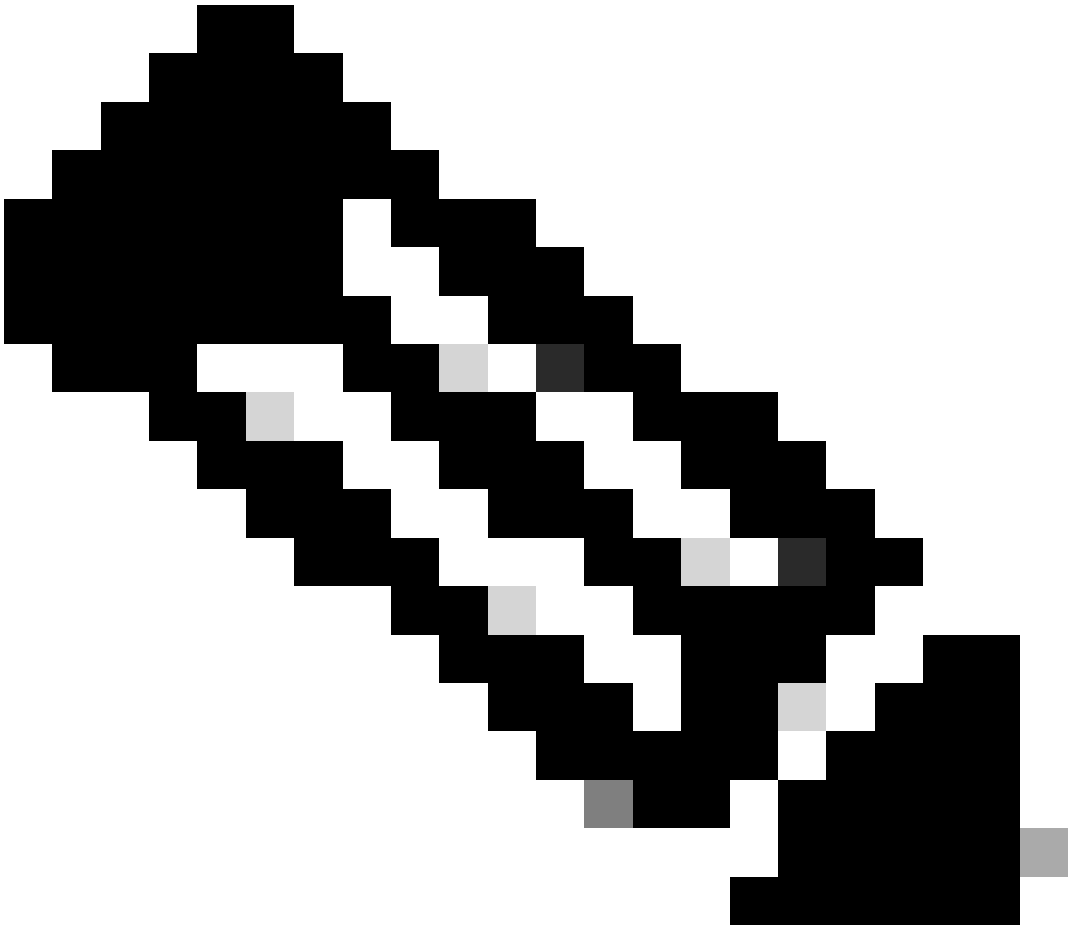
이 문서에서는 Inventory(인벤토리) 디바이스 관리 용이성 및 Last Syncing(마지막 동기화) 상태에 초점을 맞추어 일반적인 문제를 검토할 수 있습니다.

관리 상태

- 녹색 눈금 아이콘으로 관리: 장치에 연결할 수 있으며 완전히 관리됩니다.
- 주황색 오류 아이콘으로 관리됨: 디바이스는 연결할 수 없음, 인증 실패, Netconf 포트 누락, 내부 오류 등과 같은 일부 오류로 관리됩니다. 오류 메시지 위에 커서를 올려 놓으면 오류 및 영향을 받는 애플리케이션에 대한 자세한 정보를 볼 수 있습니다.
- 관리되지 않음: 장치에 연결할 수 없으며 장치 연결 문제로 인해 인벤토리 정보가 수집되지 않았습니다.

마지막 동기화 상태

- 관리됨: 디바이스가 완전히 관리되는 상태입니다.
- 부분 수집 실패: 디바이스가 일부 수집된 상태이며 모든 인벤토리 정보가 수집된 것은 아닙니다. 정보(i) 아이콘 위에 커서를 올려 놓으면 장애에 대한 추가 정보가 표시됩니다.
- 연결할 수 없음: 장치에 연결할 수 없으며 장치 연결 문제로 인해 인벤토리 정보가 수집되지 않았습니다. 이 조건은 정기적인 수집이 이루어질 때 발생합니다.
- 잘못된 자격 증명: 인벤토리에 디바이스를 추가한 후 디바이스 자격 증명이 변경된 경우 이 조건이 표시됩니다.
- 진행 중: 인벤토리 수집이 진행 중입니다.



