Examiner le service d'inventaire du centre DNA et les problèmes courants

Table des matières

Introduction

Ce document décrit les concepts de base du service d'inventaire Cisco DNA Center et les problèmes courants rencontrés lors de la production.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Détails du service d'inventaire

Le service d'inventaire Cisco DNA Center est basé sur un pod Kubernetes (K8s) qui s'exécute dans l'espace de noms « fusion » avec le nom « apic-em-inventory-manager-service-<id> » comme type d'environnement de déploiement.

À l'intérieur de la zone K8s, vous pouvez trouver un conteneur Docker appelé "apic-em-inventory-manager-service".

Les tâches principales de la zone "apic-em-inventory-manager-service" sont : Détection des

périphériques et gestion du cycle de vie des périphériques.

Cela garantit que les données des périphériques sont disponibles dans Postgres SQL (base de données utilisée par les services de fusion).

L'espace de noms « fusion » (Appstack) également appelé NCP (Network Controller Platform) fournit les services SPF (Service Provisioning Framework) pour toutes les exigences d'automatisation du réseau.

Il s'agit notamment de la découverte, de l'inventaire, de la topologie, de la politique, de la gestion des images logicielles (SWIM), de l'archivage de la configuration, du programmeur réseau, des sites, du regroupement, de la télémétrie, de l'intégration Tesseract, du programmeur de modèles, des cartes, de l'IPAM, des capteurs, de l'orchestration/du workflow/de la planification, de l'intégration ISE, etc.

L'état du pod d'inventaire peut être vérifié en exécutant la commande :

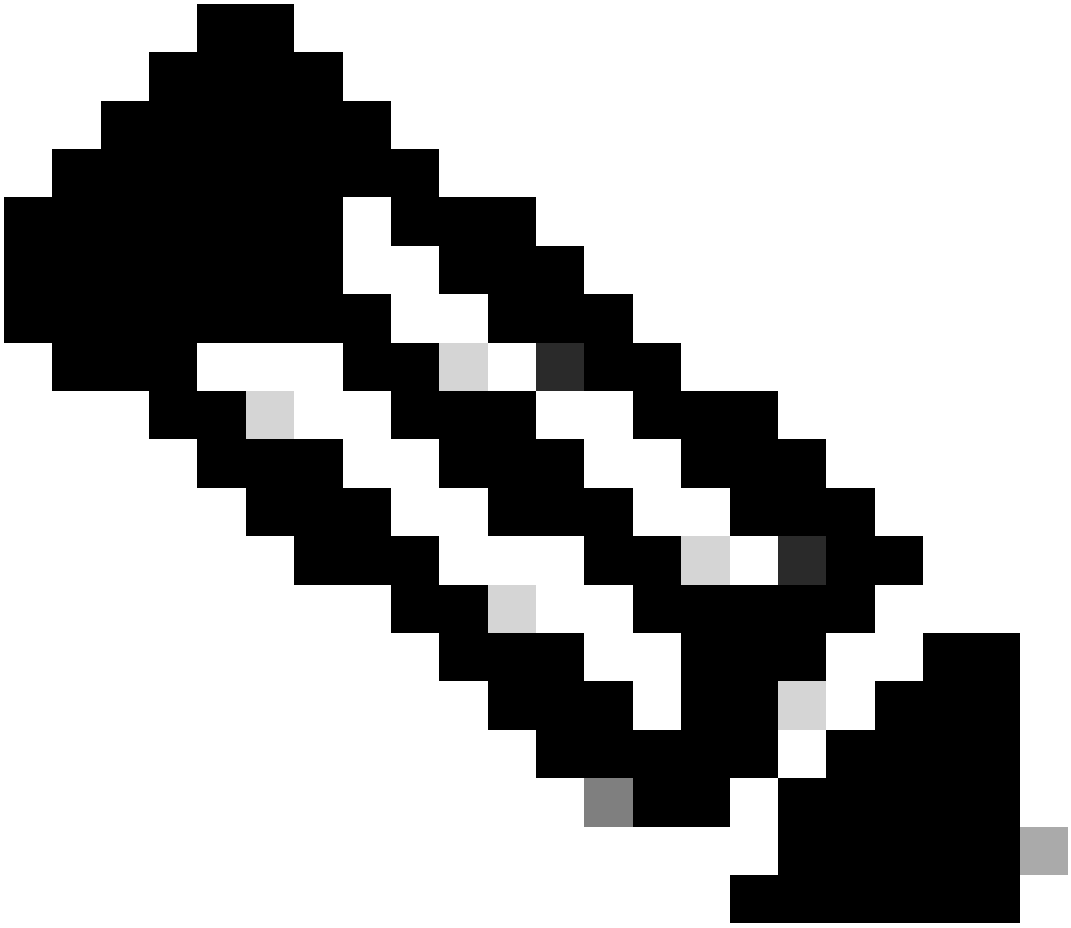
```
$ magctl appstack status | grep inventory
```

L'état du service d'inventaire peut être vérifié avec la commande :

```
$ magctl service status
```

Les journaux de service d'inventaire peuvent être vérifiés à l'aide de la commande :

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



Remarque : Le service d'inventaire peut également consister en deux pod en cours d'exécution. Vous devez donc spécifier un pod unique dans les commandes en utilisant le nom complet du pod d'inventaire, y compris l'ID du pod.

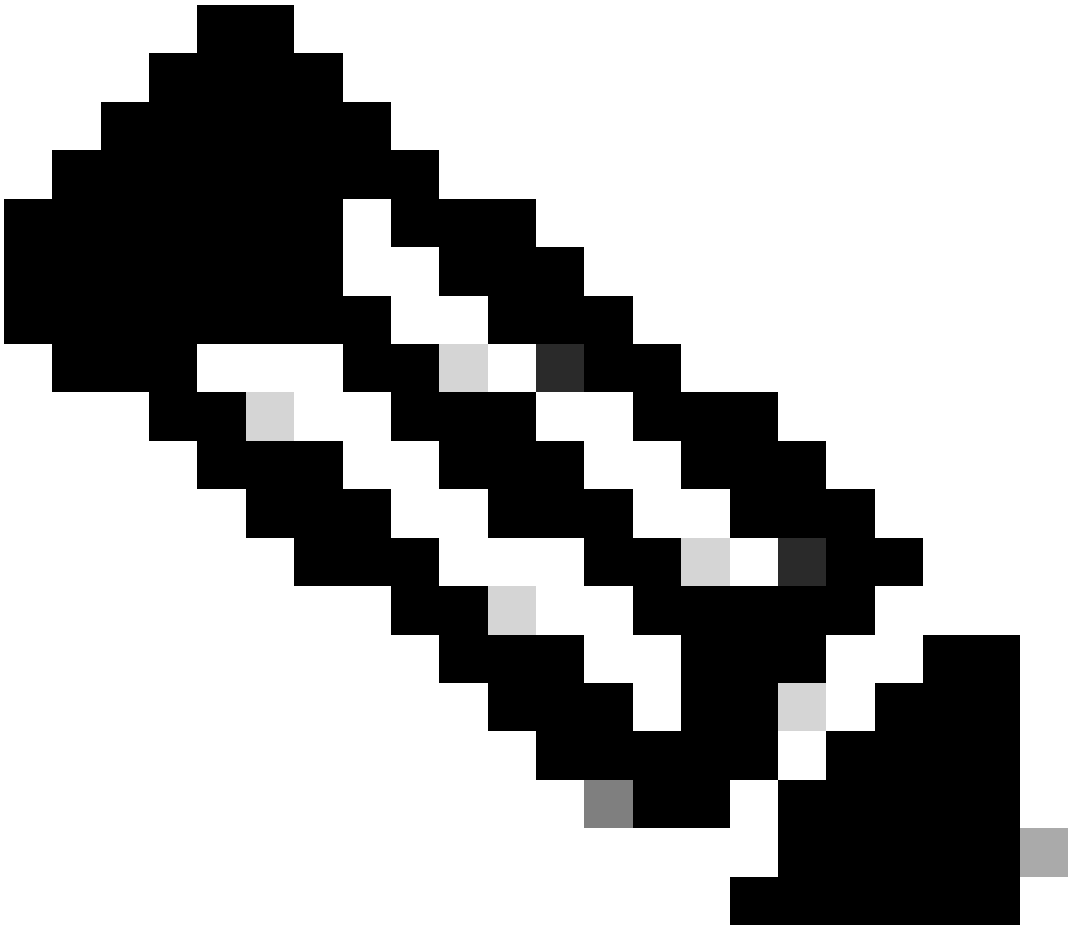
Dans ce document, nous pouvons nous concentrer sur l'état de gestion et de dernière synchronisation des périphériques d'inventaire pour examiner les problèmes courants :

État de gérabilité

- Icône de coche verte gérée : Le périphérique est accessible et entièrement géré.
- Icône d'erreur orange gérée : Le périphérique est géré avec des erreurs telles que inaccessible, échec d'authentification, ports Netconf manquants, erreur interne, etc. Vous pouvez placer le curseur sur le message d'erreur pour afficher plus de détails sur l'erreur et les applications affectées.
- Non géré : Le périphérique est inaccessible et aucune information d'inventaire n'a été collectée en raison de problèmes de connectivité du périphérique.

