通過Catalyst Center即插即用瞭解交換機自註冊

目錄

簡介

本文檔介紹用於自動交換機自註冊的Catalyst Center即插即用、完整的生命週期、發現方法和故障排除。

說明

Catalyst Center即插即用(PnP)通過Cisco IOS® XE嵌入式PnP代理自動化Cisco Catalyst交換機登入。此過程實現了安全的發現、身份驗證和初始資源調配，最大程度地減少了手動操作，顯著加快了部署速度，提高了配置一致性。PnP通過標準化的設定和可選的0天模板支援可擴展的部署，可確保大規模可靠的部署。

本文檔概述了完整的自註冊生命週期，包括PnP工作流、發現方法、自註冊選項和證書驗證。它還提供有關裝置申報、驗證、故障排除和行業最佳實踐的詳細指導。

對象

本文檔適用於通過Catalyst Center部署和管理Cisco Catalyst交換機的網路管理員、部署工程師和系統整合商。

需求

本文檔的讀者最好具備以下主題的基本工作知識：

- Catalyst Center
- Cisco Catalyst 交換器
- 網路自動化與布建
- DHCP和DNS基礎

必要條件

在開始註冊過程之前，請確保滿足以下前提條件：

- Catalyst Center 2.3.7.9或更高版本已安裝並正常運行。
- Cisco Catalyst交換機運行支援的Cisco IOS XE版本16.12.x或更高版本。
- Catalyst交換機和Catalyst Center之間提供網路連線。
- DHCP伺服器配置了指向Catalyst Center的企業介面IP地址或FQDN的選項43。
- 交換器處於出廠預設值（開箱即用）狀態，而IOS XE 16.12.1及更新版本上提供的pnpa service reset命令可用於將交換器重設為此狀態。

即插即用概念概述

檢視以下關鍵概念，這些概念解釋了Catalyst Center即插即用在新交換機上的方式。

1. PnP伺服器的DHCP發現

當出廠預設的Cisco Catalyst交換機通電時，PnP代理會嘗試使用DHCP發現即插即用控制器（如Catalyst Center）。

發現過程使用標準DHCP交換：

- DHCP發現
- DHCP提供
- DHCP請求
- DHCP確認

如果配置正確，DHCP伺服器包括選項43，為交換機提供PnP伺服器的連線詳細資訊。

2. DHCP選項43格式

DHCP選項43值是一個以分號分隔的ASCII字串，它指定交換機如何連線到PnP伺服器。

範例：

```
option 43 ascii 5A1N;B2;K4;I10.127.212.43;J80;
```

選項43欄位定義

- 5A1N
  - 5 - PnP子選項
  - A — 主用模式（裝置啟動通訊）
  - 1 - PnP代理模板版本
  - N — 禁用調試（D啟用調試）
- B2 - PnP伺服器IP地址型別
  - 1 — 主機名
  - 2 - IPv4地址
  - 3 - IPv6地址
- K4 — 傳輸協定

    - 4 - HTTP
    - 5 - HTTPS
- I - PnP伺服器IP地址或FQDN
- J - TCP埠號

可選引數包括：

- T - Trustpool證書捆綁包URL（對於HTTPS為必填項）
- Z - NTP伺服器IP地址（使用Trustpool安全時必需）

3. DHCP選項43配置示例

- 範例 1：選項43 IPv4配置:10.127.212.43 [Catalyst Center企業介面IP地址]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
  default-router 10.127.212.49
```

- 範例 2：選項43主機名配置：catc1.cisco.com [Catalyst Center FQDN]

```
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
```

- 範例 3:選項43 IPv6配置:2001:60:60:60::133 [Catalyst Center企業介面IPv6地址]

```
ipv6 dhcp pool pnp_pool
 address prefix 2001:70:70:70::/64
 link-address 2001:70:70:70::7/64
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;B3;K4;I2001:60:60:60::133;J80"
```

4. PnP啟動VLAN行為

預設情況下，出廠重設交換器使用VLAN 1進行PnP管理。思科建議在生產環境中使用專用管理VLAN。 以下是設定自訂PnP啟動VLAN的命令：