참고: Cisco DNA Center의 인벤토리 기능에 대한 자세한 내용은 버전 2.3.5.x: 인벤토리 관리 공식 가이드를 참조하십시오

문제

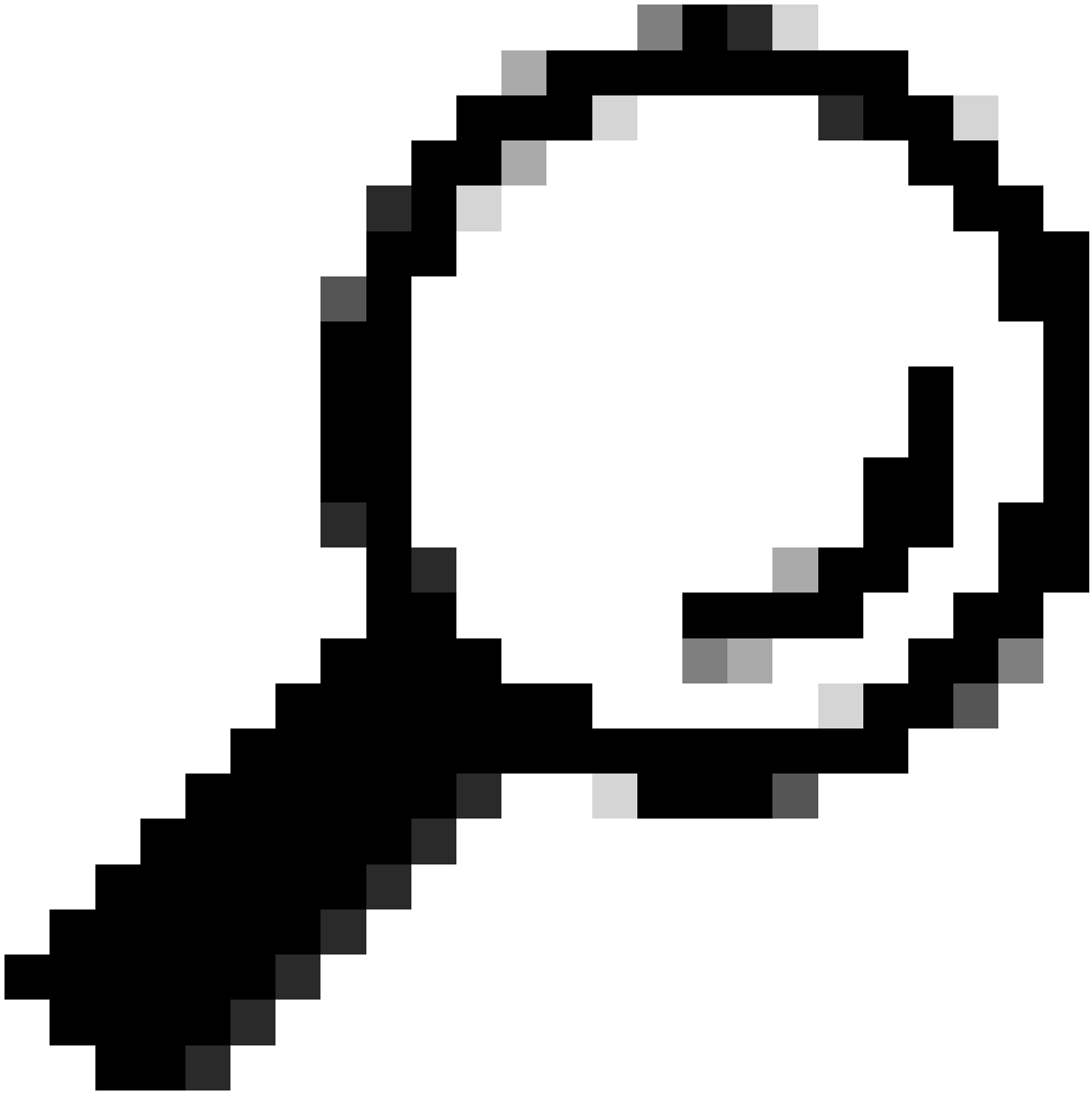
내부 오류

Cisco DNA Center Inventory(Cisco DNA 센터 인벤토리) 페이지는 데이터 수집을 방해하는 일종의 충돌이 있는 장비의 Manageability(관리 가능성) 상태에 경고 메시지를 표시할 수 있습니다.

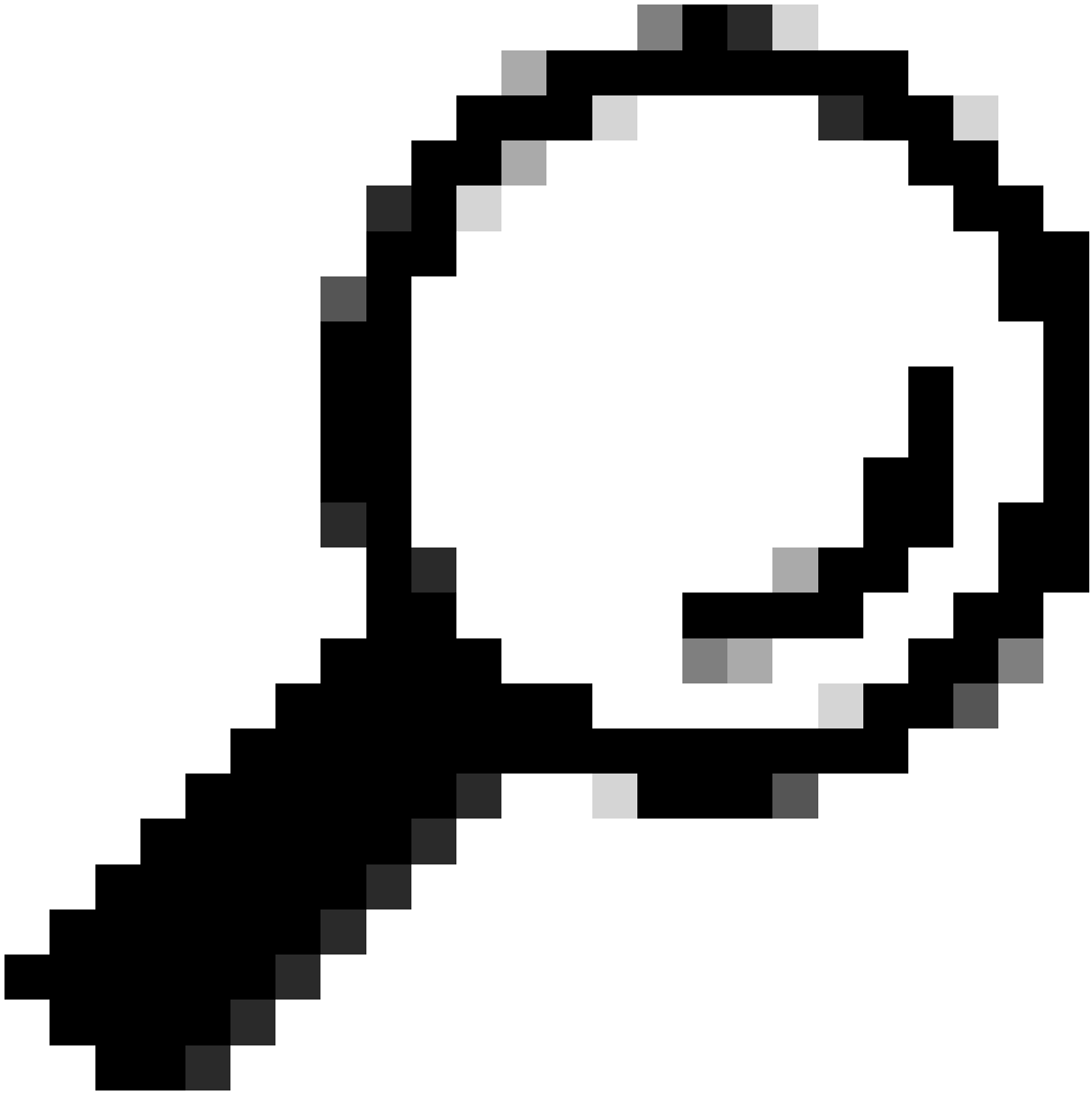
"내부 오류: NCIM12024: 디바이스의 모든 정보를 성공적으로 수집할 수 없거나 이 디바이스에 대한 인벤토리 수집이 아직 시작되지 않았습니다. 그것은 자동으로 해결될 수 있는 일시적인 문제일 수 있다. 장치를 다시 동기화해도 문제가 해결되지 않을 경우 Cisco TAC에 문의하십시오."

오류가 자동으로 또는 디바이스를 재동기화한 후에도 해결되지 않을 경우 초기 문제 해결부터 시작할 수 있습니다. 이 오류는 여러 가지 이유로 인해 발생할 수 있지만 여기서는 가장 일반적인 몇 가지 예를 살펴보겠습니다.

- SNMP, SSH 및 Netconf에 대한 디바이스 자격 증명이 잘못되었습니다.
- SNMP, SSH 및 Netconf와 관련된 네트워크 연결 문제
- 디바이스의 Netconf 컨피그레이션 문제로 인해 Netconf가 제대로 작동하지 않습니다.
- 장치 동기화가 이미 진행 중인 동안 장치 재동기화를 트리거합니다.
- 디바이스에서 여러 트랩이 수신되어 단기간에 여러 재동기화 트리거가 발생합니다.
- 장치와 관련된 여러 테이블의 인벤토리 데이터베이스 항목과 관련된 백엔드 문제입니다.



팁: 네트워크 디바이스를 제거하고 올바른 CLI, SNMP 및 NETCONF 자격 증명을 사용하여 다시 검색하면 내부 오류를 일으킬 수 있는 오래된 데이터베이스 항목을 제거하는 데 도움이 될 수 있습니다.



팁: 인벤토리 서비스 로그를 검토하고 디바이스 IP 또는 호스트 이름을 기준으로 필터링하면 내부 오류 근본 원인을 파악하는 데 도움이 됩니다.

디바이스 자격 증명

디바이스 자격 증명을 검토하려면 Cisco DNA Center 메뉴 -> Provision(프로비저닝) -> Inventory(인벤토리) -> Select Device(디바이스 선택) -> Actions(작업) -> Inventory(인벤토리) -> Edit Device(디바이스 수정)로 이동하여 "Validate(검증)"를 클릭하고 필수 자격 증명(CLI 및 SNMP)이 녹색 확인(적용되는 경우 netconf 포함)으로 검증을 통과하는지 확인합니다.