Dernier état de synchronisation

- Géré : Le périphérique est dans un état entièrement géré.
- Échec de la collecte partielle : L'état du périphérique est partiellement collecté et toutes les informations d'inventaire n'ont pas été collectées. Placez le curseur sur l'icône Informations (i) pour afficher des informations supplémentaires sur l'échec.
- Inaccessible : Le périphérique est inaccessible et aucune information d'inventaire n'a été collectée en raison de problèmes de connectivité du périphérique. Cette condition se produit lorsque la collecte périodique a lieu.
- Informations d'identification incorrectes : Si les informations d'identification du périphérique sont modifiées après l'ajout du périphérique à l'inventaire, cette condition est notée.
- En cours : Collecte d'inventaire en cours.



Remarque : Pour plus d'informations sur les fonctions d'inventaire dans Cisco DNA

Center, consultez le guide officiel de la version 2.3.5.x : Gérer votre inventaire

Problèmes

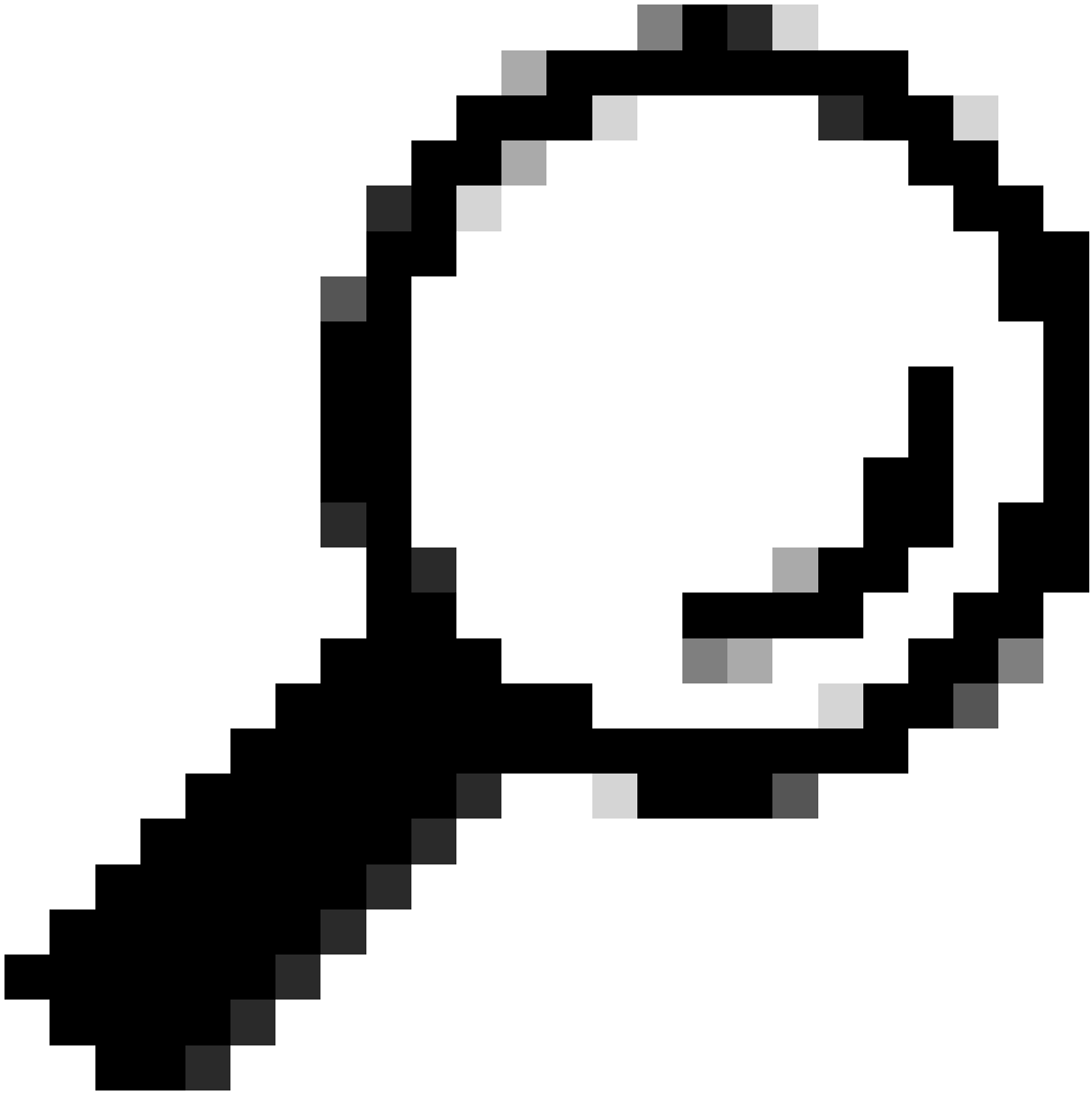
Internal Error

La page d'inventaire de Cisco DNA Center peut afficher un message d'avertissement dans l'état de gérabilité pour les périphériques présentant un type de conflit empêchant la collecte de données :

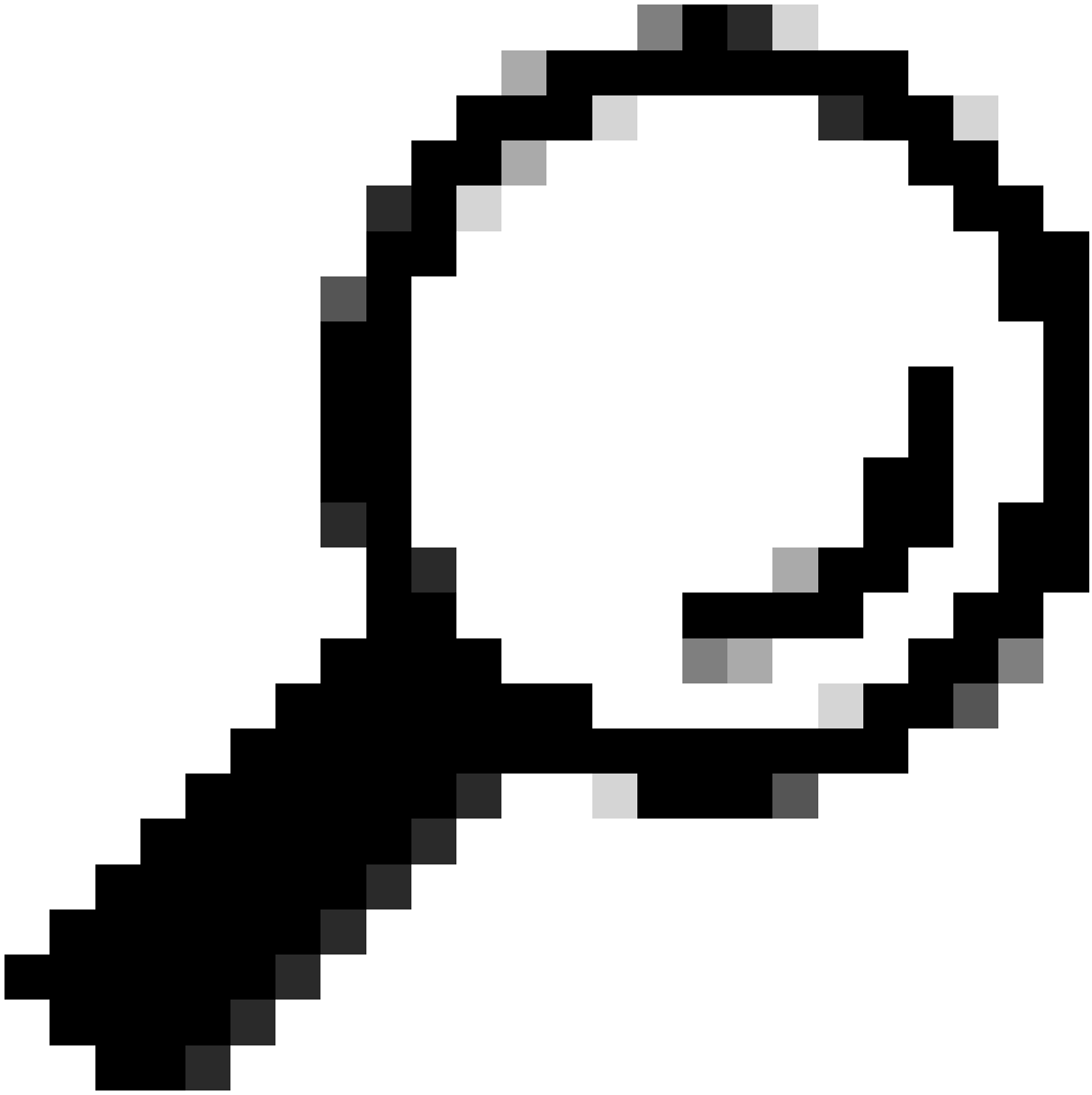
"Erreur interne : NCIM12024 : Toutes les informations du périphérique n'ont pas pu être collectées correctement ou la collecte d'inventaire pour ce périphérique n'a pas encore commencé. Il peut s'agir d'un problème temporaire pouvant être résolu automatiquement. Resynchronisez le périphérique. Si cela ne résout pas le problème, contactez le TAC Cisco."

