Esaminare il servizio di inventario di DNA Center e i problemi comuni

Sommario

Introduzione

Questo documento descrive i concetti base del servizio Cisco DNA Center Inventory e i problemi comuni riscontrati nella produzione.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Dettagli servizio di inventario

Il servizio Cisco DNA Center Inventory è basato su un Pod Kubernetes (K8s) che è possibile eseguire nello spazio dei nomi "fusion" con il nome "apic-em-inventory-manager-service-<id>" come tipo di ambiente di distribuzione.

All'interno del pod K8s, è possibile trovare un contenitore Docker chiamato "apic-em-inventory-manager-service".

Le attività principali del pod "apic-em-inventory-manager-service" sono: rilevamento dei dispositivi e gestione del ciclo di vita dei dispositivi.

In questo modo i dati dei dispositivi saranno disponibili in Postgres SQL (database utilizzato dai servizi Fusion).

Lo spazio dei nomi "fusion" (Appstack), noto anche come NCP (Network Controller Platform), fornisce i servizi SPF (Service Provisioning Framework) per tutti i requisiti di automazione della rete.

Tra questi vi sono discovery, inventario, topologia, policy, gestione delle immagini software (SWIM), archivio di configurazione, programmatore di rete, siti, raggruppamento, telemetria, integrazione Tesseract, programmatore di modelli, mappe, IPAM, sensori, orchestrazione/flusso di lavoro/pianificazione, integrazione ISE e simili.

È possibile controllare lo stato del pod di inventario eseguendo il comando:

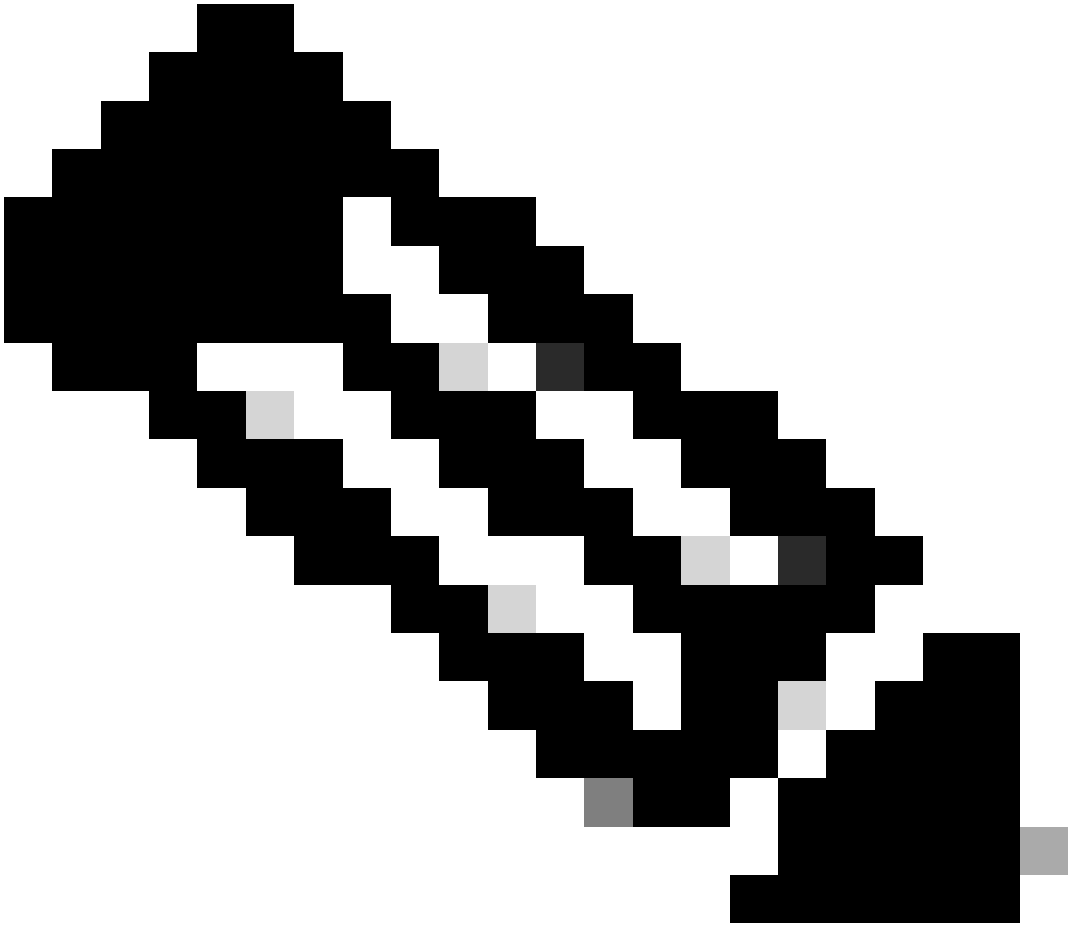
```
$ magctl appstack status | grep inventory
```

Per controllare lo stato del servizio di inventario, usare il comando:

```
$ magctl service status
```

I log del servizio di inventario possono essere controllati con il comando:

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



Nota: Il servizio di inventario può anche consistere in due pod in esecuzione, pertanto è necessario specificare un singolo pod nei comandi utilizzando il nome completo del pod di inventario, incluso l'id del pod.

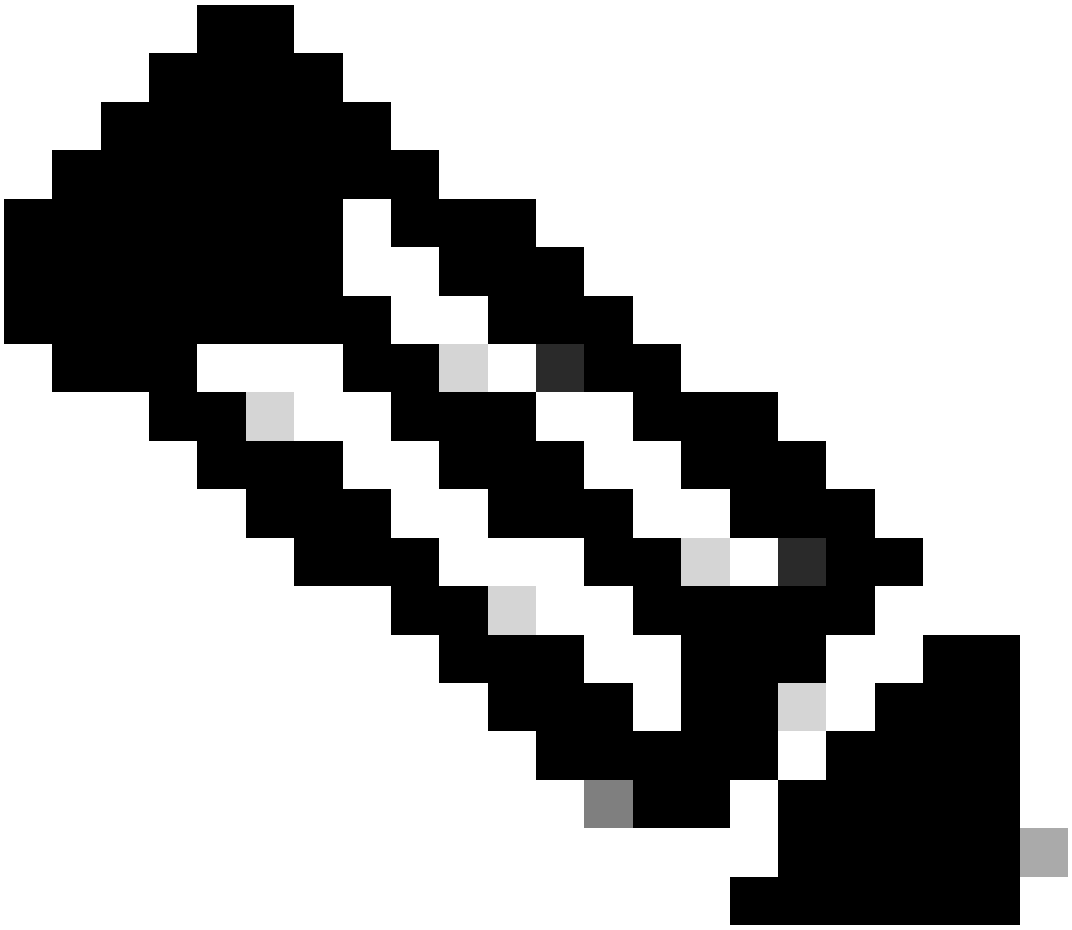
In questo documento è possibile esaminare i problemi comuni evidenziando la gestibilità dei dispositivi di inventario e lo stato Ultima sincronizzazione:

Stato gestibilità

- Gestito con l'icona di segno di spunta verde: Il dispositivo è raggiungibile e completamente gestito.
- Gestito con icona di errore arancione: Il dispositivo viene gestito con alcuni errori, ad esempio non raggiungibile, errore di autenticazione, porte Netconf mancanti, errore interno e così via. È possibile posizionare il cursore sul messaggio di errore per visualizzare ulteriori dettagli sull'errore e sulle applicazioni interessate.
- Non gestito: Impossibile raggiungere il dispositivo. Nessuna informazione di inventario raccolta a causa di problemi di connettività del dispositivo.