검증이 실패할 경우 Cisco DNA Center에서 네트워크 디바이스 관리에 사용하는 사용자 이름 및 비밀번호가 디바이스 명령줄에서 직접 유효한지 검토하십시오.

로컬로 구성된 경우 또는 AAA 서버(TACACS 또는 RADIUS)에서 구성된 경우 AAA 서버에서 사용

자 이름과 비밀번호가 올바르게 구성되었는지 확인하십시오.

또한 사용자 이름 권한이 Cisco DNA C의 Device Credentials Settings(디바이스 자격 증명 설정)에서 "Enable" 비밀번호를 설정해야 하는지 확인합니다Inventory(인벤토리)를 입력합니다.

CLI 자격 증명 오류가 발생하면 인벤토리에서 관리 용이성 오류 메시지가 나타날 수 있습니다. CLI 인증 실패.

Netconf

Netconf는 RPC(원격 프로시저 호출)를 통해 호환되는 네트워크 디바이스를 원격으로 관리하기 위한 프로토콜입니다.

Cisco DNA Center는 Netconf 기능을 사용하여 네트워크 디바이스에서 컨피그레이션을 푸시하거나 제거하여 Assurance를 통한 모니터링과 같은 기능을 활성화합니다.

Cisco DNA Center Inventory는 Netconf 요구 사항이 올바른지 확인할 수 있으며, 여기에는 다음이 포함됩니다.

- Netconf 기본 포트 830은 열려 있으며 네트워크에서 작동합니다.
- 네트워크 디바이스에 대한 SSH 액세스 권한이 있는 15의 사용자(로컬로 또는 AAA가 구성됨).
- 네트워크 디바이스에서 Netconf를 활성화합니다.

<#root>

(config)#

netconf-yang

- aaa new-model(aaa 새 모델)이 활성화된 경우 AAA 기본 설정 요구 사항도 구성해야 합니다.

<#root>

(config)#

aaa authorization exec default

(config)#

aaa authentication login default

Netconf 자격 증명의 오류로 인해 인벤토리에서 관리 용이성 오류 메시지가 나타날 수 있습니다. Netconf 연결 실패.

네트워크 검사

또한 버전에 따라 네트워크 연결 및 SNMP 설정과 같은 프로토콜 설정을 검증할 수 있습니다.

예를 들어 SNMP 버전에 따라 커뮤니티, 사용자, 그룹, engineID, 인증 및 암호화 설정 등을 두 번 확인할 수 있습니다.

또한 디바이스 명령줄의 ping 및 traceroute 명령과 방화벽, 프록시 또는 액세스 목록의 SSH(22) 및 SNMP(161 및 162) 포트를 사용하여 SSH 및 SNMP 연결을 검토할 수 있습니다.

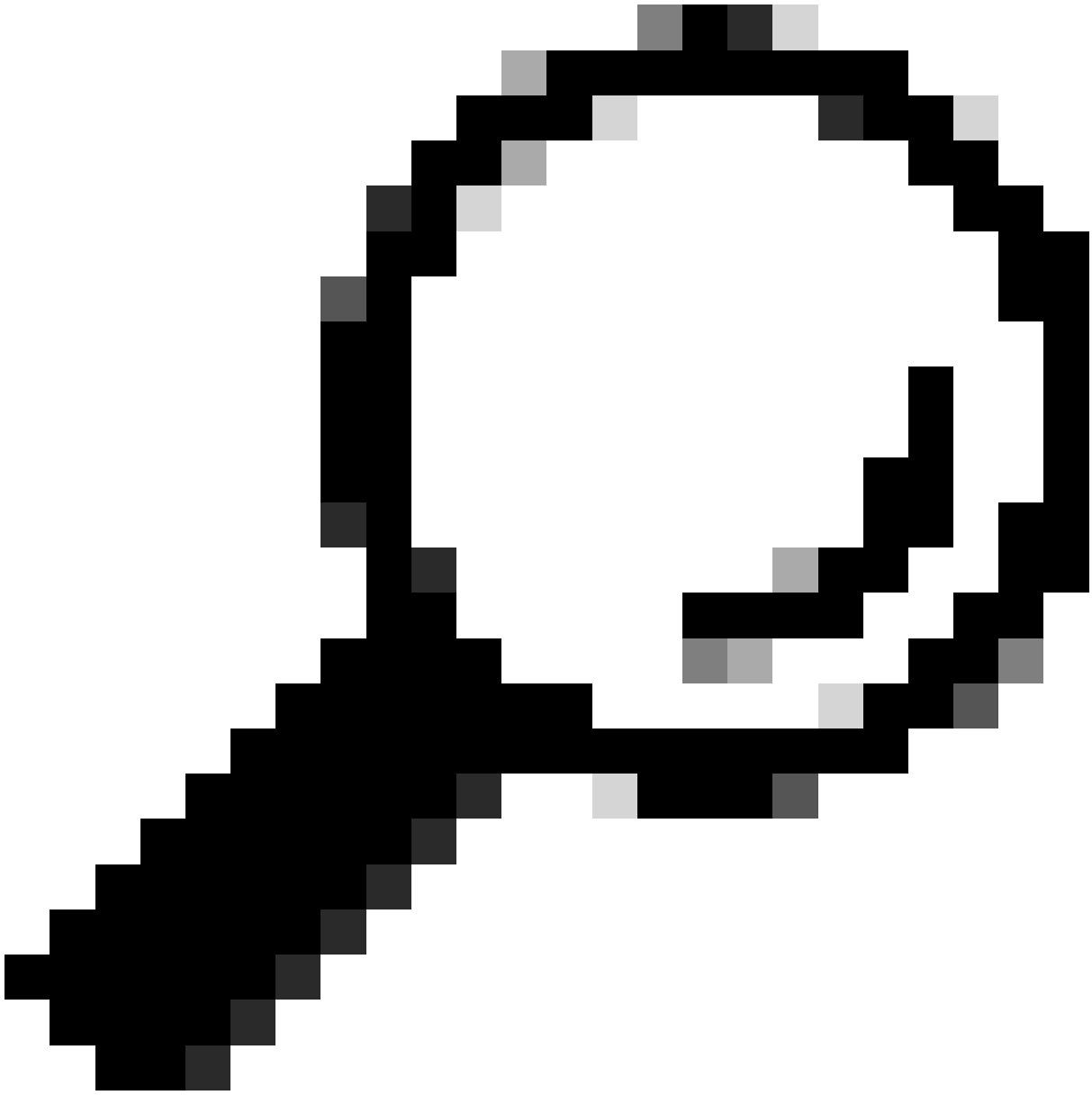
Cisco DNA Center에서 maglev CLI는 ip route 명령을 사용하여 네트워크 디바이스에 대한 연결을 검증합니다.

SNMP Walk를 사용하여 문제를 해결할 수도 있습니다.

SNMP 자격 증명의 오류는 인벤토리의 관리 효율성 오류 메시지를 일으킬 수 있습니다. SNMP 인증 실패 또는 디바이스 연결 불가.