Si l'erreur ne se résout pas automatiquement ou après une resynchronisation du périphérique, nous pouvons commencer par le dépannage initial. Cette erreur peut être due à plusieurs raisons, mais ici, nous énumérons quelques-unes des plus courantes :

- Identifiants de périphérique incorrects pour SNMP, SSH et Netconf.
- Problèmes de connectivité réseau liés à SNMP, SSH et Netconf.
- Des problèmes de configuration Netconf dans le périphérique provoquent un dysfonctionnement de Netconf.
- Déclenchez la resynchronisation d'un périphérique alors qu'elle est déjà en cours.
- Plusieurs déroutements ont été reçus du périphérique, entraînant plusieurs déclencheurs de resynchronisation en peu de temps.
- Problèmes de back-end avec les entrées de la base de données d'inventaire dans plusieurs tables liées au périphérique.



Conseil : Le retrait du périphérique réseau et sa nouvelle détection à l'aide de l'interface de ligne de commande appropriée, des identifiants SNMP et NETCONF peuvent aider à supprimer les entrées de base de données périmées qui pourraient être à l'origine de l'erreur interne.



Conseil : L'examen des journaux de service d'inventaire et le filtrage par IP de périphérique ou nom d'hôte peuvent être utiles pour identifier la cause première de l'erreur interne.

Identifiants des périphériques

Pour vérifier les informations d'identification des périphériques, accédez au menu Cisco DNA Center -> Provisionner -> Inventaire -> Sélectionner un périphérique -> Actions -> Inventaire -> Modifier un périphérique et cliquez sur "Valider" et vérifiez que les informations d'identification obligatoires (CLI et SNMP) sont validées par une coche verte (y compris netconf si elle s'applique).

Si la validation échoue, vérifiez que le nom d'utilisateur et le mot de passe que Cisco DNA Center utilise pour gérer le périphérique réseau sont valides directement dans la ligne de commande du

périphérique.

S'ils sont configurés localement ou s'ils sont configurés dans un serveur AAA (TACACS ou RADIUS), vérifiez que le nom d'utilisateur et le mot de passe sont correctement configurés dans le serveur AAA.

Vérifiez également si le privilège de nom d'utilisateur nécessite la configuration du mot de passe "Enable" dans les paramètres d'identification du périphérique dans Cisco DNA Csaisissez Stock.

Les erreurs dans les informations d'identification CLI peuvent entraîner un message d'erreur de gérabilité dans l'inventaire : Échec de l'authentification CLI.

Netconf

Netconf est un protocole permettant de gérer à distance un périphérique réseau compatible via les appels de procédure distante (RPC).

Cisco DNA Center utilise les fonctionnalités Netconf pour pousser ou supprimer la configuration sur les périphériques réseau afin d'activer des fonctionnalités telles que la surveillance via Assurance.

L'inventaire Cisco DNA Center peut également valider que les exigences Netconf sont correctes, ce qui inclut :

- Le port par défaut 830 de la commande Netconf doit être ouvert et fonctionnel sur le réseau.
- Utilisateur disposant du privilège 15 avec accès SSH au périphérique réseau (configuré localement ou AAA).
- Activez Netconf dans le périphérique réseau :

<#root>

(config)#

netconf-yang

- Si aaa new-model est activé, vous devez également configurer les exigences des paramètres AAA par défaut :

<#root>

(config)#

aaa authorization exec default

(config)#

```
aaa authentication login default
```

Les erreurs dans les informations d'identification Netconf peuvent entraîner un message d'erreur de gérabilité dans Inventory : Échec de la connexion Netconf.

Contrôles réseau

Nous pouvons également valider les paramètres de connectivité réseau et de protocoles, tels que les paramètres SNMP, en fonction de la version.

Par exemple, nous pouvons vérifier les paramètres de communauté, d'utilisateur, de groupe, d'ID de moteur, d'authentification et de cryptage, etc. en fonction de la version SNMP.

Nous pouvons également examiner la connectivité SSH et SNMP en utilisant les commandes ping et traceroute dans la ligne de commande du périphérique et les ports pour SSH (22) et SNMP (161 et 162) dans le pare-feu, le proxy ou les listes d'accès.

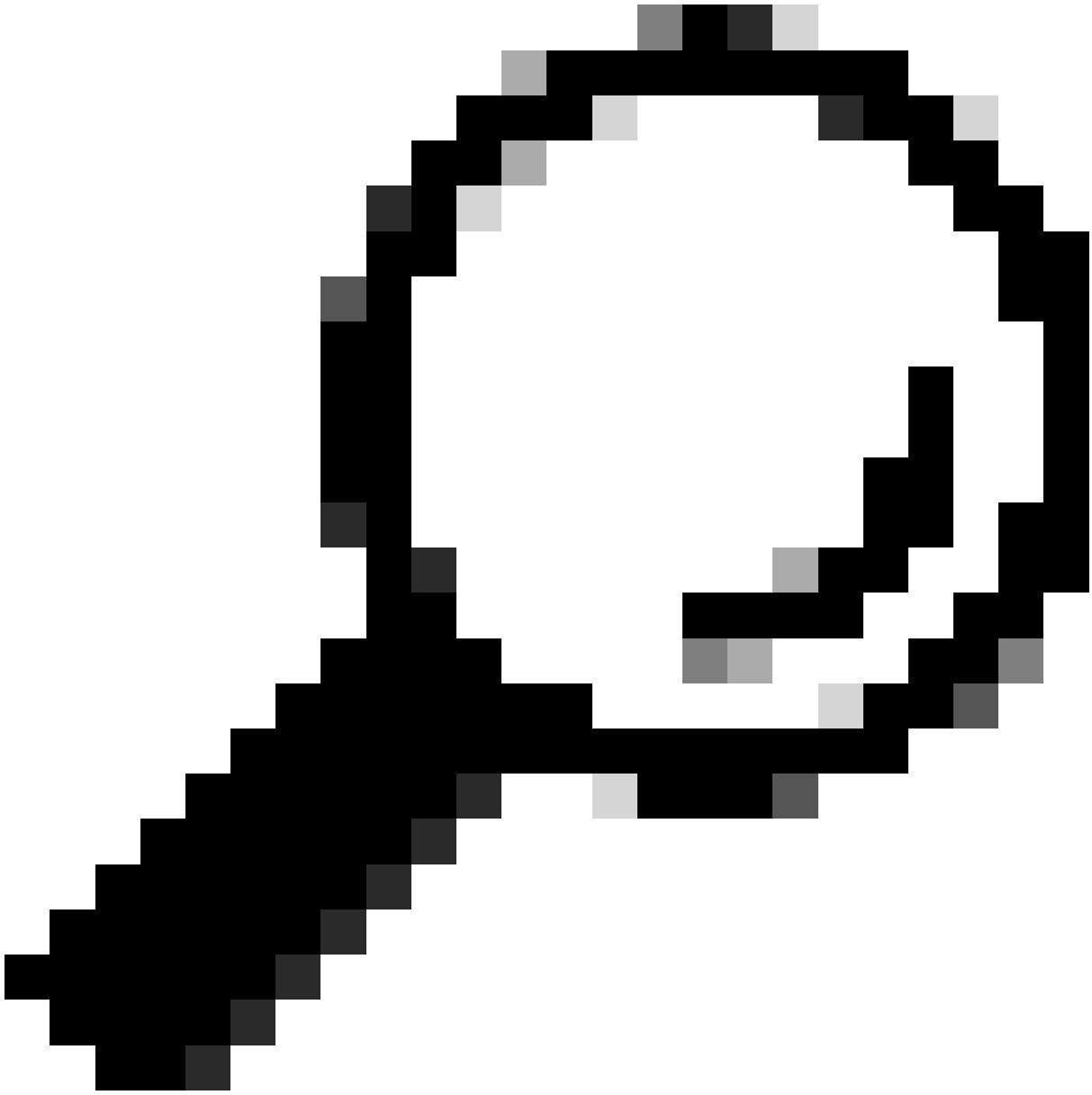
À partir de Cisco DNA Center, maglev CLI, nous utilisons les commandes ip route pour valider la connectivité au périphérique réseau.

