

# DNA Centerインベントリサービスと一般的な問題の調査

## 内容

---

### [はじめに](#)

[使用するコンポーネント](#)

### [インベントリサービスの詳細](#)

[管理容易性の状態](#)

[前回の同期ステータス](#)

### [課題](#)

[Internal Error](#)

[Device Credentials](#)

[Netconf](#)

[ネットワークチェック](#)

[データベーステーブル](#)

[同期ループとトラップ](#)

[デバイスの同期を強制するAPI](#)

[トラップの確認](#)

[サービスのクラッシュ状態](#)

[デバイスを削除できない](#)

[デバイスを強制的に削除するAPI](#)

---

## はじめに

このドキュメントでは、Cisco DNA Center Inventory Serviceの基本概念と、実稼働環境で見られる一般的な問題について説明します。

### 使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### インベントリサービスの詳細

Cisco DNA Center Inventory Serviceは、Kubernetes(K8s)Podに基づいています。このポッドは、展開環境タイプとして「apic-em-inventory-manager-service-`<id>`」という名前の名前空間「fusion」で実行されていることがわかります。

K8sポッドの内部には、「apic-em-inventory-manager-service」というDockerコンテナがあります。

「apic-em-inventory-manager-service」ポッドの主なタスクは、デバイス検出およびデバイスライフサイクル管理です。

これにより、デバイスデータがPostgres SQL ( Fusion Servicesで使用されるデータベース ) で使用できるようになります。

「fusion」ネームスペース(Appstack)は、ネットワークコントローラプラットフォーム(NCP)とも呼ばれ、すべてのネットワーク自動化要件に対応するサービスプロビジョニングフレームワーク(SPF)サービスを提供します。

これには、検出、インベントリ、トポロジ、ポリシー、ソフトウェアイメージ管理(SWIM)、設定アーカイブ、ネットワークプログラマ、サイト、グループ化、テレメトリ、テスト統合、テンプレートプログラマ、マップ、IPAM、センサー、オーケストレーション/ワークフロー/スケジューリング、ISE統合などが含まれます。

インベントリポッドのステータスは、次のコマンドを実行して確認できます。

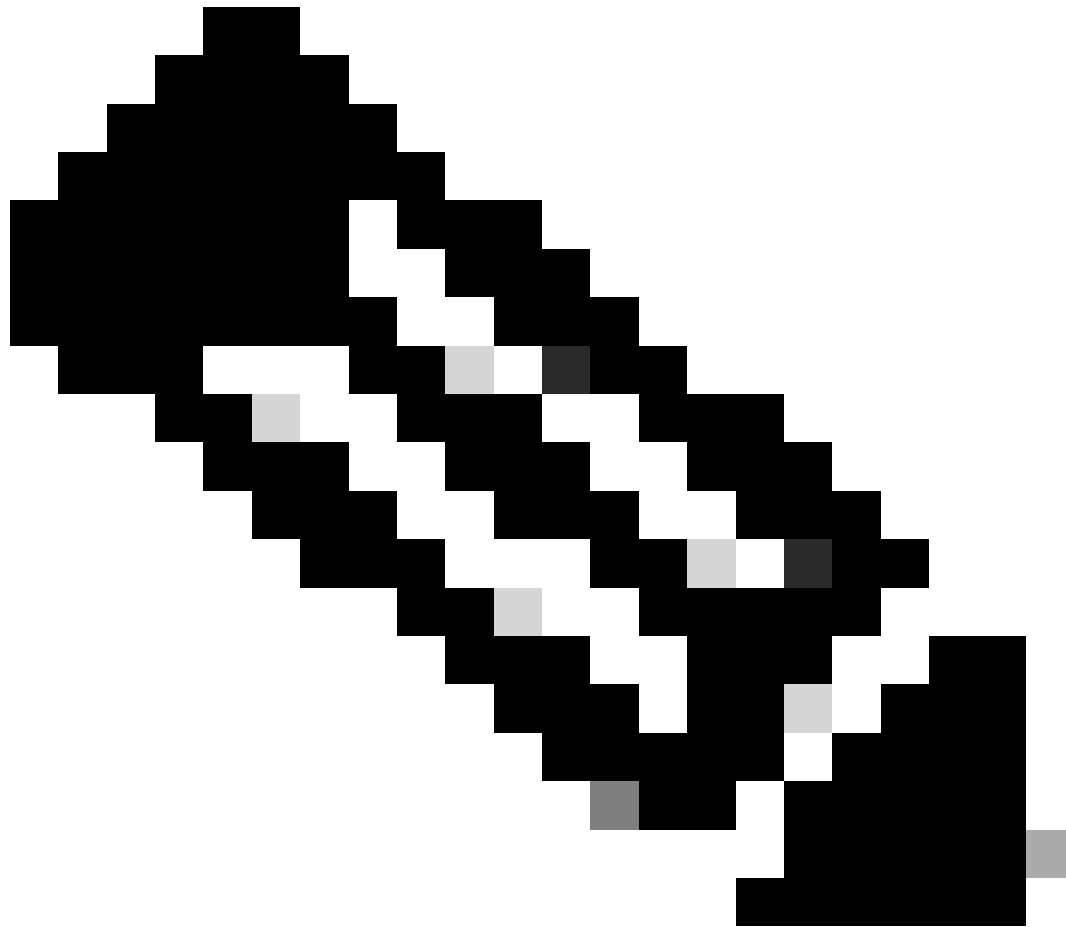
```
$ magctl appstack status | grep inventory
```

インベントリサービスのステータスは、次のコマンドで確認できます。

```
$ magctl service status
```

インベントリサービスログは、次のコマンドを使用して確認できます。

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



注：インベントリサービスは2つの連続するポッドで構成されることがあるため、ポッドIDを含む完全なインベントリポッド名を使用して、コマンドで1つのポッドを指定する必要があります。

