

Configurazione e richiesta di Nexus standalone per la connettività di Intersight

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Vantaggi della connettività](#)

[Video QuickStart](#)

[Richiedi manualmente un dispositivo NXOS](#)

[Verifica connettività](#)

[Verifica TLS con client OpenSSL](#)

[Verifica raggiungibilità HTTPS](#)

[Configurazione](#)

[Richiedi il dispositivo withinintersight.com](#)

[Sul dispositivo Nexus](#)

[Sul portale Intersight](#)

[Claim One to Many Standalone Nexus Devices all'interno di intersight.com tramite Ansible®](#)

[Configurare Nexus NXAPI \(utilizzato solo se si utilizza ansible.netcommon.httapi\)](#)

[Genera chiavi API di Intersight](#)

[Esempio: Ansibleinventory.yaml](#)

[Esempio:playbook.yamlExecution](#)

[Verifica](#)

[Su switch Nexus](#)

[Release precedenti alla 10.3\(4a\)M](#)

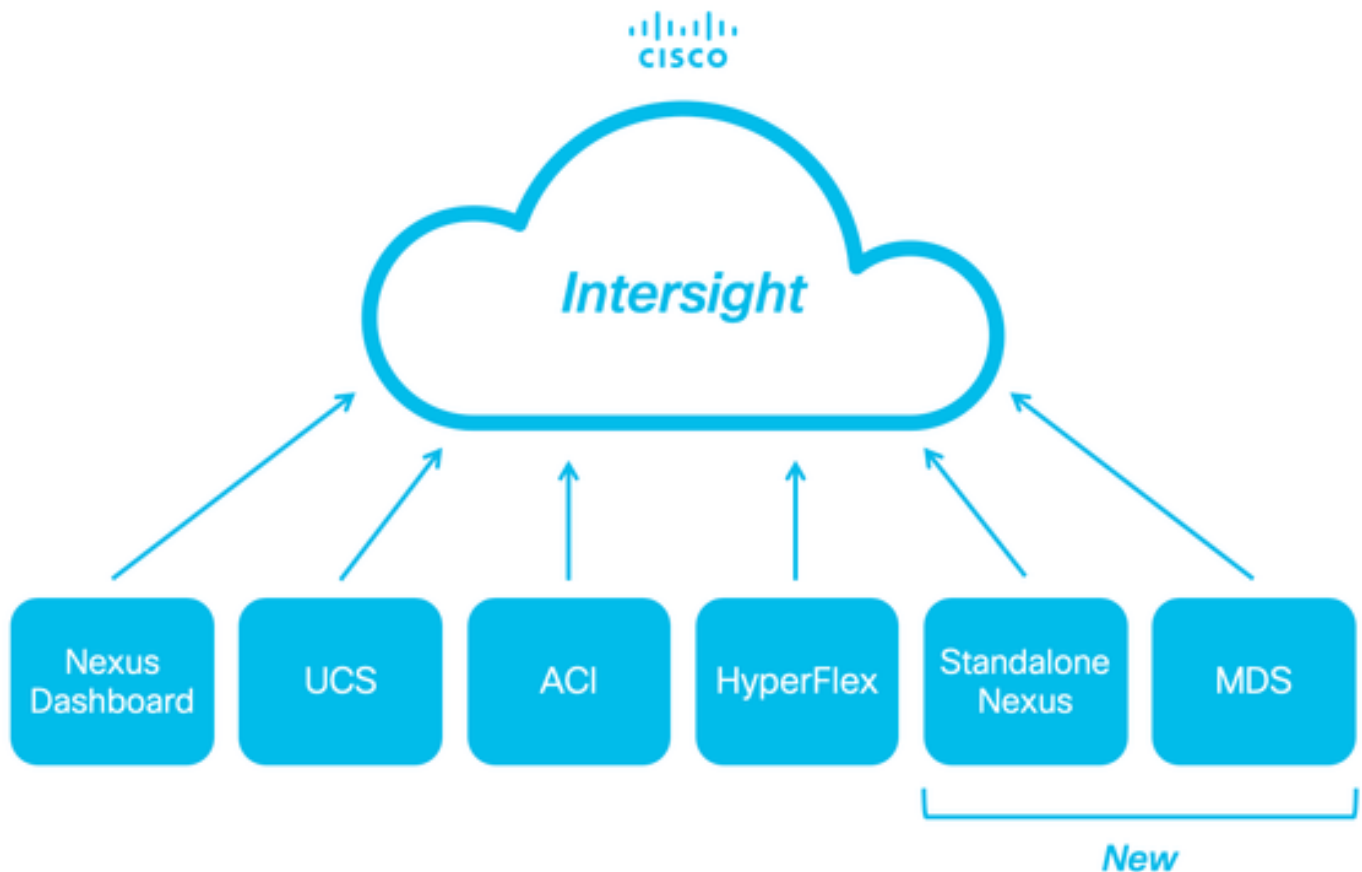
[Versioni che iniziano con 10.3\(4a\)M](#)

[Ansioso](#)

[Disabilita connettore dispositivo](#)

Introduzione

Questo documento descrive i passaggi necessari per abilitare e richiedere gli switch Nexus standalone in Intersight per un supporto Cisco TAC avanzato.



Prerequisiti

È necessario avere un account su [Intersight.com](https://intersight.com); per richiedere la licenza per Cisco NX-OS®, non è richiesta alcuna licenza. Se è necessario creare un nuovo account Intersight, vedere [Creazione di account](#).