La marche SNMP peut également être utilisée pour le dépannage.

Les erreurs dans les informations d'identification SNMP peuvent entraîner un message d'erreur de gérabilité dans l'inventaire : Échec de l'authentification SNMP ou périphérique inaccessible.

Tables de base de données

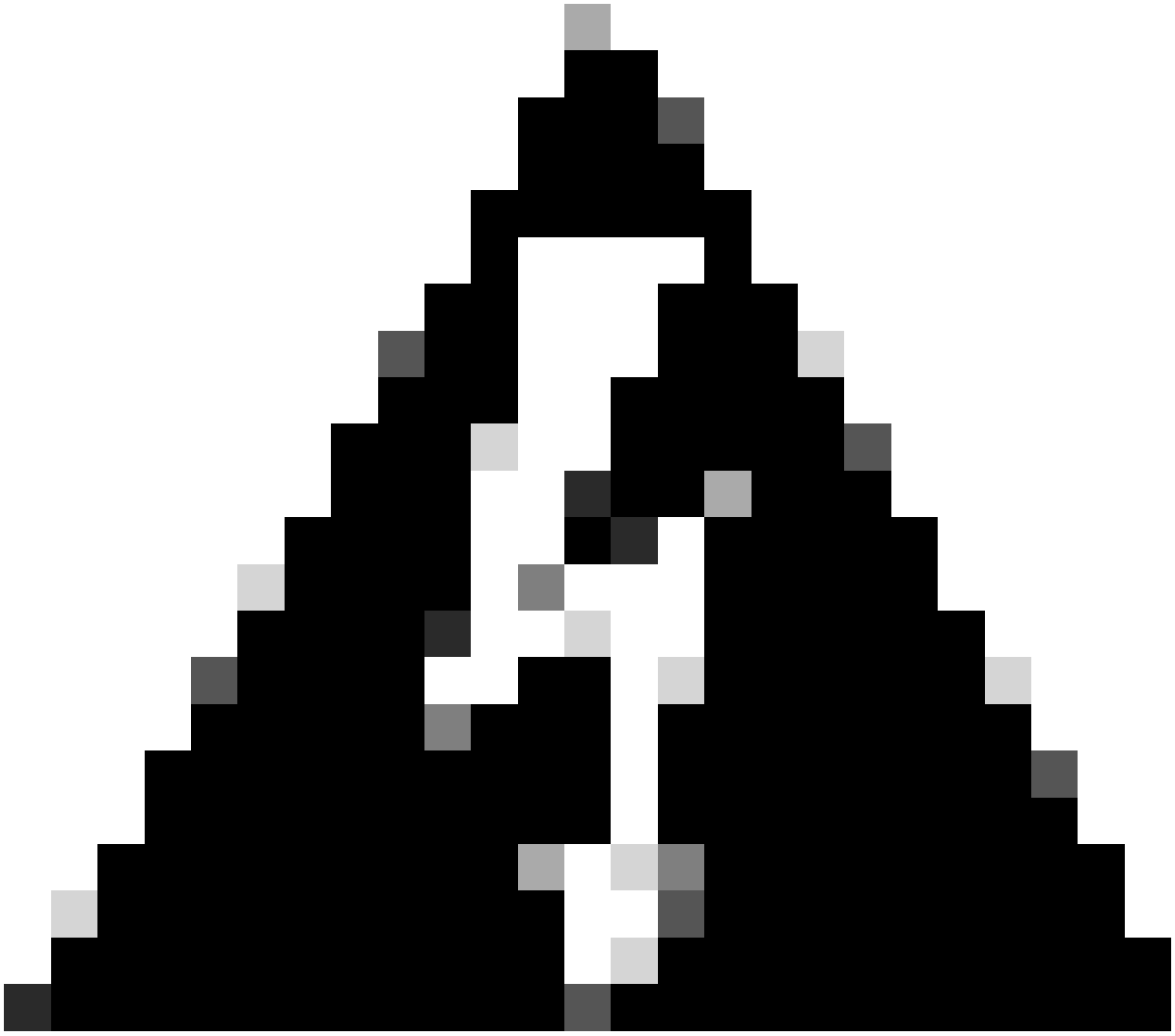
En tant qu'utilisateur final, vous pouvez utiliser l'interface graphique de Cisco DNA Center avec Grafana pour exécuter des requêtes SQL afin de ne pas avoir besoin d'accéder à l'interpréteur de commandes Postgres via maglev CLI.



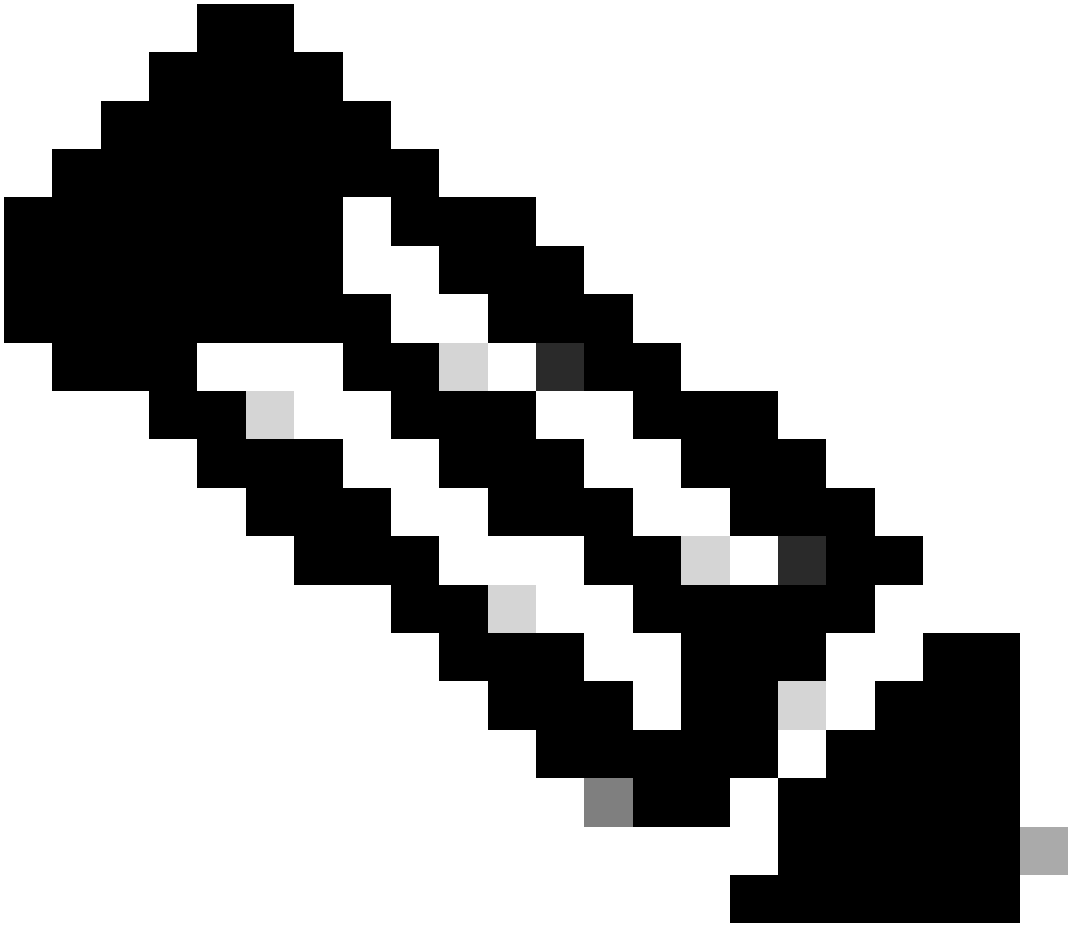
Conseil : Si vous souhaitez apprendre à utiliser Grafana, consultez le guide officiel : [Execute Postgres Queries in Cisco DNA Center GUI]