```
pnp startup-vlan
```

必須在上游交換機上配置此命令。上游交換機使用Cisco發現協議(CDP)將PnP啟動VLAN傳送到新交換機。 那麼下游交換器：

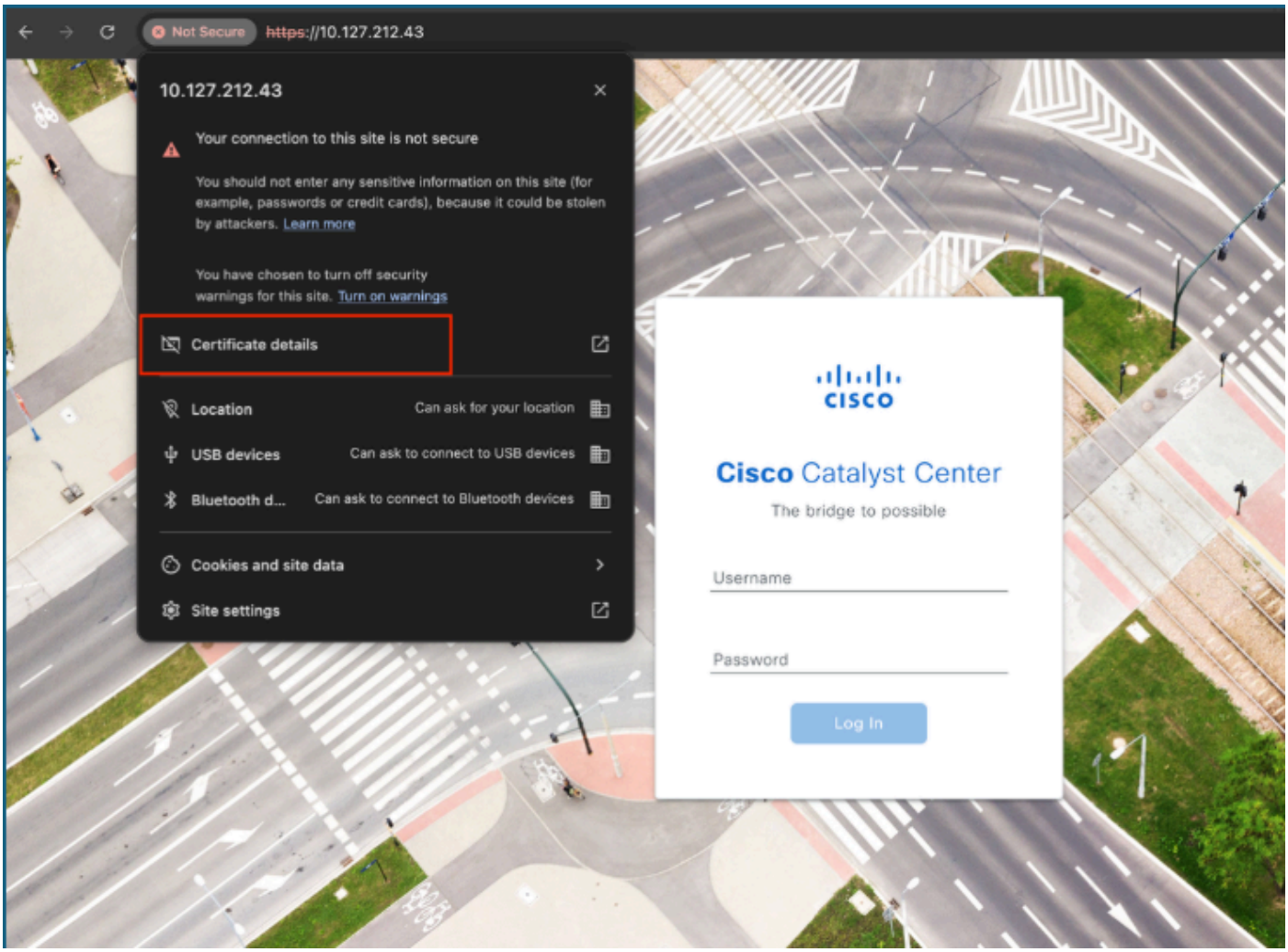
- 禁用VLAN 1上的DHCP
- 在已配置的啟動VLAN上啟用DHCP
- 更新TRUNK以允許新的VLAN

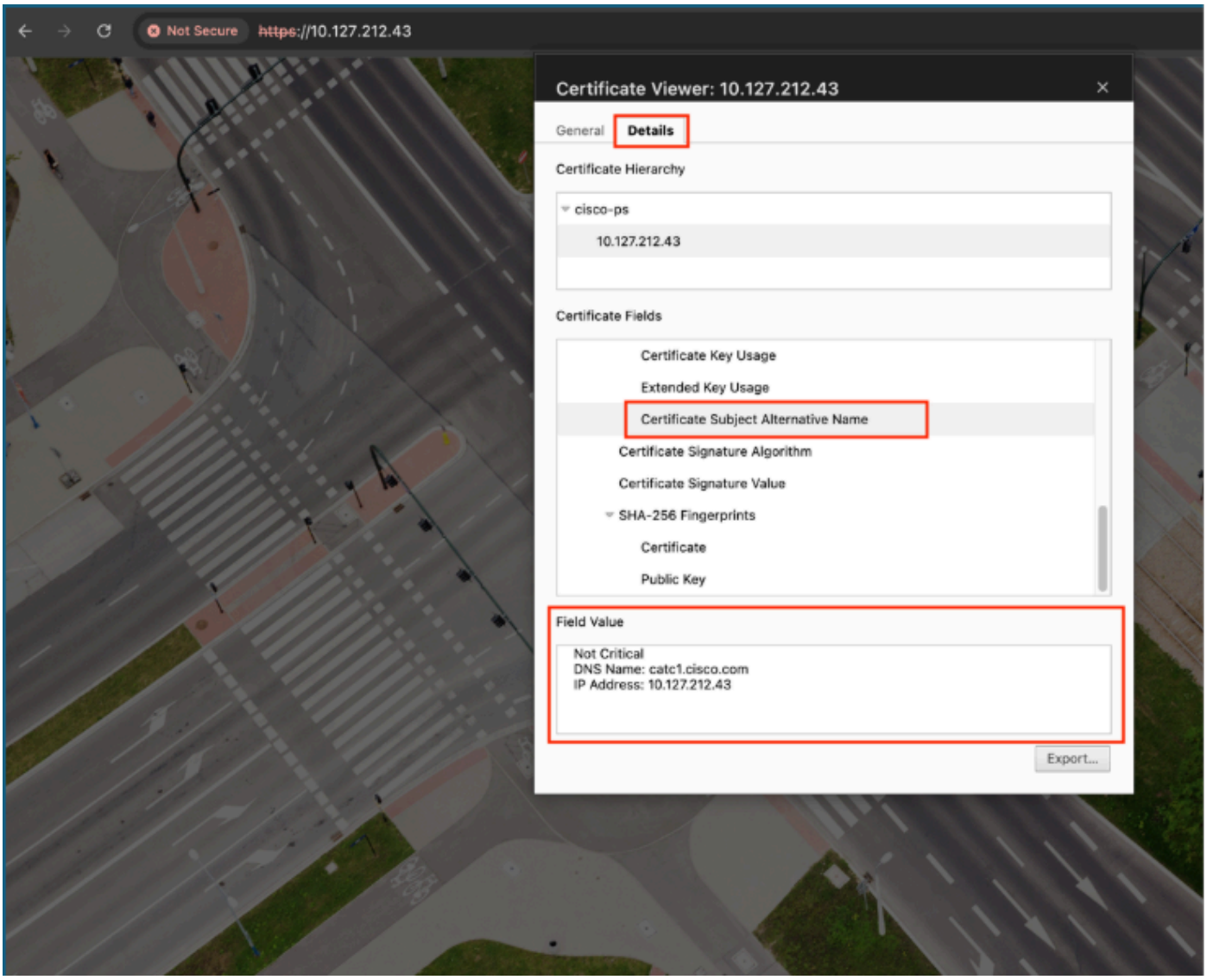
Catalyst Center憑證驗證

安全自註冊要求Catalyst Center SSL證書在Subject Alternative Name(SAN)欄位中包含交換機使用的IP地址或FQDN。

GUI驗證

1. 在瀏覽器中開啟Catalyst Center登入頁面
