

配置並宣告獨立Nexus實現Intersight連線

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[連線優勢](#)

[快速入門視訊](#)

[手動宣告NXOS裝置](#)

[連線驗證](#)

[使用OpenSSL使用者端的TLS驗證](#)

[HTTPS可達性驗證](#)

[設定](#)

[宣告裝置withinintersight.com](#)

[在Nexus裝置上](#)

[在Intersight門戶上](#)

[使用Ansible在intersight.com中宣告一對多獨立的Nexus裝置@](#)

[配置Nexus NXAPI \(僅在使用ansible.netcommon.httpapi時使用 \)](#)

[產生Intersight API金鑰](#)

[範例：Ansibleinventory.yaml](#)

[範例：playbook.yamlExecution](#)

[驗證](#)

[在Nexus交換機上](#)

[10.3\(4a\)M之前的版本](#)

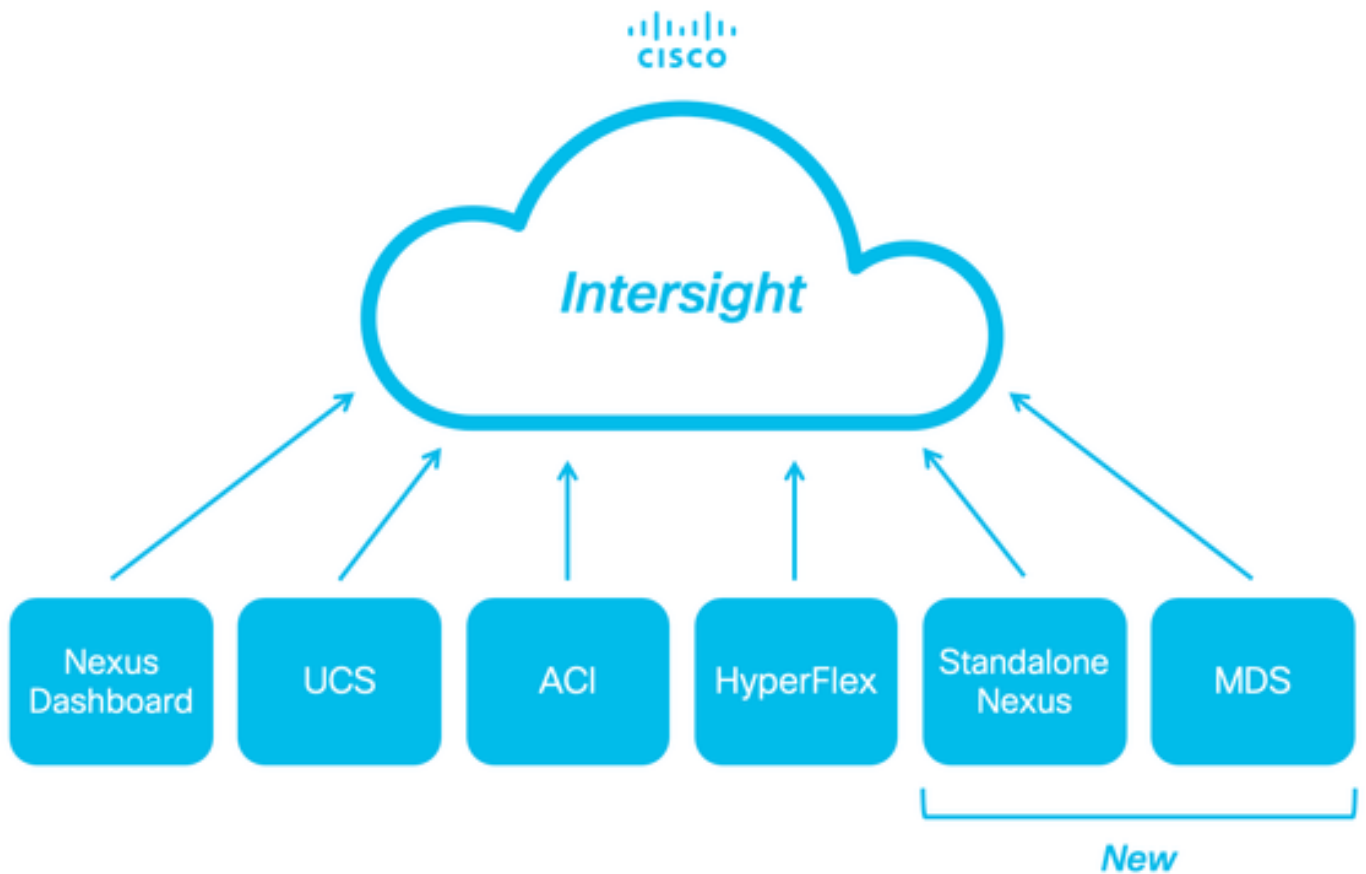
[以10.3\(4a\)M開頭的版本](#)

[阿尼塞](#)

[停用裝置連結器](#)

簡介

本文檔介紹在Intersight中啟用和宣告獨立Nexus交換機以獲得增強型Cisco TAC支援所需的步驟。



必要條件

您必須在[Intersight.com](https://intersight.com)上擁有帳戶，Cisco NX-OS®申請無需許可證。如果需要建立新的Intersight帳戶，請參閱[帳戶建立](#)。