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Sullo switch Nexus standalone, NXDC presenta le seguenti linee guida e limitazioni:

- Cisco NX-OS deve essere in esecuzione la versione 10.2(3)F o successive
- [Il DNS](#) deve essere configurato nel VRF (Virtual Routing and Forwarding) appropriato
- `svc.intersight.com` è necessario ottenere risolto e consentire le connessioni HTTPS avviate in uscita sulla porta 443. È possibile controllare con `openssl` e **ricciolo**. Le richieste ICMP (Internet Control Message Protocol) vengono ignorate.
- Se è necessario un proxy per una connessione HTTPS a `svc.intersight.com`, è possibile configurarlo nella configurazione Nexus Switch Device Connector (NXDC). Per la configurazione del proxy, consultare il documento sulla [configurazione di NXDC](#).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Nexus N9K-C93240YC-FX2
- Cisco NX-OS 10.3(4a)M

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.

Premesse

Cisco Intersight è una piattaforma operativa per il cloud che include funzionalità opzionali e modulari per infrastrutture avanzate, ottimizzazione dei carichi di lavoro e servizi Kubernetes. Per ulteriori informazioni, visitare la [panoramica di Intersight](#).

I dispositivi sono collegati al portale Intersight tramite un NXDC incorporato nell'immagine Cisco NX-OS di ciascun sistema. A partire da Cisco NX-OS versione 10.2(3)F, è supportata la funzionalità Device Connector, che consente ai dispositivi collegati di inviare informazioni e ricevere istruzioni di controllo dal portale Cisco Intersight tramite una connessione Internet sicura.

Vantaggi della connettività

La connettività Intersight offre le seguenti caratteristiche e vantaggi per le piattaforme basate su Cisco NX-OS:

- Raccolta automatica delle richieste di assistenza tramite `show tech-support details` [Rapid Problem Resolution](#) (RPR per le richieste di assistenza TAC aperte)
- Raccolta remota su richiesta di `show tech-support details`
- Le caratteristiche future includono:
 - Apertura di TAC SR proattivi basati su errori di telemetria o hardware
 - Raccolta remota su richiesta di singoli comandi `show` e altro ancora

Video QuickStart

Richiedi manualmente un dispositivo NXOS

Verifica connettività



Nota: le risposte ping vengono eliminate (i pacchetti ICMP vengono eliminati).

Per verificare la connettività TLS (Transport Layer Security) e HTTPS, si consiglia di abilitare l'accesso e l'esecuzione openssl e i comandi curl nel VRF (ip netns exec <VRF>) desiderato.

! Enable bash

```
config terminal ; feature bash ; end
```

! Verify TLS

```
run bash ip netns exec management openssl s_client -connect svc.intersight.com:443
```