데이터베이스 테이블

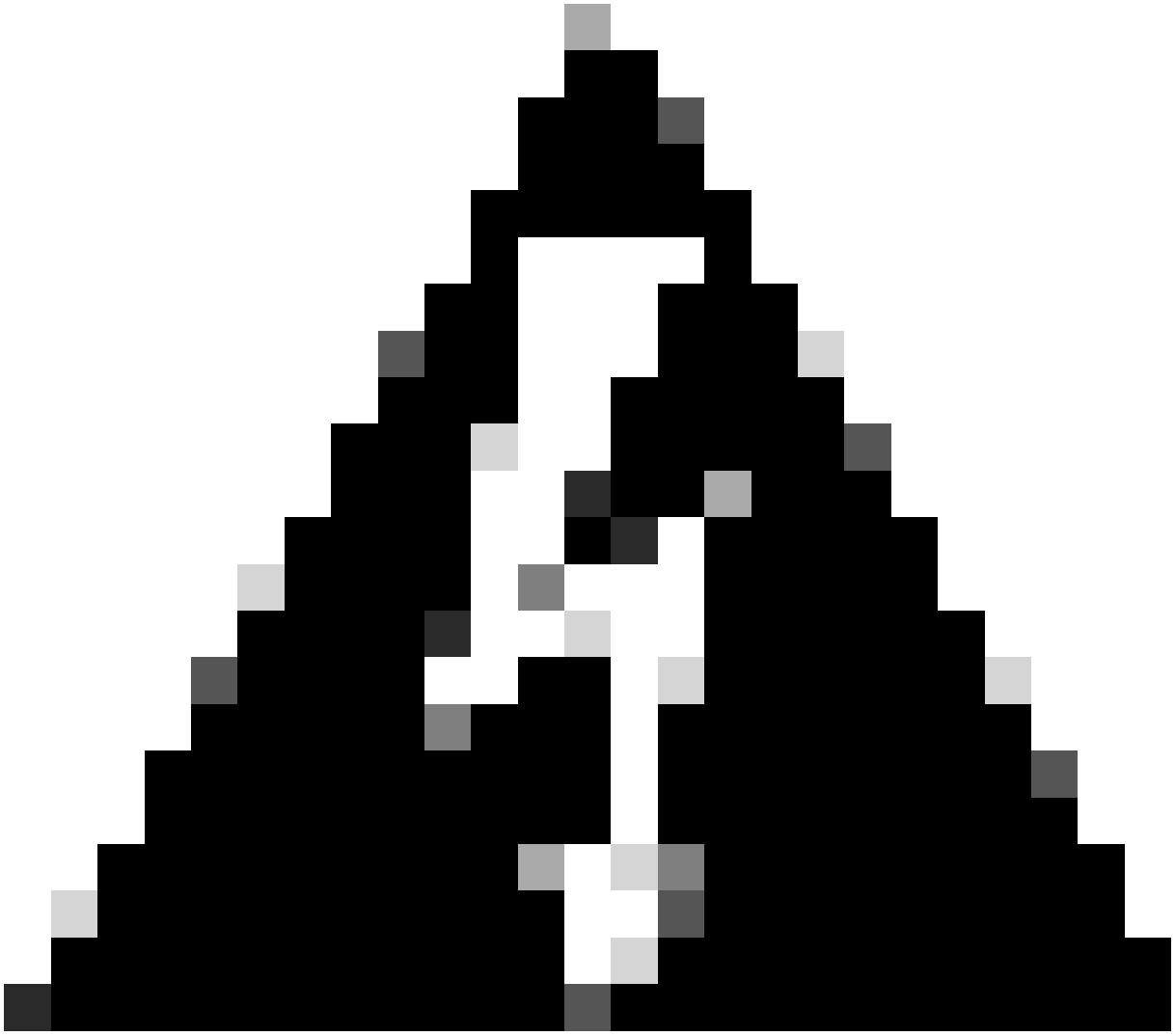
최종 사용자는 Cisco DNA Center GUI와 Grafana를 사용하여 SQL 쿼리를 실행할 수 있으므로 maglev CLI를 통해 Postgres 셸에 액세스할 필요가 없습니다.



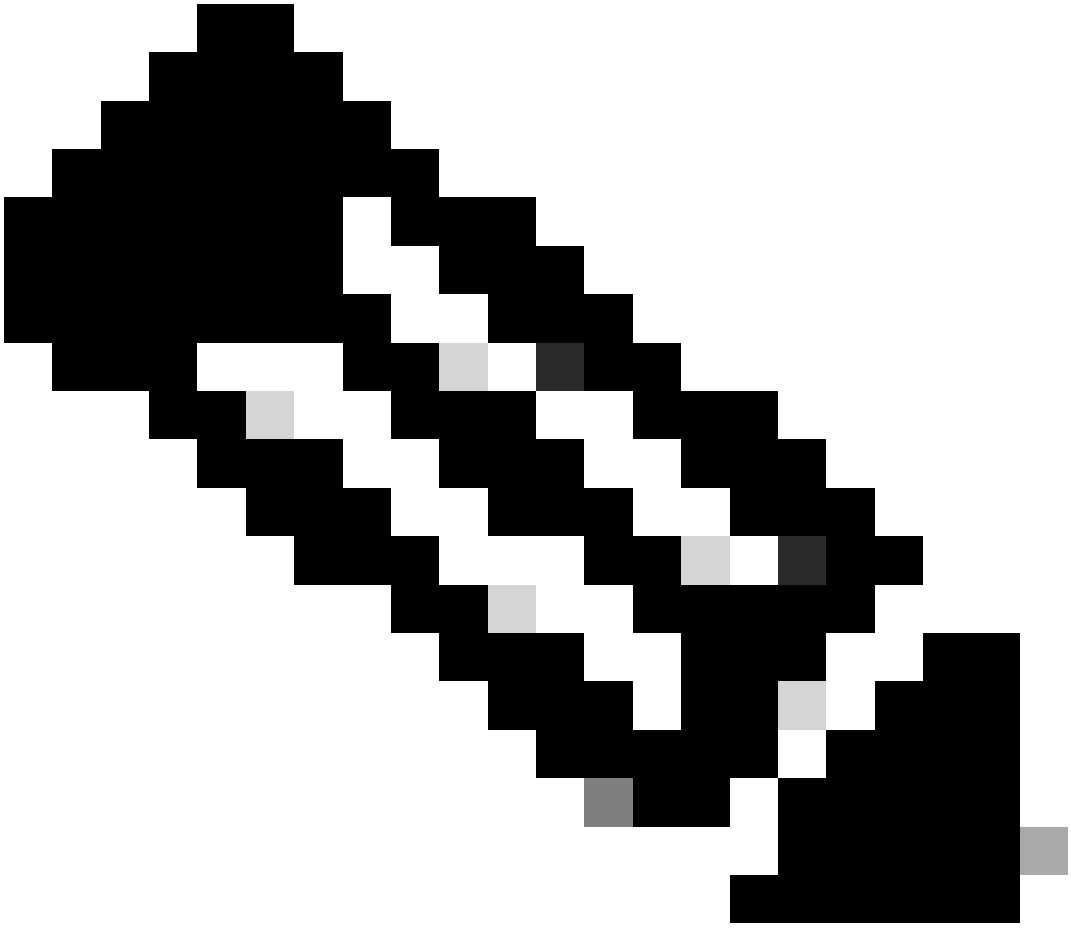
팁: Grafana를 사용하는 방법을 알아보려면 공식 가이드: Cisco DNA Center GUI에서 Execute Postgres Queries(사후 쿼리 실행)를 검토하십시오.

인벤토리의 네트워크 디바이스에 문제가 있을 때 검토할 일부 postgres 데이터베이스 테이블은 다음과 같습니다.