Stato ultima sincronizzazione

- Gestito: Dispositivo in stato completamente gestito.
- Errore di raccolta parziale: Il dispositivo è in uno stato di raccolta parziale e non tutte le informazioni di inventario sono state raccolte. Posizionare il cursore sull'icona Information (i) per visualizzare ulteriori informazioni sull'errore.
- Non raggiungibile: Impossibile raggiungere il dispositivo. Nessuna informazione di inventario raccolta a causa di problemi di connettività del dispositivo. Questa condizione si verifica quando viene eseguita la raccolta periodica.
- Credenziali errate: Se le credenziali del dispositivo vengono modificate dopo l'aggiunta del dispositivo all'inventario, questa condizione viene segnalata.
- In corso: È in corso la raccolta dell'inventario.



Nota: Per ulteriori informazioni sulle funzioni di inventario in Cisco DNA Center, consultare

---

la guida ufficiale alla versione 2.3.5.x: Gestione dell'inventario

Problemi

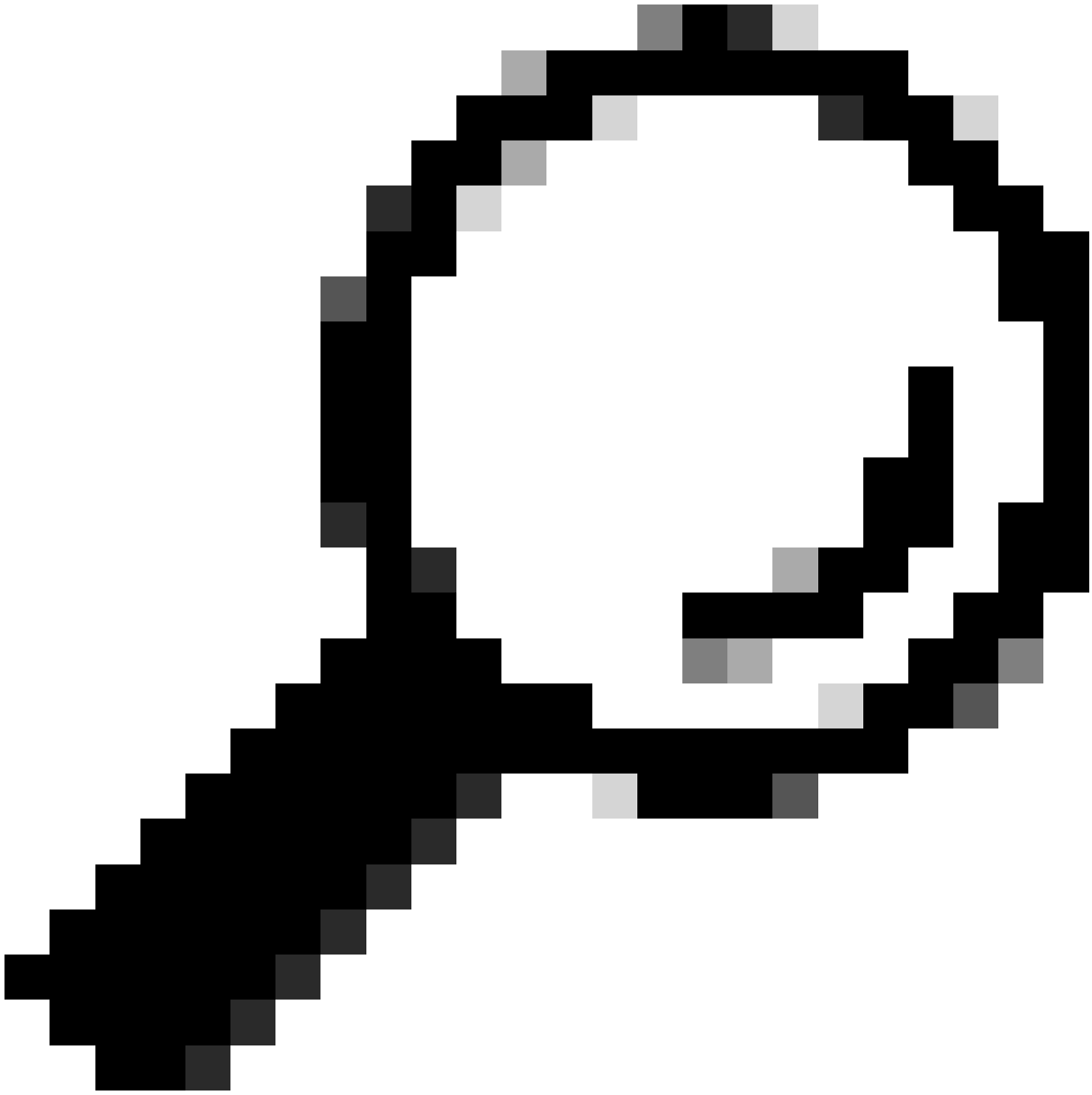
Errore interno

La pagina Inventario di Cisco DNA Center può visualizzare un messaggio di avviso nello stato di gestibilità per i dispositivi con un tipo di conflitto che impedisce la raccolta dei dati:

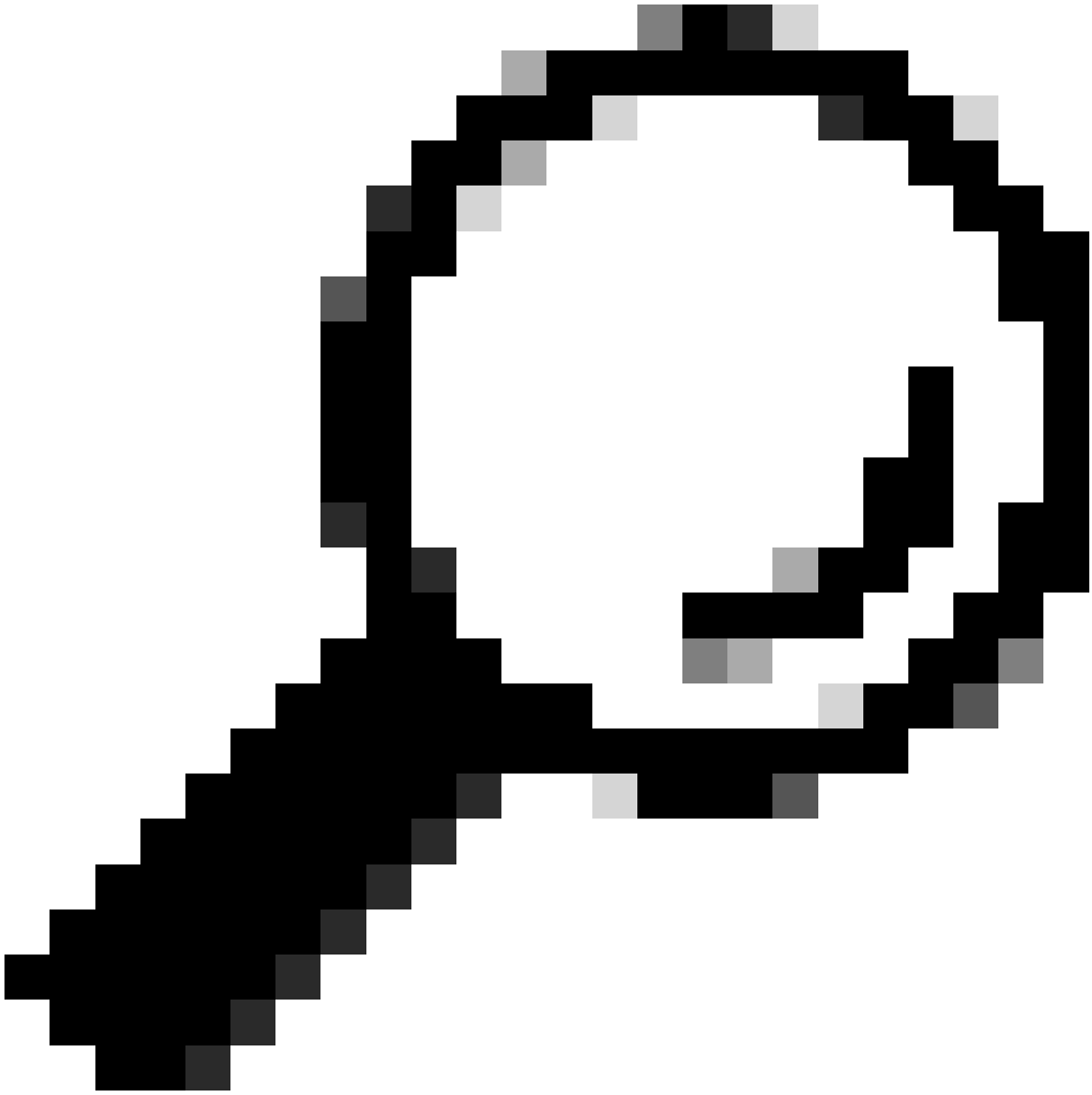
"Errore interno: NCIM12024: Impossibile raccogliere tutte le informazioni dal dispositivo oppure la raccolta dell'inventario per il dispositivo non è stata ancora avviata. Può trattarsi di un problema temporaneo che può essere risolto automaticamente. Risincronizzare il dispositivo. Se il problema persiste, contattare Cisco TAC."

Se l'errore non si risolve automaticamente o dopo la risincronizzazione di un dispositivo, è possibile iniziare con la risoluzione iniziale dei problemi. L'errore può essere dovuto a più motivi, ma qui vengono elencati solo alcuni dei più comuni:

- Credenziali del dispositivo non corrette per SNMP, SSH e Netconf.
- Problemi di connettività di rete relativi a SNMP, SSH e Netconf.
- Problemi di configurazione di Netconf nel dispositivo che causano il malfunzionamento di Netconf.
- Attiva la risincronizzazione di un dispositivo mentre è già in corso la sincronizzazione di un dispositivo.
- Sono state ricevute più trap dal dispositivo che hanno causato più trigger di risincronizzazione in un breve periodo di tempo.
- Problemi di back-end con voci del database di inventario in più tabelle correlate al dispositivo.



Suggerimento: La rimozione del dispositivo di rete e la sua individuazione tramite la CLI corretta, le credenziali SNMP e NETCONF possono contribuire a rimuovere le voci del database non aggiornate che potrebbero causare l'errore interno.



Suggerimento: L'analisi dei log del servizio di inventario e l'applicazione di un filtro in base all'indirizzo IP o al nome host del dispositivo possono essere utili per identificare la causa principale dell'errore interno.

Credenziali dispositivo

Per rivedere le credenziali del dispositivo, selezionare Cisco DNA Center Menu -> Provision -> Inventory -> Select Device -> Actions -> Inventory -> Edit Device (Centro Cisco DNA -> Provisioning e fare clic su "Validate" (Convalida) e confermare che le credenziali obbligatorie (CLI e SNMP) stiano superando la convalida con un controllo verde (incluso netconf, se applicabile).

Se la convalida non riesce, verificare che il nome utente e la password utilizzati da Cisco DNA Center per gestire il dispositivo di rete siano validi direttamente nella riga di comando del dispositivo.

Se sono configurati localmente o se sono configurati in un server AAA (TACACS o RADIUS), verificare che il nome utente e la password siano configurati correttamente nel server AAA.

Verificare inoltre se per il privilegio del nome utente è necessario configurare la password "Enable" nelle impostazioni delle credenziali del dispositivo in Cisco DNA Cinserire Inventory.

Gli errori nelle credenziali CLI possono causare un messaggio di errore di gestibilità in Inventory: Errore di autenticazione CLI.

Netconf

Netconf è un protocollo per la gestione remota di un dispositivo di rete compatibile tramite chiamate di procedura remota (RPC, Remote Procedure Call).

Cisco DNA Center utilizza le funzionalità Netconf per eseguire il push o rimuovere la configurazione sui dispositivi di rete per abilitare funzionalità quali il monitoraggio tramite Assurance.

Cisco DNA Center Inventory può anche convalidare la correttezza dei requisiti Netconf, che includono:

- La porta predefinita Netconf 830 deve essere aperta e funzionante nella rete.
- Utente con privilegio 15 e accesso SSH al dispositivo di rete (configurato localmente o con AAA).
- Abilitare Netconf nel dispositivo di rete:

<#root>

(config)#

netconf-yang

- Se è abilitato un nuovo modello, è necessario configurare anche i requisiti delle impostazioni predefinite AAA:

<#root>

(config)#

aaa authorization exec default

(config)#

aaa authentication login default

Errori nelle credenziali Netconf possono causare un messaggio di errore di gestibilità in Inventory: Errore di connessione Netconf.

Controlli di rete

Possiamo anche convalidare le impostazioni della connettività di rete e dei protocolli come le impostazioni SNMP a seconda della versione.

Ad esempio, è possibile verificare le impostazioni di community, utente, gruppo, engineID, autenticazione e crittografia e così via a seconda della versione SNMP.

Inoltre, è possibile esaminare la connettività SSH e SNMP utilizzando i comandi ping e traceroute nella riga di comando del dispositivo e le porte per SSH (22) e SNMP (161 e 162) negli elenchi di firewall, proxy o accessi.

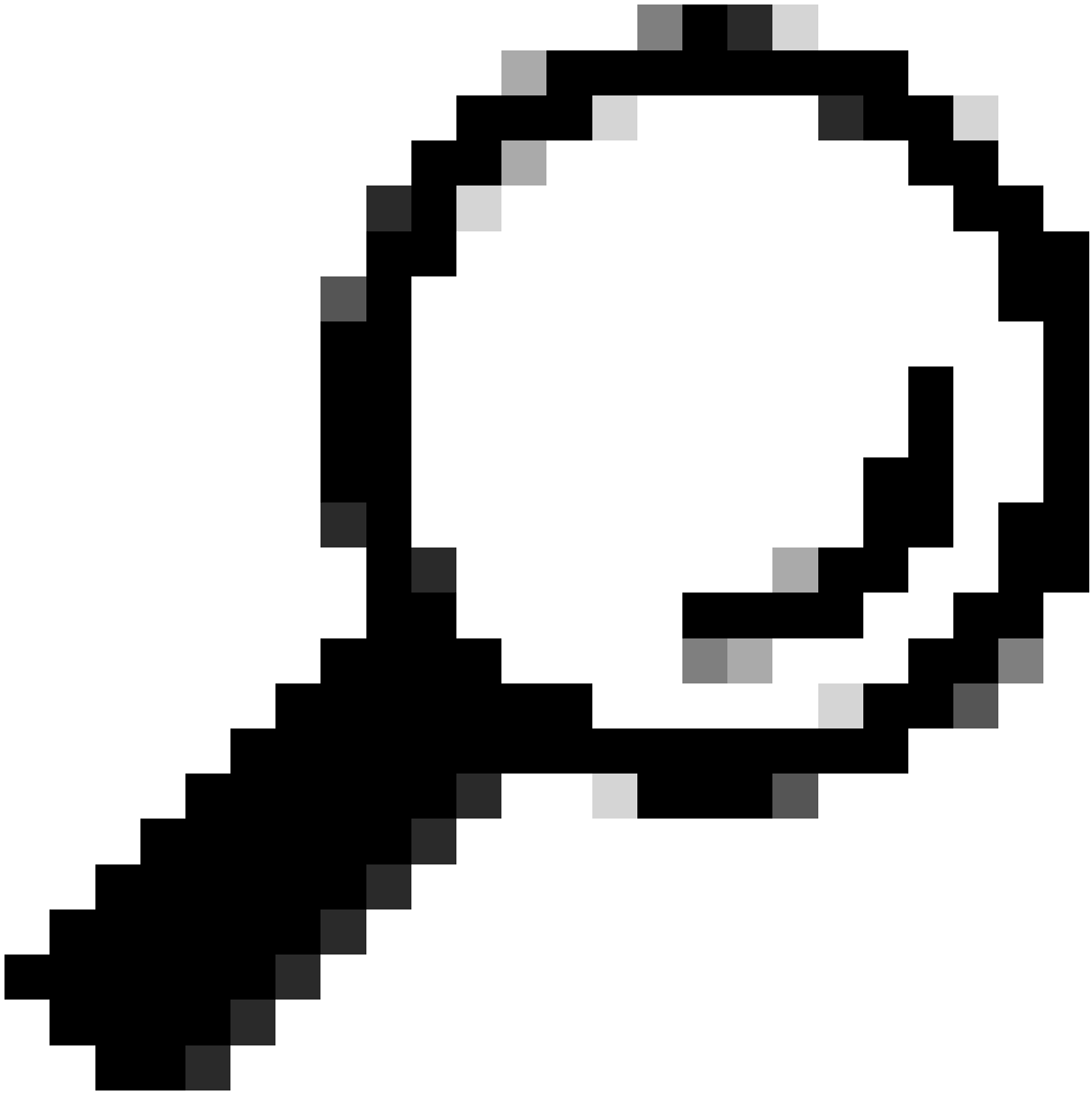
Da Cisco DNA Center, maglev CLI usa i comandi ip route per convalidare la connettività al dispositivo di rete.