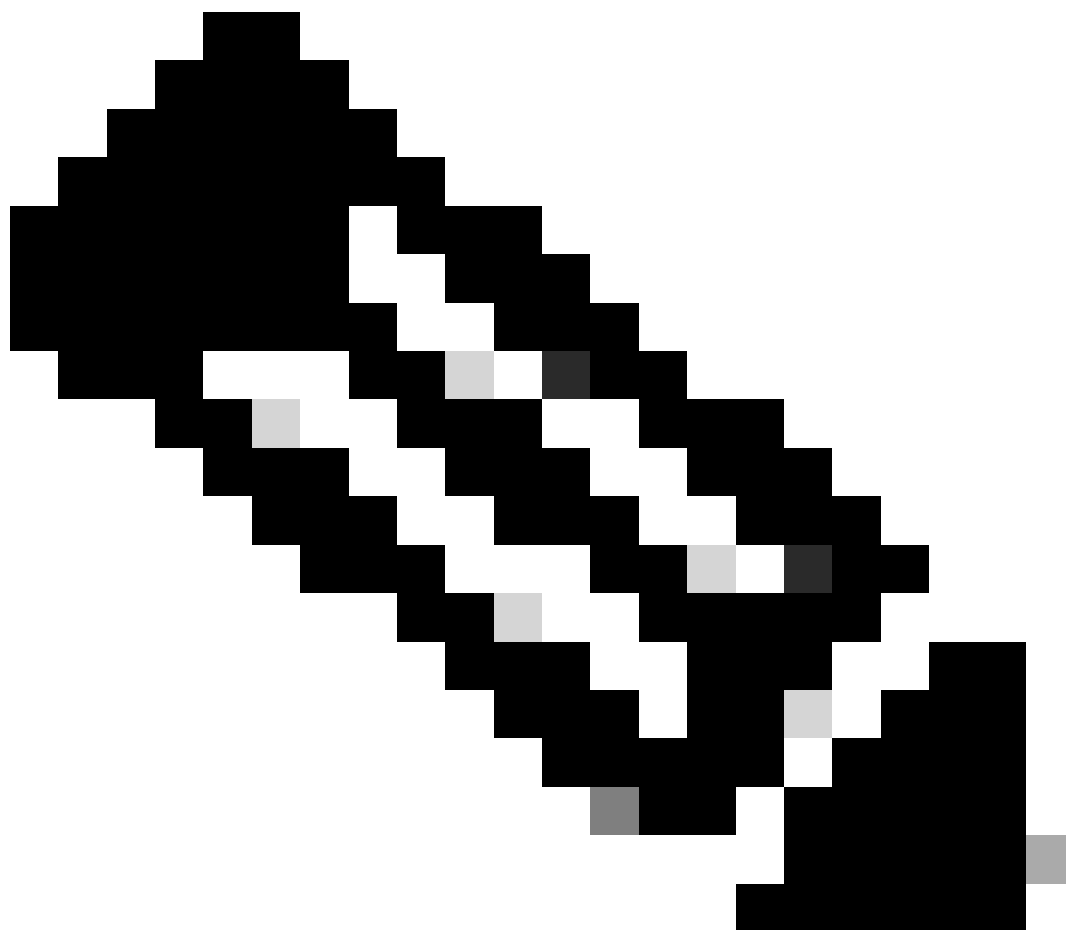
! Verify https

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443 --proxy [protocol://]host[:port]
```

Verifica TLS con client OpenSSL

Utilizzando OpenSSL, è possibile controllare la connettività TLS a `svc.intersight.com:443`. Se l'operazione ha esito positivo, recuperare il certificato firmato pubblico dal server e visualizzare la catena di certificati.

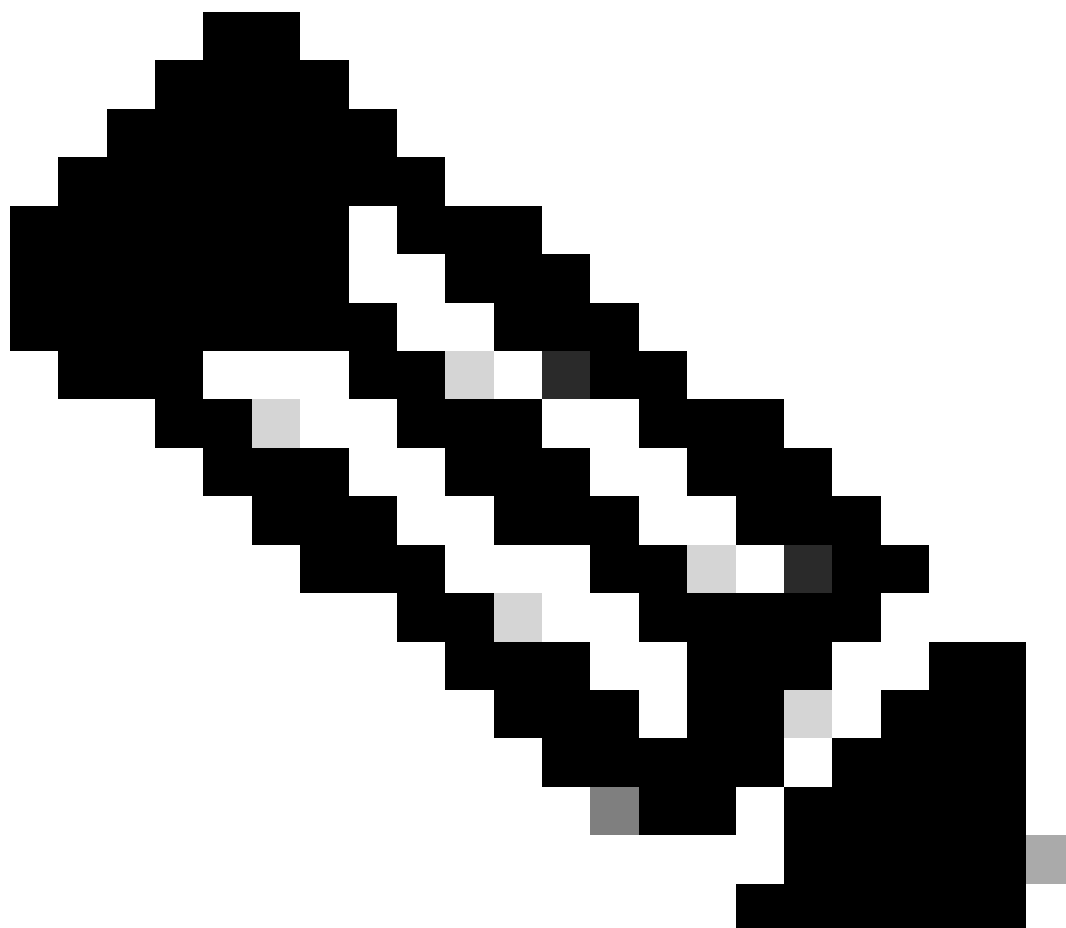


Nota: nell'esempio seguente viene eseguito il comando `openssl s_client` nella gestione VRF. Sostituire la parte desiderata nel `ip netns exec <VRF> costruito`.

```
Switch# run bash ip netns exec management openssl s_client -connect svc.intersight.com:443 CONNECTED(00
```

Verifica raggiungibilità HTTPS

Per controllare la connettività HTTPS, usare il comando **curl** con il comando **-v** verbose flag (visualizza se un proxy è usato o meno).



Nota: per verificare l'impatto dell'attivazione o della disattivazione di un proxy, è possibile aggiungere le opzioni `--proxy [protocol://]host[:port]` o `--noproxy [protocol://]host[:port]`.

Il costrutto ip netns exec <VRF> viene utilizzato per eseguire l'arricciatura nel VRF desiderato, ad esempio ip netns exec management per la gestione del VRF.

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443 --proxy [protocol://]host[:port]
```

```
<#root>
```

```
#
```

```
run bash ip netns exec management curl -v -I -L -X POST https://svc.intersight.com:443 --proxy http://pr
```

```
Trying 10.201.255.40:80...
```

```
*
```

```
Connected to proxy.es1.cisco.com (10.201.255.40) port 80
```

```
* CONNECT tunnel: HTTP/1.1 negotiated
* allocate connect buffer
* Establish HTTP proxy tunnel to svc.intersight.com:443
> CONNECT svc.intersight.com:443 HTTP/1.1
> Host: svc.intersight.com:443
> User-Agent: curl/8.4.0
> Proxy-Connection: Keep-Alive
>
```

```
< HTTP/1.1 200 Connection established
```