Voici quelques tables de base de données postgres à consulter en cas de problèmes avec les périphériques réseau dans l'inventaire :

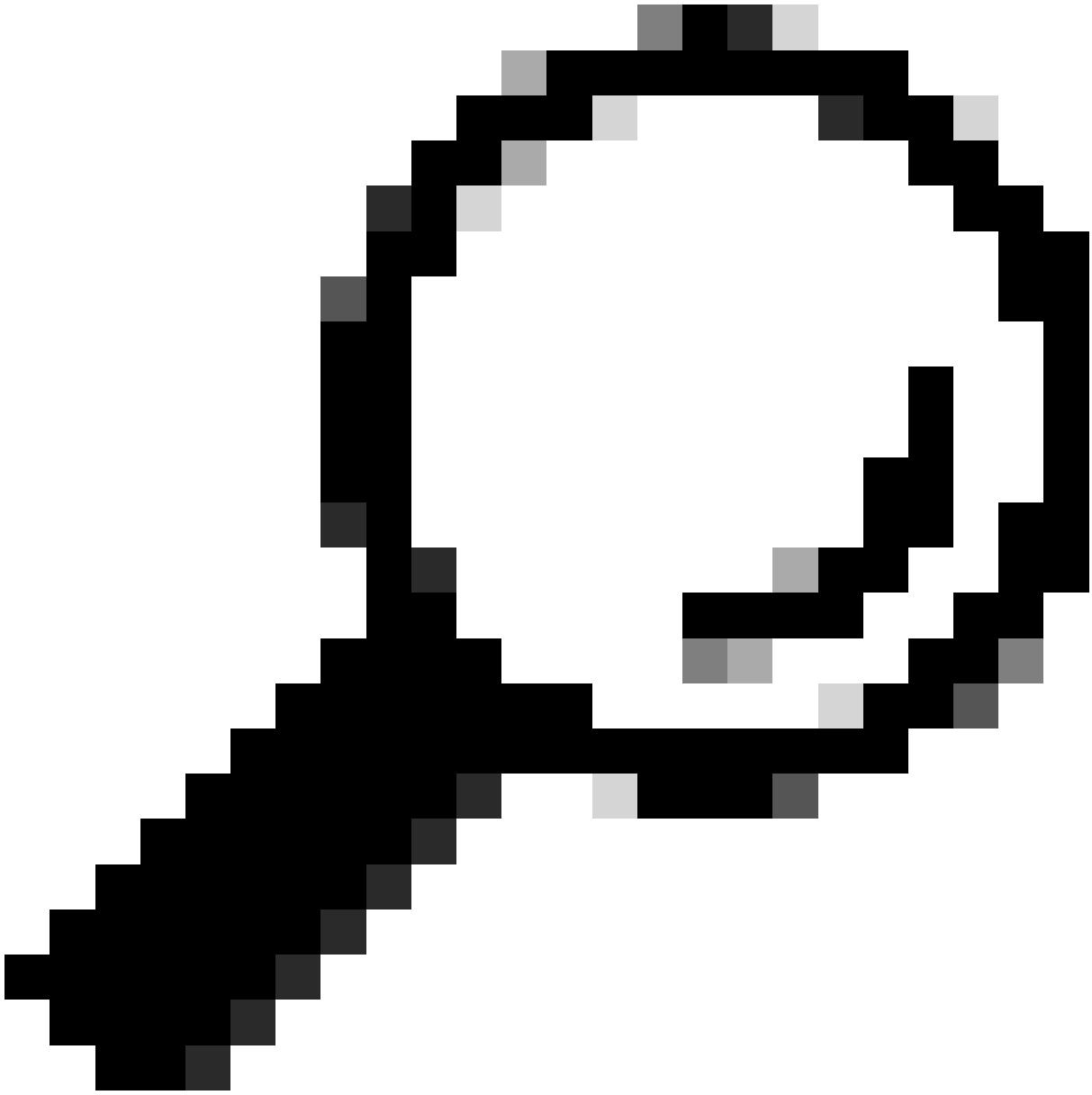
- périphérique réseau
- interface d'élément géré
- élément de réseau
- ressource du réseau
- appareil
- adresse IP



Avertissement : Seul le TAC Cisco est autorisé à exécuter des requêtes show dans l'interpréteur de commandes Postgres et seules les équipes BU/DE sont autorisées à apporter des modifications aux tables DB.



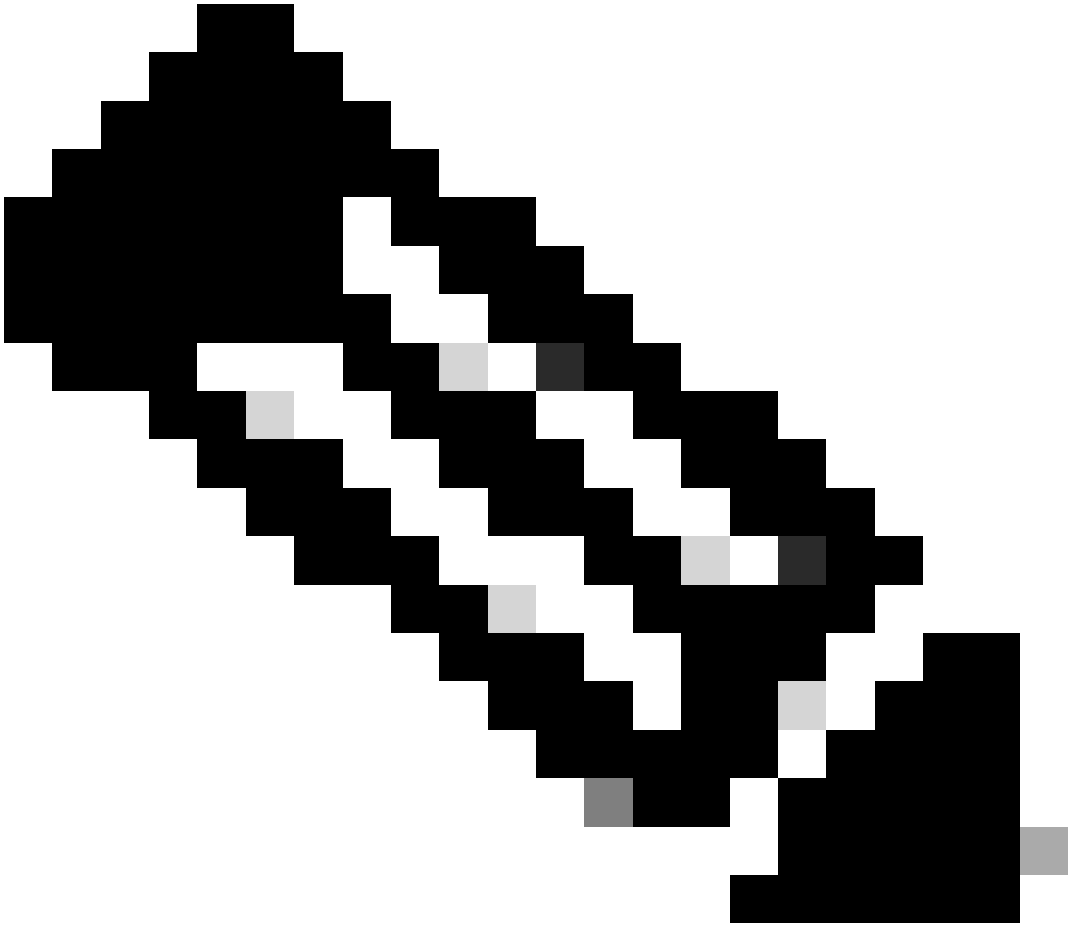
Remarque : Les problèmes de base de données peuvent également entraîner le message d'erreur interne pour les périphériques, ce qui peut empêcher la collecte de données et le provisionnement des périphériques.



