

Examinar o Serviço de inventário do DNA Center e problemas comuns

Contents

[Introdução](#)

[Componentes Utilizados](#)

[Detalhes do Serviço de Inventário](#)

[Status da capacidade de gerenciamento](#)

[Status da Última Sincronização](#)

[Problemas](#)

[Internal Error](#)

[Credenciais do dispositivo](#)

[Netconf](#)

[Verificações de rede](#)

[Tabelas de banco de dados](#)

[Loop e Armadilhas de Sincronização](#)

[API para Forçar Sincronização de Dispositivos](#)

[Traps de revisão](#)

[Status de travamento de serviço](#)

[Não é possível excluir um dispositivo](#)

[API para forçar exclusão de dispositivo](#)

Introdução

Este documento descreve os conceitos básicos do serviço de inventário do Cisco DNA Center e os problemas comuns encontrados na produção.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Detalhes do Serviço de Inventário

O serviço Inventário do Cisco DNA Center é baseado em um Pod Kubernetes (K8s) que pode ser executado no namespace "fusion" com o nome "apic-em-inventory-manager-service-`<id>`" como um tipo de ambiente de Implantação.

Dentro do pod K8s, você pode encontrar um contêiner Docker chamado "apic-em-inventory-manager-service".

As principais tarefas do pod "apic-em-inventory-manager-service" são: Detecção de dispositivos e gerenciamento do ciclo de vida do dispositivo.

Isso garante que os dados do dispositivo estejam disponíveis no SQL Postgres (banco de dados usado pelos serviços de fusão).

O namespace de "fusão" (Appstack), também conhecido como Plataforma de Controlador de Rede (NCP), fornece os serviços Service Provisioning Framework (SPF) para todos os requisitos de automação de rede.

Eles incluem descoberta, inventário, topologia, política, gerenciamento de imagem de software (SWIM), arquivo de configuração, programador de rede, sites, agrupamento, telemetria, integração com Tesseract, programador de modelo, mapas, IPAM, sensores, orquestração/fluxo de trabalho/agendamento, integração com ISE e similares.

O status do pod de inventário pode ser verificado executando o comando:

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

O status do serviço de inventário pode ser verificado com o comando:

```
$ magctl service status
```

Os logs de serviço de inventário podem ser verificados com o comando:

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



Note: O serviço de inventário também pode consistir em dois pods em execução, portanto você precisa especificar um único pod nos comandos usando o nome completo do pod de inventário, incluindo o pod id.

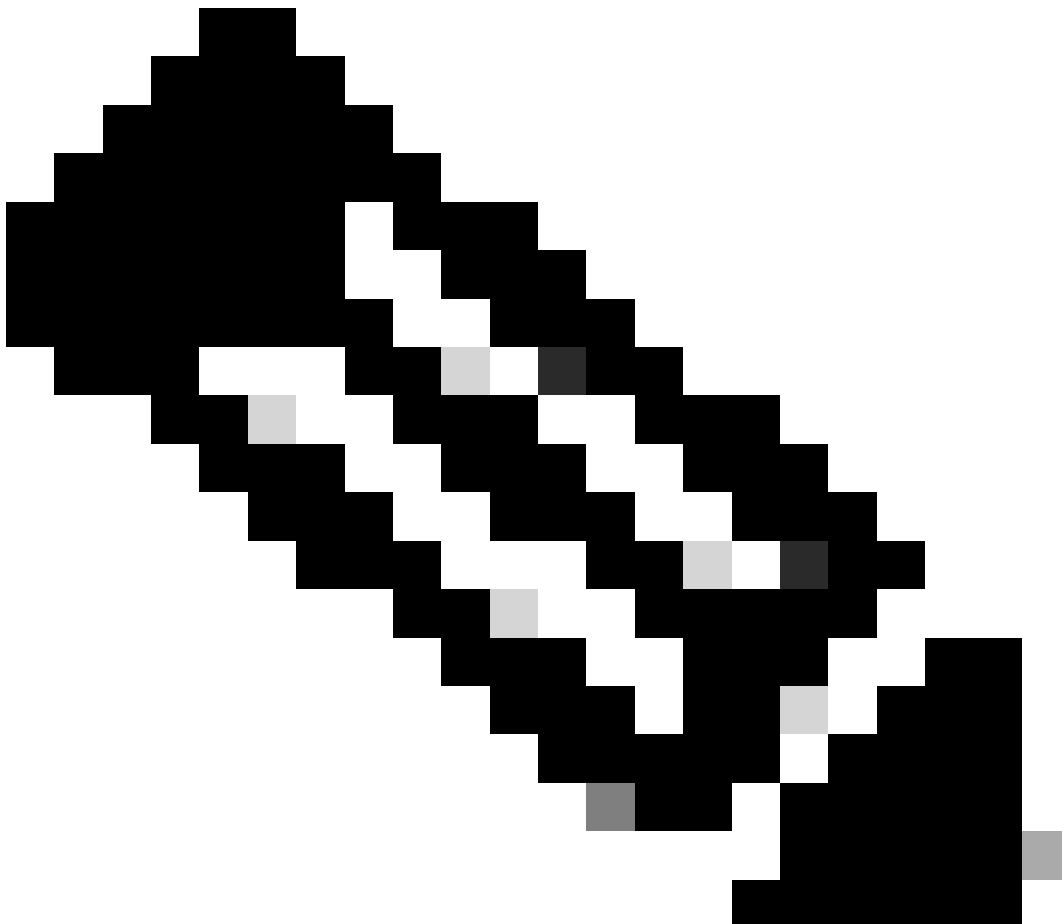
Neste documento, podemos nos concentrar no status da gerenciabilidade do dispositivo de inventário e da última sincronização para revisar os problemas comuns:

Status da capacidade de gerenciamento

- Gerenciado com ícone de marca verde: O dispositivo está acessível e é totalmente gerenciado.
- Gerenciado com ícone de erro laranja: O dispositivo é gerenciado com erros como inalcançável, falha de autenticação, portas Netconf ausentes, erro interno e assim por diante. Você pode passar o cursor sobre a mensagem de erro para exibir mais detalhes sobre o erro e os aplicativos afetados.
- Não gerenciado: O dispositivo não pode ser acessado e nenhuma informação de inventário foi coletada devido a problemas de conectividade do dispositivo.