需求

思科建議您瞭解以下主題：

在獨立Nexus交換機上，NXDC具有以下準則和限制：

- Cisco NX-OS必須運行版本10.2(3)F或更高版本
- 必須在正確的虛擬路由和轉發(VRF)下配置[DNS](#)
- `svc.intersight.com` 必須解決並允許在埠443上發起出站的HTTPS連線。可以透過`openssl`和`curl`進行檢查。網際網路控制訊息通訊協定(ICMP)要求被忽略。
- 如果與`svc.intersight.com`的HTTPS連線需要Proxy，可在Nexus交換機裝置聯結器(NXDC)配置中配置Proxy。有關代理配置，請參閱[配置NXDC](#)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Intersight是一個雲運營平台，由高級基礎設施、工作負載最佳化和Kubernetes服務的可選模組化功能組成。有關詳細資訊，請訪問[Intersight概述](#)。

裝置透過嵌入每個系統的Cisco NX-OS映像中的NXDC連線到Intersight門戶。從Cisco NX-OS版本10.2(3)F開始，支援裝置聯結器功能，該功能為連線的裝置提供了一種安全方式，可使用安全的網際網路連線從Cisco Intersight門戶傳送資訊和接收控制指令。

連線優勢

Intersight連線可為基於Cisco NX-OS的平台提供以下功能和優勢：

- 透過[快速問題解決](#)自動收集show tech-support details(RPR for the TAC Service Requests open)
- 遠端按需收集 show tech-support details
- 未來的功能包括：
 - 根據遙測或硬體故障打開主動式TAC SR
 - 單個show命令的遠端按需收集等

快速入門視訊

手動宣告NXOS裝置

連線驗證



注意：Ping響應被抑制（ICMP資料包被丟棄）。

要檢查傳輸層安全(TLS)和HTTPS連線，建議在所需的VRF (ip netns exec <VRF>)中啟用bash和執行openssl和curl命令。

```
! Enable bash
```

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

```
! Verify TLS
```

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

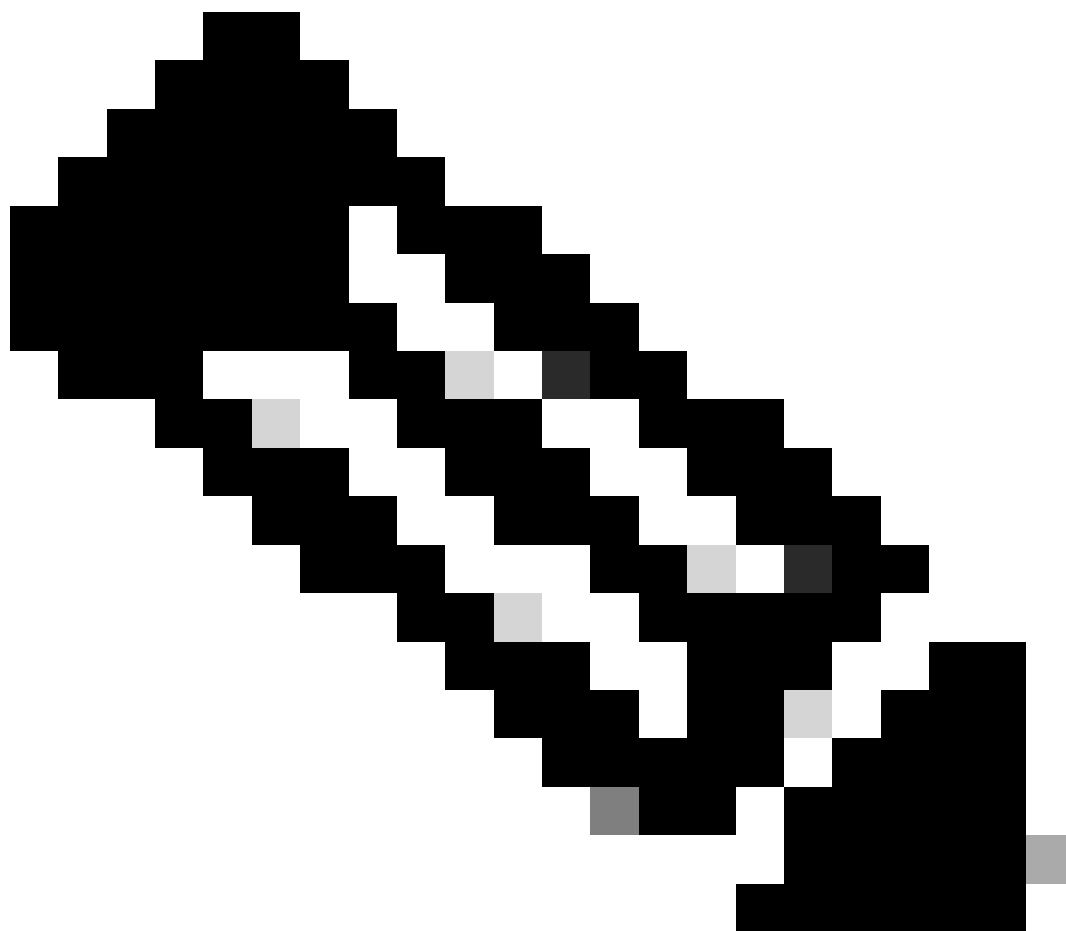
! Verify https

```
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]
```

