

检查DNA Center Inventory Service和常见问题

目录

[简介](#)

[使用的组件](#)

[库存服务详细信息](#)

[可管理性状态](#)

[上次同步状态](#)

[问题](#)

[Internal Error](#)

[设备凭证](#)

[Netconf](#)

[网络检查](#)

[数据库表](#)

[同步环路和陷阱](#)

[用于强制设备同步的API](#)

[检查陷阱](#)

[服务崩溃状态](#)

[无法删除设备](#)

[强制设备删除的API](#)

简介

本文档介绍Cisco DNA Center Inventory服务的基本概念和生产中发现的常见问题。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

库存服务详细信息

Cisco DNA Center Inventory服务基于Kubernetes(K8s)Pod，您可以在名为“apic-em-inventory-manager-service-`<id>`”的名称空间“fusion”中发现该服务在部署环境类型中运行。

在K8s pod中，您可以找到一个Docker容器，称为“apic-em-inventory-manager-service”。

“apic-em-inventory-manager-service”Pod的主要任务包括：设备发现和设备生命周期管理。

这可确保设备数据在Postgres SQL（fusion services使用的数据库）中可用。

“fusion”命名空间(Appstack)也称为网络控制器平台(NCP)，为所有网络自动化需求提供服务调配框架(SPF)服务。

这些功能包括发现、库存、拓扑、策略、软件映像管理(SWIM)、配置存档、网络程序员、站点、分组、遥测、Tesseract集成、模板程序员、地图、IPAM、传感器、协调/ workflows/调度、ISE集成以及类似功能。

通过运行以下命令，可以检查inventory pod状态：

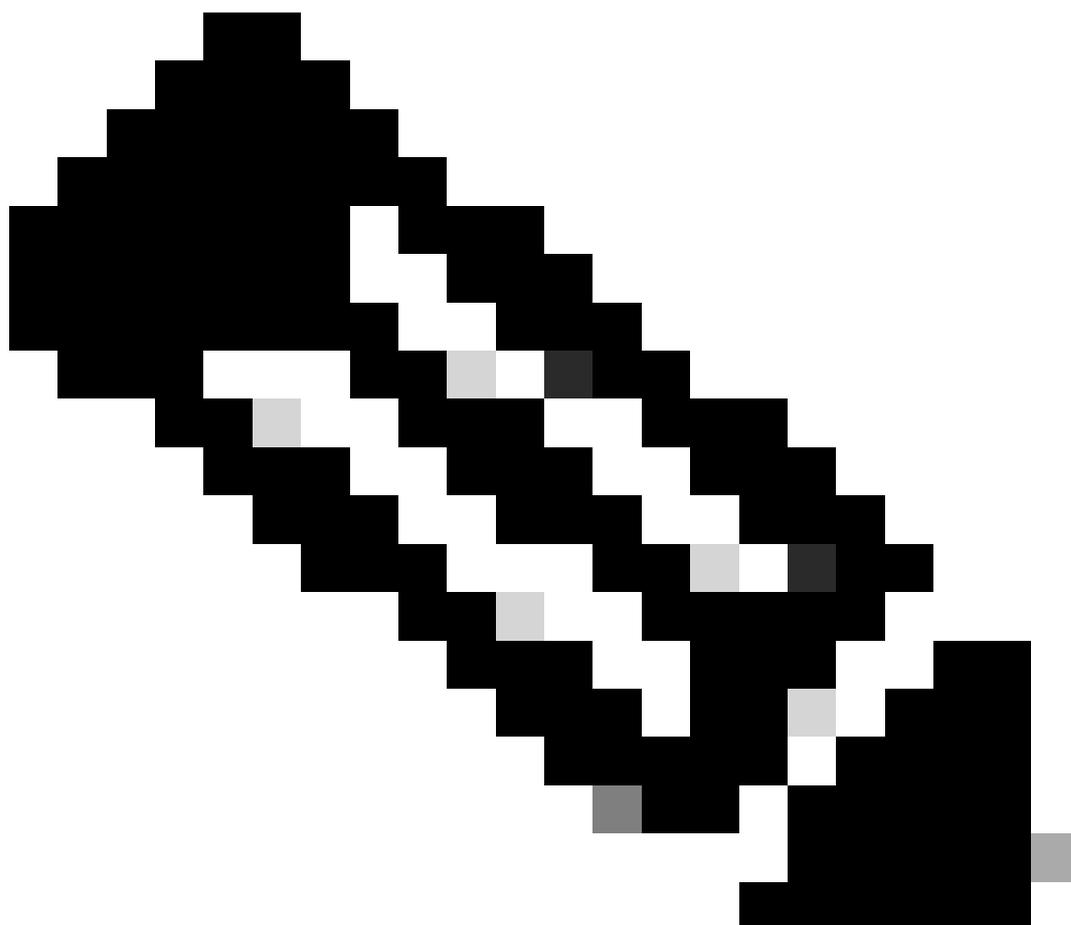
```
$ magctl appstack status | grep inventory
```