Status da Última Sincronização

- Gerenciado: O dispositivo está em um estado totalmente gerenciado.
 - Falha na coleta parcial: O dispositivo está em um estado coletado parcial e nem todas as informações de inventário foram coletadas. Passe o cursor sobre o ícone Information (i) para exibir informações adicionais sobre a falha.
 - Não Acessível: O dispositivo não pode ser acessado e nenhuma informação de inventário foi coletada devido a problemas de conectividade do dispositivo. Essa condição ocorre quando ocorre a coleta periódica.
 - Credenciais incorretas: Se as credenciais do dispositivo forem alteradas após a adição do dispositivo ao inventário, essa condição será observada.
 - Em andamento: Está ocorrendo coleta de estoque.
-



Note: Para obter mais informações sobre as funções de inventário no Cisco DNA Center,

consulte o guia oficial da versão 2.3.5.x: [Manage Your Inventory](#)

Problemas

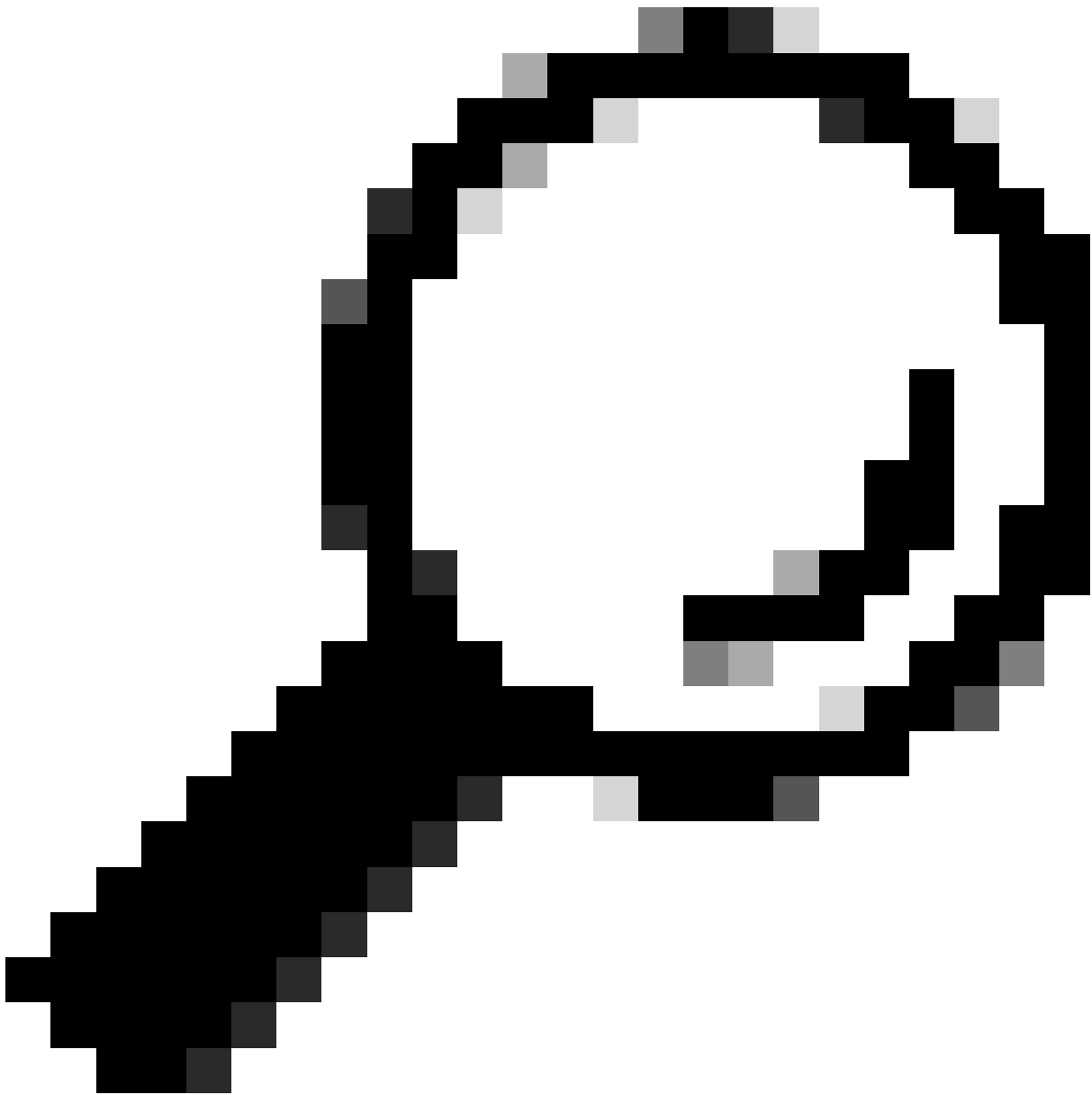
Internal Error

A página Inventário do Cisco DNA Center pode exibir uma mensagem de aviso no status Gerenciabilidade para dispositivos com algum tipo de conflito impedindo a coleta de dados:

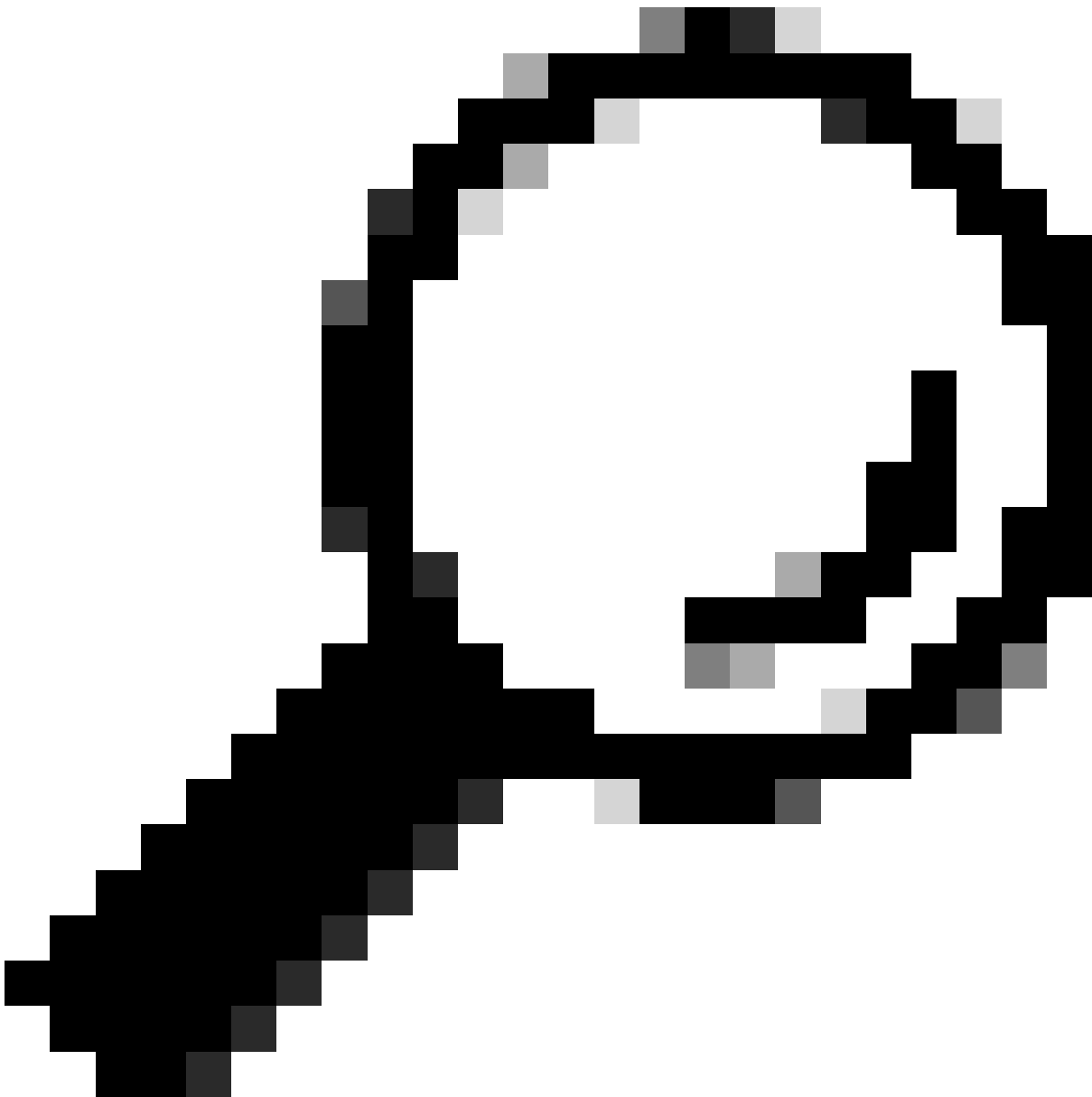
"Erro interno: NCIM12024: Não foi possível coletar com êxito todas as informações do dispositivo ou a coleta de inventário para este dispositivo ainda não foi iniciada. Pode ser um problema temporário que pode ser resolvido automaticamente. Ressincronize o dispositivo. Se isso não resolver o problema, entre em contato com o TAC da Cisco."

Se o erro não for resolvido automaticamente ou após a ressincronização de um dispositivo, podemos começar com a solução de problemas inicial. Esse erro pode ser devido a vários motivos, mas aqui, listamos apenas alguns dos mais comuns:

- Credenciais de dispositivo incorretas para SNMP, SSH e Netconf.
- Problemas de conectividade de rede relacionados ao SNMP, SSH e Netconf.
- Problemas de configuração do Netconf no dispositivo, fazendo com que o Netconf não funcione corretamente.
- Dispare uma ressincronização de dispositivo enquanto uma sincronização de dispositivo já está em andamento.
- Várias intercepções foram recebidas do dispositivo, causando vários gatilhos de ressincronização em um curto período de tempo.
- Problemas de back-end com entradas de banco de dados de inventário em várias tabelas relacionadas ao dispositivo.



Tip: A remoção do dispositivo de rede e sua redescoberta usando as credenciais corretas de CLI, SNMP e NETCONF pode ajudar a remover entradas obsoletas do banco de dados que poderiam estar causando o erro interno.



Tip: A análise dos registros de serviço de inventário e a filtragem por IP de dispositivo ou nome de host podem ser úteis para identificar a causa raiz do erro interno.

Credenciais do dispositivo

Para revisar as credenciais do dispositivo, navegue até o menu do Cisco DNA Center -> Provisionamento -> Inventário -> Selecionar dispositivo -> Ações -> Inventário -> Editar dispositivo e clique em "Validar" e confirme se as credenciais obrigatórias (CLI e SNMP) estão passando na validação com uma marca verde (incluindo netconf, se aplicável).

Se a validação falhar, verifique se o nome de usuário e a senha que o Cisco DNA Center está usando para gerenciar o dispositivo de rede são válidos diretamente na linha de comando do dispositivo.

Se estiverem configurados localmente ou se estiverem configurados em um servidor AAA (TACACS ou RADIUS), valide se o nome de usuário e a senha estão configurados corretamente no servidor AAA.

Verifique também se o privilégio de nome de usuário requer a configuração da senha "Habilitar" nas Configurações de credenciais do dispositivo no Cisco DNA Cinforme Inventário.

Erros nas credenciais de CLI podem causar uma mensagem de erro de gerenciabilidade no Inventário: Falha de autenticação de CLI.

Netconf

O Netconf é um protocolo para gerenciar remotamente um dispositivo de rede compatível através de RPC (Remote Procedure Calls).

O Cisco DNA Center usa os recursos do Netconf para enviar ou remover a configuração nos dispositivos de rede para ativar recursos como o monitoramento através do Assurance.

O Inventário do Cisco DNA Center também pode validar se os requisitos da Netconf estão corretos, o que inclui:

- A porta 830 padrão do Netconf deve ser aberta e funcional na rede.
- Usuário com privilégio 15 com acesso SSH ao dispositivo de rede (configurado localmente ou AAA).
- Ative o Netconf no dispositivo de rede:

```
<#root>
```

```
(config)#
```

```
netconf-yang
```

- Se aaa new-model estiver habilitado, então você também precisará configurar os requisitos de configuração padrão de AAA:

```
<#root>
```

```
(config)#
```

```
aaa authorization exec default
```

```
(config)#
```

```
aaa authentication login default
```


Erros nas credenciais do Netconf podem causar uma mensagem de erro de gerenciabilidade no Inventário: Falha De Conexão Netconf.

Verificações de rede

Também podemos validar as configurações de conectividade de rede e protocolos como configurações SNMP, dependendo da versão.

Por exemplo, podemos verificar novamente as configurações de comunidade, usuário, grupo, engineID, autenticação e criptografia, etc., dependendo da versão do SNMP.

Também podemos rever a conectividade SSH e SNMP usando os comandos ping e traceroute na linha de comando do dispositivo e portas para SSH (22) e SNMP (161 e 162) no firewall, proxy ou listas de acesso.