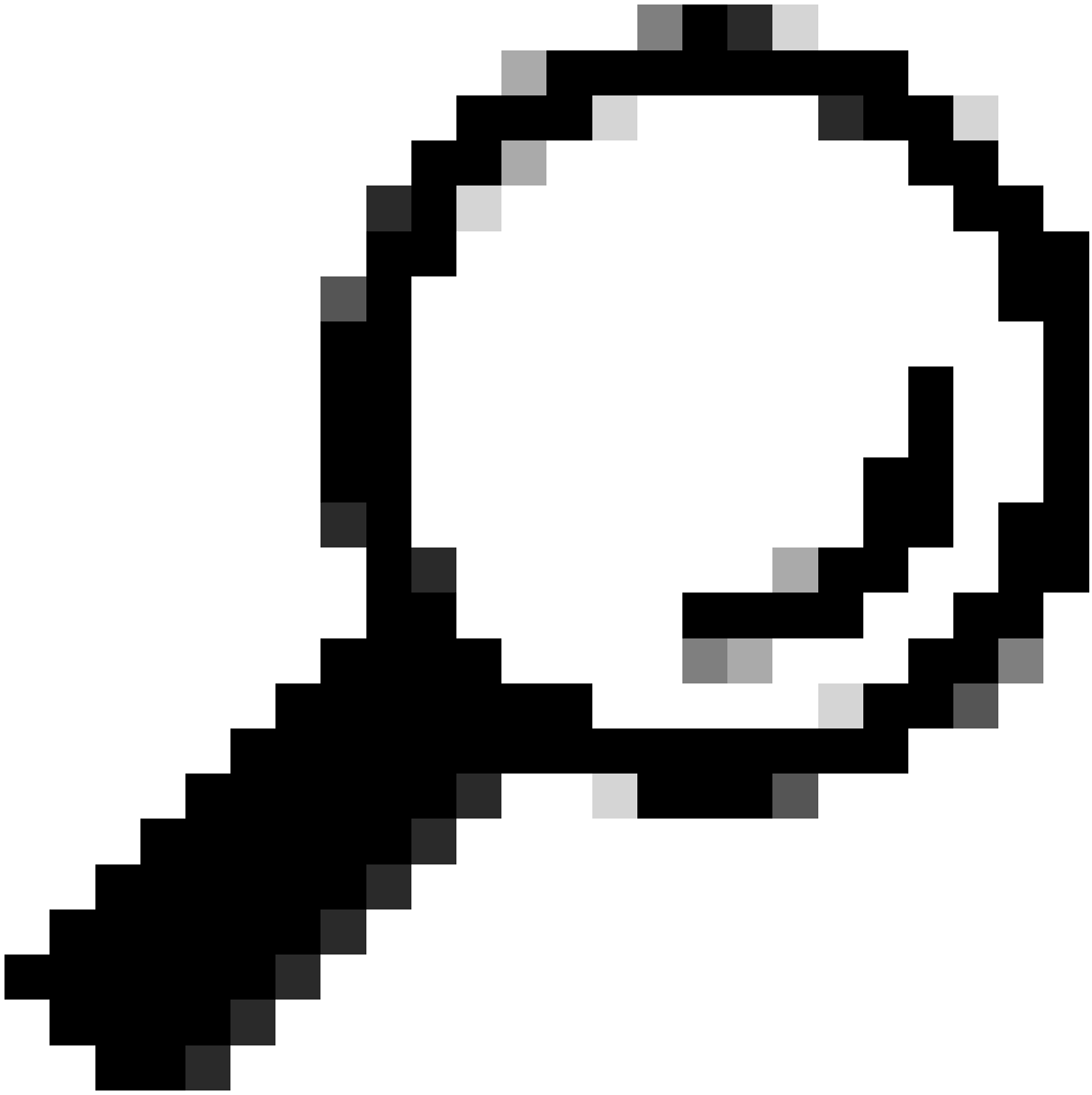
- 네트워크 장치
- 관리인터페이스
- 네트워크 요소
- 네트워크 리소스
- 장치 IF
- ip 주소



경고: Cisco TAC에서만 Postgres 셸에서 표시 쿼리를 실행할 수 있으며 BU/DE 팀에서만 DB 테이블을 수정할 수 있습니다.



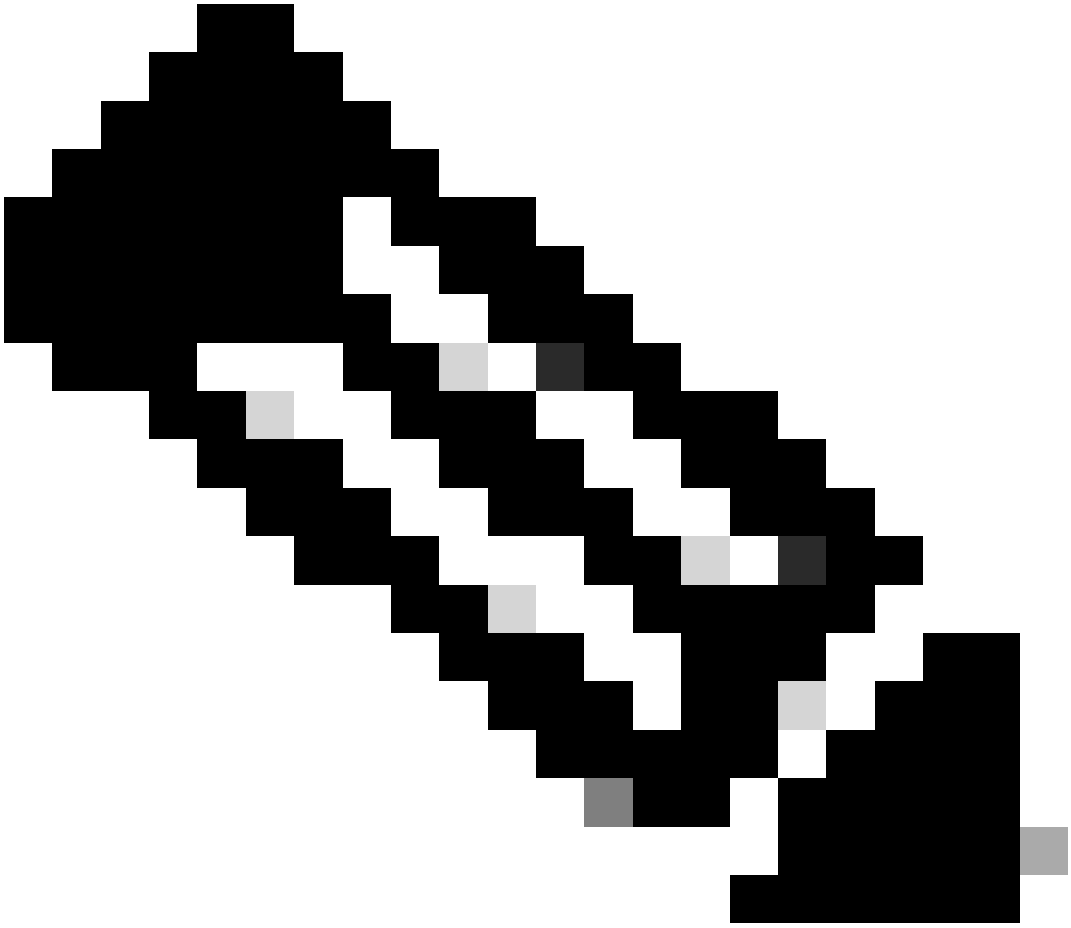
참고: 또한 데이터베이스 문제로 인해 디바이스에 대한 내부 오류 메시지가 나타나 데이터 수집 및 디바이스 프로비저닝을 방지할 수 있습니다.



팁: Cisco DNA Center System 360 페이지에서 Kibana를 사용하여 Postgres 로그를 검토하고 Inventory Service가 Postgres 데이터베이스 테이블의 항목을 저장하거나 업데이트하려고 할 때 제약 조건 위반을 찾을 수 있습니다.

루프 및 트랩 동기화

Cisco DNA Center는 Cisco DNA Center 인벤토리를 업데이트하기 위해 장치 자체에서 주요 변경을 수행한 후 장치에서 트랩을 수신할 때마다 장치 Resycn을 실행하도록 설계되었습니다. 때때로 Cisco DNA Center Inventory 페이지는 네트워크 장치를 관리 가능성 섹션에서 장기간 또는 영원히 "동기화" 상태로 유지합니다.