使用OpenSSL使用者端的TLS驗證

使用OpenSSL，您可以檢查與svc.intersight.com:443的TLS連線。成功後，由伺服器檢索公共簽名證書並顯示證書頒發機構鍵。

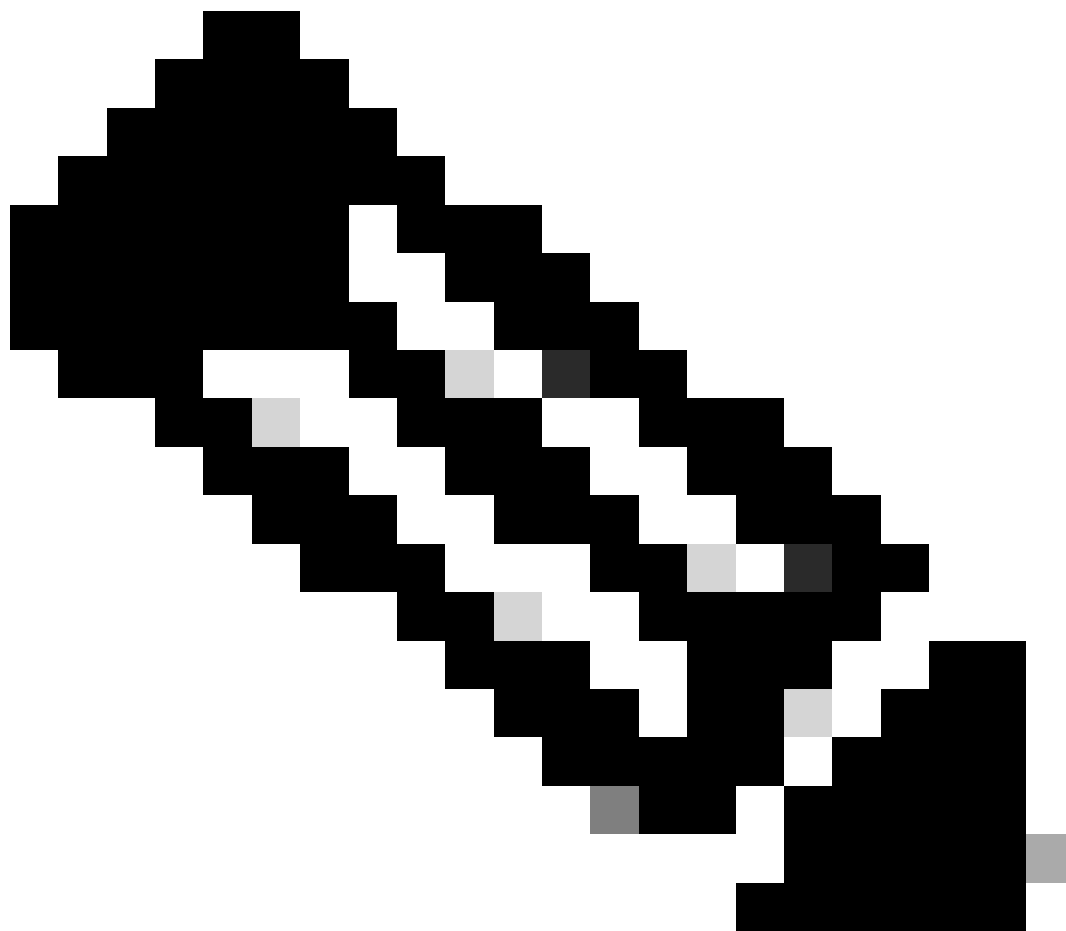


注意：下一個示例在VRF管理中執行openssl s_client命令。 取代ip netns exec <VRF>建構中所需的。

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

HTTPS可達性驗證

要檢查HTTPS連線，請將curl命令與-v verbose flag (顯示是否使用Proxy) 一起使用。



附註：若要檢查啟用或停用Proxy的影響，您可以新增選項--proxy [protocol://]host[:port]或--noproxy [protocol://]host[:port]。

該構造ip netns exec <VRF>用於執行所需VRF中的捲曲；例如，用於VRF管理的ip netns exec management。

```
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 >
```