HTTP/1.1 200 Connection established
< snip >

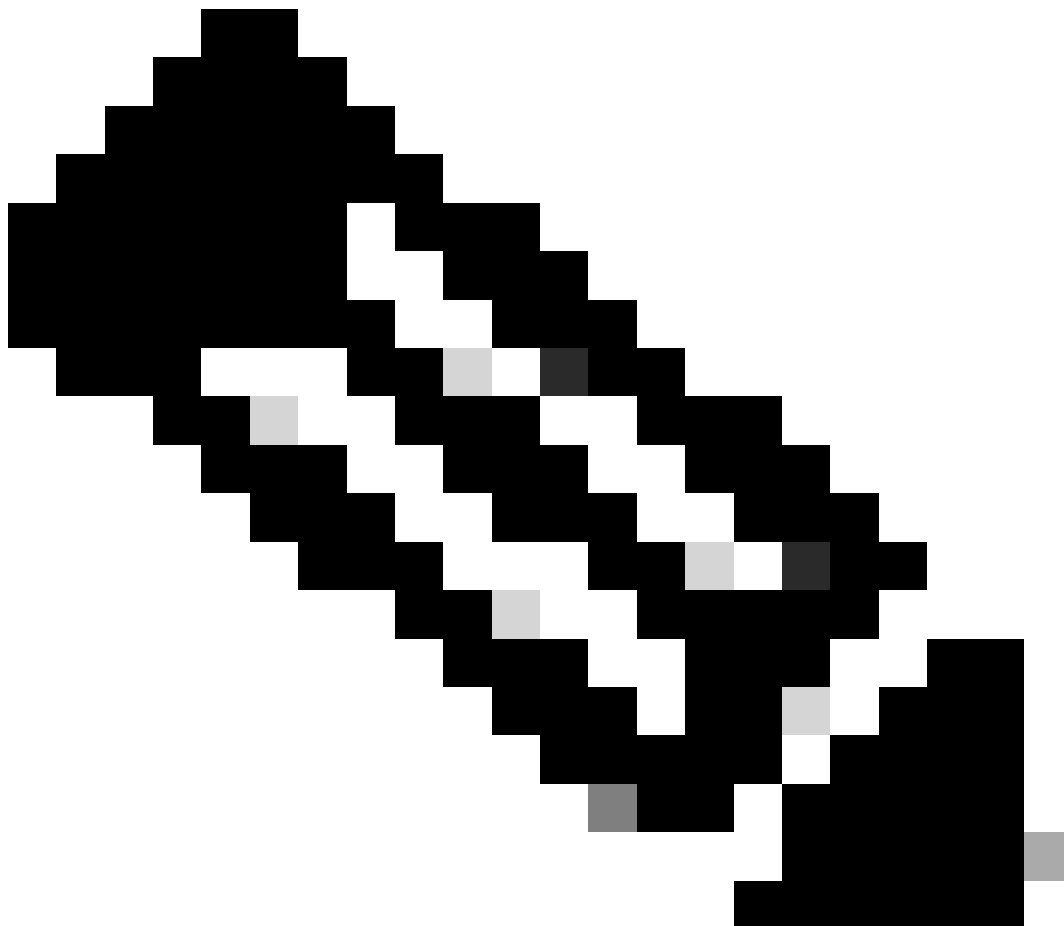
Configurazione

Richiedi il dispositivo entro intersight.com

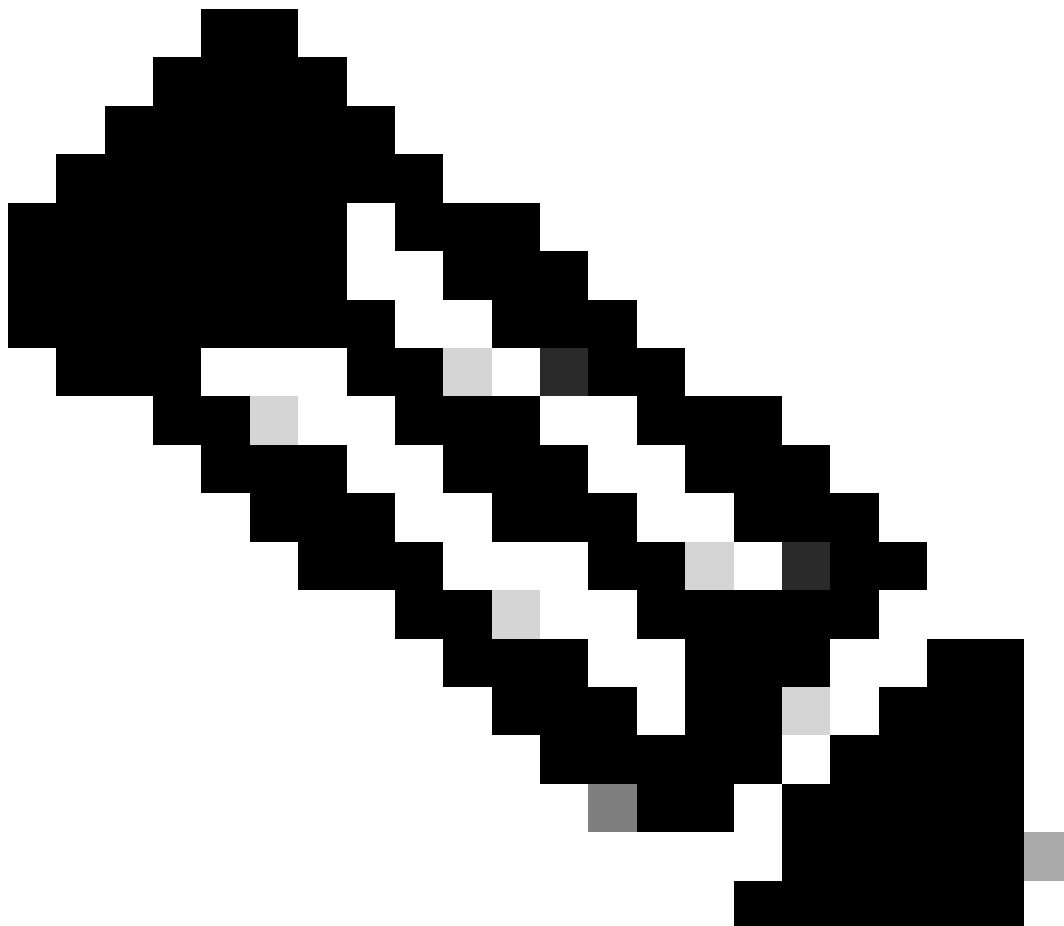
Per rivendicare un nuovo obiettivo in Intersight, eseguire le operazioni descritte.