可以使用以下命令检查资产服务状态：

```
$ magctl service status
```

可以使用以下命令检查资产服务日志：

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



注意：资产服务也可以由两个运行的pod组成，因此，您需要使用完整的资产pod名称（包

括pod id) 在命令中指定单个pod。

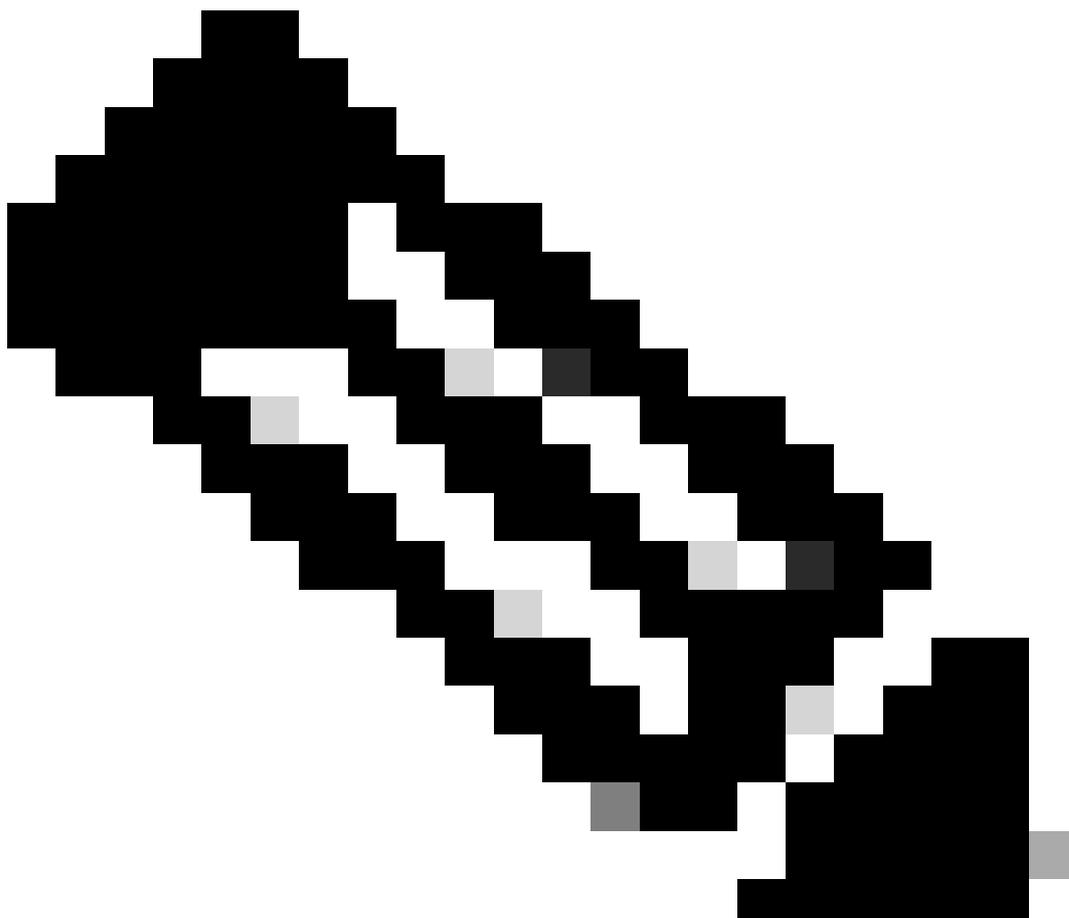
在本文档中，我们可以重点查看资产设备可管理性和上次同步状态，以查看常见问题：

可管理性状态

- 使用绿色勾选图标管理:设备可访问且完全受管理。
- 管理为橙色错误图标:设备管理存在一些错误，例如无法访问、身份验证失败、缺少Netconf端口、内部错误等。您可以将光标悬停在错误消息上，以查看有关错误和受影响应用的详细信息。
- 非托管:由于设备连接问题，无法访问设备，并且未收集任何资产信息。

上次同步状态

- 托管:设备处于完全受管状态。
- 部分收集失败:设备处于部分收集状态，并且尚未收集所有资产信息。将光标悬停在信息(i)图标上，以显示有关故障的其他信息。
- 不可到达：由于设备连接问题，无法访问设备，并且未收集任何资产信息。发生定期收集时会发生此情况。
- 错误的凭证：如果在将设备添加到资产后更改设备凭证，将记录此情况。
- 正在进行中:正在收集资产。



注意：有关Cisco DNA Center中资产功能的详细信息，请参阅2.3.5.x版本的官方指南：[管理资产](#)

问题

Internal Error

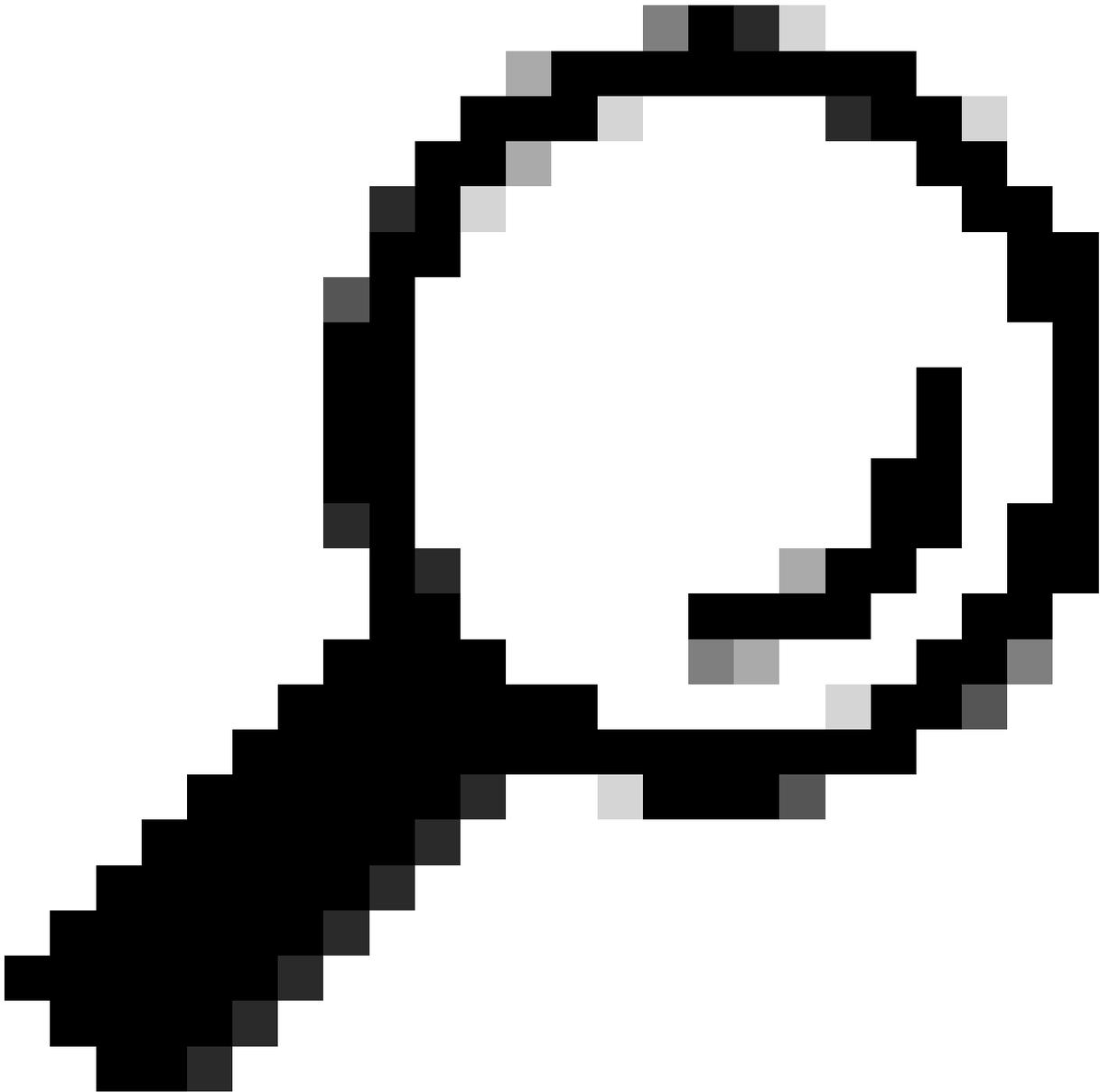
Cisco DNA Center Inventory (Cisco DNA Center库存) 页面可以在设备的可管理性状态中显示警告消息，这些设备存在某种冲突以防止数据收集：