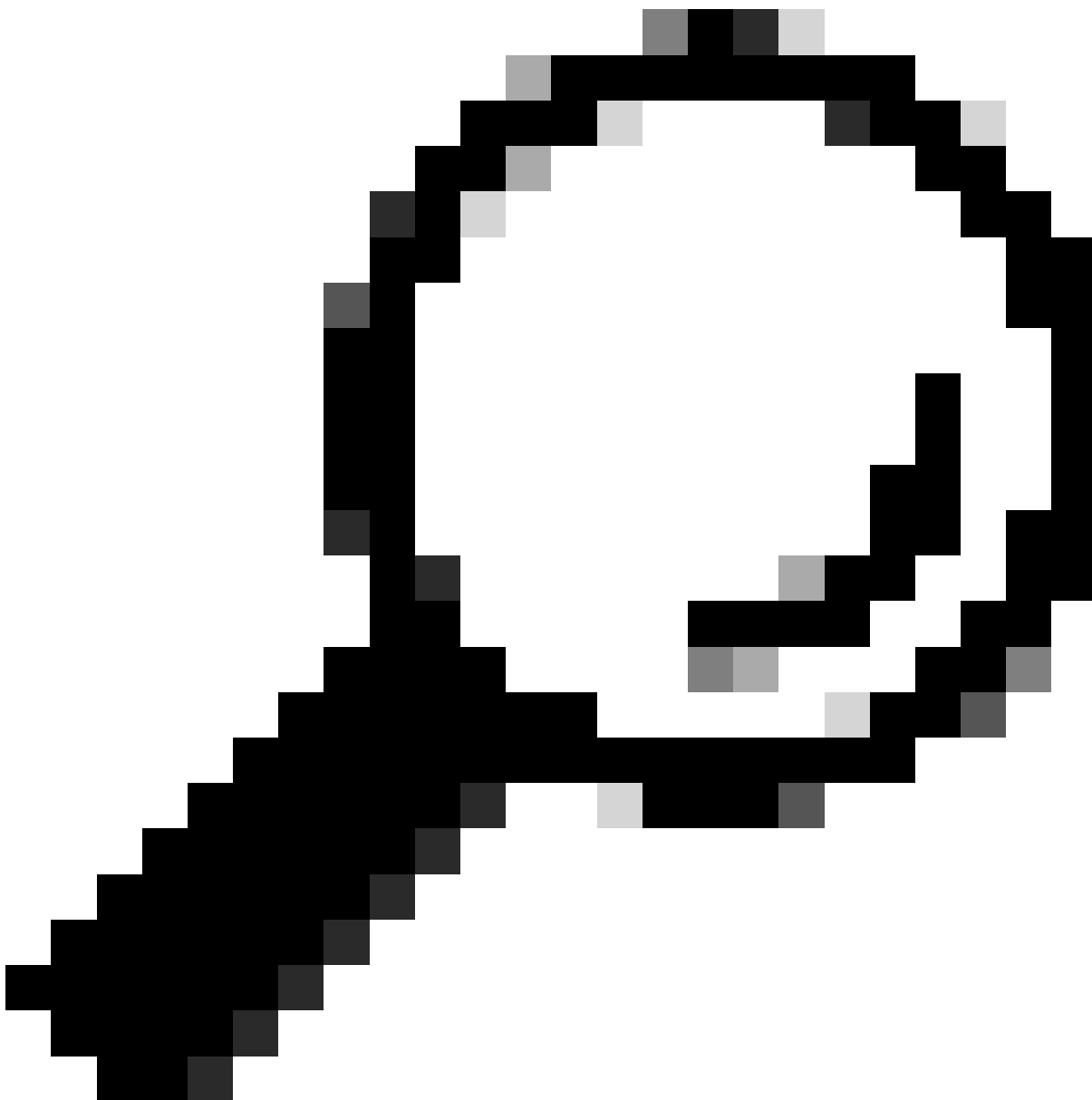
No Cisco DNA Center, maglev CLI, usamos os comandos ip route para validar a conectividade com o dispositivo de rede.

O SNMP walk também pode ser usado para solucionar problemas.

Erros nas credenciais SNMP podem causar uma mensagem de erro de gerenciabilidade no Inventário: Falha de autenticação SNMP ou dispositivo inalcançável.

Tabelas de banco de dados

Como usuário final, você pode usar a GUI do Cisco DNA Center com o Grafana para executar consultas SQL para não precisar acessar o shell Postgres via maglev CLI.



Tip: Se você quiser saber como usar o Grafana, leia o guia oficial: [Execute Postgres Queries in Cisco DNA Center GUI](#)

Algumas tabelas de banco de dados postgres para revisar quando tiver problemas com dispositivos de rede no Inventário são:

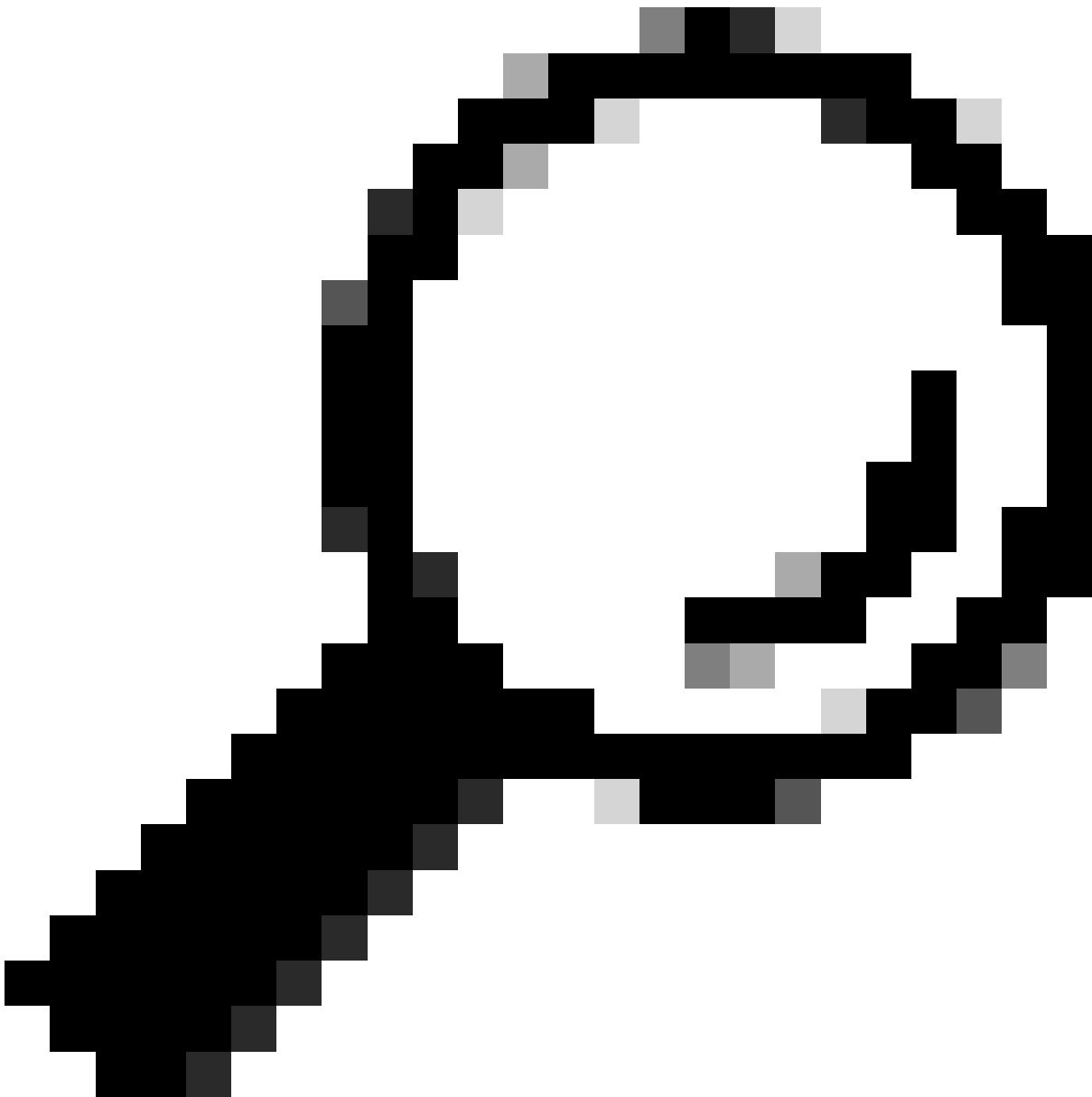
- dispositivo de rede
- interface de elementogerenciado
- elemento de rede
- recurso de rede
- deviceif
- ipaddress



aviso: Somente o TAC da Cisco tem permissão para executar consultas show no Shell Postgres e somente equipes BU/DE têm permissão para fazer modificações nas tabelas DB.



Note: Problemas de banco de dados também podem causar a mensagem de erro interna para dispositivos, o que pode impedir a coleta de dados e o provisionamento de dispositivos.



Tip: Você pode examinar os logs Postgres usando Kibana na página do Cisco DNA Center System 360 e procurar por Violações de restrição quando o serviço de Inventário estiver tentando salvar ou atualizar entradas nas tabelas do banco de dados Postgres.

Loop e Armadilhas de Sincronização

O Cisco DNA Center foi projetado para executar um dispositivo Resync cada vez que ele recebe uma interceptação do dispositivo após uma alteração importante ser executada no próprio dispositivo para manter o Inventário do Cisco DNA Center atualizado. Às vezes, a página Inventário do Cisco DNA Center mantém seus dispositivos de rede no status "Sincronização" na seção Gerenciabilidade por um longo período de tempo ou para sempre.



Note: Esses tipos de loops de sincronização devido a armadilhas maciças podem fazer com que o Cisco DNA Center autentique várias vezes em um curto período de tempo para os dispositivos que estão enviando as armadilhas devido a alterações detectadas.

API para Forçar Sincronização de Dispositivos

Se o dispositivo de rede permanecer no status Sincronizando por muito tempo, até mesmo dias, primeiro revise as verificações básicas de acessibilidade e conectividade. Em seguida, force a resincronização do dispositivo via chamada de API:

- 1.- Abra a sessão da CLI maglev do Cisco DNA Center.
- 2.- Obtenha o token de autenticação do Cisco DNA Center via API:

<#root>

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

3.- Use o token da etapa anterior para executar a API para Forçar a Sincronização do dispositivo:

<#root>

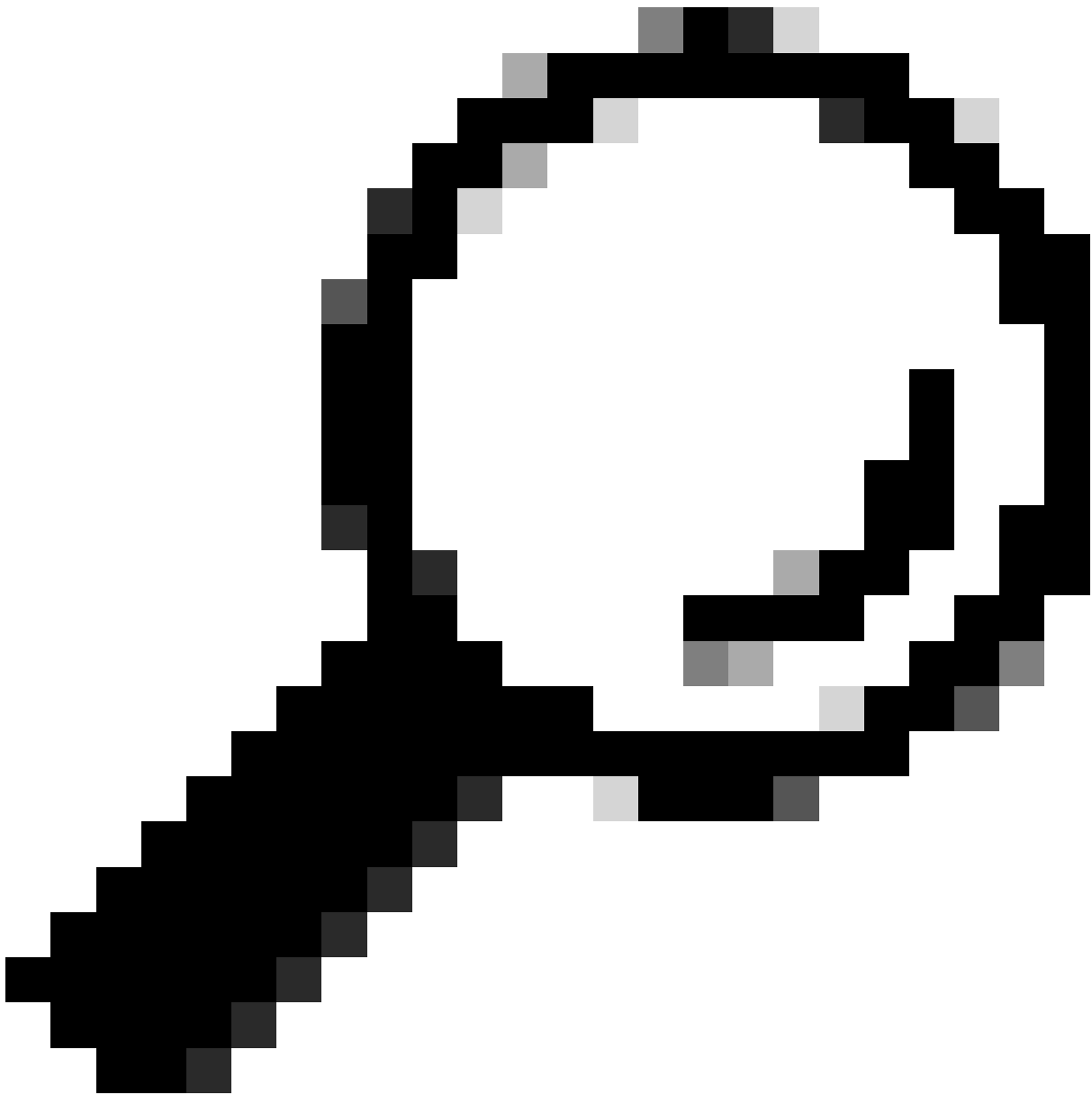
```
curl -X PUT -H "X-AUTH-TOKEN:
```

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

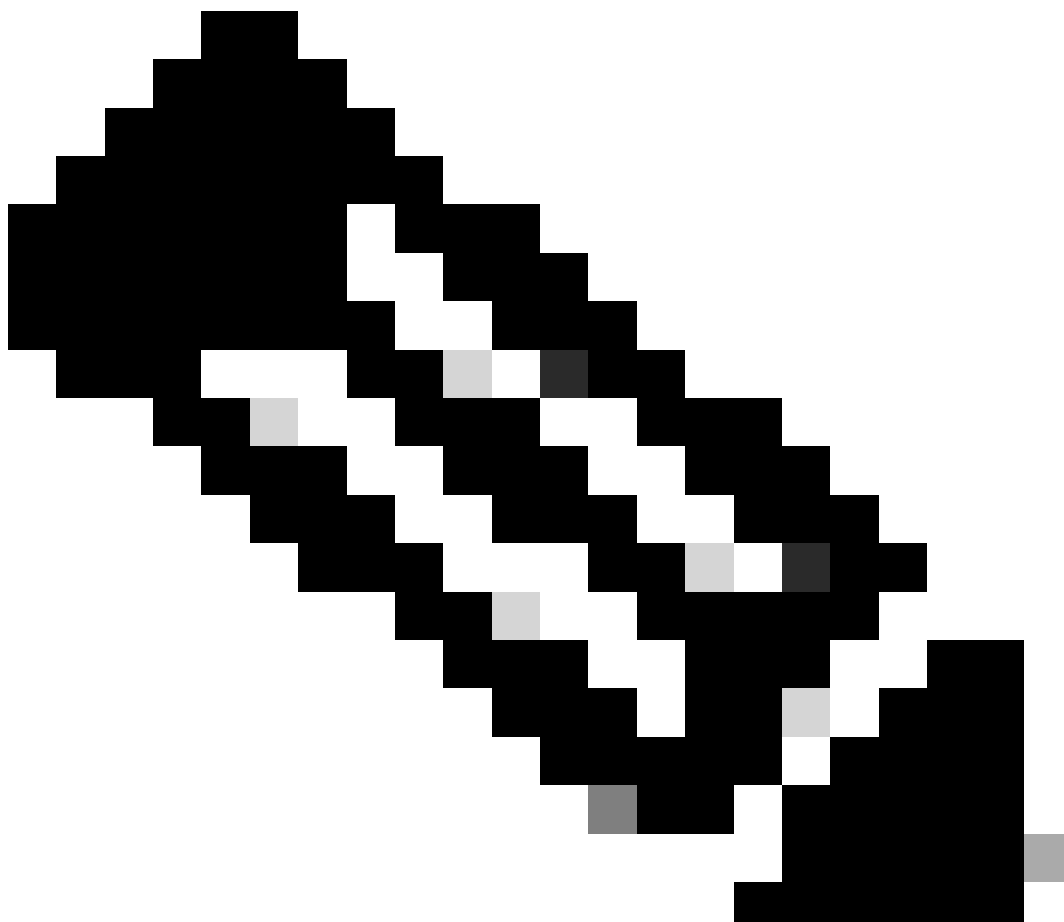
```
' https://
```

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

4.- Você pode ver o dispositivo em Sincronização novamente, mas desta vez com uma opção Forçar Sincronização via API.



Tip: Você pode obter o uuid do dispositivo na URL do navegador (id do dispositivo ou id) na página Detalhes do dispositivo de inventário do Cisco DNA Center ou na página Exibição de dispositivo 360.



Note: Para obter mais informações sobre APIs no Cisco DNA Center, consulte o [Guia de APIs do Cisco DevNet](#)

Traps de revisão

Se o problema persistir após forçar a tarefa de sincronização no dispositivo, podemos verificar se o "serviço de eventos" do Cisco DNA Center está recebendo muitas intercepções e revisar que tipo de intercepções lendo os logs de eventos de serviço:

1.- Antes de lermos os registros, podemos apenas verificar o total de armadilhas com o comando:

```
<#root>
```

```
$ echo;echo;eventsId=$(docker ps | awk '/k8s_apic-em-event/ {print $1}'); docker cp $eventsId:/opt/CSCColumns/logs/ /tmp;/for ip in $(awk -F: '/ipAddress
```

2.- Em seguida, anexamos ao contêiner de serviço de evento:

```
<#root>
```

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

3.- Depois de entrar no contêiner de serviço de eventos, altere o diretório para a pasta logs:

```
<#root>
```

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

4.- Se você revisar os arquivos dentro do diretório você pode ver alguns arquivos de registro cujo nome começa com "ncs".

Exemplo:

```
<#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.- Esses arquivos "ncs" são os que precisamos para analisar que tipo de interceptações estamos recebendo e quantos. Podemos revisar os arquivos de log que os filtram por nome de host do dispositivo ou pela palavra-chave "trapType":

```
<#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

Há muitos tipos de interceptações, algumas delas podem disparar a ressincronização do dispositivo e, se chegarem com muita frequência, poderão causar o loop de sincronização.