---

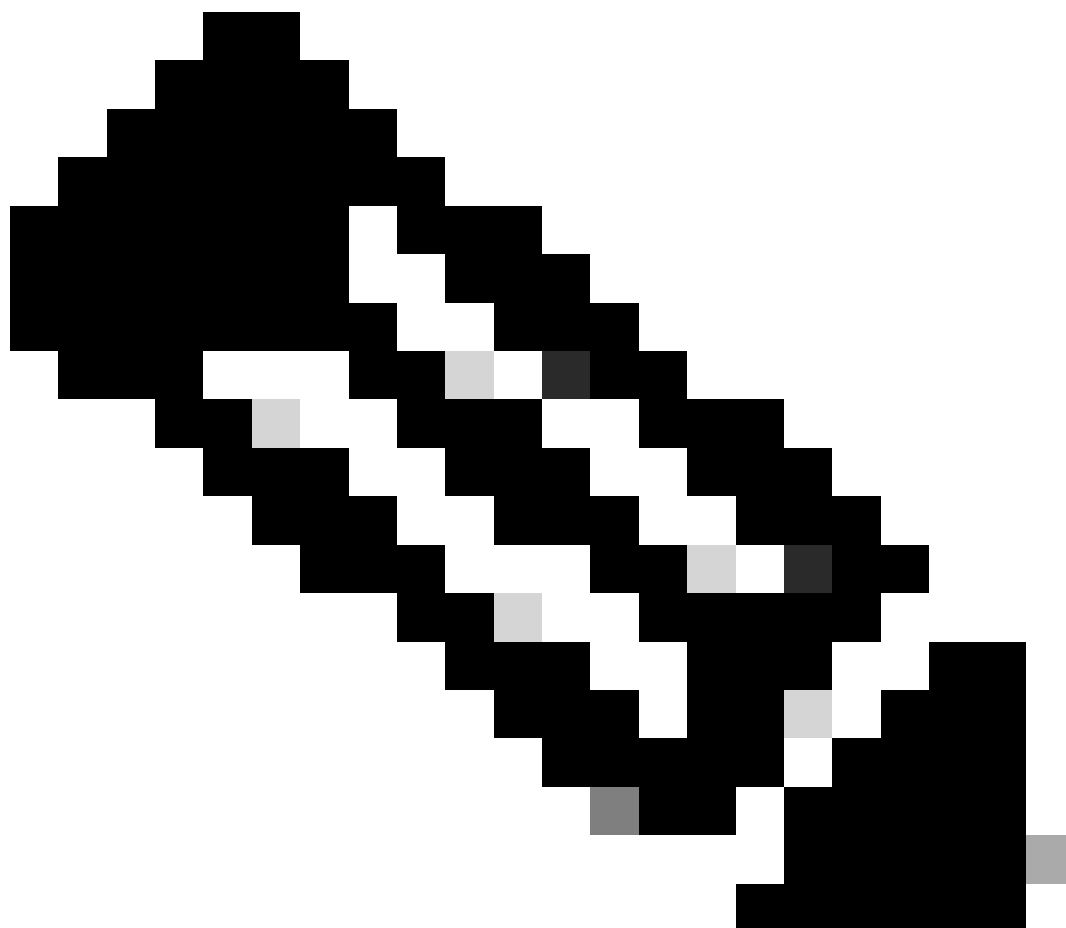
このドキュメントでは、「Inventory device Manageability」と「Last Syncing」のステータスに焦点を当てて、一般的な問題を確認できます。

#### 管理容易性の状態

- 緑のチェックアイコンで管理:デバイスは到達可能で、完全に管理されています。
- オレンジ色のエラーアイコンで管理:デバイスは、到達不能、認証障害、Netconfポートの欠落、内部エラーなどのエラーで管理されています。エラーメッセージにカーソルを合わせると、エラーと影響を受けるアプリケーションの詳細が表示されます。
- Unmanaged:デバイスに到達できず、デバイスの接続の問題によりインベントリ情報が収集されませんでした。

## 前回の同期ステータス

- Managed: デバイスは完全に管理対象の状態です。
  - 部分的な収集の失敗: デバイスが部分的に収集された状態にあり、一部のインベントリ情報が収集されていない。情報(i)アイコンの上にカーソルを移動すると、障害に関する追加情報が表示されます。
  - 到達不能: デバイスに到達できず、デバイスの接続の問題によってインベントリ情報が収集されませんでした。この状態は、定期的な収集が行われる場合に発生します。
  - 誤ったクレデンシャル: デバイスをインベントリに追加した後にデバイスのクレデンシャルを変更すると、この状態が記録されます。
  - 進行中: 在庫の収集が行われています。
- 



注: Cisco DNA Centerのインベントリ機能の詳細については、バージョン2.3.5.xの公式ガイド「[インベントリの管理](#)」を参照してください。

---

# 課題

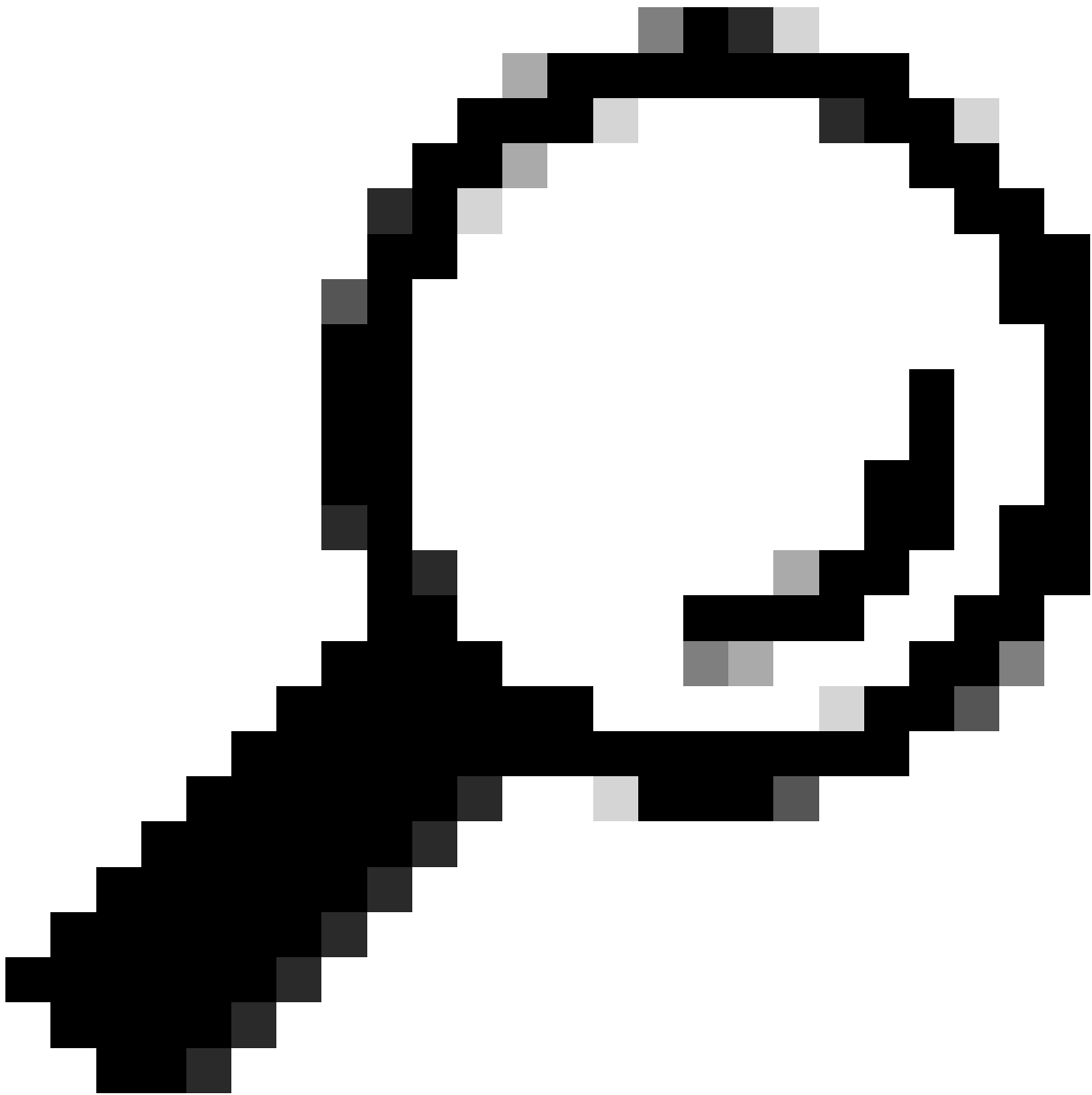
## Internal Error

Cisco DNA Centerインベントリページでは、データ収集を妨げる何らかの矛盾があるデバイスのマネージャビリティのステータスに警告メッセージを表示できます。