Sul dispositivo Nexus

Eseguire il comando Cisco NX-OS `show system device-connector claim-info`.



Nota: per le versioni precedenti a NX-OS 10.3(4a), utilizzare il comando "show intersight claim-info"



Nota: le mappe di informazioni sulle attestazioni generate da Nexus sono associate ai seguenti campi delle attestazioni di Intersight:

Numero di serie = **ID richiesta** Intersight

Device-ID Security Token = **Codice attestazione** Intersight

```
# show system device-connector claim-info SerialNumber: FD023021ZUJ SecurityToken: 9FFD4FA94DCD Duratio
```

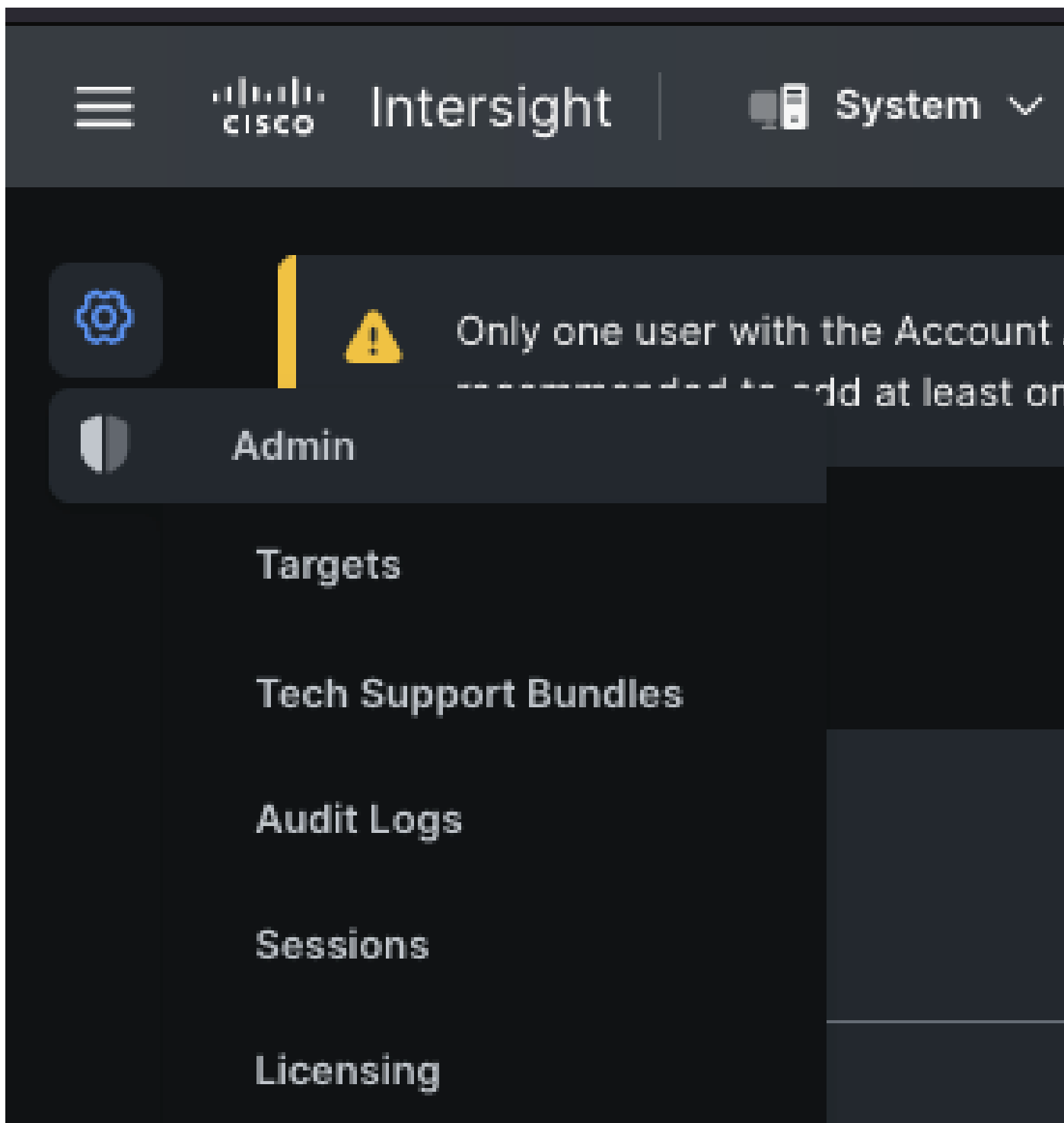
La **durata** indicata è in secondi.

Sul portale Intersight

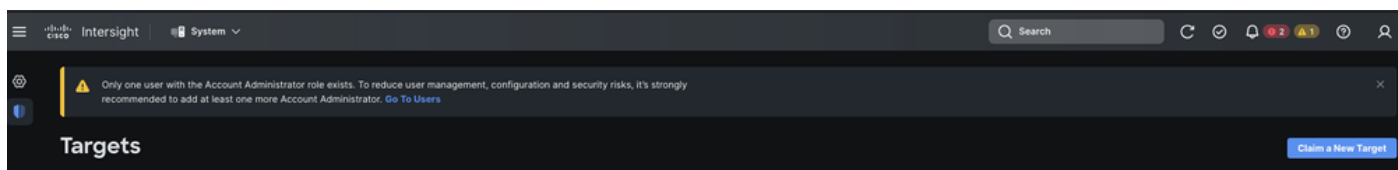
1. Entro 10 minuti, accedere a **Intersight** con i privilegi di amministratore di account, amministratore di dispositivo o tecnico di dispositivo.
2. Dall'elenco a discesa **Service Selector** (Selettore servizi), scegliere **System** (Sistema).