2. 檢視站點資訊
3. 開啟證書詳細資訊
4. 驗證Extensions（擴展）下的SAN條目


Not Secure
https://10.127.212.43
10.127.212.43
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to turn off security warnings for this site. Turn on warnings
Certificate details
Location
Can ask for your location
USB devices
Can ask to connect to USB devices
Bluetooth d...
Can ask to connect to Bluetooth devices
Cookies and site data
Site settings
cisco
Cisco Catalyst Center
The bridge to possible
Username
Password
Log In



附註：如果SAN或Subject Alternative Name欄位包含：

- 僅DNS名稱 — 在選項43字串中配置DNS名稱。
- 僅IP地址 — 在選項43字串中配置IP地址。
- IP地址和DNS名稱 — 在選項43字元串中配置IP地址。

CLI 驗證

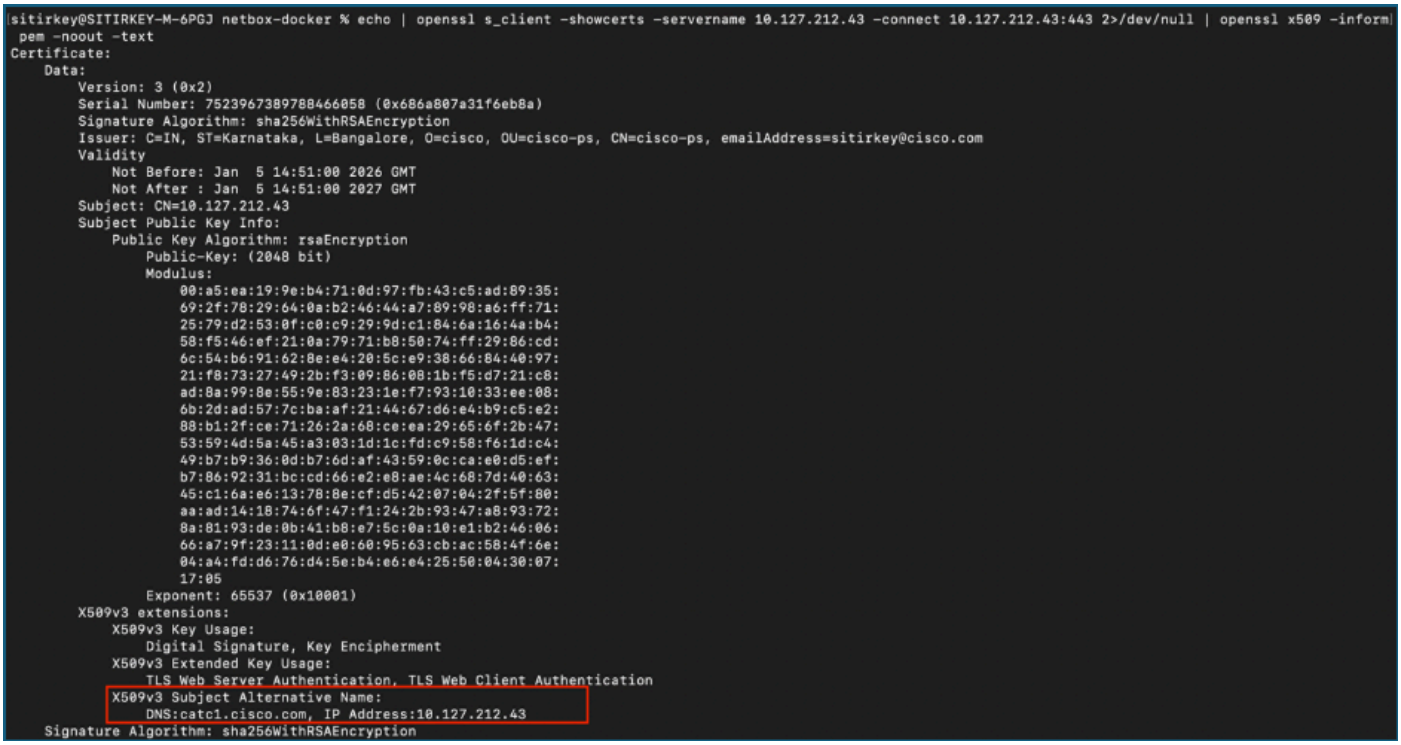
若要驗證這一點，我們需要使用Catalyst Center IP地址和可以到達Catalyst Center伺服器的電腦。在終端機或命令提示符下運行此命令。