「内部エラー： NCIM12024：デバイスからのすべての情報を正常に収集できなかったか、またはこのデバイスのインベントリ収集がまだ開始されていません。これは、自動的に解決できる一時的な問題である可能性があります。デバイスを再同期しても問題が解決しない場合は、Cisco TACにお問い合わせください」

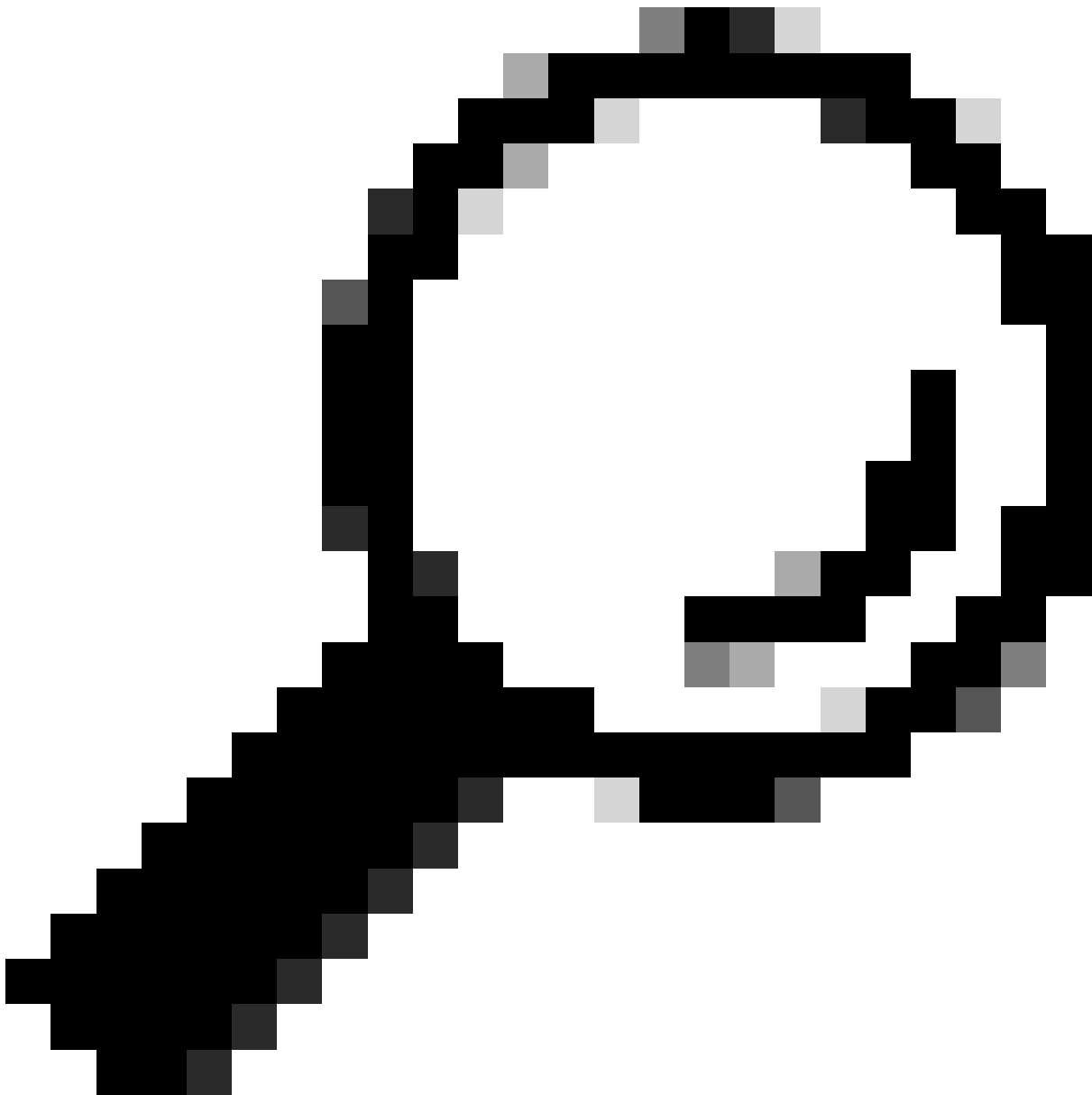
エラーが自動的に解決されない場合、またはデバイスの再同期後に解決されない場合は、最初のトラブルシューティングから始めることができます。このエラーは複数の原因で発生する可能性があります、ここでは最も一般的な原因の一部のみを示します。

- SNMP、SSH、およびNetconfのデバイスクレデンシャルが正しくない。
- SNMP、SSH、Netconfに関連するネットワーク接続の問題
- デバイスのNetconf設定の問題が原因で、Netconfが正しく動作しません。
- デバイスの同期中にデバイスの再同期をトリガーします。
- デバイスから複数のトラップが受信され、短時間のうちに複数の再同期トリガーが発生しました。
- デバイスに関連する複数のテーブルのインベントリデータベースエントリに関するバックエンドの問題。



ヒント：ネットワークデバイスを取りはずし、正しいCLI、SNMP、およびNETCONFクレデンシャルを使用してそれを再検出すると、内部エラーの原因である可能性がある古いデータベースエントリを削除するのに役立ちます。

---



ヒント：インベントリサービスのログを確認し、デバイスIPまたはホスト名でフィルタリングすると、内部エラーの根本原因を特定するのに役立ちます。

---

## Device Credentials

デバイスのクレデンシャルを確認するには、Cisco DNA Centerのメニュー> Provision -> Inventory -> Select Device -> Actions -> Inventory -> Edit Deviceの順に選択し、Validateをクリックして、必須クレデンシャル（CLIとSNMP）が緑色のチェック（適用される場合はnetconfを含む）で検証に合格したことを確認します。

検証が失敗した場合は、Cisco DNA Centerがネットワークデバイスの管理に使用しているユーザー名とパスワードが、デバイスのコマンドラインで直接有効であることを確認してください。

ローカルで設定されている場合、またはAAAサーバ（TACACSまたはRADIUS）で設定されてい

る場合は、ユーザ名とパスワードがAAAサーバで正しく設定されていることを確認してください。

また、Cisco DNA CのDevice Credentials Settingsで「Enable」パスワード設定を必要とするユーザ名権限があるかどうかを確認しinventoryと入力します。

CLIKレデンシャルのエラーにより、Inventory: CLI Authentication Failureでマネージャビリティ (管理容易性) のエラーメッセージが表示される場合があります。

## Netconf

Netconfは、リモートプロシージャコール(RPC)を介して互換性のあるネットワークデバイスをリモートで管理するためのプロトコルです。

Cisco DNA CenterはNetconf機能を使用してネットワークデバイスの設定をプッシュまたは削除し、Assuranceによるモニタリングなどの機能を有効にします。

Cisco DNA Centerインベントリでは、Netconf要件が正しいことの検証もできます。これには、次のものが含まれます。

- Netconfのデフォルトポート830は、ネットワーク内で開かれ、機能します。
- ネットワークデバイス (ローカルまたはAAAで設定) へのSSHアクセスを持つ、特権15のユーザ。
- ネットワークデバイスでNetconfを有効にします。

```
<#root>
```

```
(config)#
```

```
netconf-yang
```