"内部错误:NCIM12024:无法成功收集设备中的所有信息，或者此设备的资产收集尚未启动。它可能是一个临时问题，可以自动解决。重新同步设备，如果无法解决问题，请联系思科TAC。"

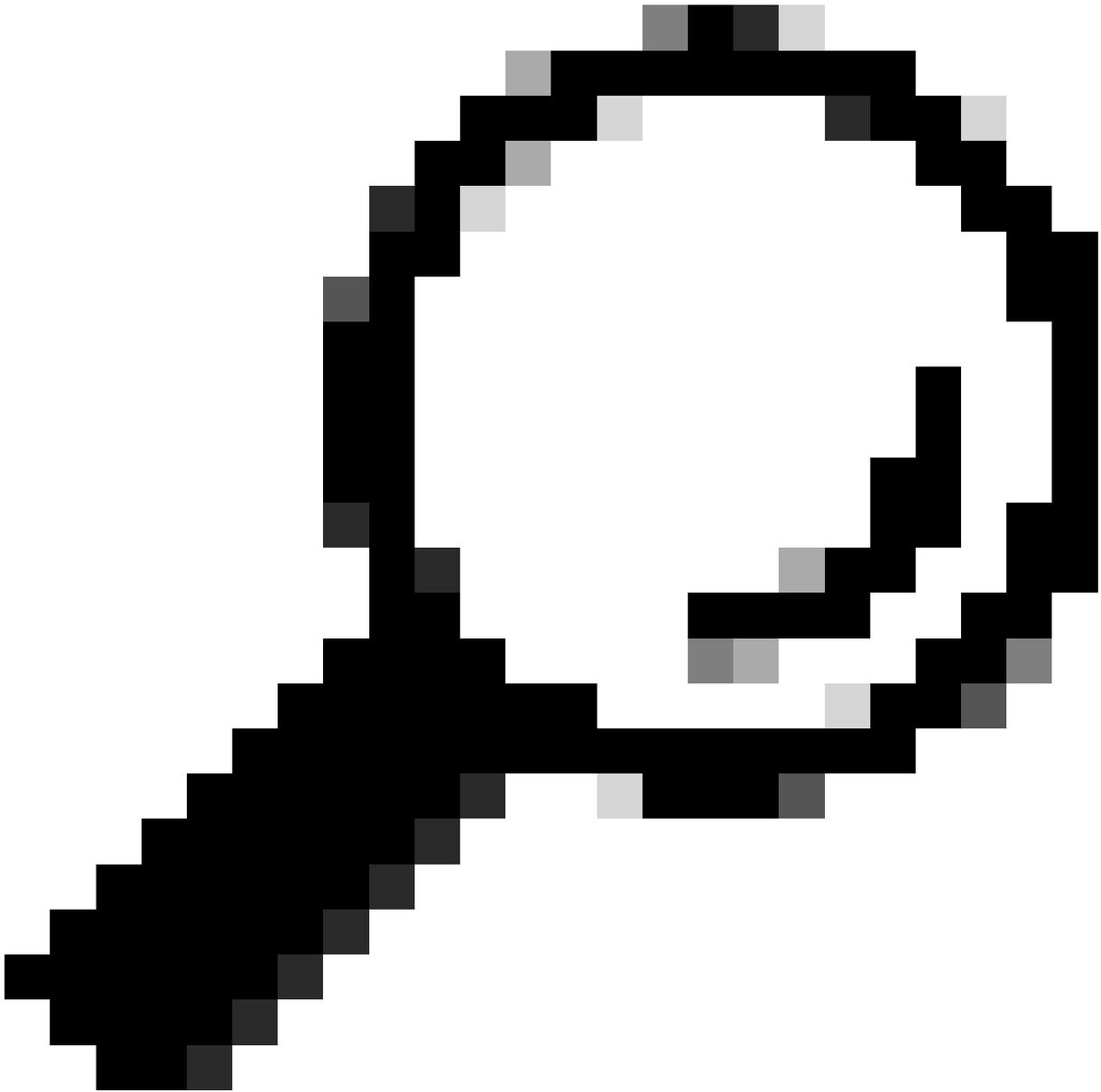
如果错误不能自动解决或在设备重新同步后解决，我们可以从初始故障排除开始。该错误可能是由于多种原因，但此处我们仅列出一些最常见的原因：

- SNMP、SSH和Netconf的设备凭证不正确。

- 与SNMP、SSH和Netconf相关的网络连接问题。
 - 设备中的Netconf配置问题导致Netconf无法正常工作。
 - 在设备同步正在进行时触发设备重新同步。
 - 收到来自设备的多个陷阱，导致在短时间内触发多个重新同步。
 - 与设备相关的多个表中的库存数据库条目存在后端问题。
-



提示：删除网络设备并使用正确的CLI、SNMP和NETCONF凭证重新发现它有助于删除可能导致内部错误的陈旧数据库条目。



提示：查看资产服务日志并按设备IP或主机名进行过滤有助于确定内部错误的根本原因。

设备凭证

要查看设备凭证，请导航到Cisco DNA Center Menu -> Provision -> Inventory -> Select Device -> Actions -> Inventory -> Edit Device，然后点击Validate，确认强制凭证（CLI和SNMP）通过绿色勾选验证（如果适用，包括netconf）。

如果验证失败，请查看Cisco DNA Center用于管理网络设备的用户名和密码是否直接在设备命令行中有效。

如果它们是在本地配置的，或者如果它们是在AAA服务器（TACACS或RADIUS）中配置的，请验证用户名和密码是否在AAA服务器中配置正确。

还要检查用户名权限是否要求在Cisco DNA C的“设备凭证设置”(Device Credentials Settings)中设置“启用”(Enable)密码输入Inventory。

CLI凭证中的错误可能会在资产中产生可管理性错误消息：CLI身份验证失败。

Netconf

Netconf是一种通过远程过程调用(RPC)远程管理兼容网络设备的协议。

Cisco DNA Center使用Netconf功能推送或删除网络设备上的配置，以启用通过保证进行监控等功能。

Cisco DNA Center Inventory还可以验证Netconf要求是否正确，其中包括：

- Netconf默认端口830在网络中处于打开和运行状态。
- 具有对网络设备的SSH访问权限（本地或配置AAA）的权限15的用户。
- 在网络设备上启用Netconf:

```
<#root>
```

```
(config)#
```

```
netconf-yang
```

- 如果启用aaa new-model，则还需要配置AAA默认设置要求：

```
<#root>
```

```
(config)#
```

```
aaa authorization exec default
```

```
(config)#
```

```
aaa authentication login default
```