Conseil : Vous pouvez consulter les journaux Postgres à l'aide de Kibana dans la page Cisco DNA Center System 360 et rechercher des violations de contraintes lorsque le service d'inventaire tente d'enregistrer ou de mettre à jour des entrées dans les tables de base de données Postgres.

Boucle et déroutements de synchronisation

Cisco DNA Center est conçu pour exécuter un périphérique Resycn chaque fois qu'il reçoit un déroutement du périphérique après une modification majeure effectuée dans le périphérique lui-même afin de maintenir l'inventaire Cisco DNA Center à jour. Parfois, la page d'inventaire Cisco DNA Center garde vos périphériques réseau dans l'état "Synchronisation" dans la section Facilité de gestion pendant une longue période ou pour toujours.



Remarque : Ce type de boucles de synchronisation dues à des déroutements massifs peut entraîner l'authentification de Cisco DNA Center plusieurs fois en un court laps de temps aux périphériques qui envoient les déroutements en raison des modifications détectées.

API pour forcer la synchronisation des périphériques

Si votre périphérique réseau conserve l'état Synchronisation trop longtemps, voire plusieurs jours, vérifiez d'abord les vérifications de base de l'accessibilité et de la connectivité. Forcez ensuite la resynchronisation du périphérique via l'appel API :

1.- Ouvrez la session Cisco DNA Center maglev CLI.

2.- Obtenez le jeton d'authentification Cisco DNA Center via l'API :

<#root>

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

3.- Utilisez le jeton de l'étape précédente pour exécuter l'API pour forcer la synchronisation du périphérique :

<#root>

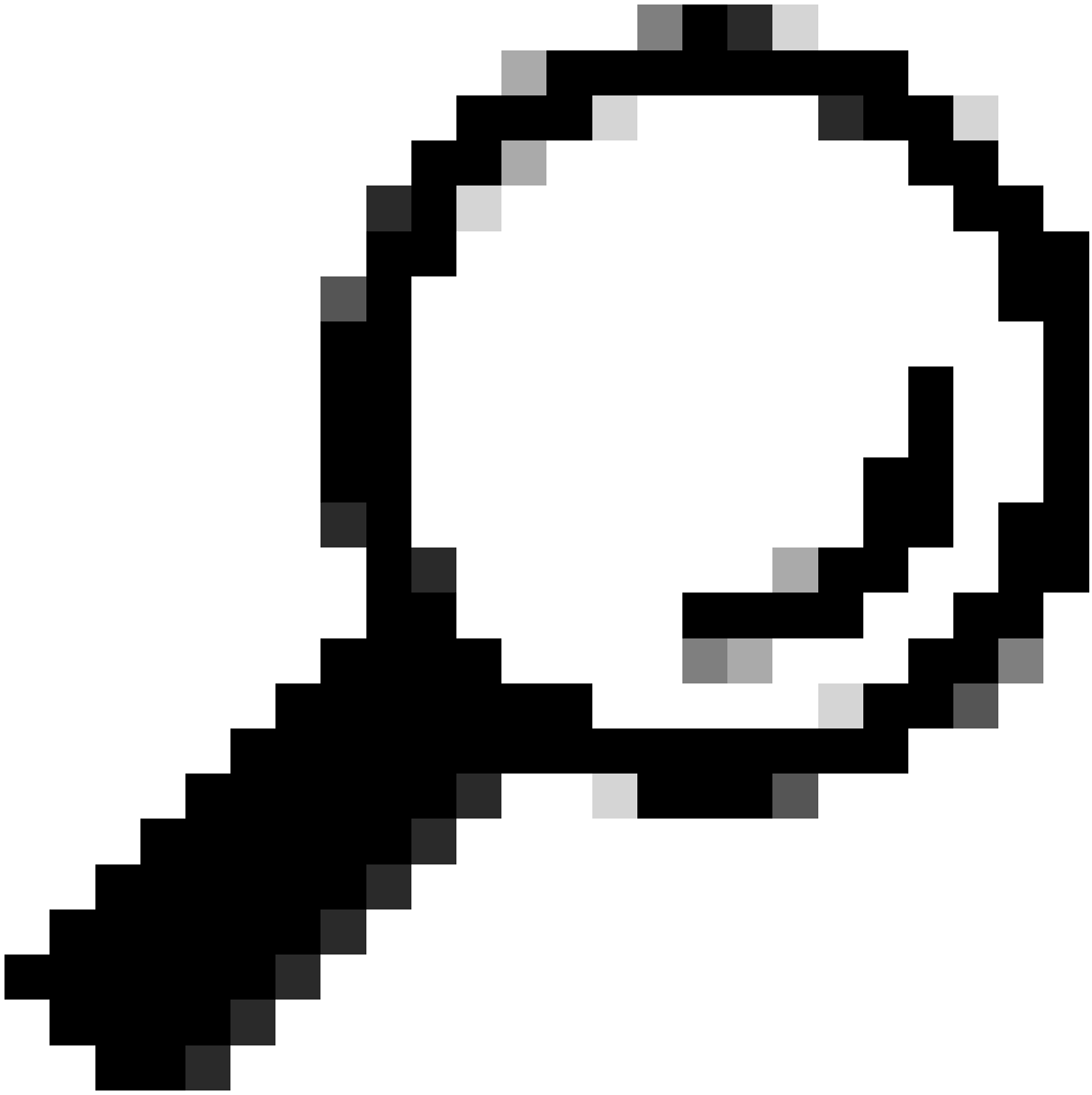
curl -X PUT -H "X-AUTH-TOKEN:

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

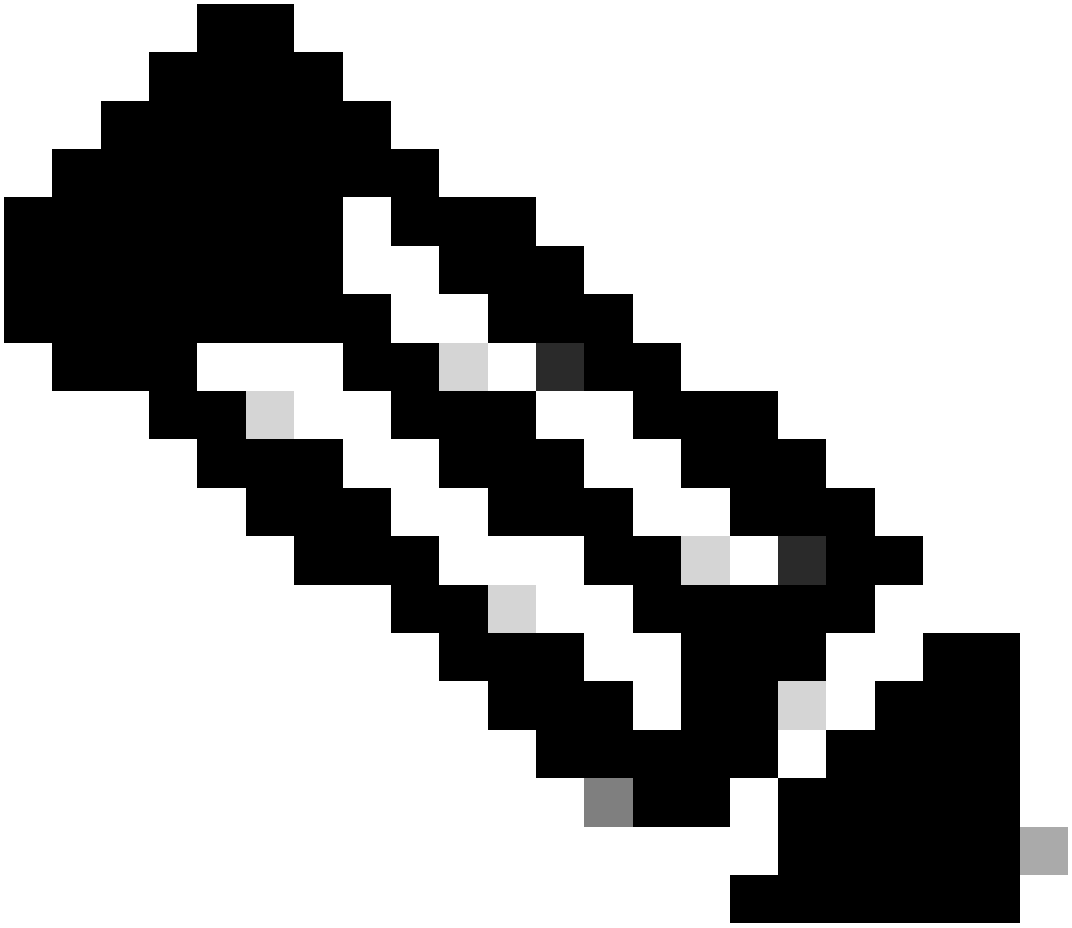
' https://

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

4.- Vous pouvez voir le périphérique dans Synchronisation une fois de plus, mais cette fois avec une option Force Sync via l'API.



Conseil : Vous pouvez obtenir l'uuid du périphérique à partir de l'URL du navigateur (deviceid ou id) à partir de la page Cisco DNA Center Inventory Device Details ou de la page Device View 360.



Remarque : Pour plus d'informations sur les API dans Cisco DNA Center, consultez le Guide des API de Cisco DevNet

Vérifier les déroutements

Si le problème persiste après avoir forcé la tâche de synchronisation dans le périphérique, nous pouvons vérifier si le "service d'événements" Cisco DNA Center reçoit trop de déroutements et vérifier quel type de déroutements en lisant les journaux de service d'événements :

1.- Avant de lire les journaux, il suffit de vérifier le nombre total de déroutements à l'aide de la commande :

<#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.- Ensuite, nous attachons au conteneur event-service :

<#root>

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

3.- Une fois que vous êtes entré dans le conteneur event-service, changez de répertoire pour le dossier logs :

<#root>

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

4.- Si vous examinez les fichiers à l'intérieur du répertoire, vous pouvez voir certains fichiers journaux dont le nom commence par "ncs".

Exemple :

<#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.- Ces fichiers "ncs" sont ceux dont nous avons besoin pour analyser le type de pièges que nous recevons et combien. Nous pouvons examiner les fichiers journaux en les filtrant par nom d'hôte du périphérique ou par le mot clé « 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

Il y a trop de types d'interruptions, certaines peuvent déclencher la resynchronisation du périphérique et si elles arrivent trop souvent, elles peuvent provoquer la boucle de synchronisation.

En analysant les déroutements, nous pouvons identifier la cause première et faire en sorte que les déroutements s'arrêtent, par exemple un AP dans un cycle de redémarrage.

Vous pouvez enregistrer le résultat des déroutements dans un fichier et les partager avec l'équipe de remontée si nécessaire.

État de blocage du service

Si vous pensez que le pod d'inventaire tombe en panne en raison d'un comportement étrange dans la page d'inventaire de Cisco DNA Center lors de la gestion des périphériques réseau, vous pouvez d'abord valider l'état du pod :

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

En examinant le résultat de l'état de la zone, si vous voyez un nombre élevé de redémarrages ou un état d'erreur, vous pouvez attacher au conteneur d'inventaire et collecter le fichier de vidage de

la pile qui peut avoir les données qui peuvent aider l'équipe de remontée d'urgence à analyser et définir la cause première de l'état de blocage :

<#root>

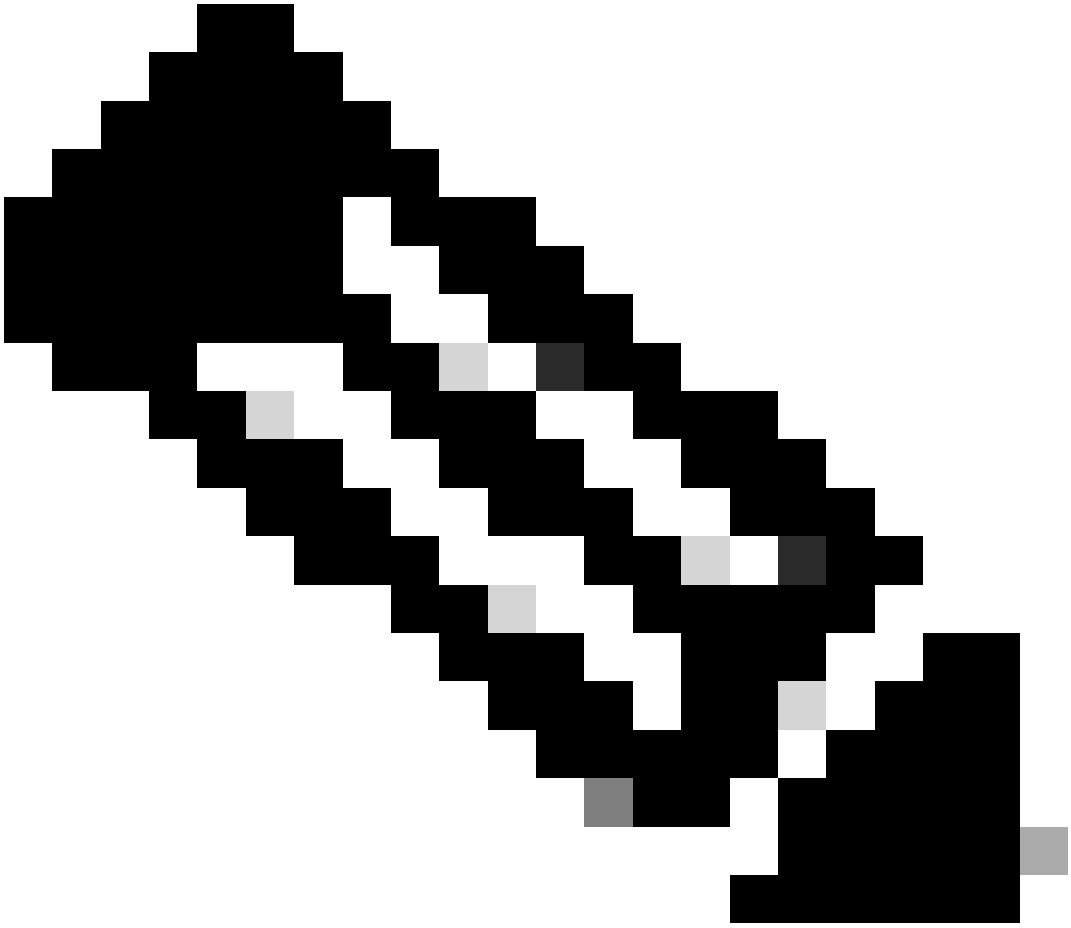
$ magctl service attach -D

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



Remarque : Si aucun fichier heapdump n'a été trouvé dans le répertoire du conteneur, alors aucun état de blocage n'était présent dans le conteneur.

Impossible de supprimer un périphérique

Dans certaines situations, Cisco DNA Center peut ne pas être en mesure de supprimer un périphérique réseau de l'interface utilisateur d'inventaire en raison d'un problème de back-end.