- aaa new-modelがイネーブルになっている場合は、AAAのデフォルト設定要件：

```
<#root>
```

```
(config)#
```

```
aaa authorization exec default
```

```
(config)#
```

```
aaa authentication login default
```



Netconfクレデンシャルのエラーにより、インベントリに「Netconf Connection Failure」というマネージャビリティのエラーメッセージが表示される場合があります。

## ネットワークチェック

バージョンに応じて、ネットワーク接続とプロトコル設定(SNMP設定など)を検証することもできます。

たとえば、コミュニティ、ユーザ、グループ、エンジンID、認証および暗号化の設定などを、SNMPのバージョンに応じてダブルチェックできます。

また、デバイスのコマンドラインでpingコマンドとtracerouteコマンドを使用し、ファイアウォール、プロキシ、またはアクセスリストでSSH(22)とSNMP ( 161と162 ) のポートを使用して、SSHとSNMPの接続を確認することもできます。

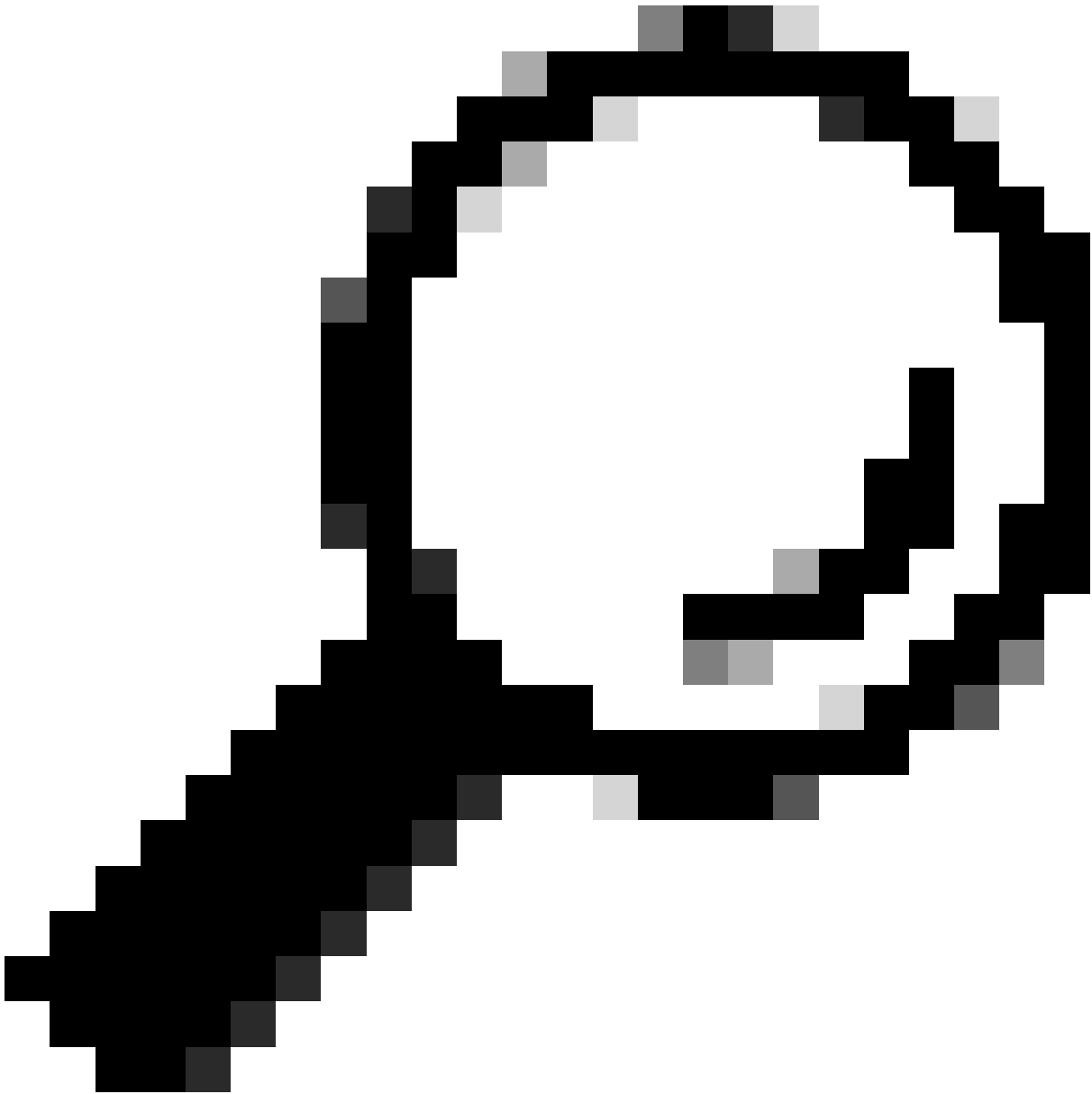
Cisco DNA Centerのmaglev CLIから、ip routeコマンドを使用して、ネットワークデバイスへの接続を確認します。

SNMP walkはトラブルシューティングにも使用できます。

SNMPクレデンシャルのエラーにより、インベントリに「SNMP Authentication Failure」または「Device Unreachable」というマネージャビリティのエラーメッセージが表示される場合があります。

## データベーステーブル

エンドユーザは、Cisco DNA Center GUIとGrafanaを使用してSQLクエリを実行できるため、maglev CLI経由でPostgresシエルにアクセスする必要はありません。



ヒント:Grafanaの使用方法については、公式ガイド「[Cisco DNA Center GUIでPostgresクエリを実行する](#)」を参照してください。