Per la risoluzione dei problemi è inoltre possibile utilizzare SNMP Walk.

Gli errori nelle credenziali SNMP possono causare un messaggio di errore di gestibilità in Inventory: Errore di autenticazione SNMP o dispositivo non raggiungibile.

Tabelle di database

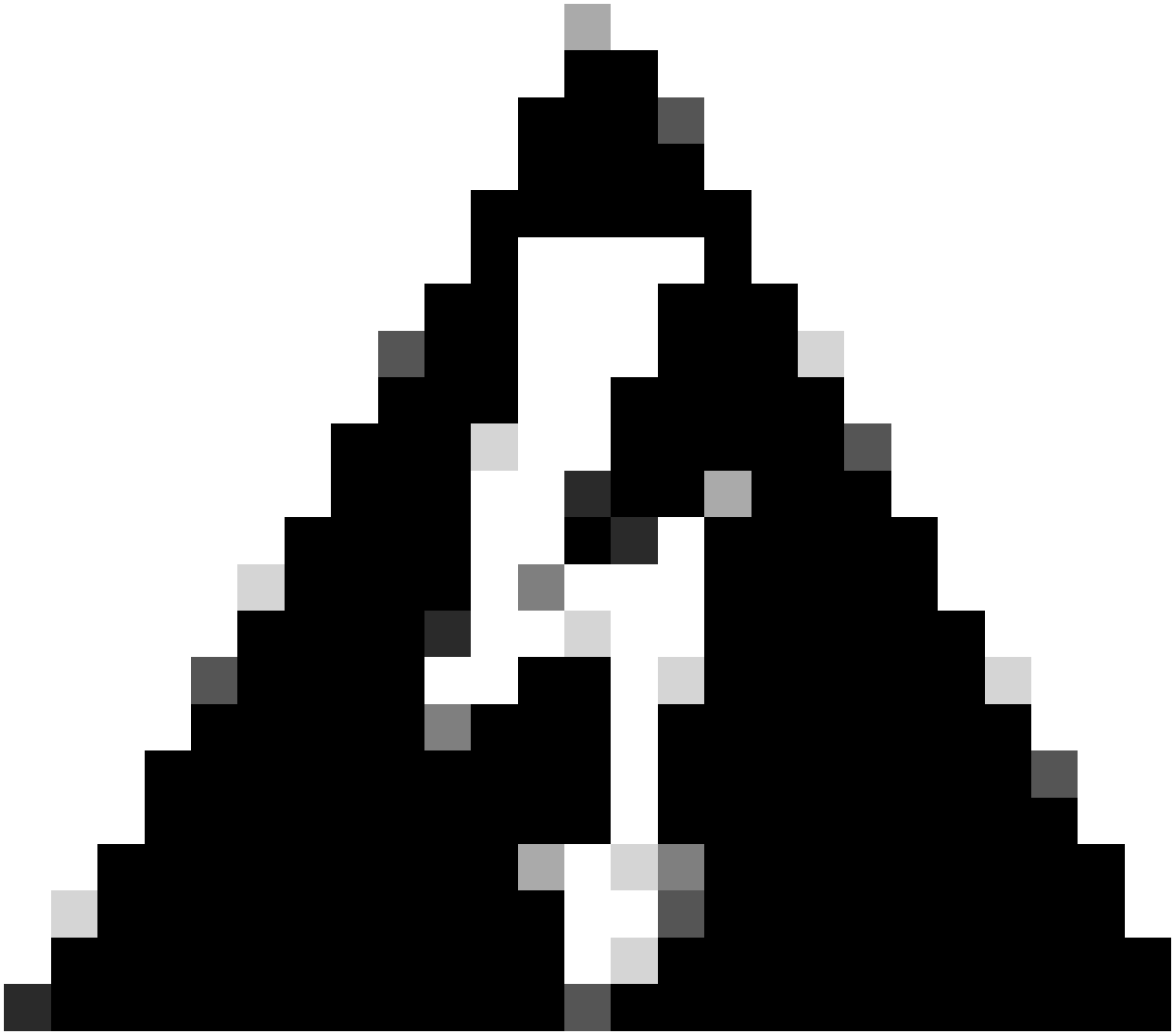
Come utente finale, è possibile usare l'interfaccia GUI di Cisco DNA Center con Grafana per eseguire le query SQL in modo da non aver bisogno di accedere alla shell Postgres tramite la CLI di Maglev.



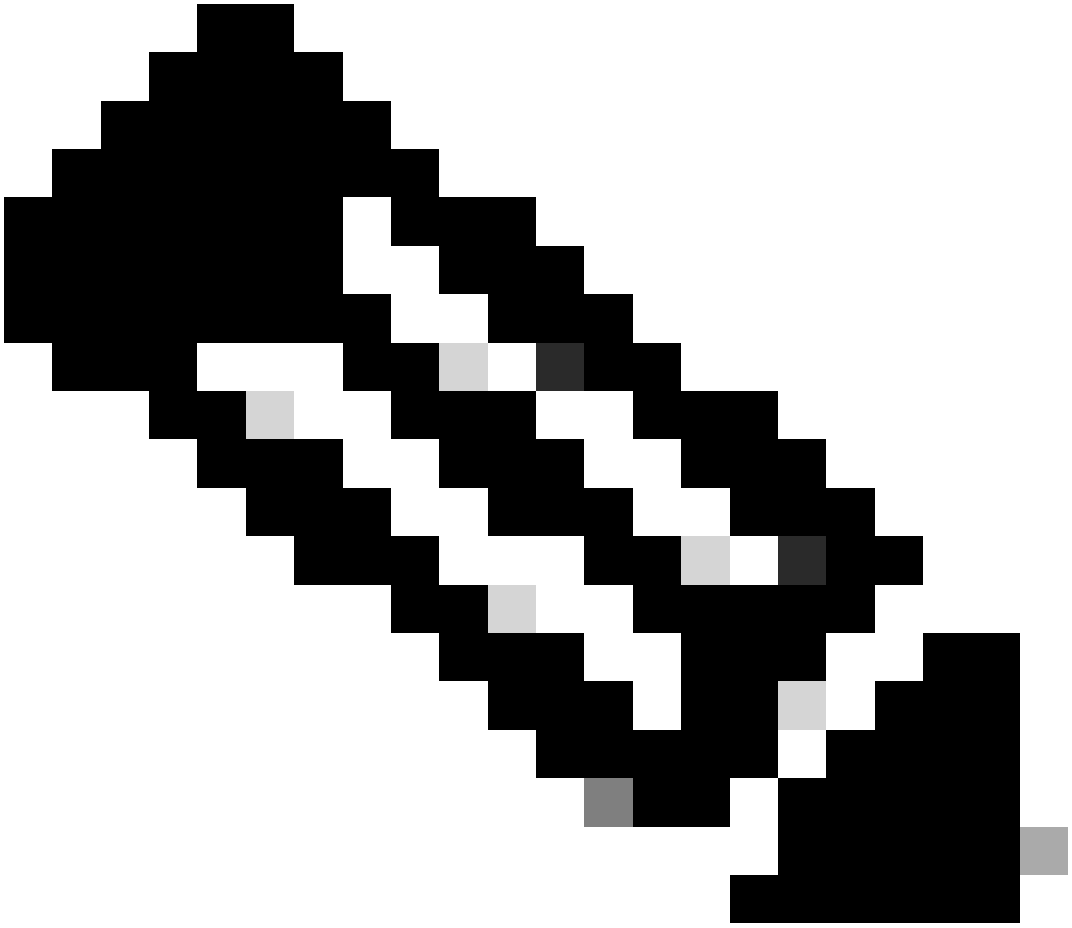
Suggerimento: Se vuoi imparare a usare Grafana consulta la guida ufficiale: Execute Postgres Queries in Cisco DNA Center GUI