3. Passare a ADMIN > Targets > Claim a New Target.



3.1. Fare clic su **Richiedi una nuova destinazione** come mostrato nell'immagine.



4. Scegliere **Disponibile per richiesta di rimborso** e scegliere il **tipo di oggetto** (ad esempio, Rete) che si desidera richiedere. Fare clic su **Start**.

⚙️

⚠️ Only one user with the Account Administrator role exists. To reduce user management, configuration and security risks, it's strongly recommended to add at least one more Account Administrator. [Go To Users](#) ✕

🛡️

← Targets

Claim a New Target

Select Target Type

Filters

Available for Claiming

Categories

All

Cloud

Compute / Fabric







Hyperconverged

Network

Orchestrator

🔍 Search

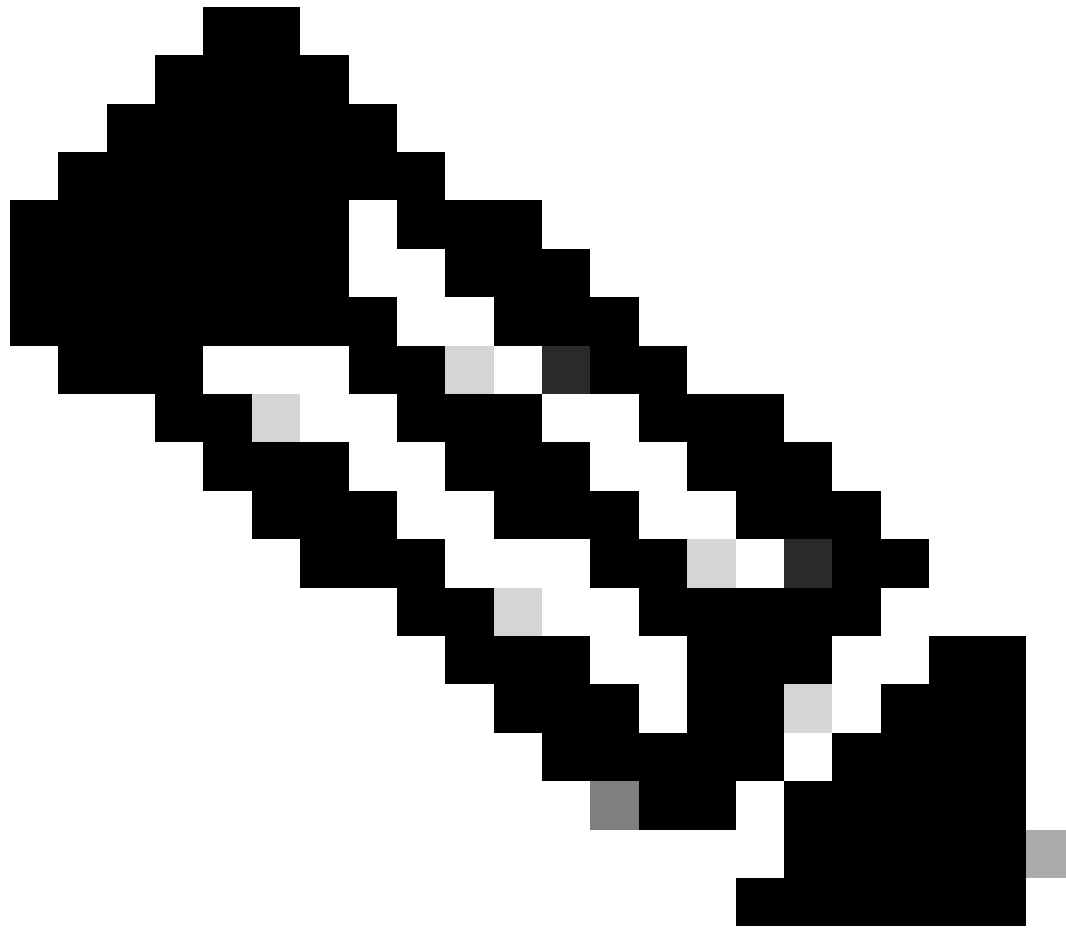
Network

 Cisco MDS Switch	<input checked="" type="checkbox"/>  Cisco Nexus Switch	 Cisco APIC
 Cisco Cloud APIC	 Cisco DCNM	 Cisco Nexus Dashboard

5. Inserire i dettagli richiesti e fare clic su **Richiesta di rimborso** per completare il processo.



Nota: il **token di sicurezza** sullo switch viene utilizzato come codice attestazione e il **numero di serie** dello switch è l'ID dispositivo.



Nota: il token di sicurezza scade. Dovete completare l'attestazione prima di oppure il sistema vi chiede di rigenerarne una.



The security token has expired. Please obtain a new security token to claim the device