---

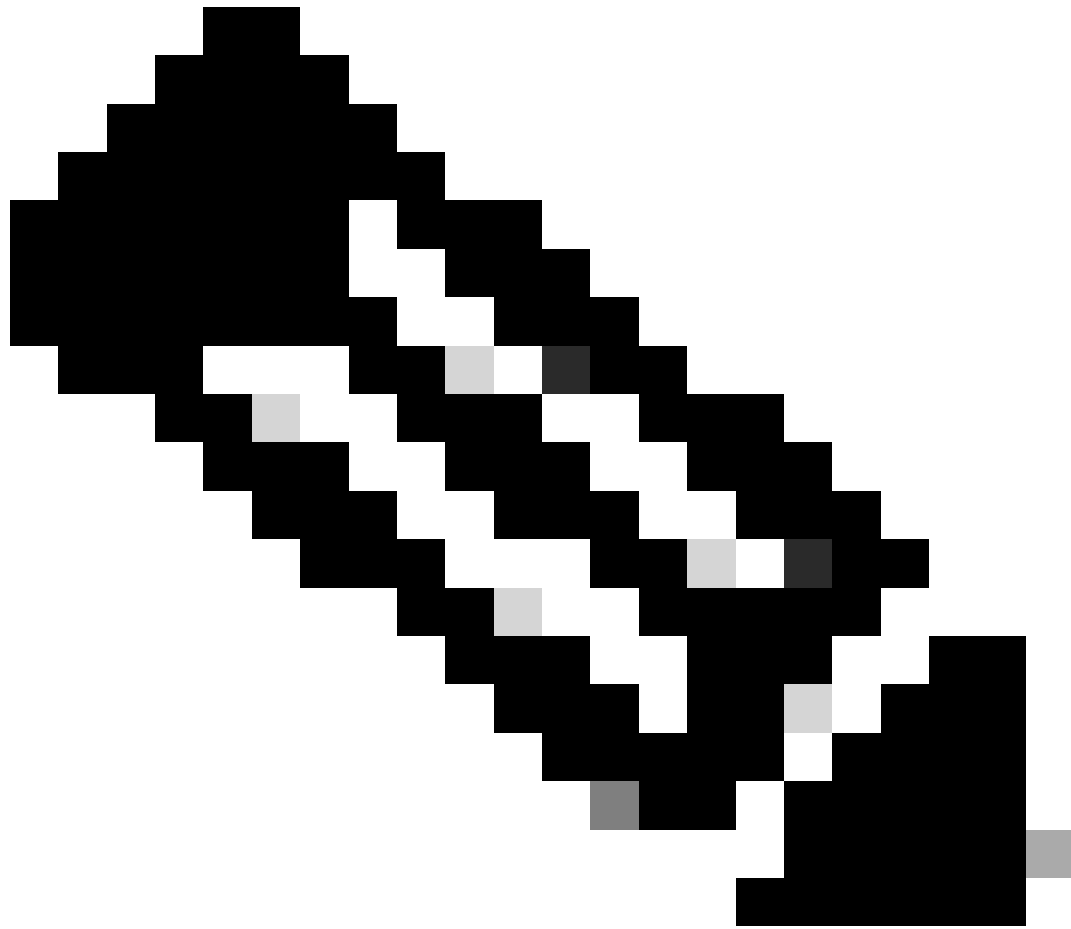
インベントリ内のネットワークデバイスに問題がある場合に確認するpostgresデータベーステーブルには、次のものがあります。

- ネットワークデバイス
- managedelementinterface
- ネットワーク要素
- ネットワークリソース
- デバイスif
- IPアドレス



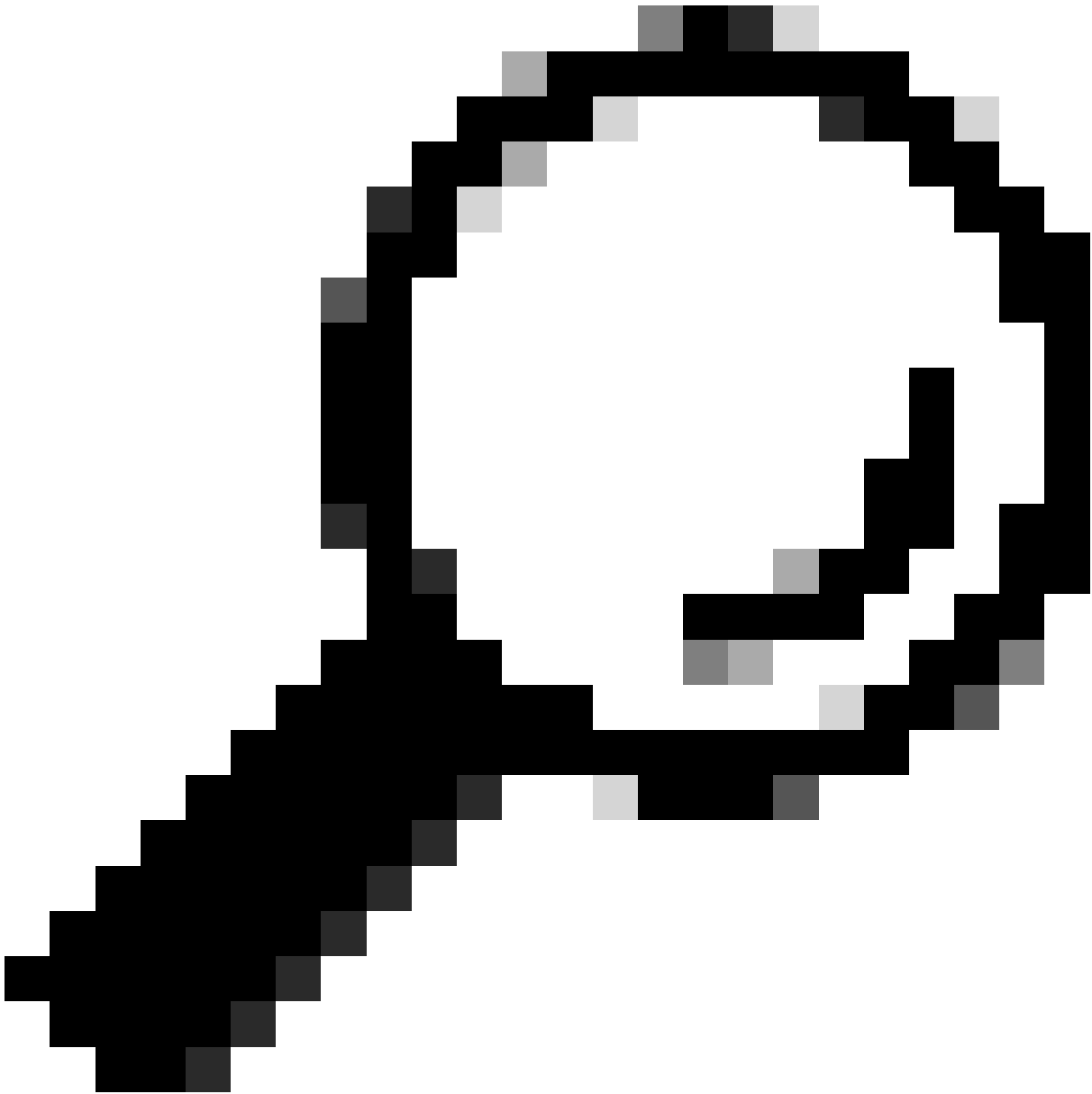
警告:Postgresシェルでのshowクエリの実行が許可されているのはCisco TACだけで、DBテーブルの変更が許可されているのはBU/DEチームだけです。