Netconf凭证中的错误可能导致资产清单中出现可管理性错误消息：Netconf连接故障。

网络检查

我们还可以根据版本验证网络连接和协议设置(如SNMP设置)。

例如，我们可以根据SNMP版本仔细检查社区、用户、组、engineID、身份验证和加密设置等。

我们还可以在设备命令行中使用ping和traceroute命令查看SSH和SNMP连接，并在防火墙、代理或访问列表中使用SSH(22)和SNMP (161和162) 的端口。

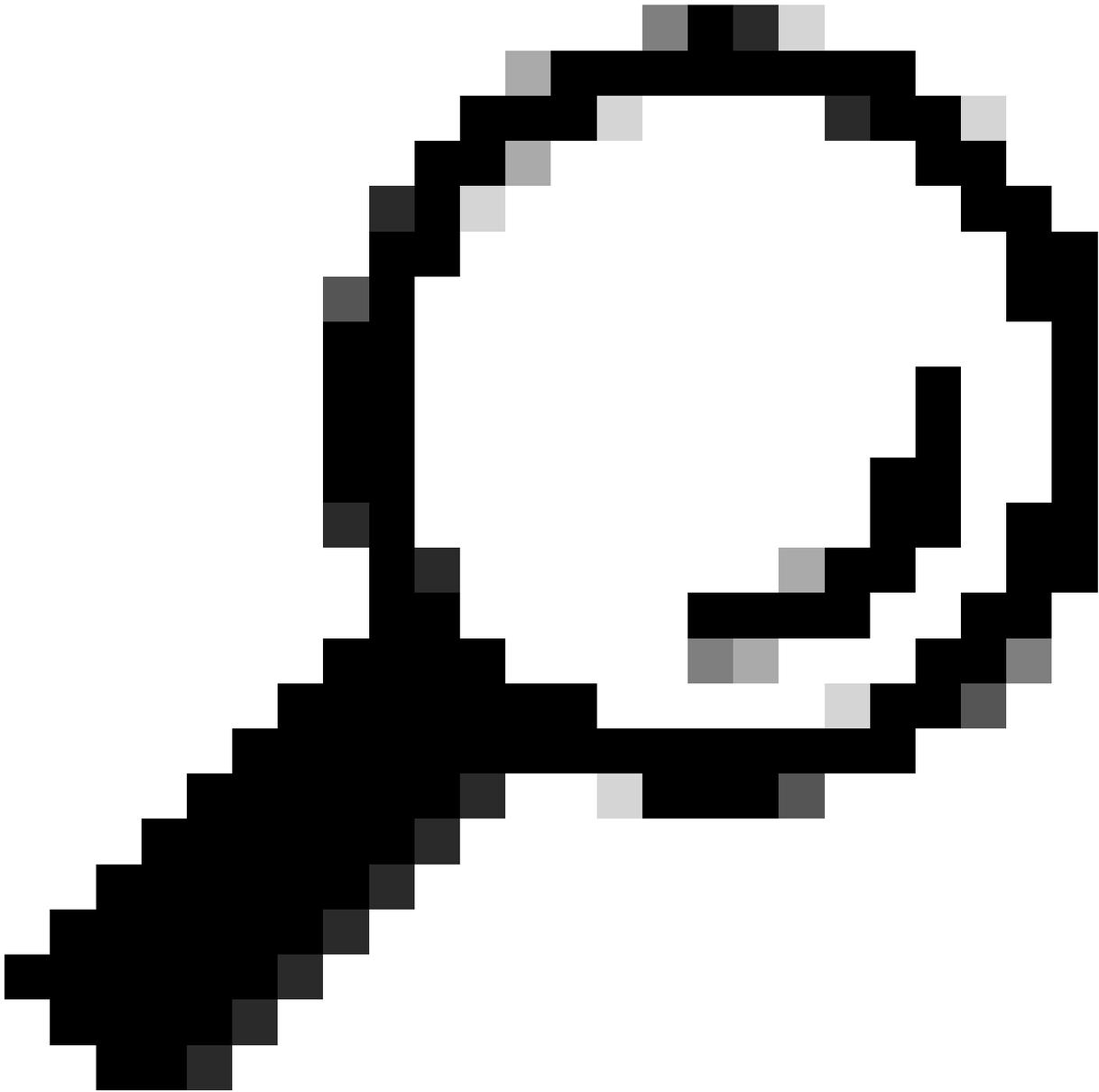
在Cisco DNA Center中，我们使用ip route命令来验证与网络设备的连接。

SNMP walk也可用于进行故障排除。

SNMP凭证中的错误可能会在资产中产生可管理性错误消息：SNMP身份验证失败或设备无法访问。

数据库表

作为最终用户，您可以使用带Grafana的Cisco DNA Center GUI执行SQL查询，因此您无需通过磁悬浮命令行界面访问Postgres外壳。



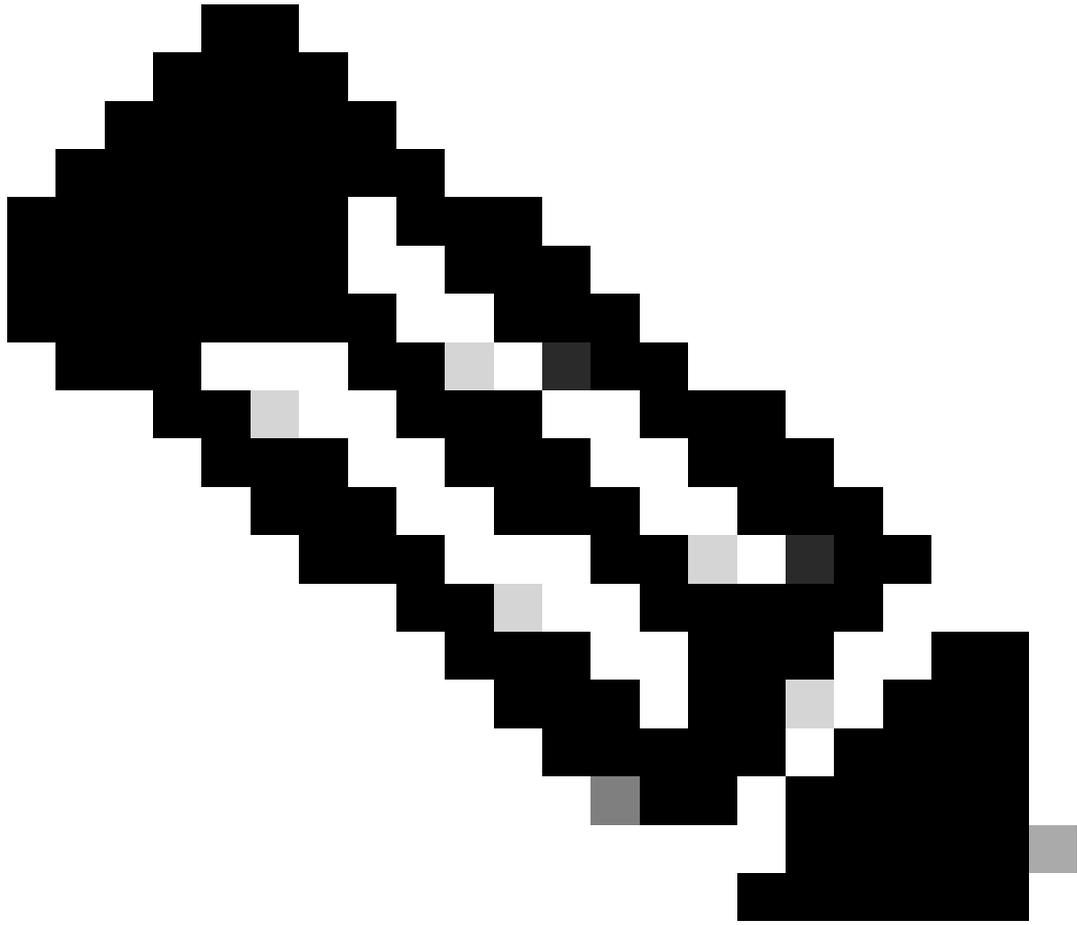
提示：如果您想了解如何使用Grafana，请查看官方指南：在[Cisco DNA Center GUI中执行Postgres查询](#)