Di seguito sono riportate alcune tabelle di database di postgres da esaminare quando si verificano problemi con i dispositivi di rete in Inventory.

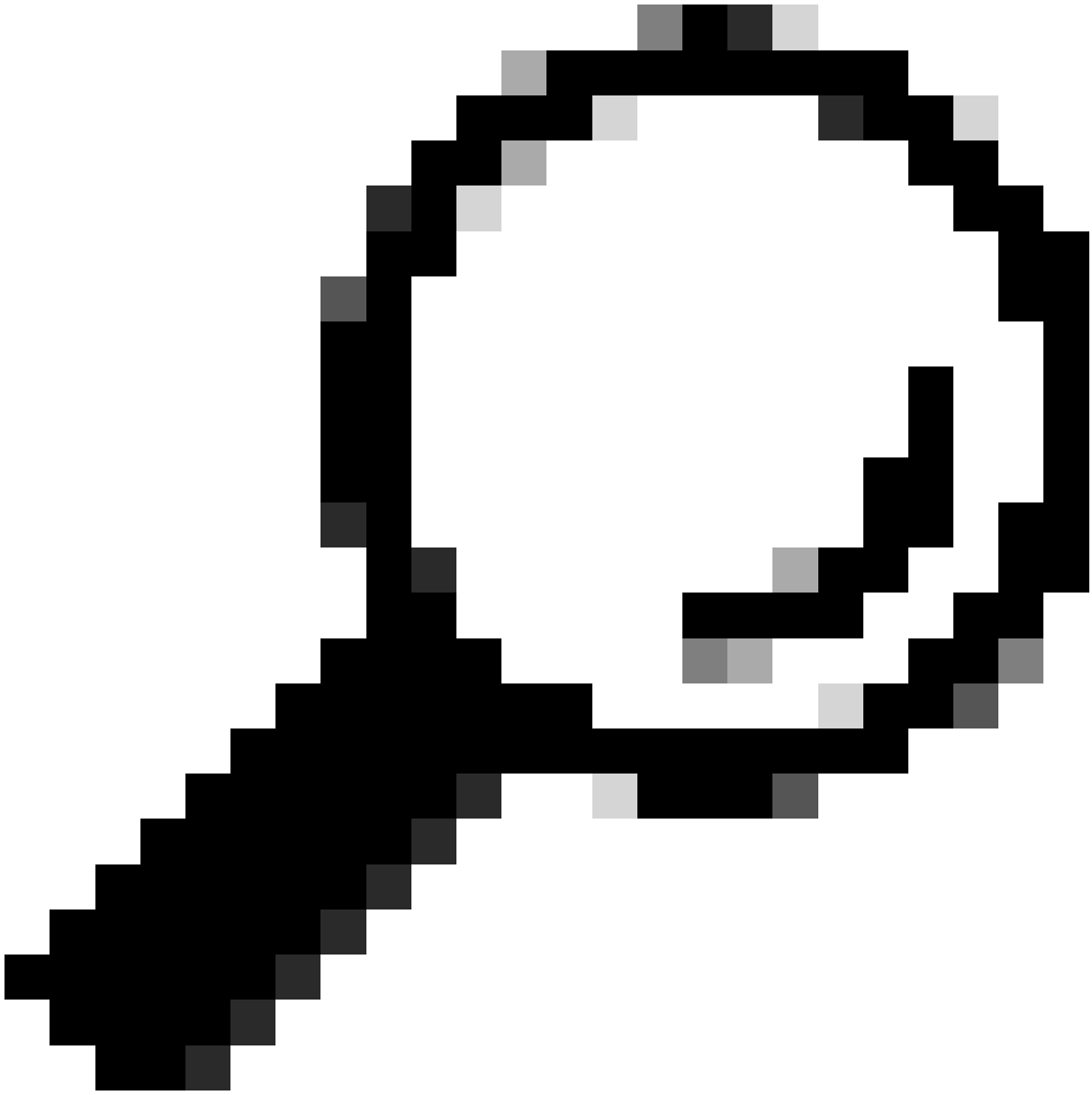
- dispositivo di rete
- interfaccia managerdelement
- elemento di rete
- risorsa di rete
- dispositivo
- indirizzoip



Avviso: Solo Cisco TAC è autorizzato a eseguire query di visualizzazione nella shell Postgres e solo i team BU/DE possono apportare modifiche alle tabelle DB.



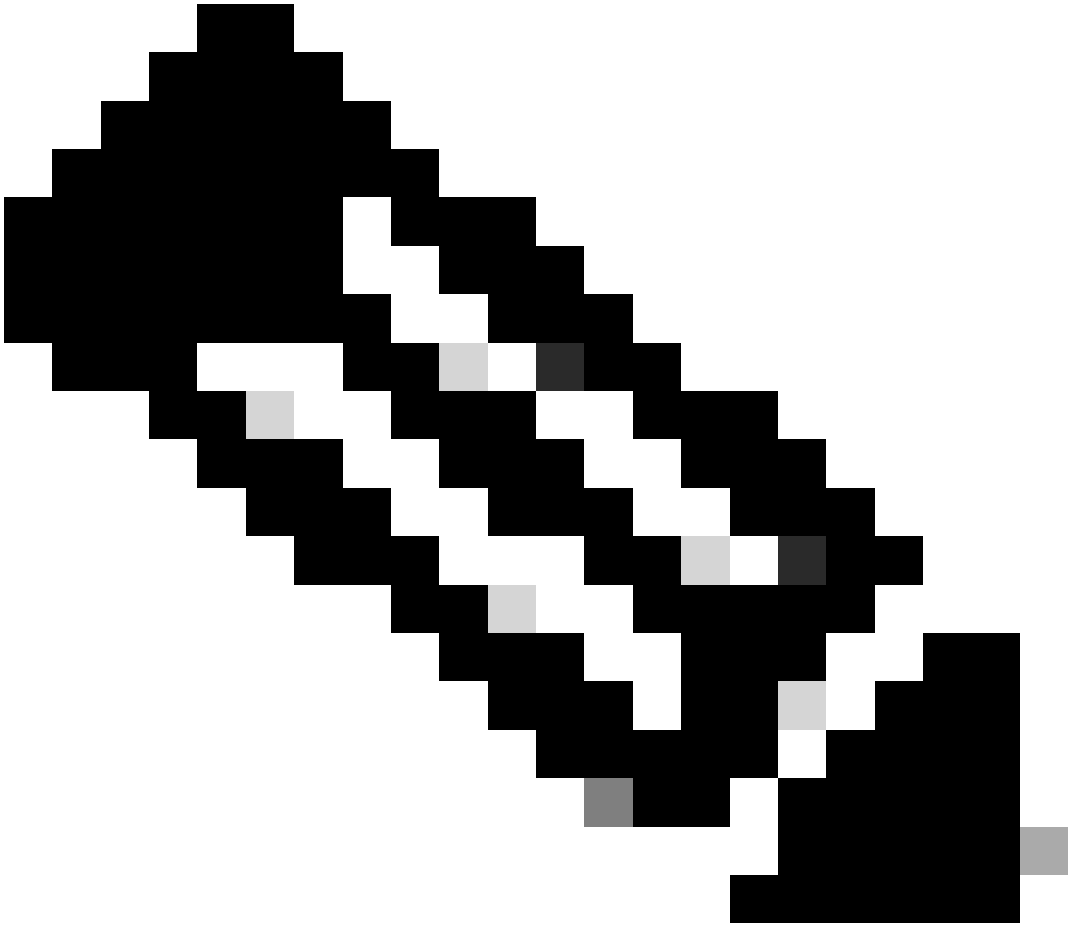
Nota: I problemi del database possono inoltre causare un messaggio di errore interno per i dispositivi che può impedire la raccolta dei dati e il provisioning dei dispositivi.