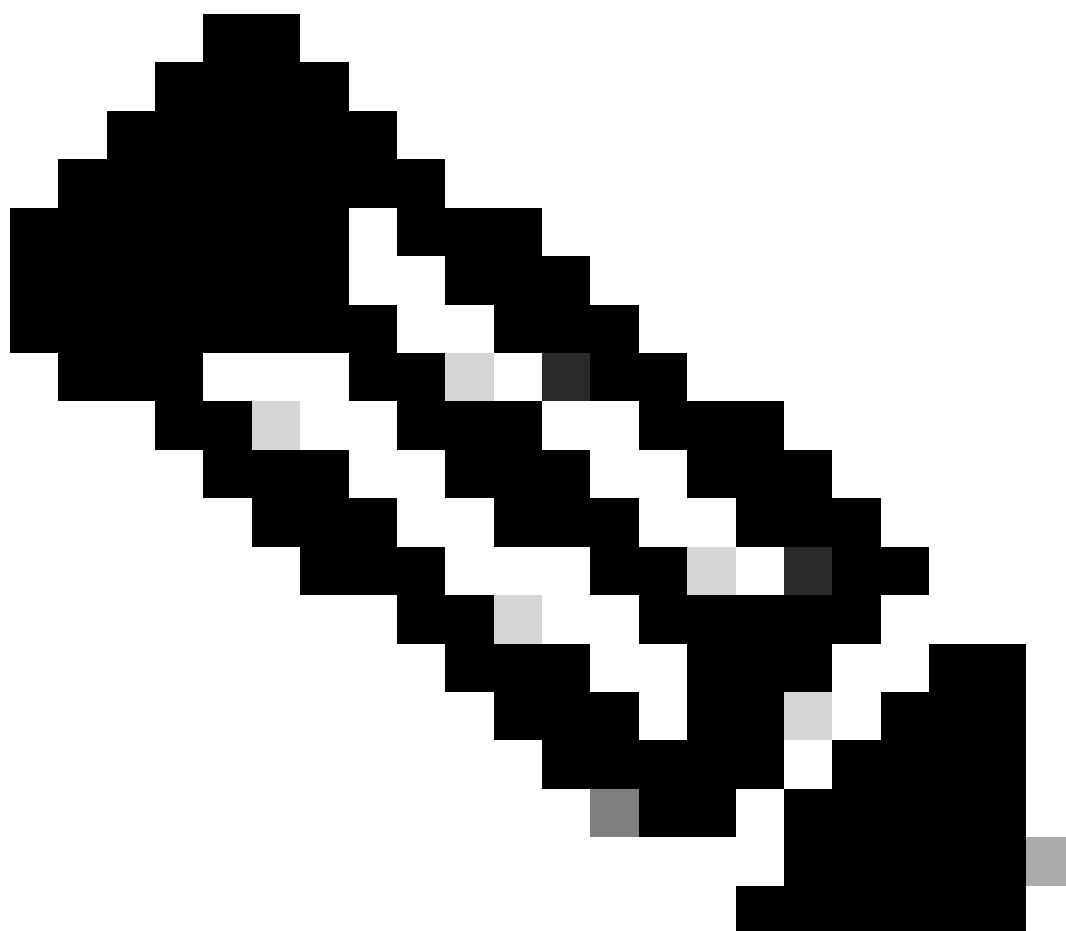
設定

宣告裝置位於 intersight.com

為了在Intersight中宣告一個新目標，請完成上述步驟。

在Nexus裝置上

發出Cisco NX-OS命令show system device-connector claim-info。



注意：對於NX-OS 10.3(4a)之前的版本，請使用「show intersight claim-info」命令



注意：Nexus生成的宣告資訊對映到以下Intersight宣告欄位：

序列號= Intersight宣告ID

Device-ID安全令牌= Intersight宣告代碼

```
# show system device-connector claim-info  
SerialNumber: FDO23021ZUJ  
SecurityToken: 9FFD4FA94DCD
```

Duration: 599

Message:

Claim state: Not Claimed

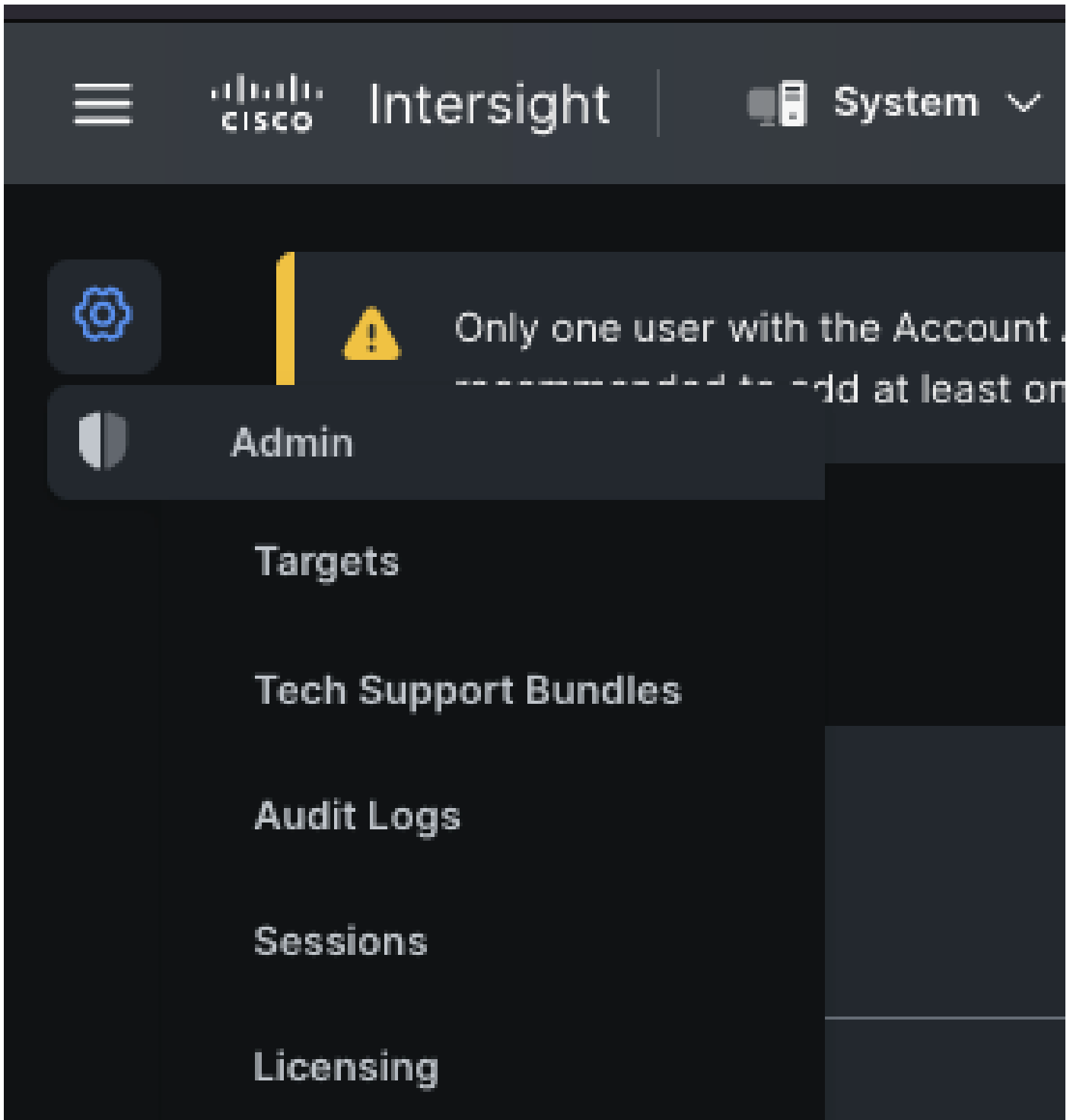
此處報告的Duration以秒為單位。

在Intersight門戶上

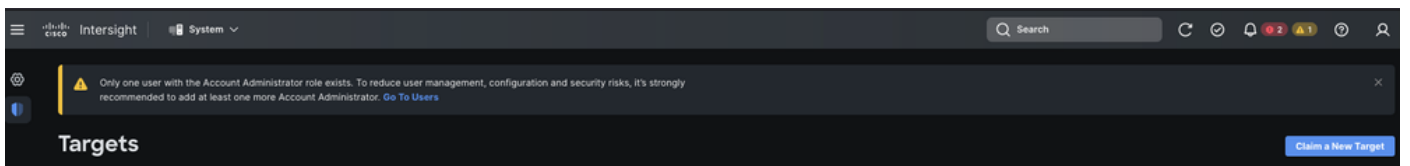
1. 在10分鐘內以「帳戶管理員」、「裝置管理員」或「裝置技術人員」許可權登入Intersight。
2. 從Service Selector下拉選單中選擇System。



3. 定位至ADMIN > Targets > Claim a New Target。



3.1. 按一下宣告新目標，如圖所示。



4. 選擇可用於申請，並選擇要申請的目標型別（例如，網路）。按一下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