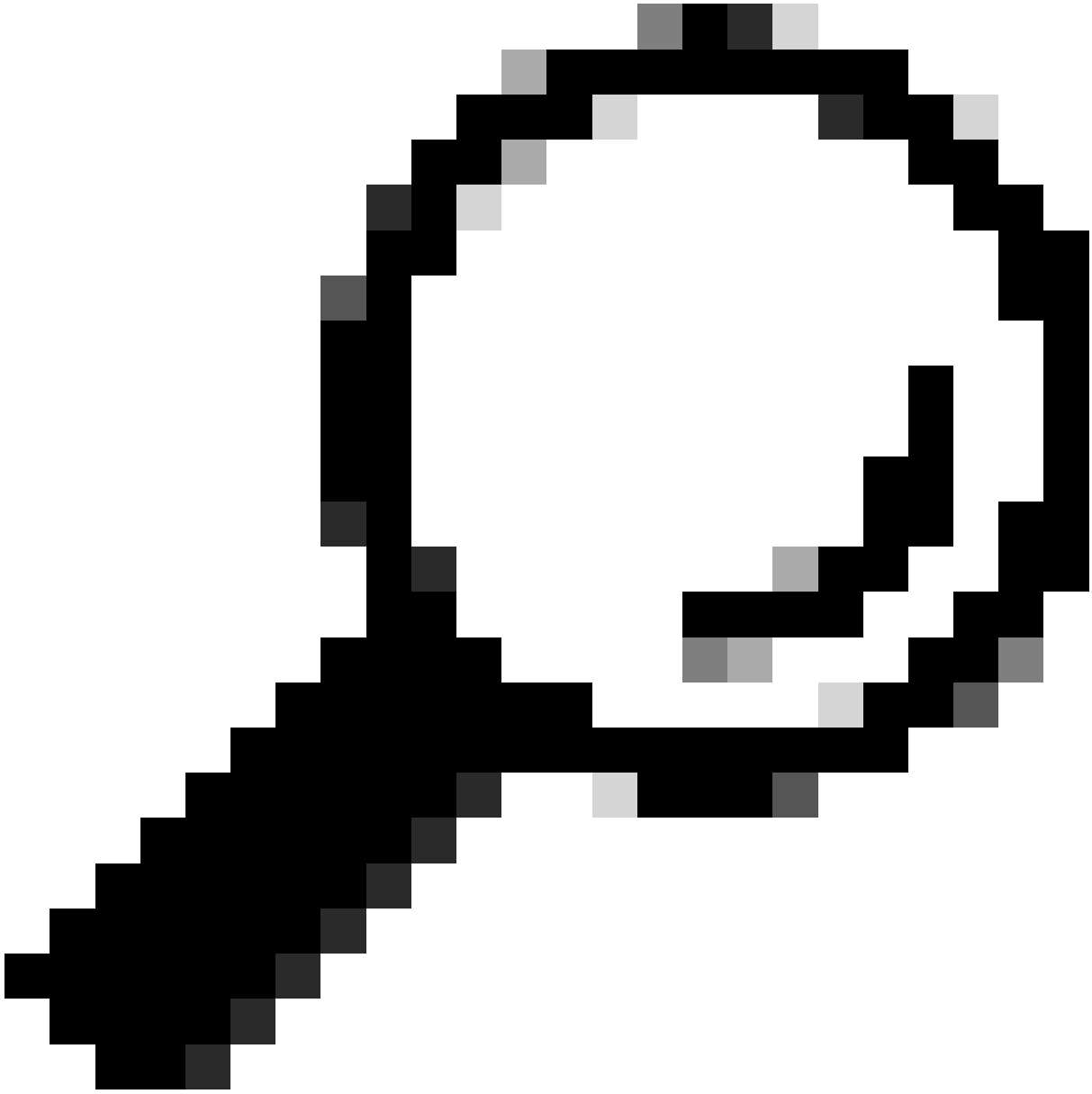
API pour forcer la suppression du périphérique

Si vous ne parvenez pas à supprimer le périphérique de l'inventaire à l'aide de l'interface utilisateur graphique de Cisco DNA Center, vous pouvez utiliser l'API pour supprimer le périphérique par ID :

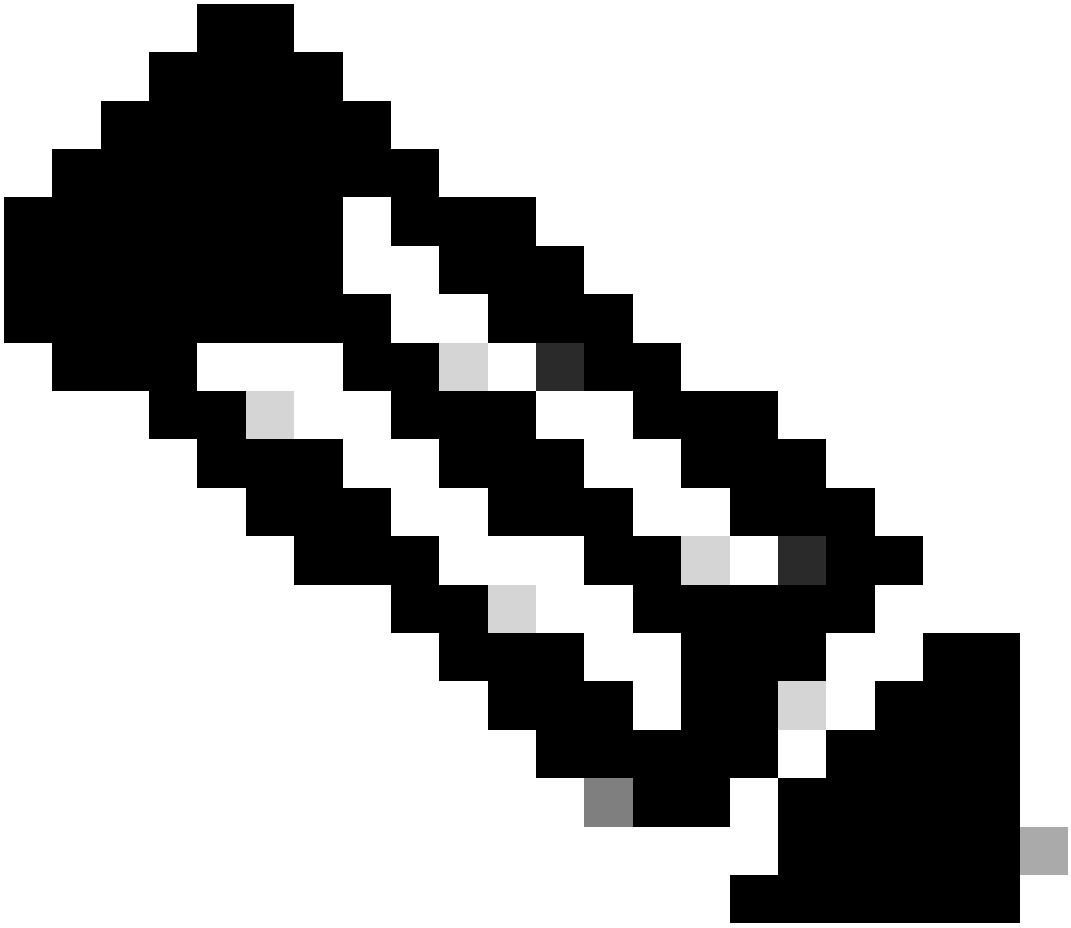
1.- Accédez au menu Cisco DNA Center -> Plate-forme -> Developer Toolkit -> onglet API et recherchez Devices dans la barre de recherche. À partir des résultats, cliquez sur Devices dans la section Know your network et recherchez l'API DELETE by Device Id.

2.- Cliquez dans l'API DELETE by Device Id, cliquez sur Try et fournissez l'ID du périphérique souhaité à supprimer de l'inventaire.

3.- Attendez que l'API s'exécute et obtenez une réponse 200 OK, puis vérifiez que le périphérique réseau n'est plus présent dans la page d'inventaire.



Conseil : Vous pouvez obtenir l'uuid du périphérique à partir de l'URL du navigateur (deviceid ou id) à partir de la page Cisco DNA Center Inventory Device Details ou de la page Device View 360.



Remarque : Pour plus d'informations sur les API dans Cisco DNA Center, consultez le Guide des API de Cisco DevNet

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.