当资产中的网络设备有问题时，需要查看的一些postgres数据库表包括：

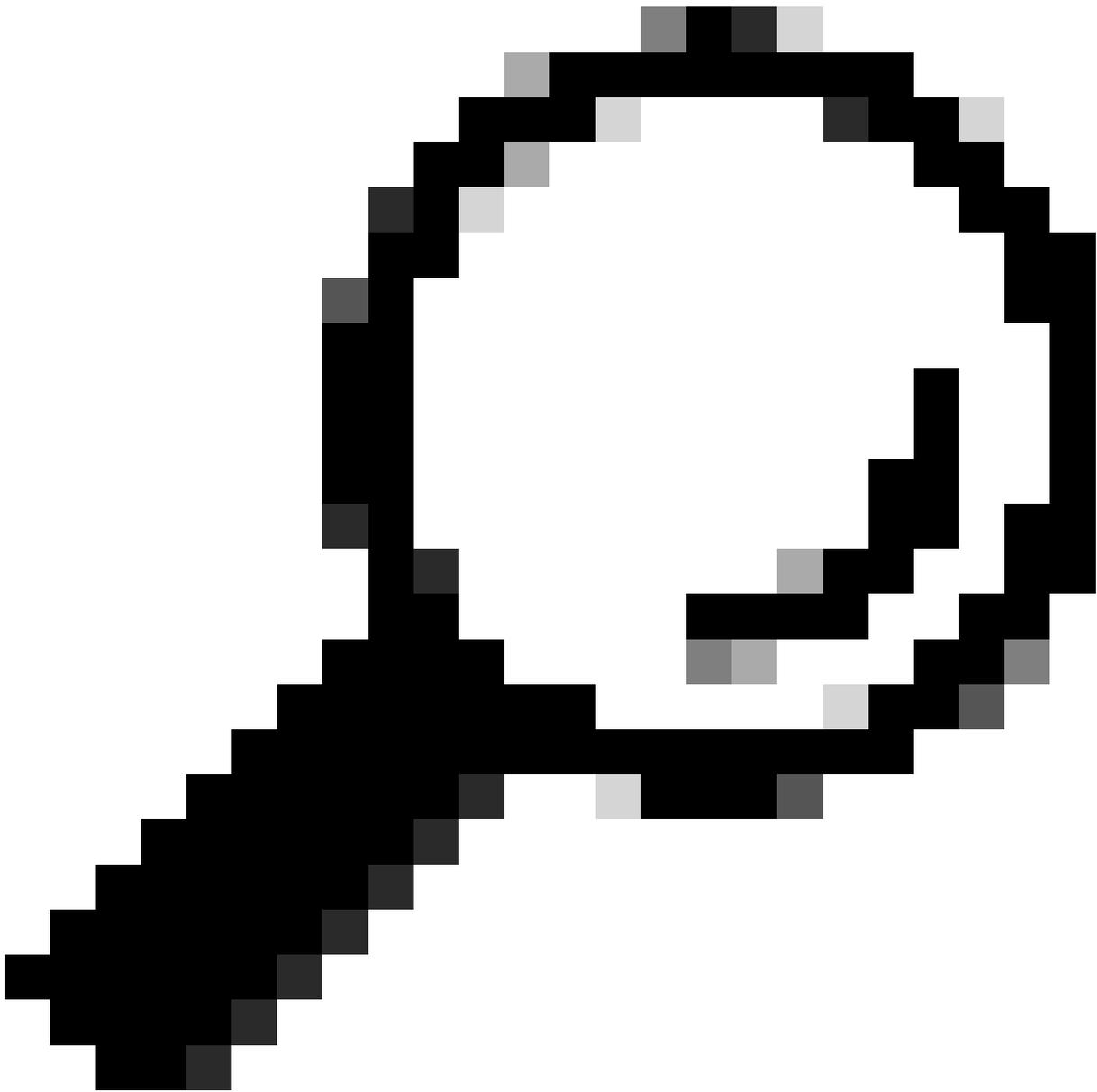
- 网络设备
- managedelementinterface
- 网络元素
- 网络资源
- 设备if
- IP地址



警告：仅允许思科TAC在Postgres Shell中运行show queries，且仅允许BU/DE团队修改DB表。



注意：数据库问题还可能导致设备出现内部错误消息，从而阻止数据收集和设备调配。



提示：在Cisco DNA Center System 360页面中，您可以使用Kibana查看Postgres日志，并在Inventory服务尝试保存或更新Postgres数据库表中的条目时查找约束冲突。

同步环路和陷阱

Cisco DNA Center设计为在设备本身执行重大更改后每次收到来自设备的陷阱时执行设备重新同步，以保持Cisco DNA Center资产清单的更新。有时，Cisco DNA Center资产页面会长时间或永久地使网络设备在可管理性部分保持“同步”状态。