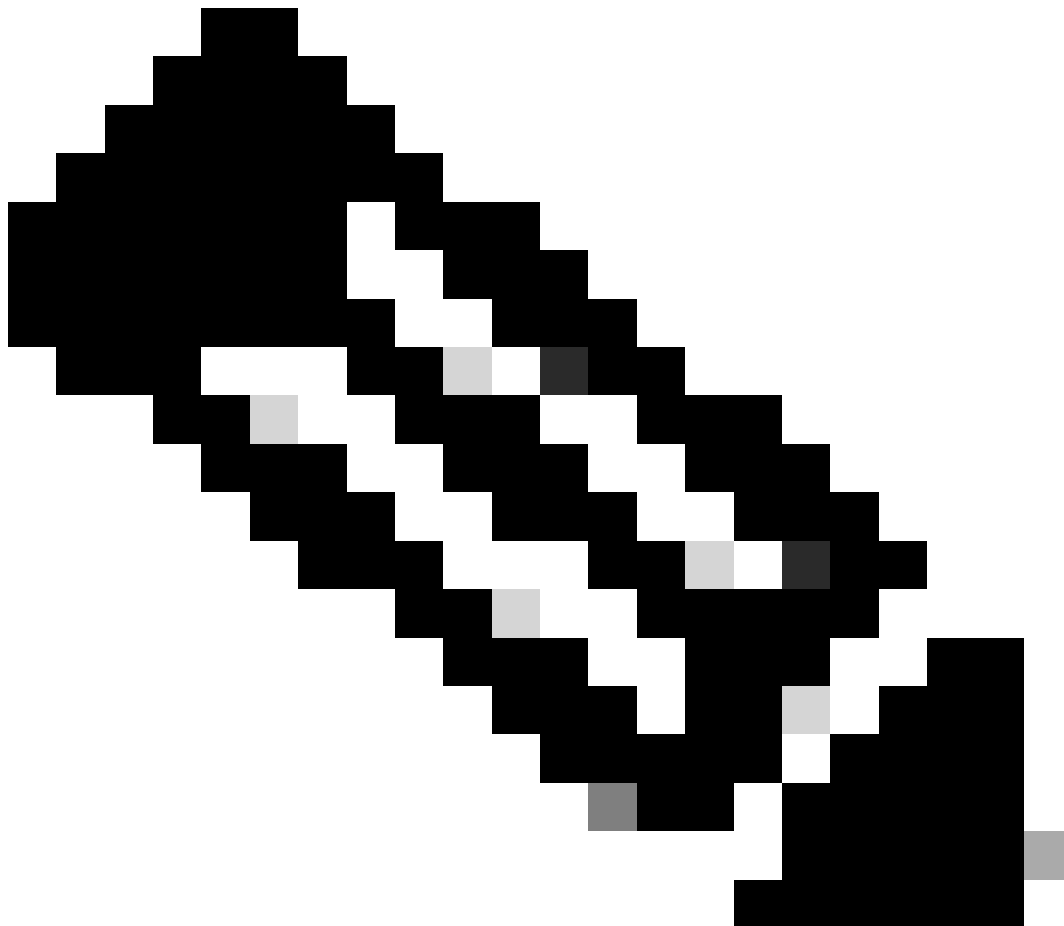
[Details](#)

Pretendiamo uno a molti dispositivi Nexus standalone all'interno di intersight.com utilizzando Ansible®

Per rivendicare uno a molti dispositivi Nexus, è possibile eseguire un playbook Ansible.

- L'inventario andibile e il playbook possono essere clonati da <https://github.com/datacenter/ansible-intersight-nxos>.
- Nell'Ansible inventory.yaml, il tipoansible_connection è impostato su ansible.netcommon.network_cli per inviare i comandi allo switch Nexus. Questa opzione può essere modificata in peransible.netcommon.httpapi consentire la connettività tramite NXAPI.
- Per una connessione flessibile all'endpoint di Intersight è necessaria una chiave API, che può essere generata dall'account **intersight.com**.

Configura Nexus NXAPI (utilizzato solo se si utilizza ansible.netcommon.httpapi)

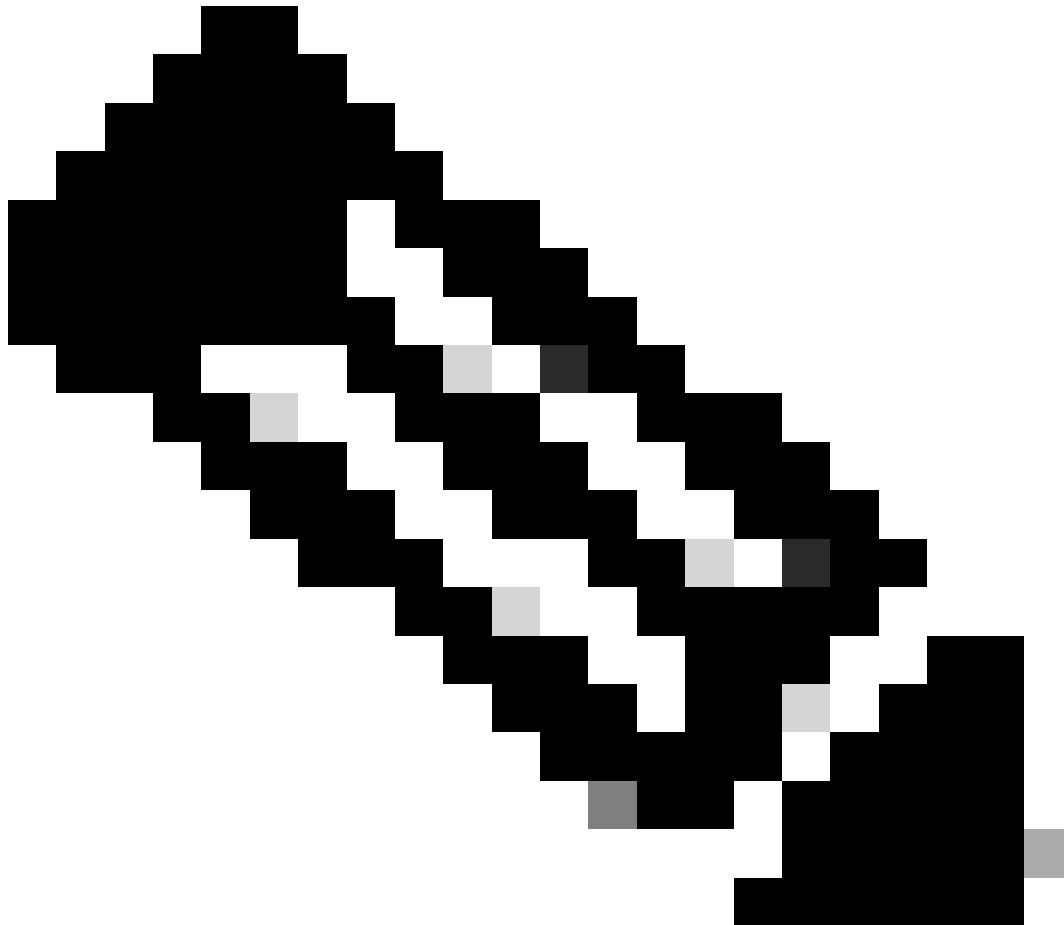


Nota: nel caso in cui un proxy a livello di sistema sia configurato (**HTTP(S)_PROXY**) e Ansible non debba utilizzare un proxy per connettersi all'endpoint Nexus NXAPI, è consigliabile impostare `ansible_httppapi_use_proxy: False` (il valore predefinito è `True`).

```
# configure terminal # cfeature nxapi # nxapi port 80 # no nxapi https port 443 # end # show nxapi nxap
```