Suggerimento: È possibile esaminare i log di Postgres utilizzando Kibana nella pagina Cisco DNA Center System 360 e cercare le violazioni dei vincoli quando il servizio Inventory tenta di salvare o aggiornare le voci nelle tabelle del database di Postgres.

Loop e trap di sincronizzazione

Cisco DNA Center è progettato per eseguire una risincronizzazione del dispositivo ogni volta che riceve una trap dal dispositivo dopo che è stata eseguita una modifica importante nel dispositivo stesso, in modo da mantenere aggiornato l'inventario di Cisco DNA Center. A volte la pagina Inventario di Cisco DNA Center mantiene lo stato "Sincronizzazione" dei dispositivi di rete nella sezione Gestibilità per un lungo periodo di tempo o per sempre.



Nota: Questo tipo di loop di sincronizzazione causati da abbondanti trap può causare l'autenticazione di Cisco DNA Center più volte in un breve periodo di tempo ai dispositivi che inviano le trap a causa delle modifiche rilevate.

API per forzare la sincronizzazione del dispositivo

Se il dispositivo di rete mantiene lo stato di sincronizzazione troppo a lungo, anche per giorni, esaminare innanzitutto i controlli di base per verificare la raggiungibilità e la connettività. Imponi quindi la risincronizzazione del dispositivo tramite chiamata API:

1.- Aprire la sessione CLI maglev di Cisco DNA Center.

2.- Ottenere il token di autenticazione di Cisco DNA Center tramite l'API:

<#root>

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

3.- Utilizzare il token del passaggio precedente per eseguire l'API e forzare la sincronizzazione del dispositivo:

<#root>

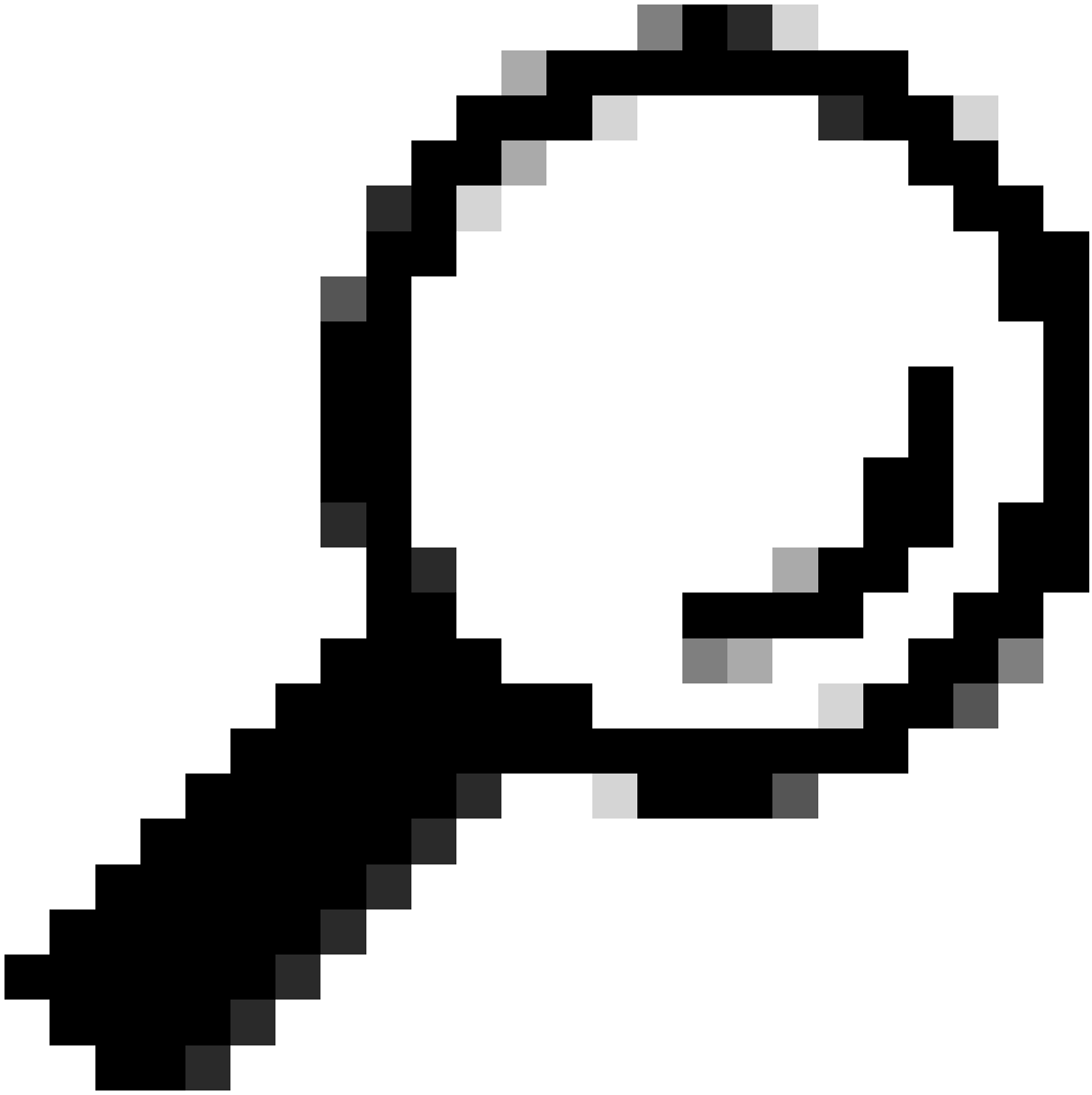
curl -X PUT -H "X-AUTH-TOKEN:

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

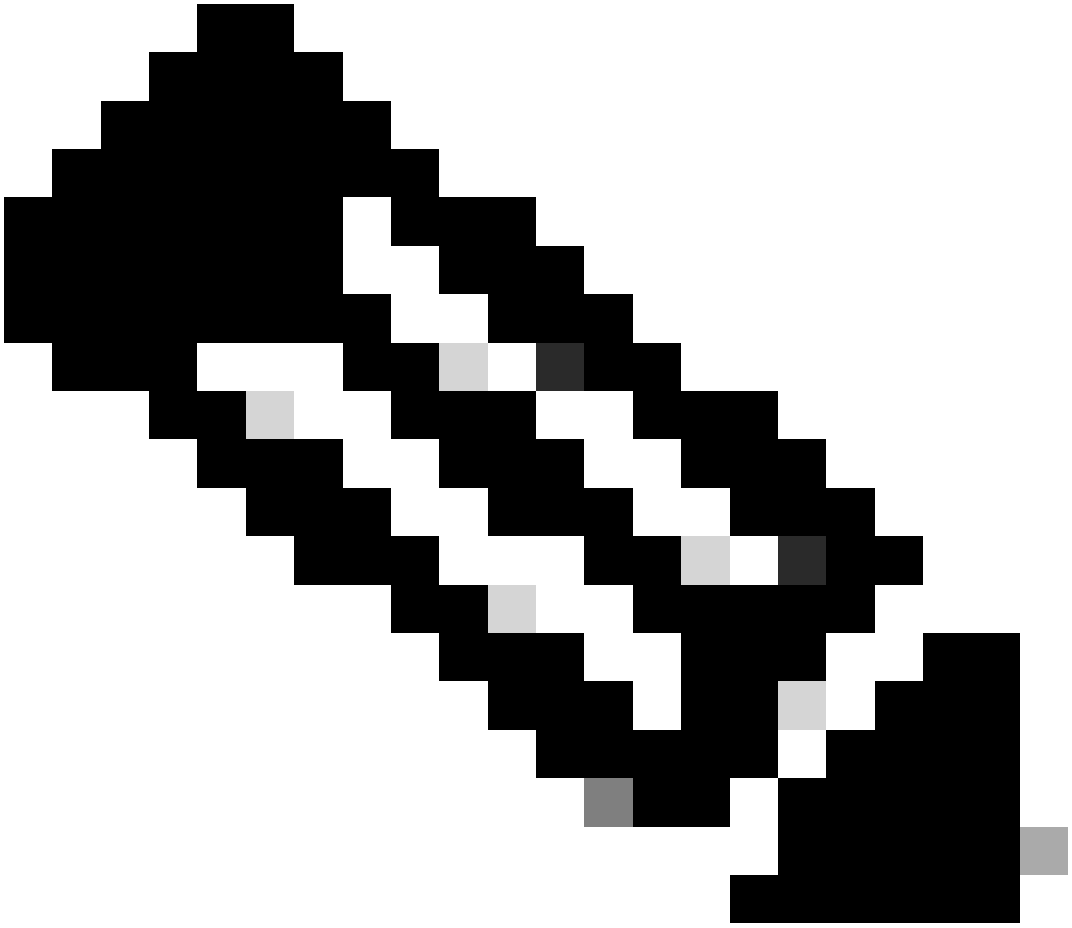
' https://

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

4.- È possibile vedere il dispositivo in Sincronizzazione ancora una volta, ma questa volta con un'opzione Force Sync via API.



Suggerimento: L'uuid del dispositivo può essere ottenuto dall'URL del browser (ID dispositivo o ID) dalla pagina Cisco DNA Center Inventory - Dettagli dispositivo o dalla pagina Device View 360.



Nota: Per ulteriori informazioni sulle API in Cisco DNA Center, consultare la Guida alle API di Cisco DevNet

---

Revisione di trap

Se il problema persiste dopo aver forzato l'operazione di sincronizzazione nel dispositivo, è possibile verificare se il "servizio eventi" di Cisco DNA Center riceve troppe trap ed esaminare il tipo di trap leggendo i registri del servizio eventi:

1.- Prima di leggere i log, è possibile controllare il totale dei trap con il comando:

<#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.- Quindi ci colleghiamo al contenitore del servizio eventi:

<#root>

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

3.- Una volta entrati nel contenitore del servizio eventi, passare alla cartella dei log:

<#root>

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

4.- Se si esaminano i file all'interno della directory è possibile vedere alcuni file di log il cui nome inizia con "ncs".

Esempio:

<#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.- I file "ncs" sono quelli che dobbiamo analizzare per quali tipi di trap riceviamo e per quanti. Possiamo esaminare i file di log filtrandoli in base al nome host del dispositivo o alla parola chiave "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
```

Sono presenti troppi tipi di trap, alcuni di essi possono attivare la risincronizzazione del dispositivo e se vengono troppo frequentemente possono causare il loop di sincronizzazione.

Analizzando le trap è possibile identificare la root cause e creare trap da arrestare, ad esempio un punto di accesso in un ciclo di riavvio.

È possibile salvare l'output dei trap in un file e condividerli con il team di escalation, se necessario.

Stato arresto anomalo del servizio

Se si sospetta che il pod di inventario si stia arrestando a causa di un comportamento anomalo nella pagina Inventario di Cisco DNA Center durante la gestione dei dispositivi di rete, è possibile convalidarne prima lo stato:

<#root>

$ magctl appstack status | grep inventory

$ magctl service status

Esaminando l'output dello stato del pod, se viene visualizzato un numero elevato di riavvii o uno stato di errore, è possibile collegarsi al contenitore dell'inventario e raccogliere il file heapdump che può contenere i dati che possono aiutare il team di escalation ad analizzare e definire la causa principale dello stato di arresto anomalo:

<#root>

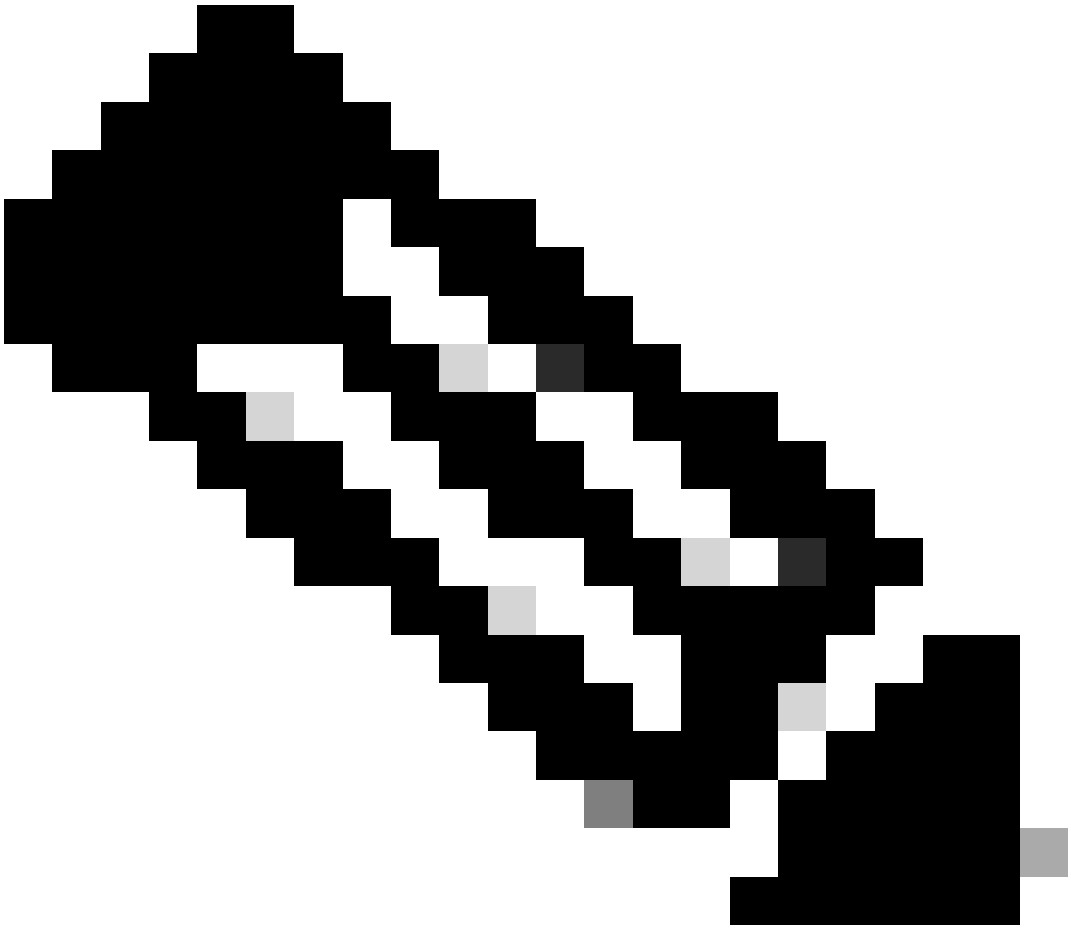
$ magctl service attach -D

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



Nota: Se nella directory del contenitore non è stato trovato alcun file heapdump, nel contenitore non è presente alcuno stato di arresto anomalo.

Impossibile eliminare un dispositivo

In alcune situazioni, Cisco DNA Center non può essere in grado di eliminare un dispositivo di rete dall'interfaccia utente di Inventory a causa di un problema di back-end.

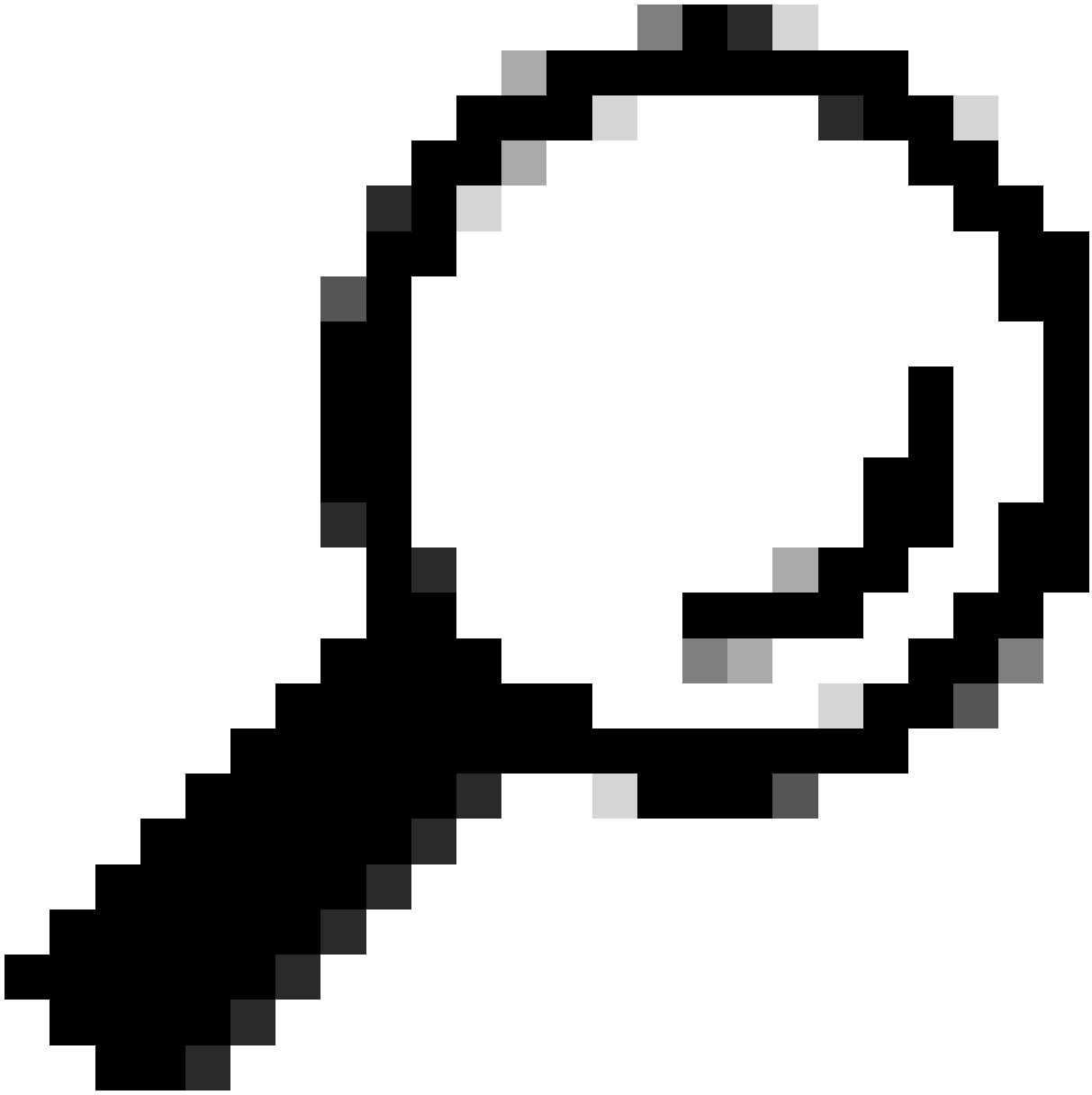
API per forzare l'eliminazione del dispositivo

Se non è possibile eliminare il dispositivo dall'inventario utilizzando l'interfaccia utente di Cisco DNA Center, è possibile utilizzare l'API per eliminare il dispositivo in base all'ID:

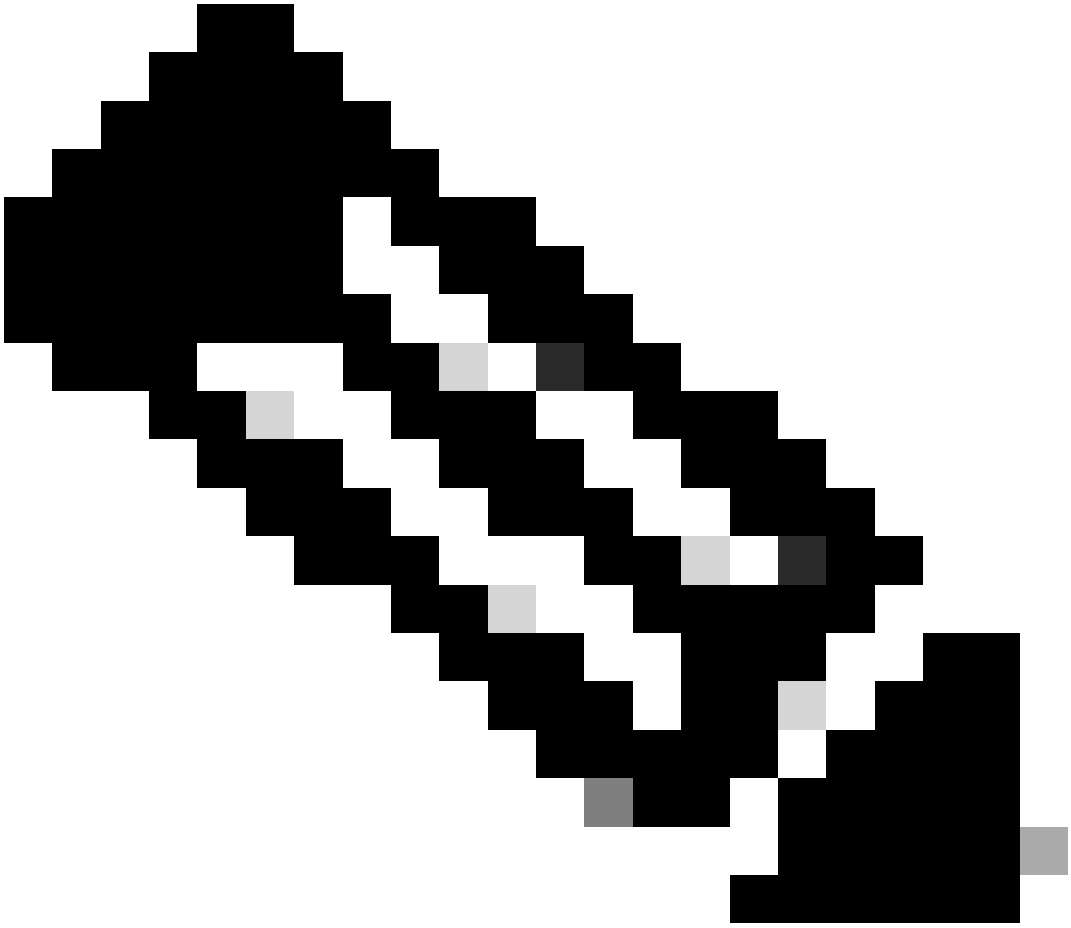
1.- Accedere al menu di Cisco DNA Center -> Platform -> Developer Toolkit -> API Tabs e cercare Devices nella barra di ricerca, dai risultati fare clic su Devices dalla sezione Know your network e cercare l'API DELETE by Device Id.

2.- Fare clic sull'API DELETE by Device Id, quindi su Try e specificare l'ID del dispositivo desiderato da rimuovere dall'inventario.

3.- Attendere l'esecuzione dell'API e ottenere una risposta 200 OK, quindi verificare che il dispositivo di rete non sia più presente nella pagina Inventory.



Suggerimento: L'uuid del dispositivo può essere ottenuto dall'URL del browser (ID dispositivo o ID) dalla pagina Cisco DNA Center Inventory - Dettagli dispositivo o dalla pagina Device View 360.



Nota: Per ulteriori informazioni sulle API in Cisco DNA Center, consultare la Guida alle API di Cisco DevNet

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).