---



注：データベースの問題が原因でデバイスの内部エラーメッセージが表示され、データ収集とデバイスのプロビジョニングができなくなる可能性もあります。

---



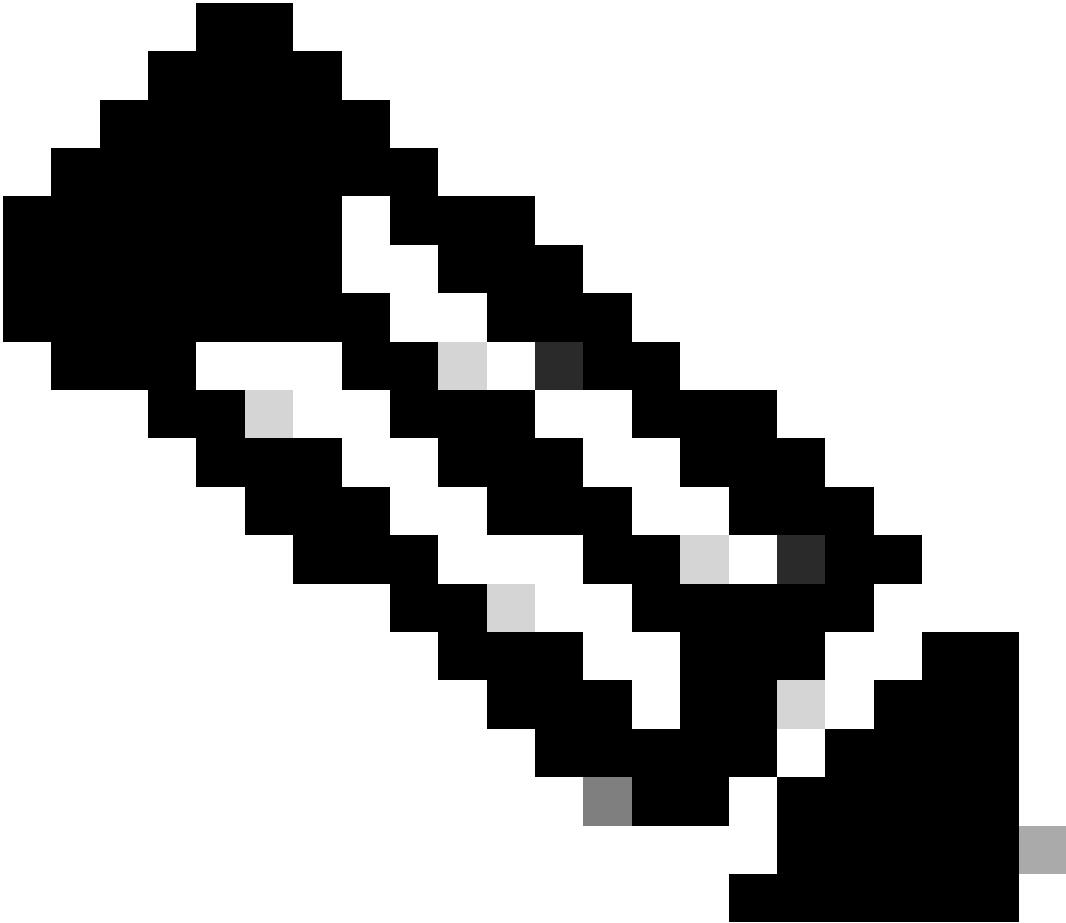
ヒント: Cisco DNA Center System 360ページのKibanaを使用してPostgresのログを確認し、インベントリサービスがPostgresデータベーステーブルのエントリを保存または更新しようとしたときに発生する制約違反を探することができます。

---

## 同期ループとトラップ

Cisco DNA Centerは、デバイス自体に大きな変更が加えられた後、デバイスからトラップを受信するたびにデバイスResyncを実行して、Cisco DNA Centerインベントリの更新を維持するように設計されています。Cisco DNA Center InventoryページのManageabilityセクションで、ネットワークデバイスが長時間またはいつまでも「Syncing」状態のままになる場合があります。

---



注：大規模なトラップによるこのような同期ループは、検出された変更が原因でトラップを送信しているデバイスに対して、Cisco DNA Centerが短時間に複数回の認証を実行する原因となる可能性があります。

---

## デバイスの同期を強制するAPI

ネットワークデバイスが長すぎる、または数日にわたって同期ステータスのままになっている場合は、最初に基本的なチェックを行って到達可能性と接続を確認します。次に、APIコールを介してデバイスを強制的に再同期します。

- 1.- Cisco DNA Center maglev CLIセッションを開きます。
- 2.- APIを介してCisco DNA Center認証トークンを取得します。

<#root>

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

3. – 前の手順のトークンを使用してAPIを実行し、デバイスを強制的に同期させます。

<#root>

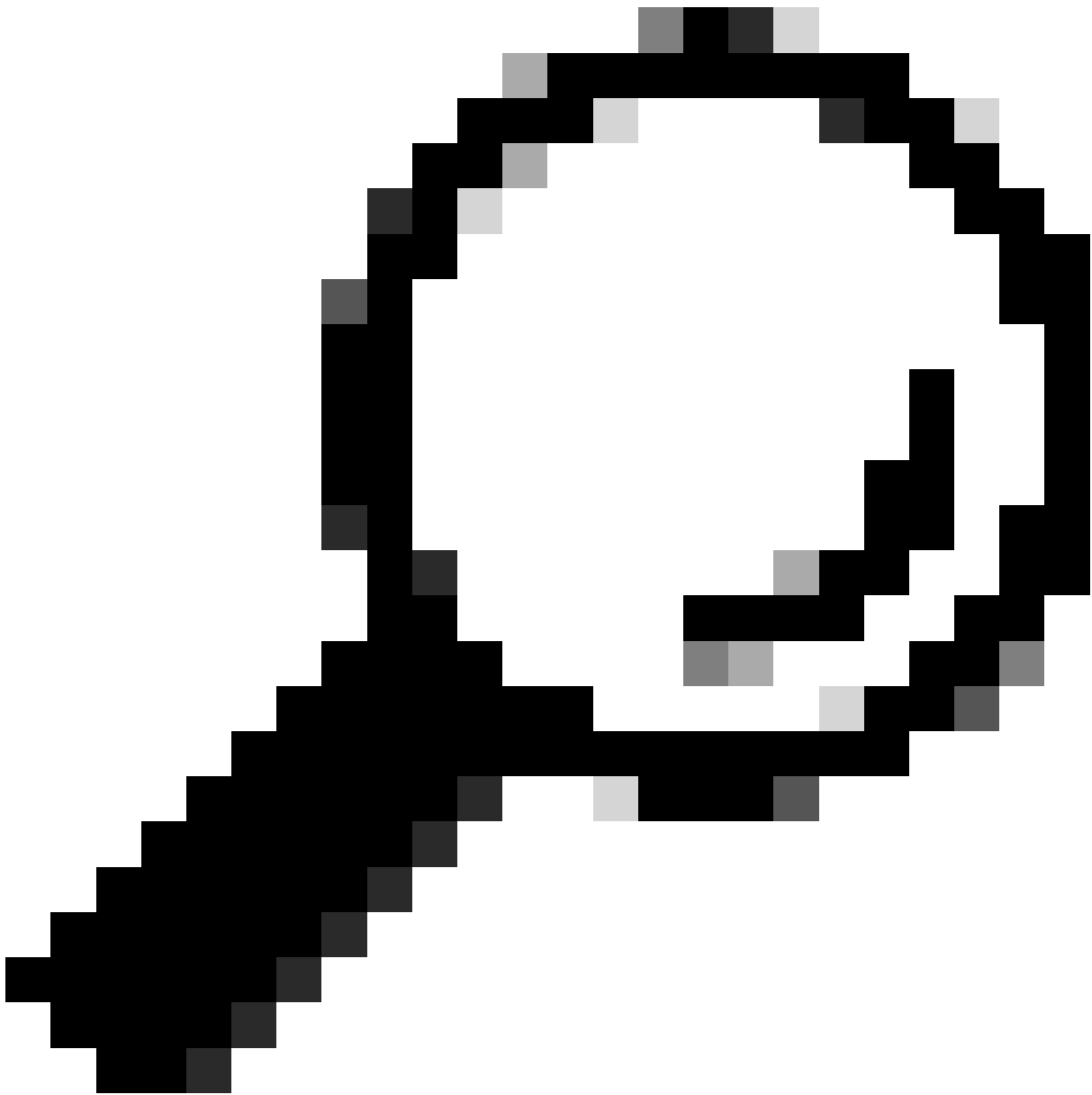
```
curl -X PUT -H "X-AUTH-TOKEN:
```

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

```
' https://
```

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

4.- API経由でForce Syncオプションを使用すると、デバイスの同期が再び行われます。



ヒント : デバイスのuuidは、ブラウザURL ( deviceidまたはid ) でCisco DNA Centerインベントリのデバイス詳細ページまたはDevice View 360ページから取得できます。