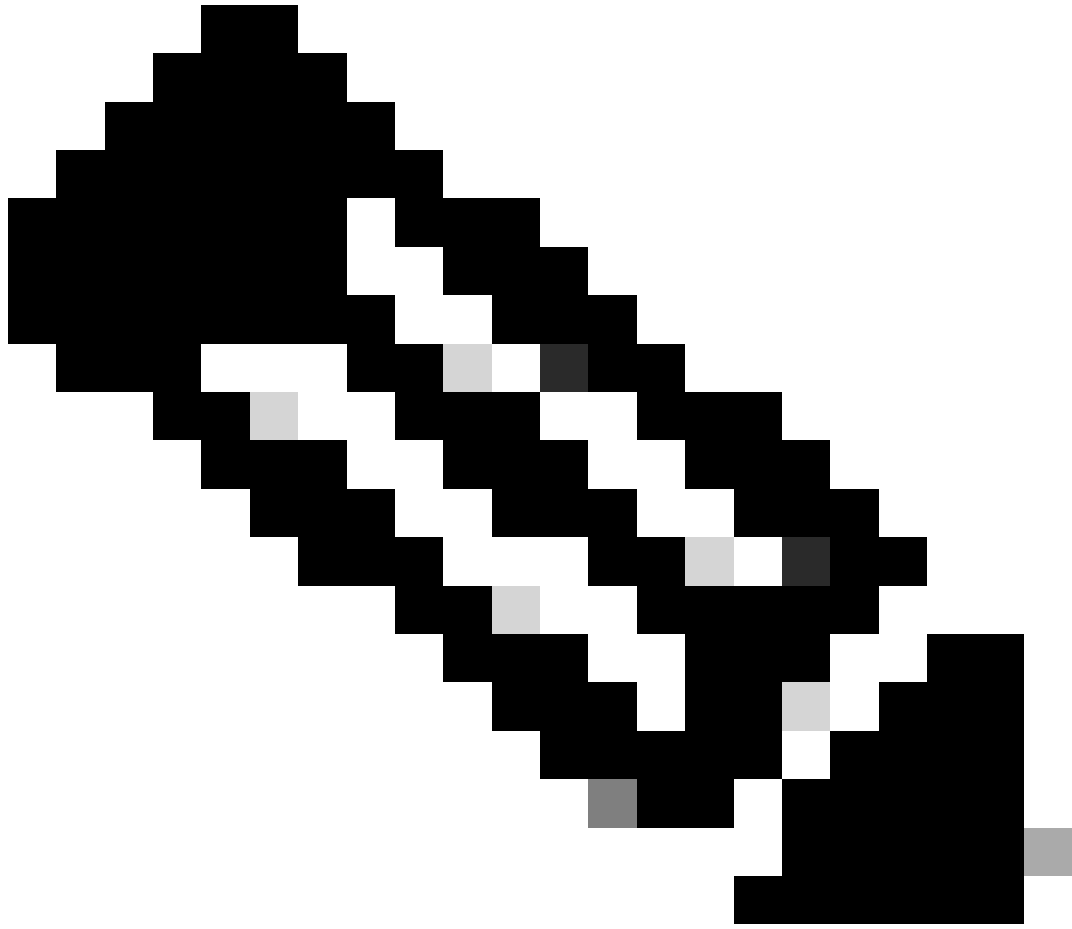
🔍 Search

Network

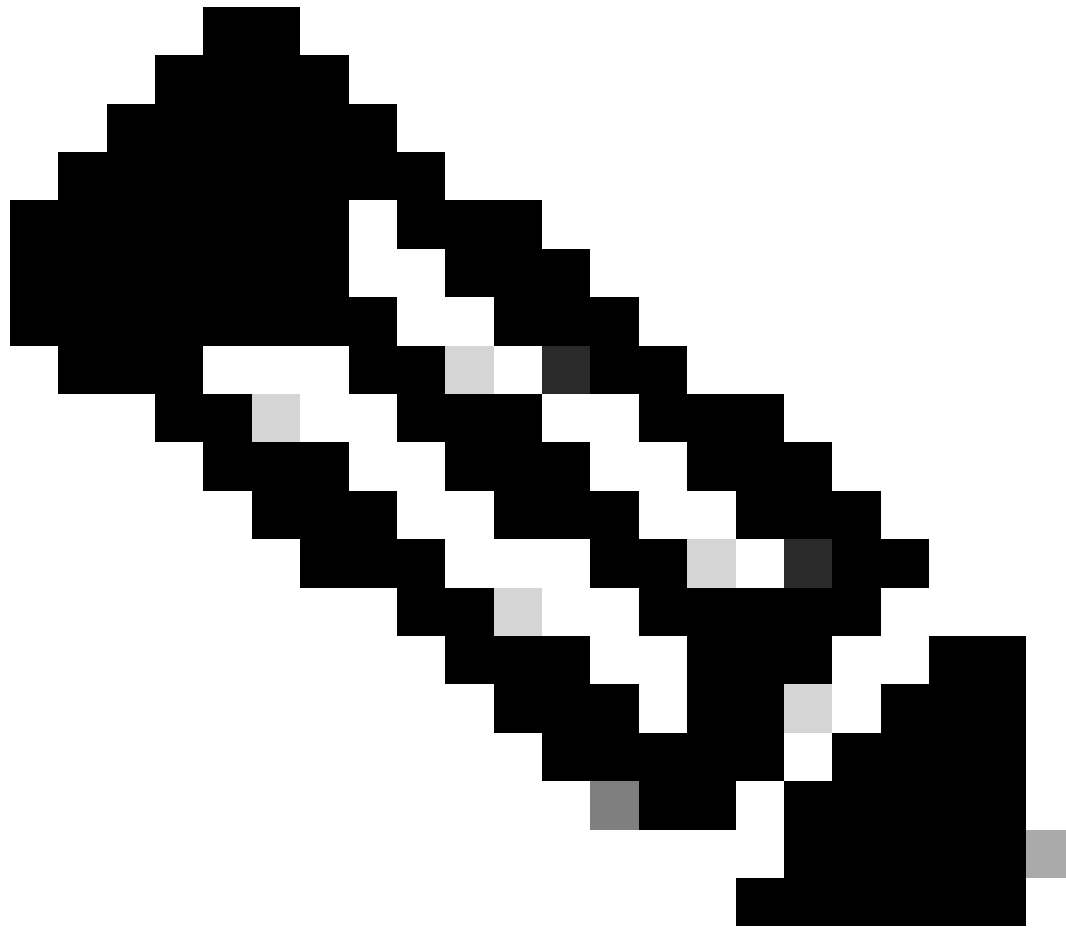
 Cisco MDS Switch	<input checked="" type="checkbox"/> Cisco Nexus Switch	 Cisco APIC
 Cisco Cloud APIC	 Cisco DCNM	 Cisco Nexus Dashboard

[Cancel](#) [Start](#)

5. 輸入所需的詳細資訊，然後按一下索賠以完成索賠流程。



註：交換機上的安全令牌用作宣告代碼，交換機的序列號為裝置ID。



注意：安全令牌過期。您必須在之前完成宣告，否則系統會提示您重新產生宣告。



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



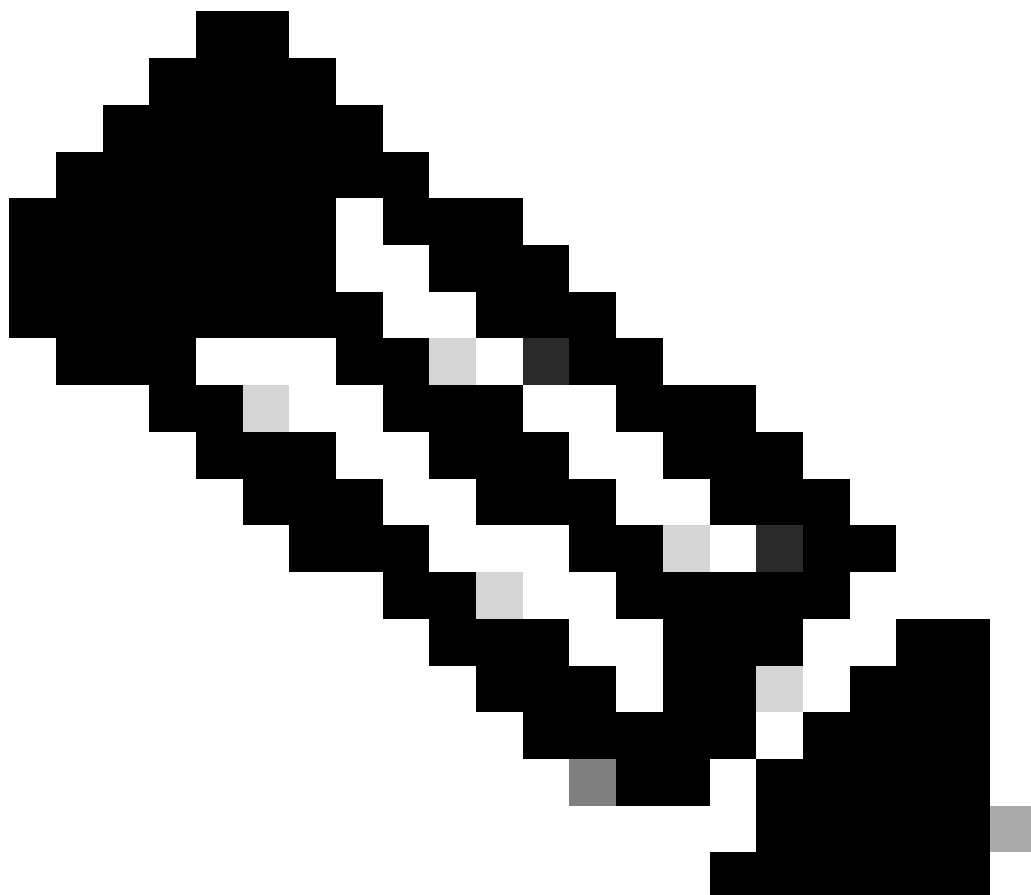
[Details](#)