```
echo | openssl s_client -showcerts -servername
```

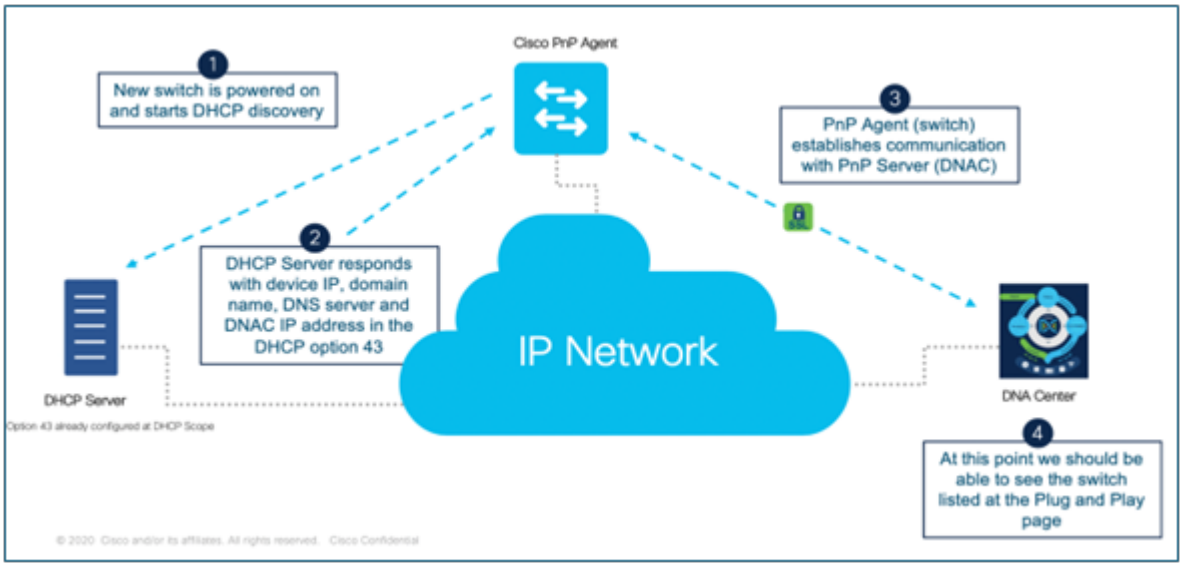
```
-connect