---



---

注: Cisco DNA CenterのAPIの詳細については、『[Cisco DevNet API Guide](#)』

---

## トラップの確認

デバイスで強制的に同期タスクを実行した後も問題が解決しない場合は、Cisco DNA Centerの「event-service」で受信されるトラップの数が多すぎるかどうかを確認し、イベントサービスログを読み取って、どのタイプのトラップであるかを確認できます。

1. – ログを読み取る前に、次のコマンドを使用してトラップの総数を確認します。

```
<#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: '/ipAddress
```

2. – 次に、イベントサービスコンテナにアタッチします。

```
<#root>
```

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

3. – イベントサービスコンテナ内に入ったら、ディレクトリをlogsフォルダに変更します。

```
<#root>
```

```
$ cd /opt/CSColumos/logs/
```

4. – ディレクトリ内のファイルを確認すると、名前が「ncs」で始まるログファイルがいくつか見えます。

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. – これらの「ncs」ファイルは、受信しているトラップのタイプと数を分析するために必要なものです。ログファイルを確認して、デバイスのホスト名またはキーワード「trapType」でフィルタリングします。

```
<#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

トラップのタイプが多すぎると、デバイスの再同期を引き起こす可能性があり、頻繁に送信される場合には同期ループが発生する可能性があります。

トラップを分析することで、根本原因を特定し、再起動サイクルのAPなど、トラップを停止させることができます。

トラップの出力をファイルに保存し、必要に応じてエスカレーションチームと共有できます。

## サービスのクラッシュ状態

ネットワークデバイスの管理中にCisco DNA Center Inventoryページで異常な動作が原因でインベントリポッドがクラッシュしたと思われる場合は、最初にポッドステータスを検証できます。

<#root>

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

```
$ magctl service status
```

ポッドステータスの出力を確認して、再起動またはエラーステータスの数が多い場合は、インベントリコンテナを添付してヒープダンプファイルを収集できます。このファイルには、エスカレーションチームがクラッシュ状態の根本原因を分析および定義するために役立つデータを含めることができます。

<#root>

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

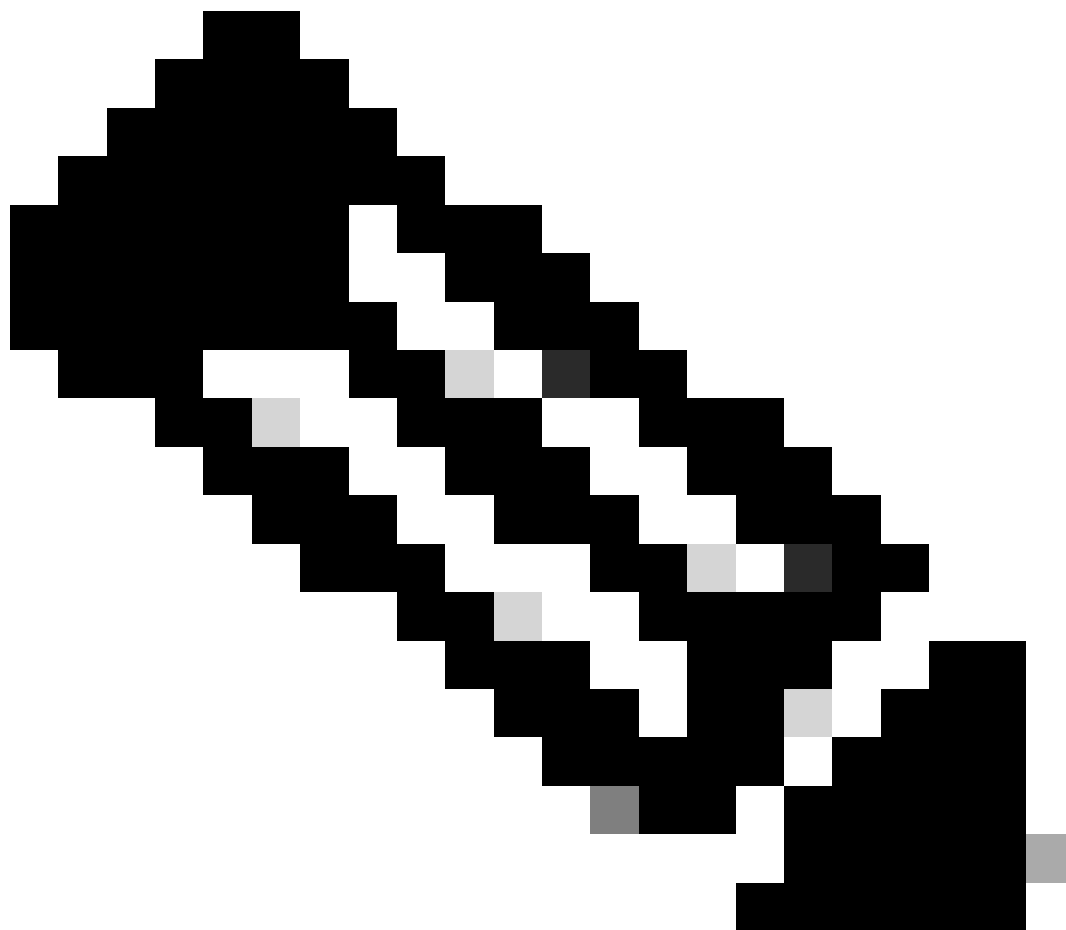
```
root@apic-em-inventory-manager-service-76f7f8d7f5-427m5:/#
```