참고: 대규모 트랩으로 인한 이러한 종류의 동기화 루프는 Cisco DNA Center가 짧은 시간 내에 여러 번 인증하여 변경 사항이 발견되어 트랩을 전송하는 디바이스에 제공할 수 있습니다.

디바이스 동기화를 강제 수행하는 API

네트워크 장치가 너무 오래, 심지어 일 동안 동기화 상태로 유지 하는 경우 먼저 기본 사항 이 연결 및 연결을 확인 합니다. 그런 다음 API 호출을 통해 디바이스를 강제로 다시 동기화합니다.

1.- Cisco DNA Center maglev CLI 세션을 엽니다.

2.- API를 통해 Cisco DNA Center 인증 토큰을 가져옵니다.

<#root>

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

3.- 이전 단계의 토큰을 사용하여 장치 동기화를 강제 수행하기 위해 API를 실행합니다.

<#root>

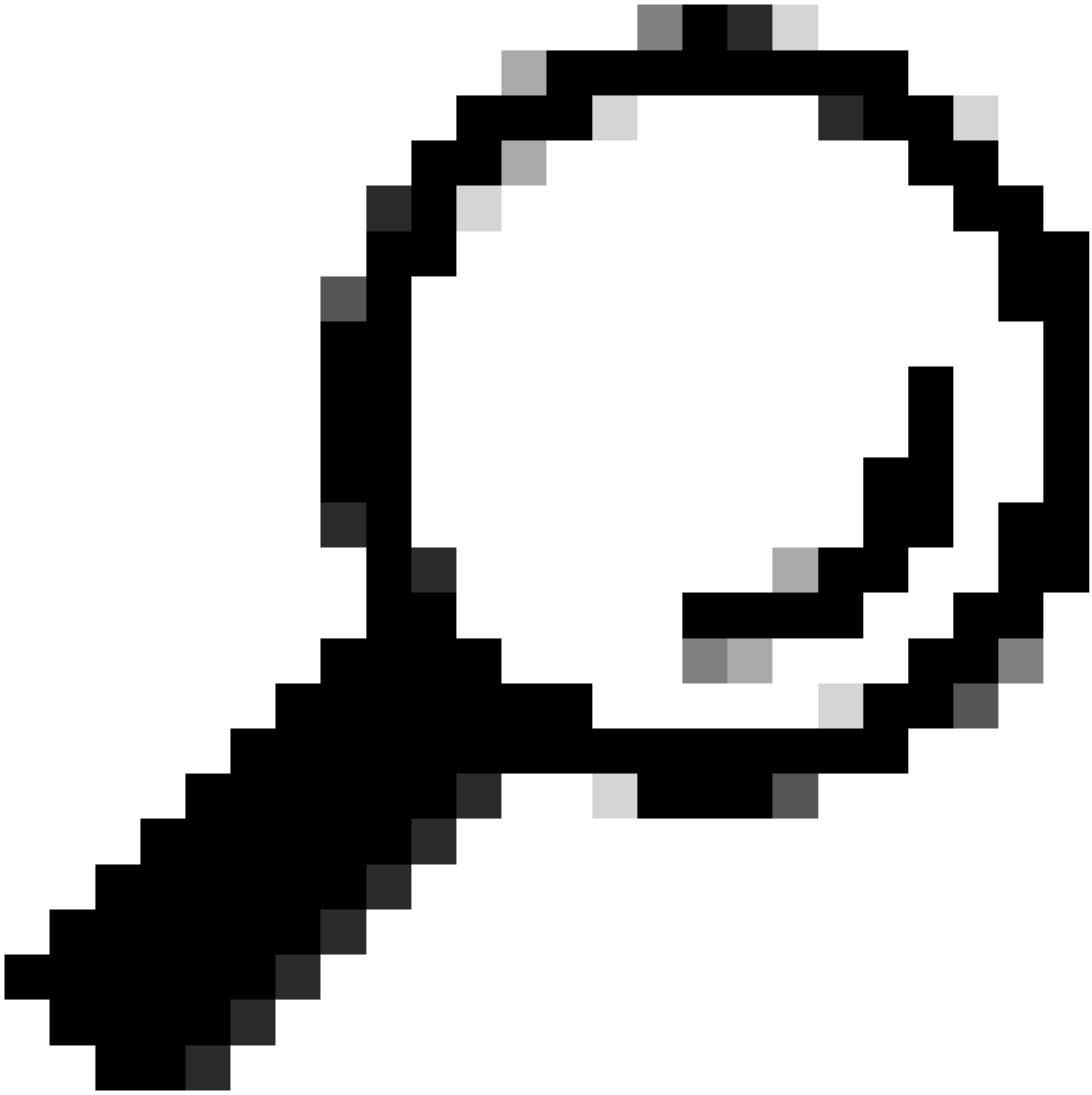
curl -X PUT -H "X-AUTH-TOKEN:

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

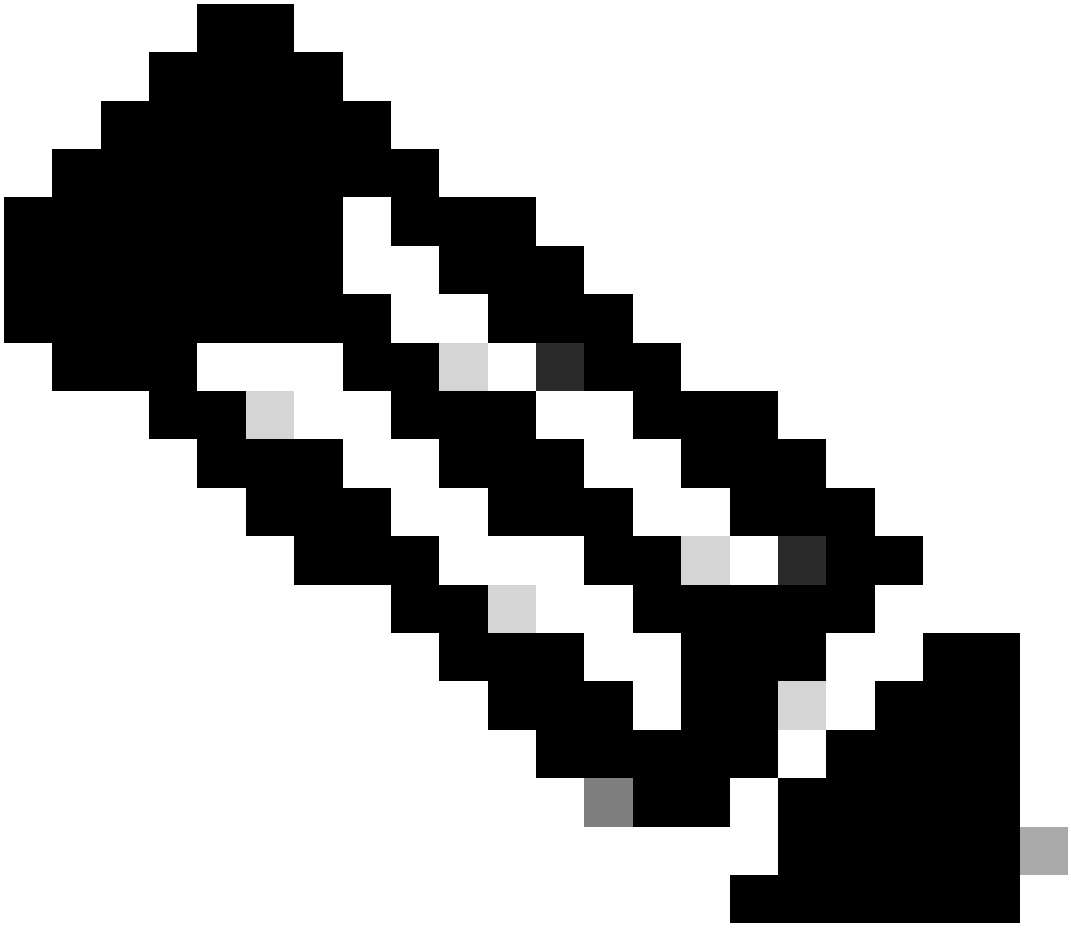
' https://

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

4.- 동기화에서 디바이스를 다시 볼 수 있지만 이번에는 API를 통해 강제 동기화 옵션을 사용할 수 있습니다.