使用Ansible在intersight.com中宣告一對多獨立式Nexus裝置®

要聲稱是一對多Nexus裝置，可以運行Ansible手冊。

- 可以從<https://github.com/datacenter/ansible-intersight-nxos>克隆ansible資產和攻略。
- 在Ansibleinventory.yaml中，ansible_connection型別設定為ansible.netcommon.network_cli，以便向Nexus交換機傳送命令。可以將其更改為ansible.netcommon.httpapi，以便透過NXAPI進行連線。
- 要連線到Intersight終結點，需要一個API金鑰，該金鑰可透過您的intersight.com帳戶生成。

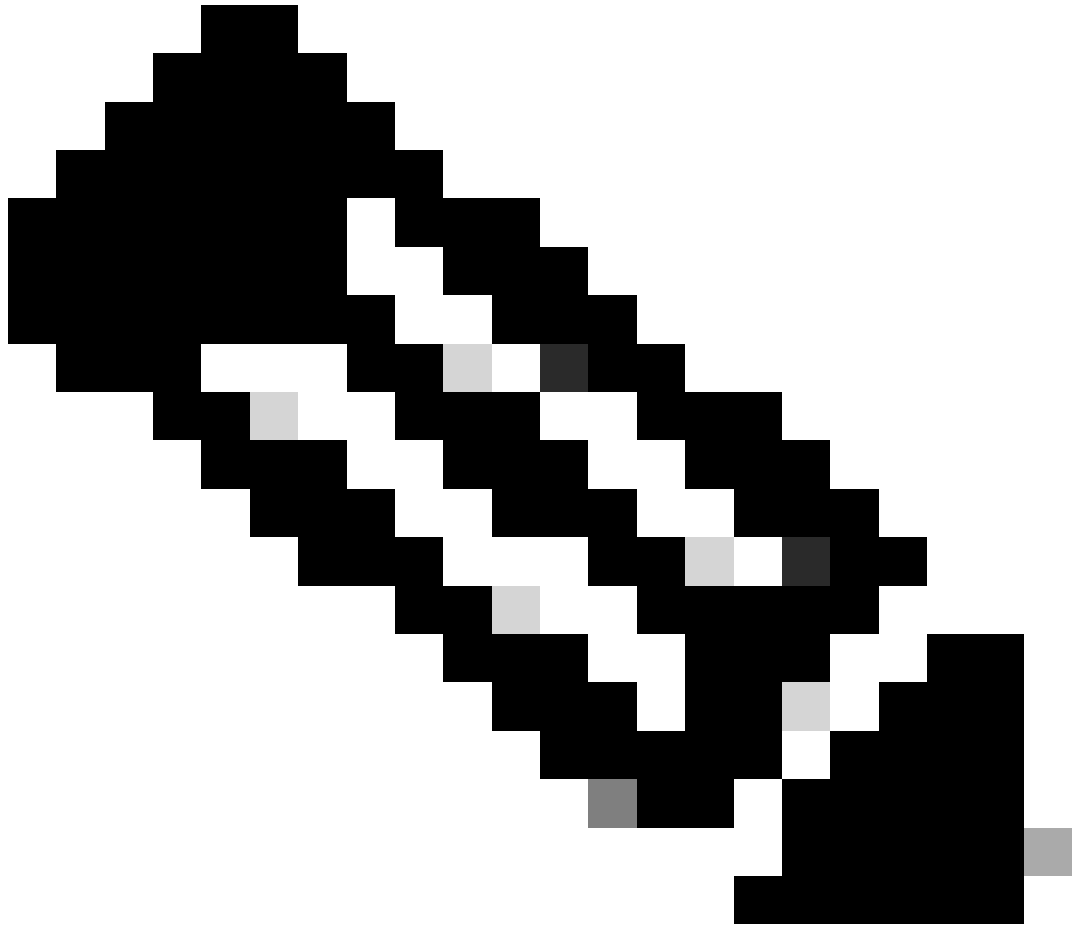
配置Nexus NXAPI(僅在使用ansible.netcommon.httpapi時使用)



注意：如果配置了系統級代理(HTTP(S)_PROXY)，並且Ansible不能使用代理來連線Nexus NXAPI終結點，則需要設定 `ansible_httppapi_use_proxy: False` (預設為True)。

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

要獨立驗證到NXAPI終端的HTTP連線，可以嘗試傳送 `show clock`。在下一個示例中，交換機使用基本身份驗證對客戶端進行身份驗證。也可以配置NXAPI伺服器，以便根據X.509使用者證書對客戶端進行身份驗證。



注意：基本身份驗證雜湊透過username : password的base64編碼獲得。在本示例中，admin : cisco ! 123 base64編碼為YWRtaW46Y2lzY28hMTIz。

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

捲曲回應：

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

產生Intersight API金鑰

有關如何從Intersight System > Settings > API keys > Generate API Key獲取API金鑰，請參閱[README.md](#)部分。

The screenshot shows the Cisco Intersight web interface. At the top, there is a navigation bar with the Cisco logo, 'Intersight', and 'System' dropdown. A search bar and several notification icons are also present. 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 features a sidebar on the left with various configuration categories. The 'API Keys' section is selected, showing a 'Generate API Key' button and a table with columns for Description, API Key ID, Purpose, Cre..., Email, Role, and Identity Provider. The table currently displays 'NO ITEMS AVAILABLE'.