注意：由于存在大量陷阱，这些类型的同步环路会导致Cisco DNA Center在短时间内多次向因检测到更改而发送陷阱的设备进行身份验证。

用于强制设备同步的API

如果您的网络设备保持同步状态的时间过长，甚至过天，请先检查基本检查连通性和连通性。然后通过API调用强制设备重新同步：

1. — 打开Cisco DNA Center maglev CLI会话。
2. — 通过API获取Cisco DNA Center身份验证令牌：

<#root>

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

3. — 使用上一步的令牌运行API以强制设备同步：

```
<#root>
```

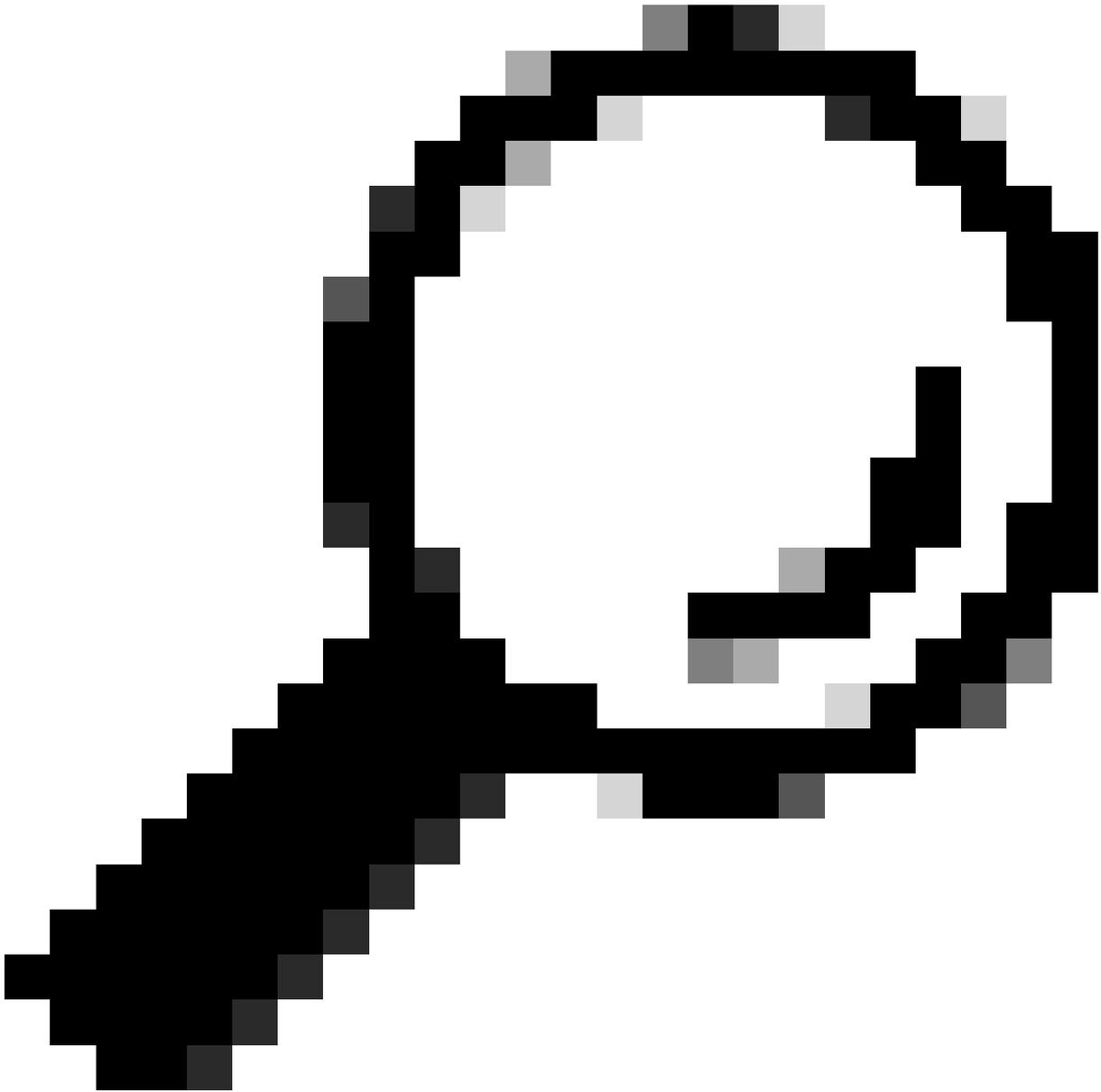
```
curl -X PUT -H "X-AUTH-TOKEN:
```

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

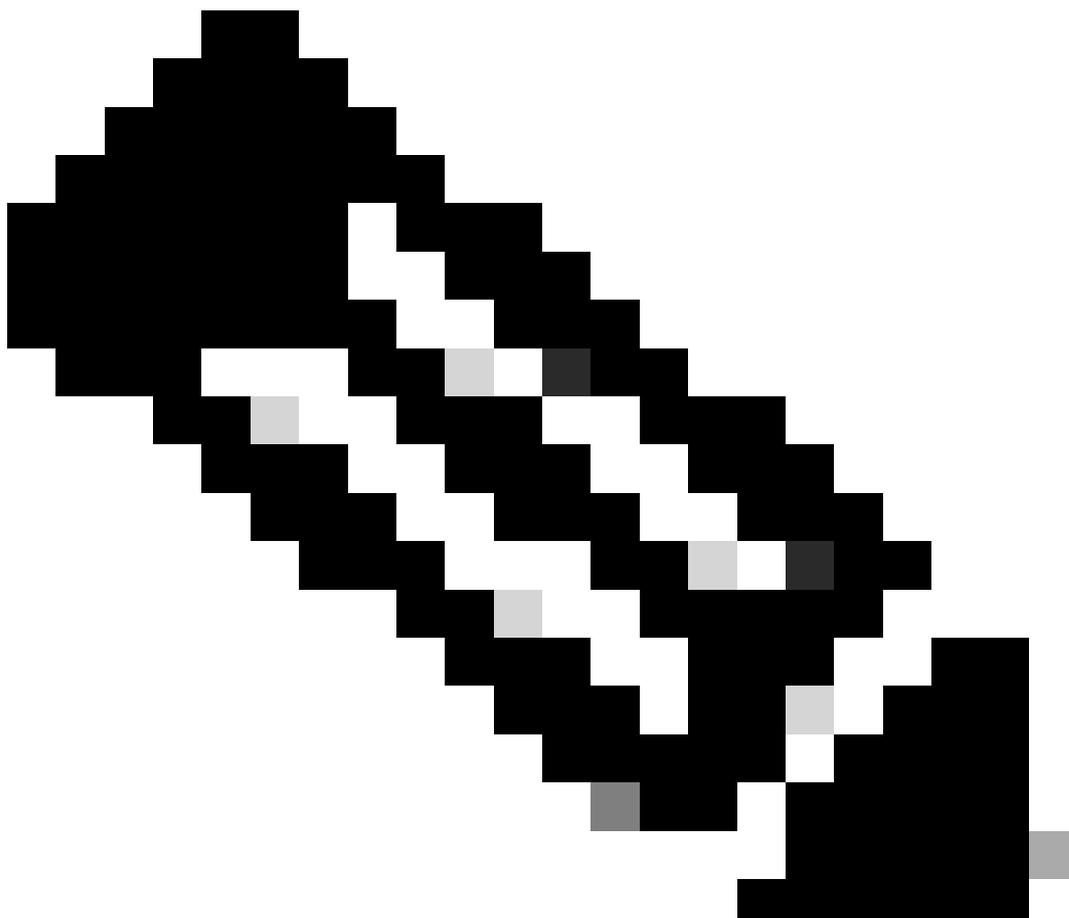
```
' https://
```

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

4. — 您可以再次看到正在同步的设备，但这次通过API使用强制同步选项。



提示：您可以从Cisco DNA Center Inventory Device Details页面或Device View 360页面从浏览器URL（设备ID或ID）获取设备UUID。