팁: Cisco DNA Center Inventory Device Details(Cisco DNA Center 인벤토리 디바이스 세부사항) 페이지 또는 Device View 360(디바이스 보기 360) 페이지의 브라우저 URL(deviceid 또는 id)에서 디바이스 uuid를 가져올 수 있습니다.



참고: Cisco DNA Center의 API에 대한 자세한 내용은 Cisco DevNet API 가이드를 참조하십시오

트랩 검토

디바이스에서 동기화 작업을 강제로 수행한 후 문제가 지속되면 Cisco DNA Center "event-service"에서 너무 많은 트랩을 수신하는지 검토하고 이벤트 서비스 로그를 읽어 어떤 유형의 트랩을 검토할 수 있습니다.

1.- 로그를 읽기 전에 다음 명령을 사용하여 전체 트랩을 확인할 수 있습니다.

<#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.- 그런 다음 이벤트 서비스 컨테이너에 연결합니다.

<#root>

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

3.- 이벤트 서비스 컨테이너에 들어가면 디렉터리를 logs 폴더로 변경합니다.

<#root>

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

4.- 디렉토리 내의 파일을 검토하면 이름이 "ncs"로 시작하는 일부 로그 파일을 볼 수 있습니다.

예:

<#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.- 이러한 "ncs" 파일은 우리가 받고 있는 트랩 유형과 수를 분석하는 데 필요한 파일입니다. 디바이스 호스트 이름 또는 키워드 "trapType"으로 필터링하는 로그 파일을 검토할 수 있습니다.