:443 2>/dev/null | openssl x509 -noout -text
```

驗證SAN欄位包含適當的IP地址或FQDN。



網路圖表



Cisco PnP通過啟用發現、配置和管理功能，最大限度地減少手動操作，從而自動執行新裝置註冊。當新交換機通電時，它將傳送DHCP發現請求，並且DHCP伺服器返回網路詳細資訊，包括通過DHCP選項43的Catalyst Center（PnP伺服器）IP地址。使用此資訊，交換機的PnP代理通過IP網路安全地連線到PnP伺服器。建立連線後，對裝置進行身份驗證和識別，然後將其新增到即插即用清單中，管理員可以在其中快速一致地應用配置和完成調配。

交換機登入方法

檢視本節中的各種自註冊方法，通過這些方法可以將交換機註冊到Catalyst Center的即插即用清單中。

1.使用VLAN1進行板載

此方法使用預設VLAN 1進行PnP管理

需求

- 在上游交換機上配置VLAN 1 SVI。
- 配置了選項43的DHCP伺服器
- Catalyst Center FQDN的DNS解析

上游交換機上的過程

步驟1.配置VLAN 1的SVI。

```
config t
interface Vlan1
  ip address 10.127.212.49 255.255.255.0
```

步驟2.使用選項43配置DHCP池（注意：可以將選項43引數與Catalyst Center的IPv4地址或FQDN配合使用）。

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

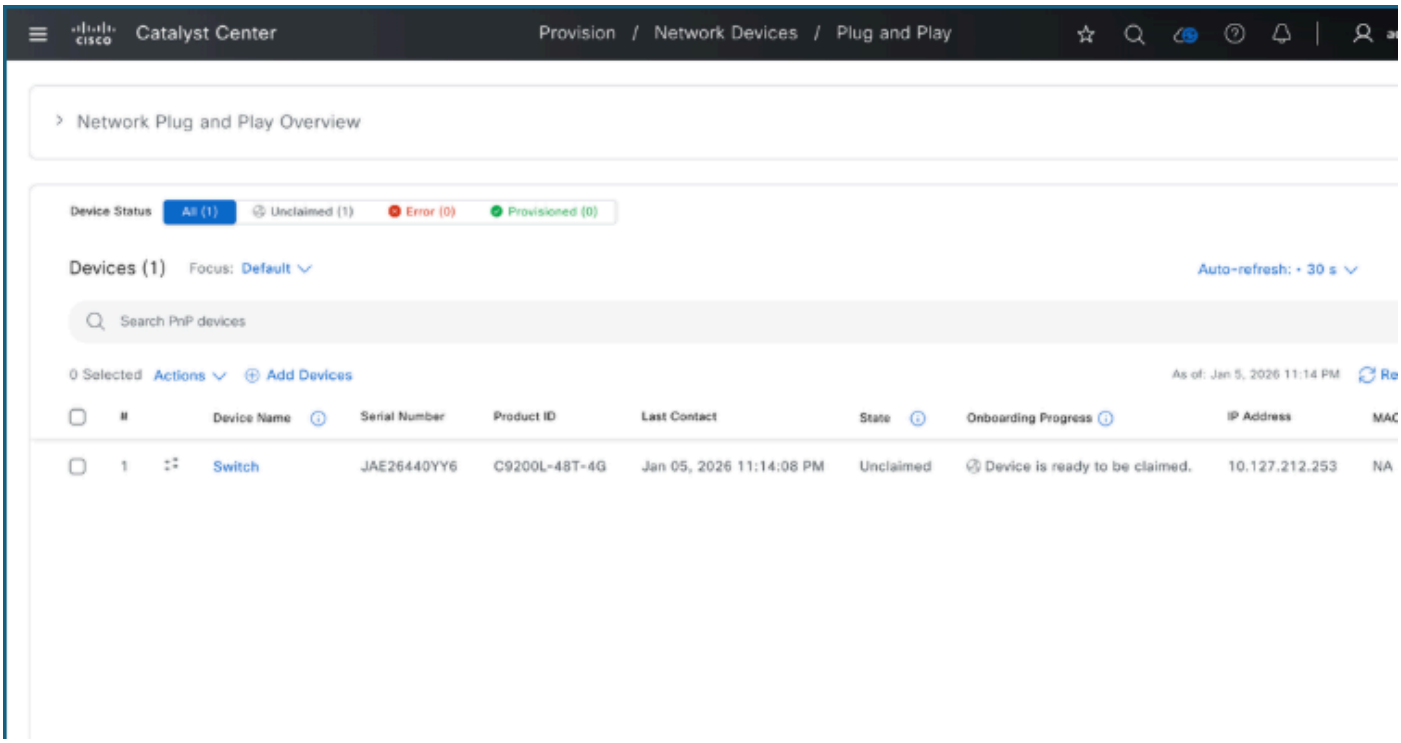
或

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

步驟3.為新交換機配置中繼介面。

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
```