Analisando as armadilhas, podemos identificar a causa raiz e fazer com que as armadilhas parem, por exemplo, um AP em um ciclo de reinicialização.

Você pode salvar a saída das interceptações em um arquivo e compartilhá-las com a equipe de escalção, se necessário.

Status de travamento de serviço

Se você suspeitar que o pod de inventário está travando devido a um comportamento estranho na página Inventário do Cisco DNA Center durante o gerenciamento de dispositivos de rede, você poderá validar o status do pod primeiro:

```
<#root>
```

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

```
$ magctl service status
```

Revisando a saída do status do pod, se você vir um alto número de reinicializações ou um status de erro, então você pode anexar ao contêiner de inventário e coletar o arquivo de despejo de pilha que pode ter os dados que podem ajudar a equipe de escalção a analisar e definir a causa raiz do estado de travamento:

<#root>

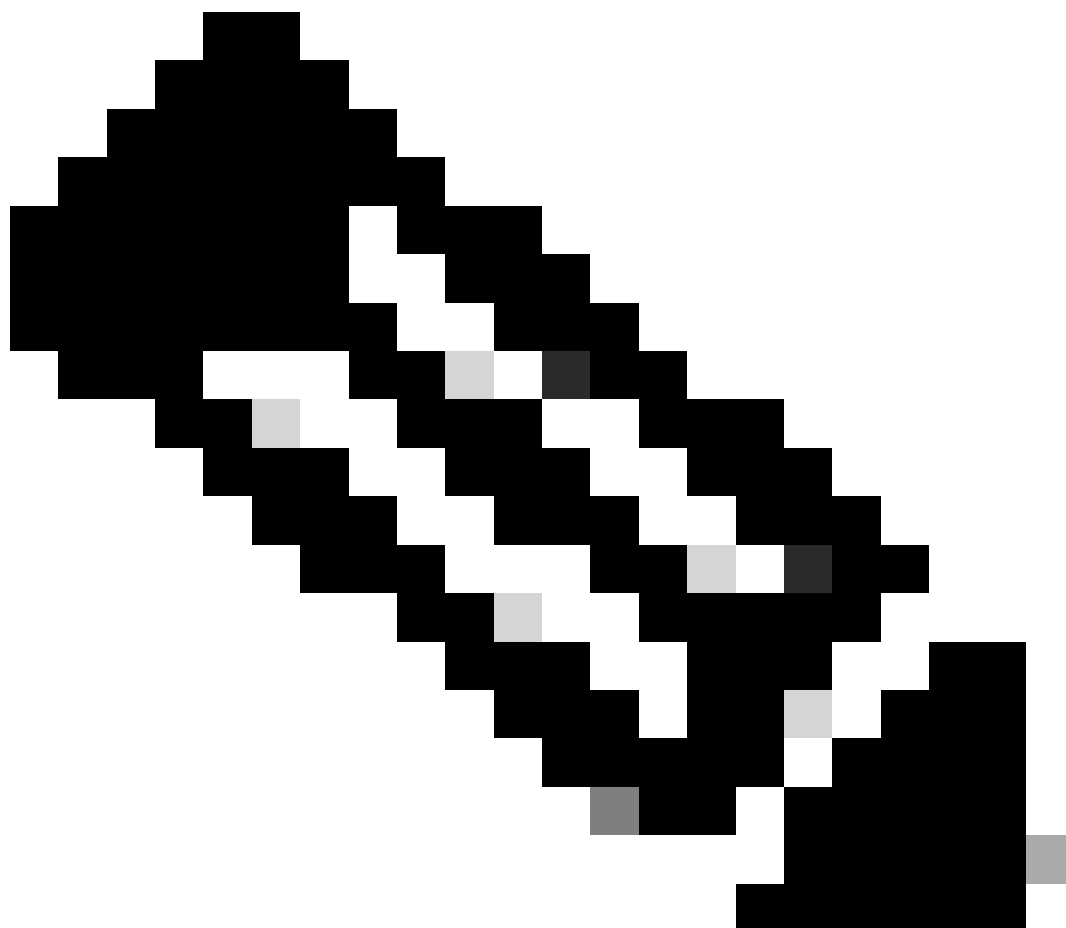
\$ magctl service attach -D

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



Note: Se nenhum arquivo de despejo de pilha foi encontrado no diretório do contêiner, então nenhum estado de travamento estava presente no contêiner.