注意：有关Cisco DNA Center中API的详细信息，请参阅[Cisco DevNet API指南](#)

检查陷阱

如果在强制在设备中执行同步任务后问题仍然存在，我们可以检查Cisco DNA Center “event-service”是否接收了过多的陷阱，并通过读取事件服务日志来查看哪种类型的陷阱：

1. — 在读取日志之前，我们只需使用以下命令检查陷阱总数：

```
<#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. — 然后我们附加到event-service容器：

```
<#root>
```

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

3. — 进入事件服务容器后，将目录更改为日志文件夹：

```
<#root>
```

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

4. — 如果查看目录中的文件，您可以看到一些名称以“ncs”开头的日志文件。

示例：

```
<#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. — 这些“ncs”文件是我们需要分析接收的陷阱类型和数量的文件。我们可以查看按设备主机名或关键字“trapType”过滤的日志文件：

```
<#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
```

陷阱的类型过多，有些陷阱会触发设备重新同步，如果它们过于频繁，则会导致同步环路。

通过分析陷阱，我们可以确定根本原因并使陷阱停止，例如重新启动周期中的AP。

您可以将陷阱输出保存到文件中，并在需要时与升级团队共享这些输出。

服务崩溃状态

如果您怀疑资产Pod由于管理网络设备时Cisco DNA Center资产页面中的异常行为而崩溃，则可以首先验证Pod状态：

```
<#root>
```

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

```
$ magctl service status
```

查看Pod状态的输出，如果您看到重新启动次数较多或出现错误状态，则您可以连接到资产容器并收集heapdump文件，该文件可以包含有助于上报团队分析和定义崩溃状态的根本原因的数据：

```
<#root>
```