```
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
```

---



注：コンテナディレクトリ内にヒープダンプファイルが見つからなかった場合、コンテナ内にクラッシュ状態は存在しませんでした。

---

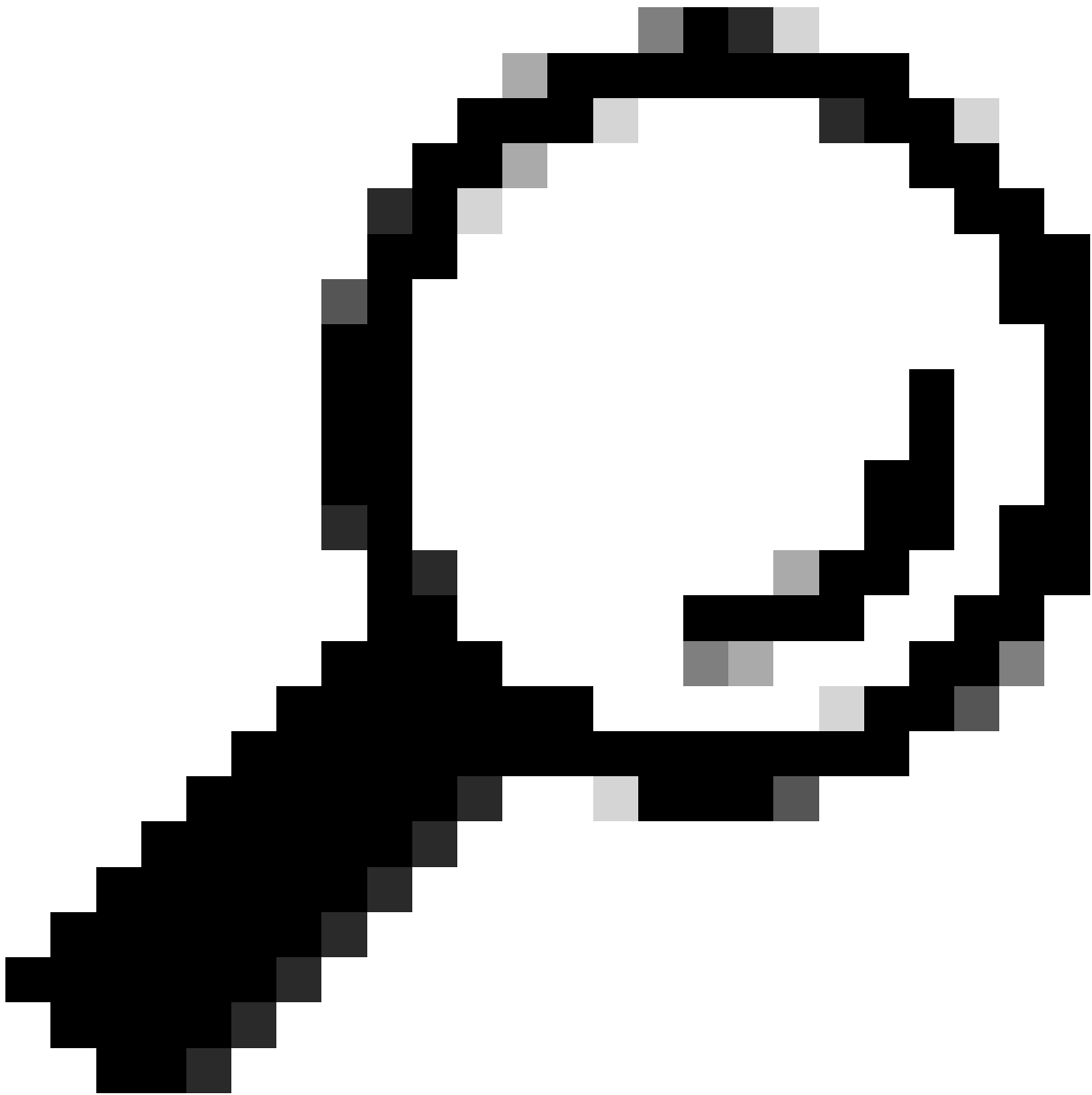
デバイスを削除できない

バックエンドの問題が原因で、Cisco DNA Centerがインベントリユーザインターフェイスからネットワークデバイスを削除できない場合があります。

#### デバイスを強制的に削除するAPI

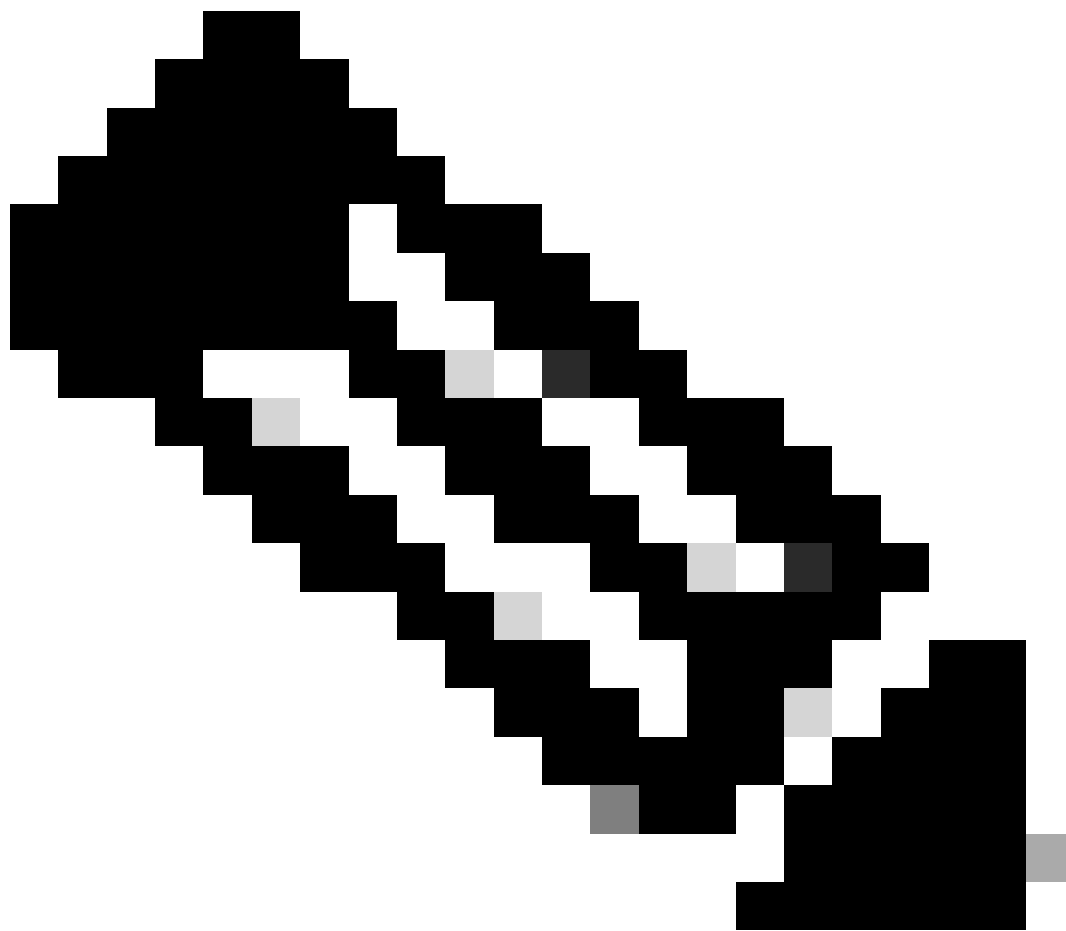
Cisco DNA Center GUIを使用してインベントリからデバイスを削除できない場合は、APIを使用してデバイスをIDで削除できます。

- 1.- Cisco DNA Centerメニュー -> Platform -> Developer Toolkit -> APIsタブに移動し、検索バーでDevicesを検索します。結果から、Know your networkセクションのDevicesをクリックして、DELETE by Device Id APIを検索します。
- 2.- DELETE by Device Id APIをクリックし、Tryをクリックして、インベントリから削除するデバイスのデバイスIDを指定します。
- 3.- APIの実行を待機し、200 OK応答を取得します。その後、ネットワークデバイスがインベントリページに表示されなくなったことを確認します。



ヒント : デバイスのuuidは、ブラウザURL ( deviceidまたはid ) でCisco DNA Centerインベントリのデバイス詳細ページまたはDevice View 360ページから取得できます。

---



注: Cisco DNA CenterのAPIの詳細については、[『Cisco DevNet API Guide』](#)

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。