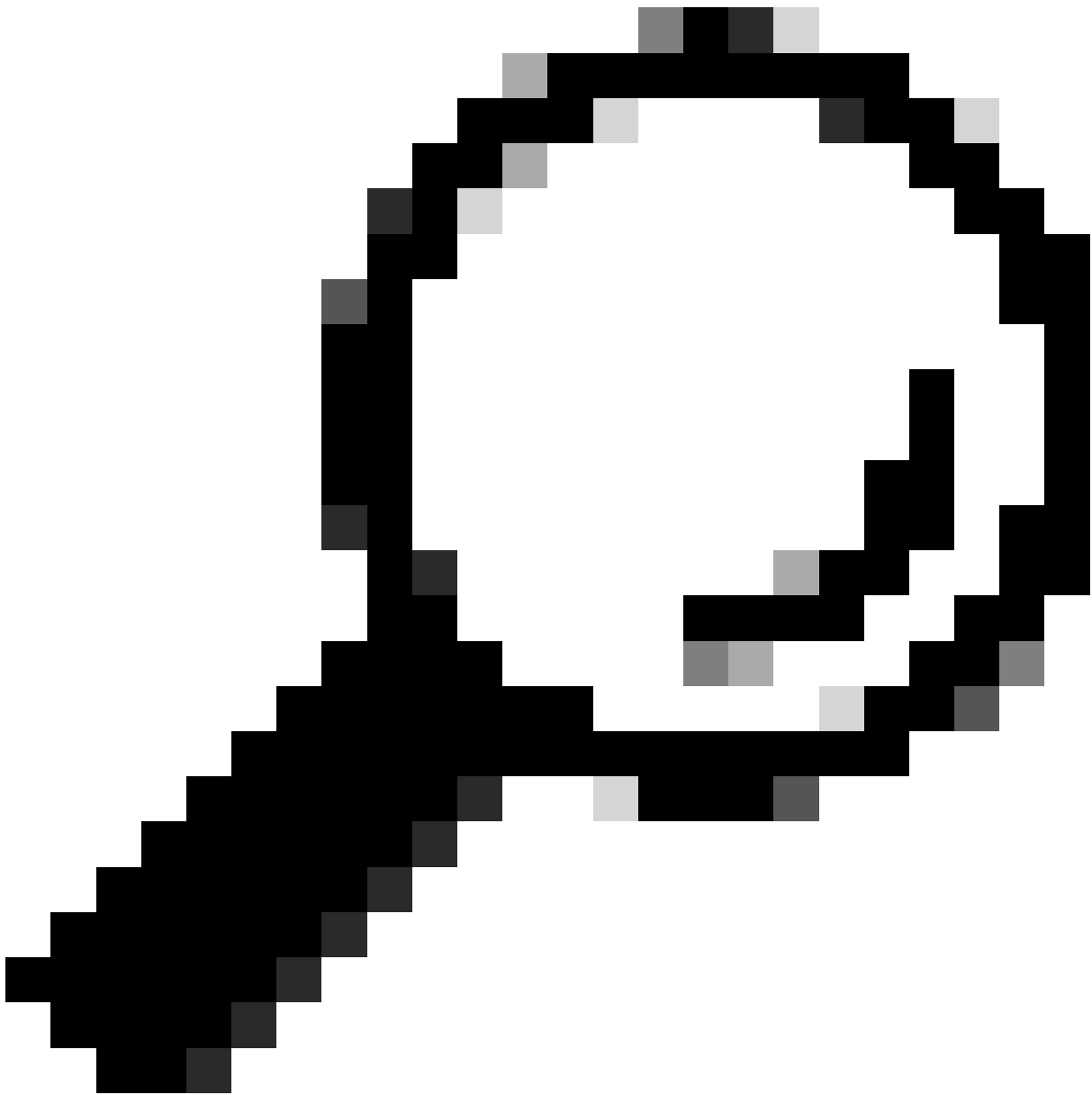
Não é possível excluir um dispositivo

Em algumas situações, o Cisco DNA Center pode não ser capaz de excluir um dispositivo de rede da interface de usuário de inventário devido a um problema de back-end.

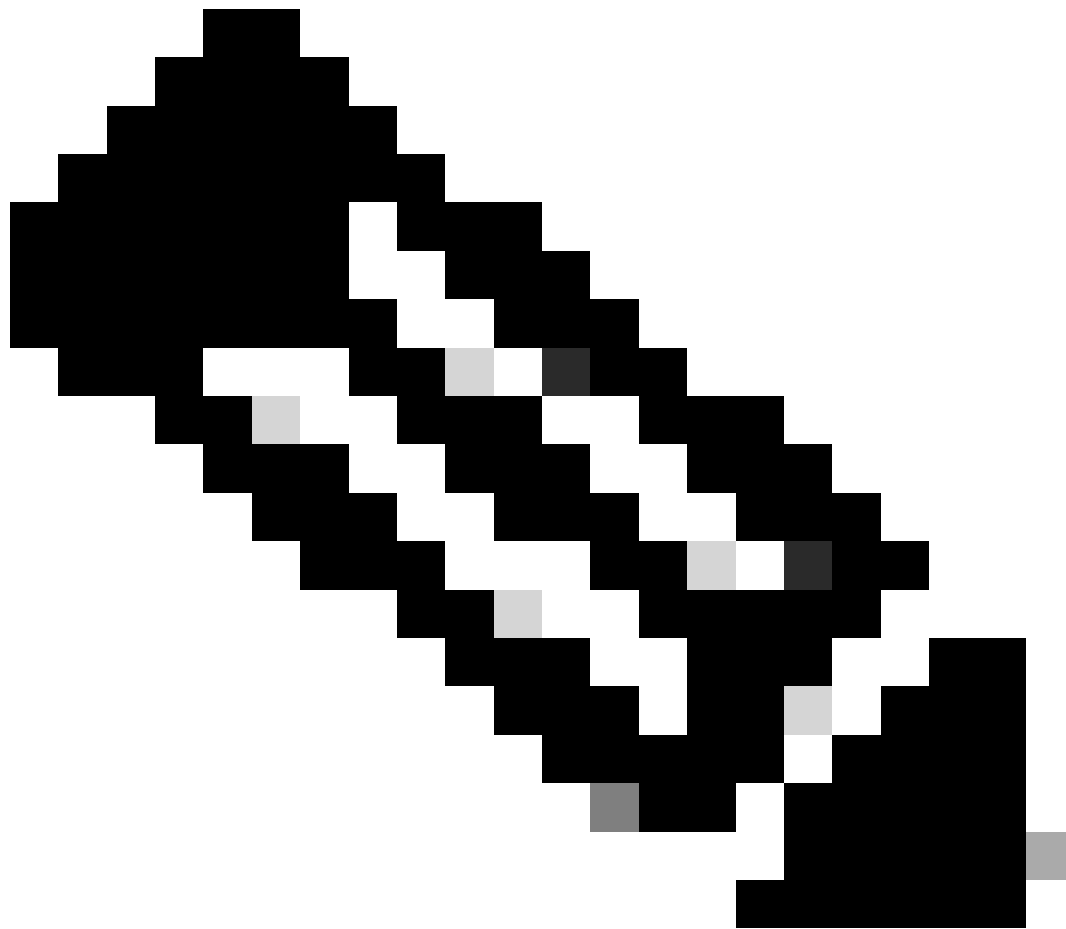
API para forçar exclusão de dispositivo

Se não for possível excluir o dispositivo do inventário usando a GUI do Cisco DNA Center, você poderá usar a API para excluir o dispositivo por ID:

- 1.- Navegue até o menu do Cisco DNA Center -> Platform -> Developer Toolkit -> guia APIs e procure Devices na barra de pesquisa. Nos resultados, clique em Devices na seção Know your network e procure a API DELETE by Device Id.
- 2.- Clique na API DELETE by Device Id, clique em Try e forneça a ID do dispositivo desejado a ser removido do inventário.
- 3.- Aguarde até que a API seja executada e obtenha uma resposta 200 OK, depois confirme se o dispositivo de rede não está mais presente na página Inventário.



Tip: Você pode obter o uuid do dispositivo na URL do navegador (id do dispositivo ou id) na página Detalhes do dispositivo de inventário do Cisco DNA Center ou na página Exibição de dispositivo 360.



Note: Para obter mais informações sobre APIs no Cisco DNA Center, consulte o [Guia de APIs do Cisco DevNet](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.