Per verificare in modo indipendente la connettività HTTP all'endpoint NXAPI, è possibile tentare di inviare un show clockpacchetto.

Nell'esempio successivo, lo switch autentica il client utilizzando l'autenticazione di base. È inoltre possibile configurare il server NXAPI per autenticare i client in base al certificato utente X.509.



Nota: l'hash di autenticazione di base viene ottenuto dalla codifica Base64 di **nomeutente:password**. In questo esempio, la codifica **admin:cisco!123** base64 è YWRtaW46Y2lzY28hMTIz.

```
curl -v --noproxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

Risposta al ricciolo:

```
* Trying 10.1.1.3... * TCP_NODELAY set * Connected to 10.1.1.3 (10.1.1.3) port 80 (#0) > POST /ins HTTP/
```

Genera chiavi API di Intersight

Fare riferimento alla sezione [README.md](#) su come ottenere la chiave API da Intersight System > Settings > API keys > Generate API Key.

The screenshot shows the Intersight web interface. At the top, there's a navigation bar with the Cisco logo, 'Intersight', and 'System' dropdown. A search bar and several notification icons are on the right. Below the navigation bar, a warning message states: 'Only one user with the Account Administrator role exists. To reduce user management, configuration and security risks, it's strongly recommended to add at least one more Account Administrator. Go To Users'. The main content area is titled 'Settings' and has a sidebar on the left with various configuration categories. The 'API Keys' section is active, showing a 'Generate API Key' button and a table with columns: Description, API Key ID, Purpose, Cre..., Email, Role, and Identity Provider. The table currently displays 'NO ITEMS AVAILABLE' and '0 Items found'.

Generate API Key





Description

Nexus Intersight key



API Key Purpose

- API key for OpenAPI schema version 2 
- API key for OpenAPI schema version 3 (This is a feature in preview and for SDK developer use only) 

Close

Generate

Esempio: Ansible inventory.yaml



Nota: nell'esempio successivo è stato configurato ansible per ignorare le impostazioni proxy del sistema operativo con `ansible_httppapi_use_proxy: False`. Se è necessario che il server Ansible utilizzi un proxy per raggiungere lo switch, è possibile rimuovere tale configurazione o impostarla su `True` (impostazione predefinita).

Nota: l'ID della chiave API è una stringa. La chiave privata API include il percorso completo di un file che contiene la chiave privata. Per l'ambiente di produzione, si consiglia di utilizzare Ansible vault.

```
---
all:
  hosts:
    switch1:
      ansible_host: "10.1.1.3"
      intersight_src: "mgmt0"
      intersight_vrf: "management"

  vars:
    ansible_user: "admin"
    ansible_password: "cisco!123"
```

```
ansible_connection: ansible.netcommon.network_cli
ansible_network_os: cisco.nxos.nxos
ansible_httpapi_use_proxy: False
remote_tmp: "/bootflash"
proxy_env:
  - no_proxy: "10.1.1.3/24"
intersight_proxy_host: 'proxy.cisco.com'
intersight_proxy_port: '80'

api_key_id: "5fcb99d97564612d33fdfca1/5fcb99d97564612d33fdf1b2/65c6c09d756461330198ce7e"
api_private_key: "/home/admin/ansible-intersight-nxos/my_intersight_private_key.txt"
...

```

Esempio: `playbook.yaml` Esecuzione

Per ulteriori informazioni sulla programmazione di dispositivi Nexus standalone con Ansible, consultare la sezione relativa [Applications/Using Ansible a Cisco NX-OS della Cisco Nexus 9000 NX-OS Programmability Guide \(Guida alla programmabilità di Cisco Nexus 9000 NX-OS\)](#) per la versione corrente.

```
> ansible-playbook -i inventory.yaml playbook.yaml PLAY [all] *****
```

Verifica

Per verificare l'attestazione di una nuova destinazione, eseguire le operazioni seguenti:

Su switch Nexus

Release precedenti alla 10.3(4a)M

```
# run bash sudo cat /mnt/pss/connector.db
```

```
Nexus# run bash sudo cat /mnt/pss/connector.db { "AccountOwnershipState": "Claimed", "AccountOwnershipU
```

Versioni che iniziano con 10.3(4a)M

```
# show system device-connector claim-info
```

```
N9k-Leaf-2# show system device-connector claim-info SerialNumber: FD023021ZUJ SecurityToken: Duration: 0
```

```
# show system internal intersight info
```

```
# show system internal intersight info Intersight connector.db Info: ConnectionState :Connected Connect
```

Ansioso

È possibile aggiungere un'attività alla fine dell'intervallo perplaybook.yaml ottenere le informazioni sull'intervista dello switch.

```
- name: Get intersight info nxos_command: commands: - show system internal intersight info register: i
```

Di seguito è riportato l'output corrispondente:

```
TASK [Get intersight info] *****
```

Disabilita connettore dispositivo

	Comando o azione	Scopo
Passaggio 1	nessuna funzionalità intersight Esempio: switch(config)# no feature intersight	Disabilita il processo di intersight e rimuove tutta la configurazione NXDC e l'archivio registri.

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).