Generate API Key





Description

Nexus Intersight key



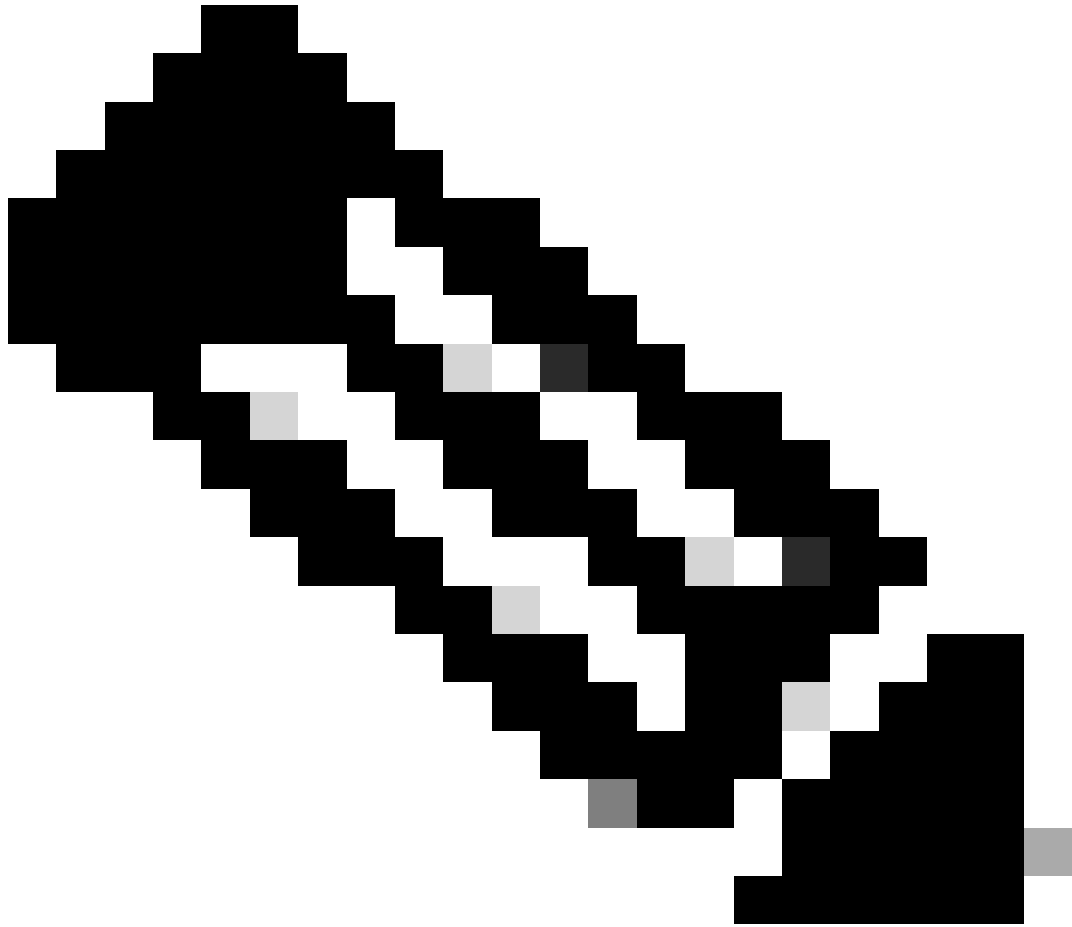
API Key Purpose

- 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

範例：Ansible inventory.yaml



注意：在下一個示例中，對ansible進行了配置，以便使用`ansible_httppapi_use_proxy: False`忽略作業系統代理設定。如果您需要Ansible伺服器使用代理才能連線到交換器，可以移除該組態或將其設定為True（預設值）。

注意：API金鑰ID是一個字串。API私鑰包含指向包含私鑰的檔案的完整路徑。對於生產環境，建議使用Ansible保管庫。

```
---
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"
...

```

範例：執行playbook.yaml

有關使用Ansible對獨立Nexus裝置進行程式設計的詳細資訊，請參閱適用於當前版本的[Cisco Nexus 9000系列NX-OS可程式設計性指南](#)使用Cisco NX-OS的Applications/Using Ansible部分。

```

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

```

驗證

若要驗證新目標的宣告，請完成以下步驟：

在Nexus交換機上

10.3(4a)M之前的版本

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

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

以10.3(4a)M開頭的版本

```
# 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
```

阿尼塞

可以在playbook.yaml末尾增加一個任務，以便獲取交換機插入資訊。

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

以下是相應的輸出：

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

停用裝置聯結器

	命令或操作	目的
步驟 1	<p data-bbox="178 501 344 533">無功能intersight</p> <p data-bbox="178 779 245 810">範例：</p> <p data-bbox="178 987 719 1019">switch(config)# no feature intersight</p>	<p data-bbox="858 600 1417 631">停用intersight進程並刪除所有NXDC配置和日誌儲存。</p>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。