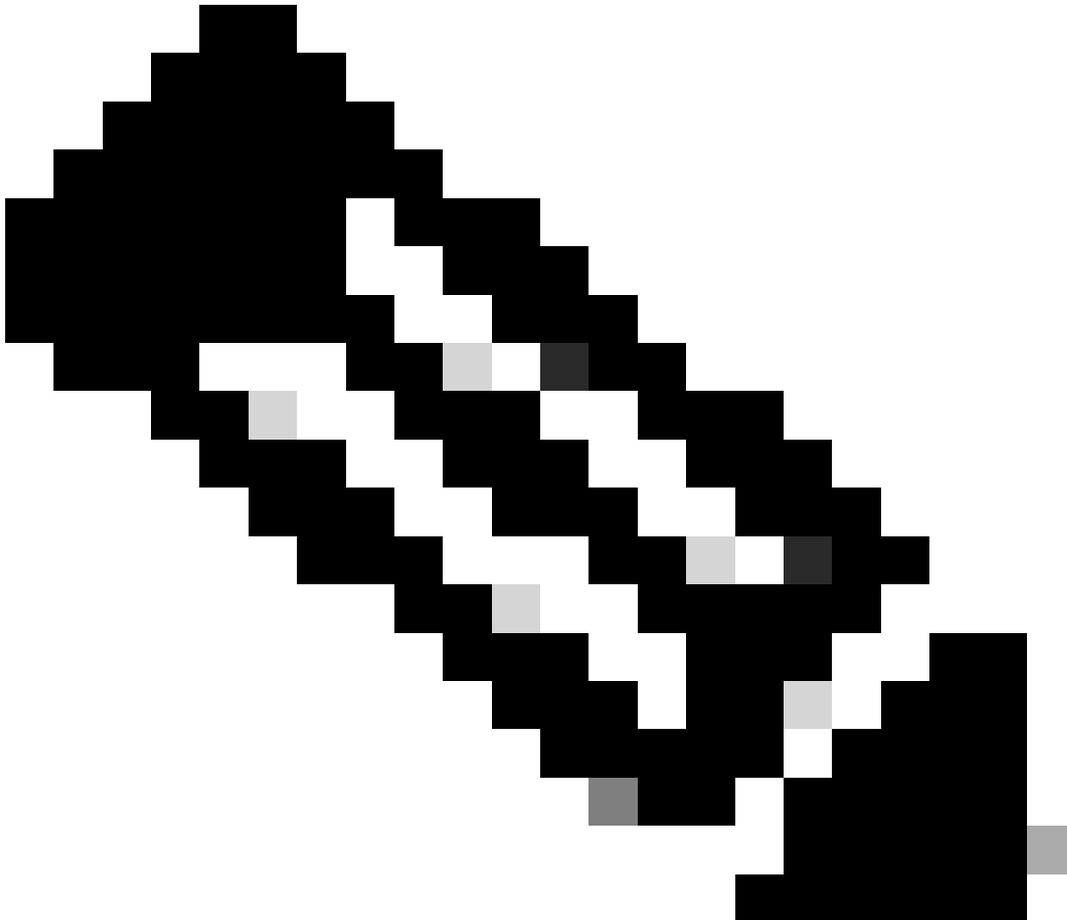
```
$ magctl service attach -D
```

```
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



注意：如果在容器目录中找不到堆转储文件，则容器中不存在崩溃状态。

无法删除设备

在某些情况下，由于后端问题，Cisco DNA Center无法从资产用户界面删除网络设备。

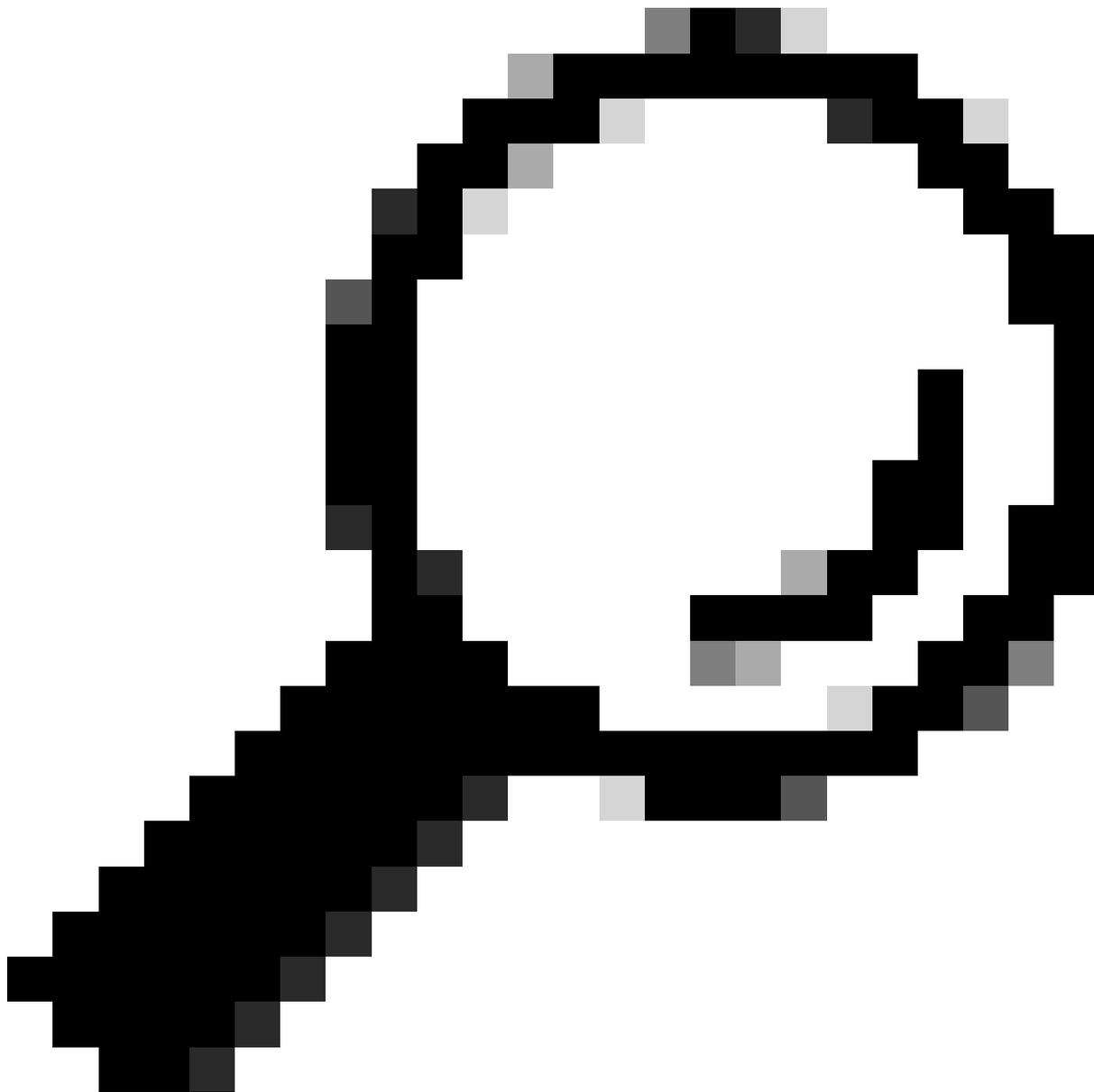
强制设备删除的API

如果无法使用Cisco DNA Center GUI从资产中删除设备，则可以使用API通过ID删除设备：

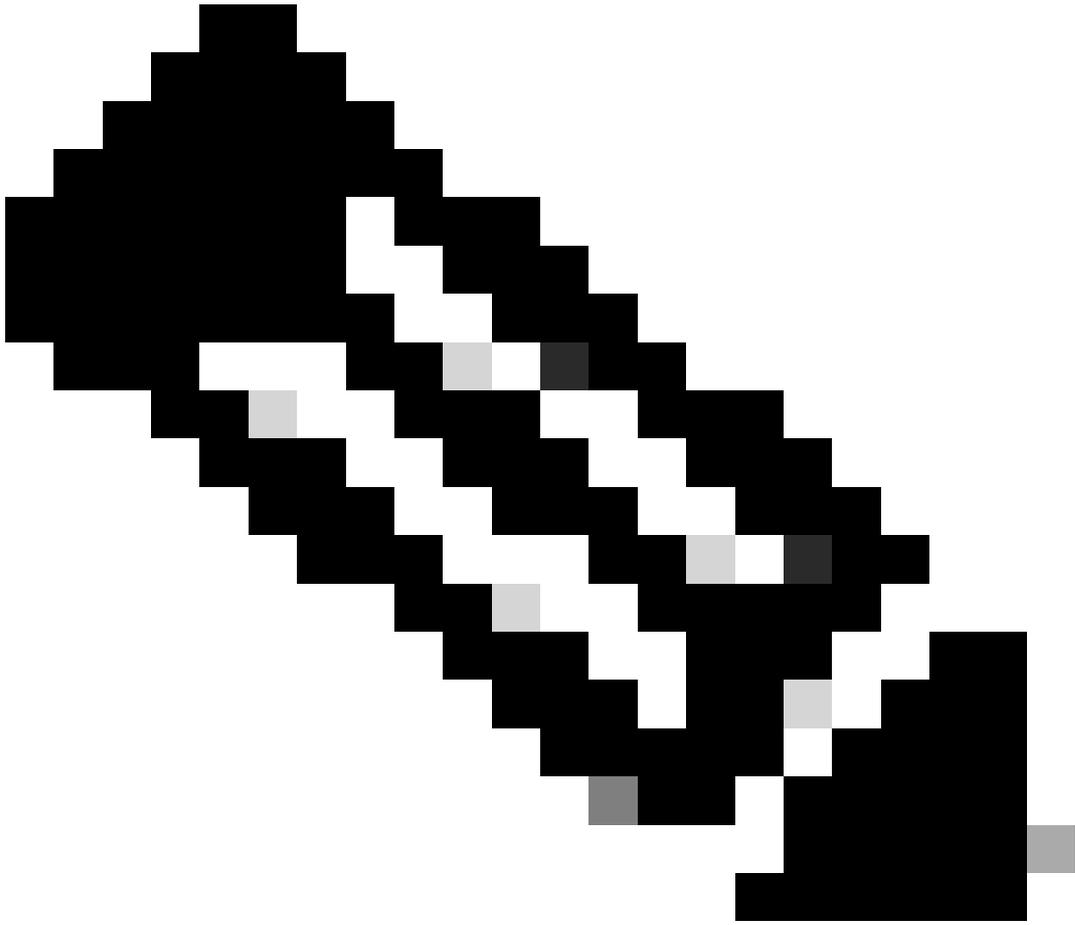
1. — 导航到Cisco DNA Center Menu -> Platform -> Developer Toolkit -> APIs选项卡，在搜索栏中搜索Devices，在结果中单击Devices从Know your network部分中的Devices，然后搜索DELETE by

Device Id API。

2. — 在DELETE by Device Id API中单击，在Try中单击，并提供要从资产清单中删除的所需设备的设备ID。
 3. — 等待API运行并获得200 OK响应，然后确认网络设备不再出现在资产页面中。
-



提示：您可以从Cisco DNA Center Inventory Device Details页面或Device View 360页面从浏览器URL（设备ID或ID）获取设备UUID。



注意：有关Cisco DNA Center中API的详细信息，请参阅[Cisco DevNet API指南](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。