<#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
```

트랩 유형이 너무 많습니다. 트랩 중 일부는 디바이스 재동기화를 트리거할 수 있으며 너무 자주 나타나면 동기화 루프가 발생할 수 있습니다.

트랩을 분석하면 근본 원인을 파악하고 트랩을 중지하도록 만들 수 있습니다(예: 재부팅 주기의 AP).

트랩 출력을 파일에 저장하고 필요한 경우 에스컬레이션 팀과 공유할 수 있습니다.

서비스 충돌 상태

네트워크 디바이스를 관리하는 동안 Cisco DNA Center Inventory(Cisco DNA 센터 인벤토리) 페이지에서 이상한 동작으로 인해 인벤토리 포드가 충돌한다고 생각되면 먼저 포드 상태를 확인할 수 있습니다.

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

Pod 상태의 출력을 검토하여 재시작 횟수가 많거나 오류 상태가 표시되면 인벤토리 컨테이너에 연결하고 Heapdump 파일을 수집하여 에스컬레이션 팀이 충돌 상태의 근본 원인을 분석하고 정의하는 데 도움이 되는 데이터를 얻을 수 있습니다.

<#root>

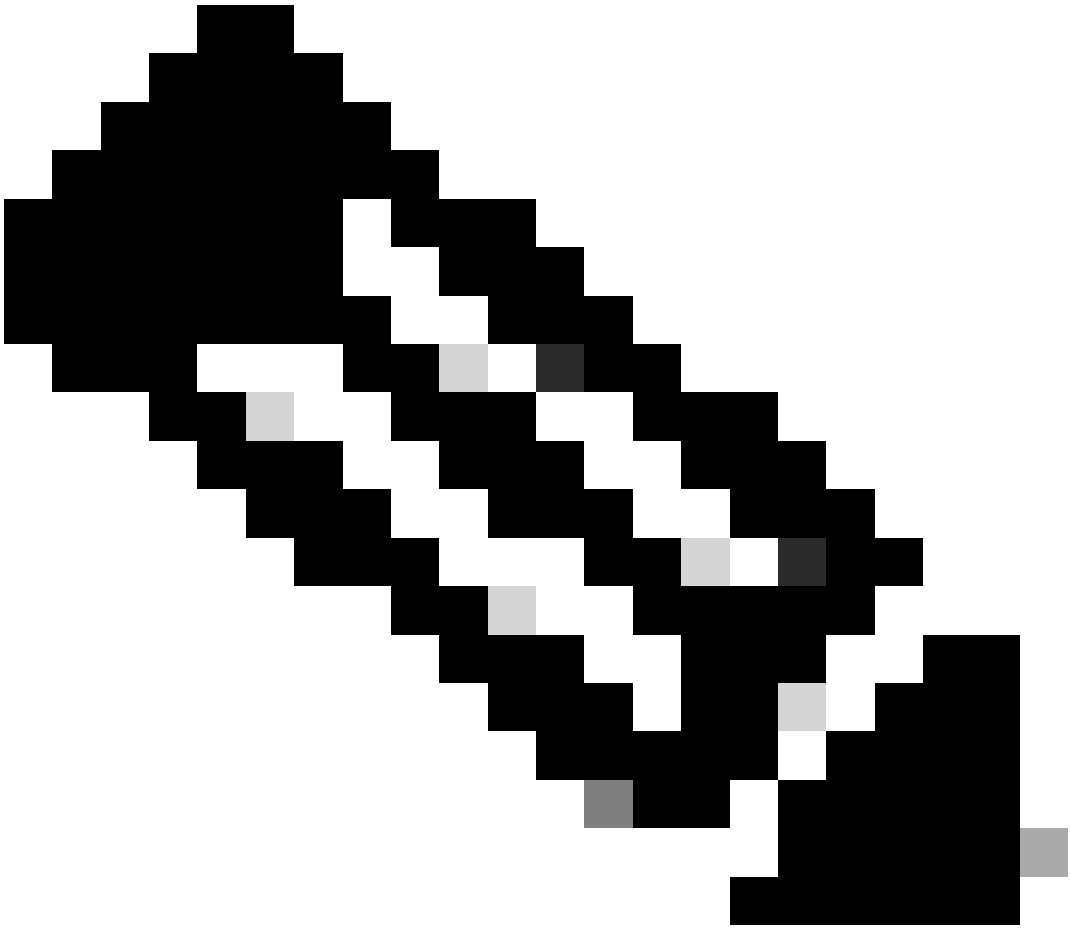
$ magctl service attach -D

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



참고: 컨테이너 디렉터리에 heapdump 파일이 없는 경우 컨테이너에 충돌 상태가 없습니다
.

디바이스를 삭제할 수 없음

경우에 따라 Cisco DNA Center에서 백엔드 문제로 인해 인벤토리 사용자 인터페이스에서 네트워크 디바이스를 삭제할 수 없습니다.

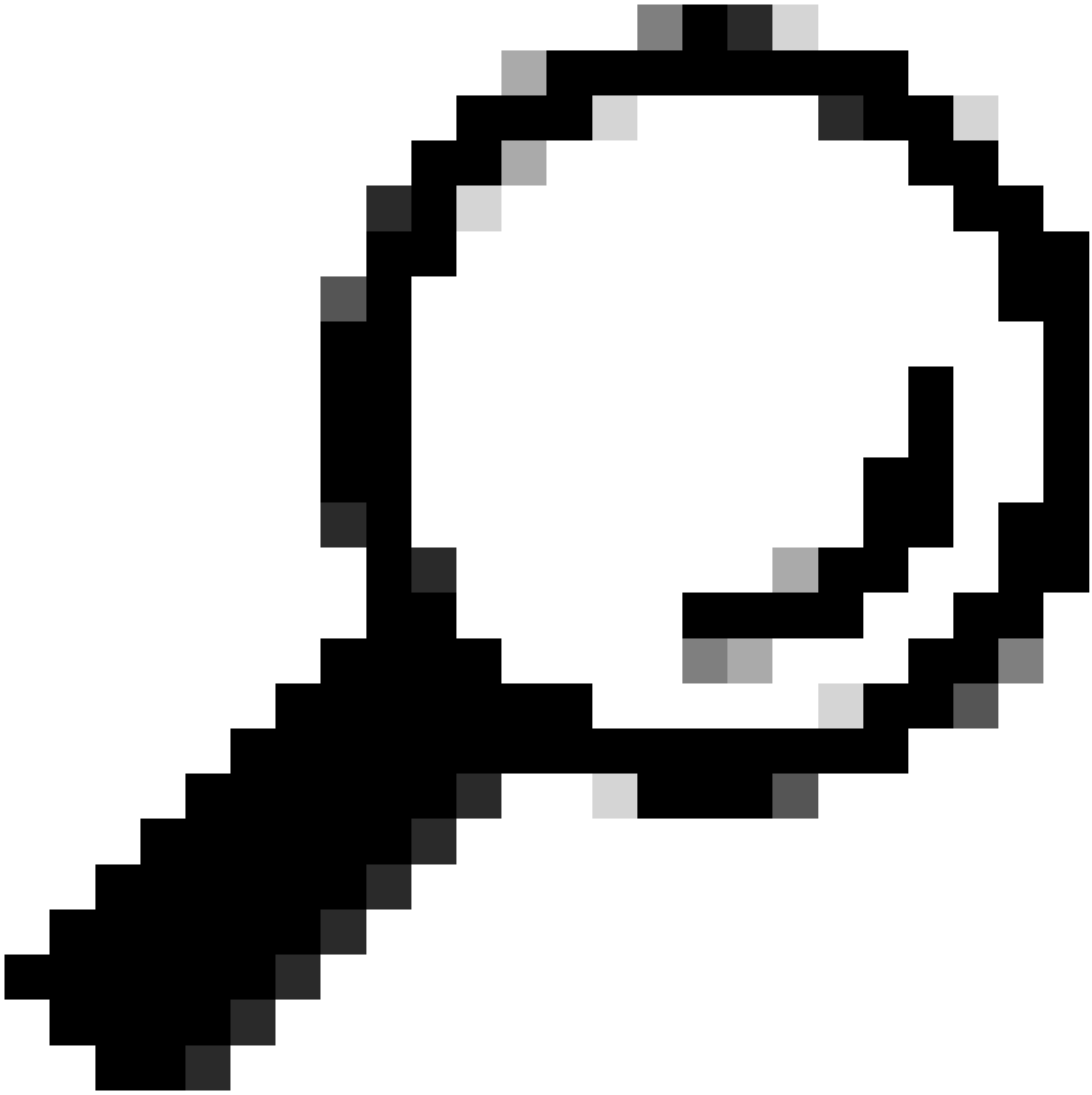
디바이스 삭제를 강제하는 API

Cisco DNA Center GUI를 사용하여 인벤토리에서 디바이스를 삭제할 수 없는 경우 API를 사용하여 ID별로 디바이스를 삭제할 수 있습니다.

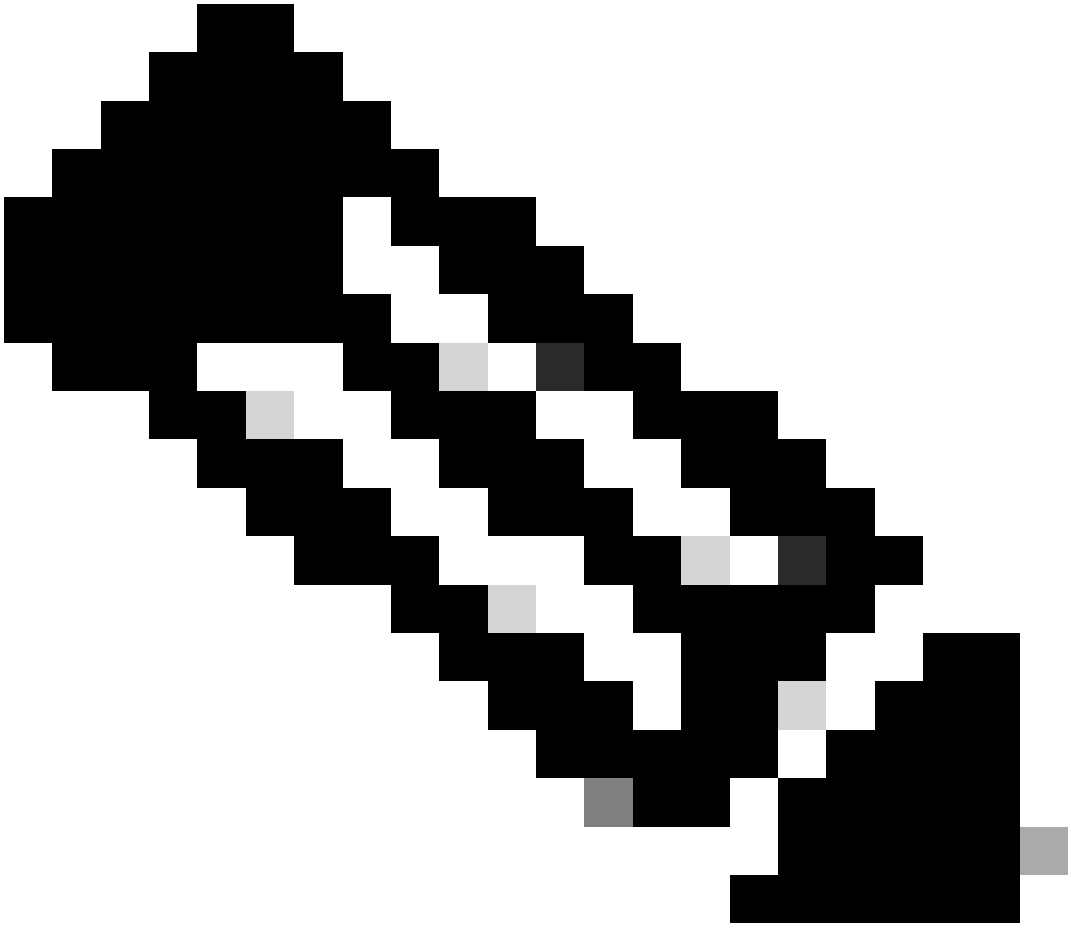
1.- Cisco DNA Center Menu(Cisco DNA 센터 메뉴) -> Platform(플랫폼) -> Developer Toolkit(개발자 툴킷) -> APIs(API) 탭으로 이동하여 검색 표시줄에서 Devices(디바이스)를 검색합니다. 검색 결과에서 Know your network(네트워크 정보) 섹션에서 Devices(디바이스)를 클릭하고 Delete by Device Id(디바이스 ID로 삭제)API를 검색합니다.

2.- DELETE by Device Id API(디바이스 ID별 삭제 API)를 클릭하고 Try(시도)를 클릭한 후 인벤토리에서 제거할 원하는 디바이스의 디바이스 ID를 제공합니다.

3.- API가 실행될 때까지 기다린 후 200 OK 응답을 받은 다음 네트워크 디바이스가 Inventory(인벤토리) 페이지에 더 이상 존재하지 않는지 확인합니다.



팁: Cisco DNA Center Inventory Device Details(Cisco DNA Center 인벤토리 디바이스 세부사항) 페이지 또는 Device View 360(디바이스 보기 360) 페이지의 브라우저 URL(deviceid 또는 id)에서 디바이스 uuid를 가져올 수 있습니다.



참고: Cisco DNA Center의 API에 대한 자세한 내용은 Cisco DevNet API 가이드를 참조하십시오

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.