步驟4.驗證交換器是否顯示在Catalyst Center的「Provision > Plug and Play」頁面上。



2.使用自定義VLAN進行板載

此方法使用專用VLAN進行管理。

需求

- 在上游交換機上配置自定義VLAN SVI。
- 配置了選項43的DHCP伺服器。
- Catalyst Center FQDN的DNS解析。
- Trunk允許自定義VLAN以及其他流量所需的任何其他VLAN。

上游交換機上的過程

步驟1.配置自定義VLAN的SVI。

```
config t
interface Vlan302
  description PnP_Vlan
    ip address 10.127.212.49 255.255.255.0
```

步驟2.使用選項43配置DHCP池（注意：可以將選項43引數與Catalyst Center的IPv4地址或FQDN配合使用）。

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B2;K4;I10.127.212.43;J80;
```

或

```
config t
ip dhcp pool pnp_pool
  network 10.127.212.0 255.255.255.0
  option 43 ascii 5A1D;B1;K4;Icatc1.cisco.com;J80;
  default-router 10.127.212.49
  dns-server 10.127.212.1
```

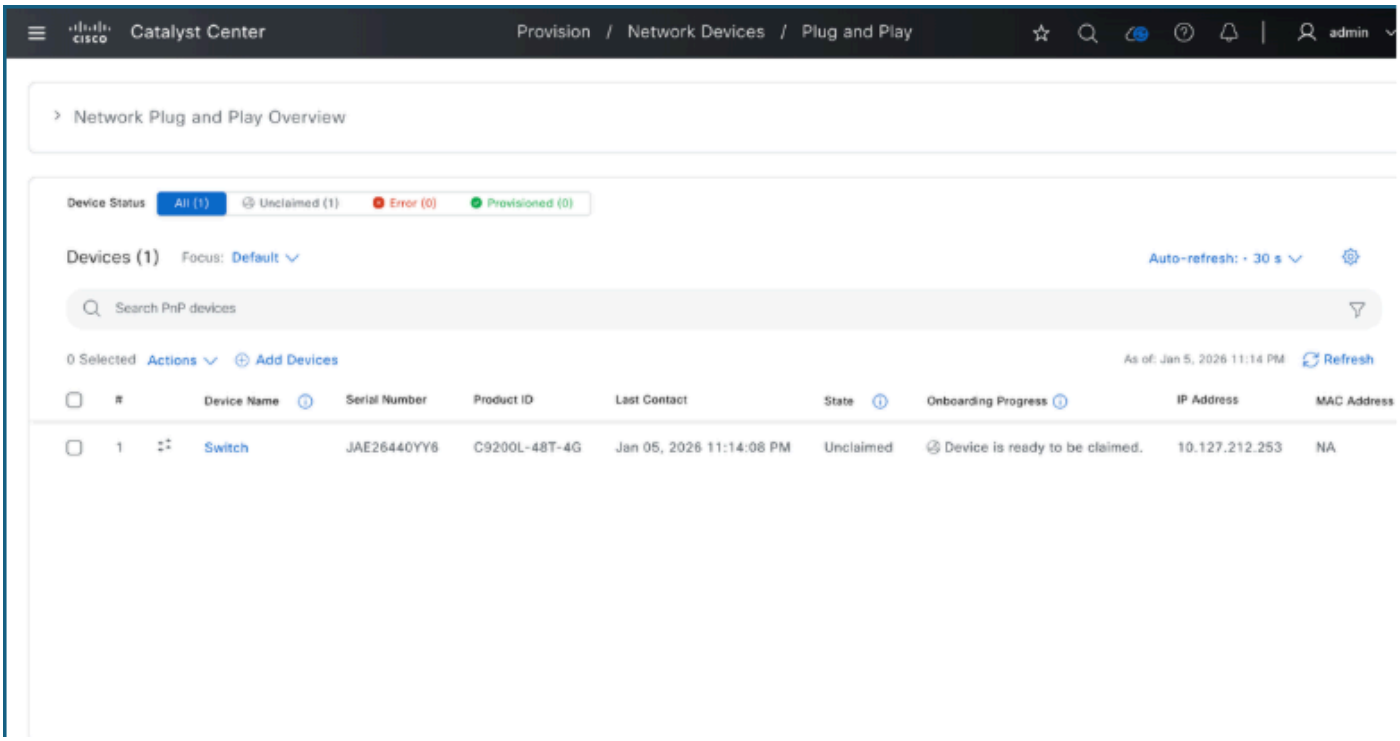
步驟3.將自定義VLAN配置為PnP VLAN。

```
config t
pnp startup-vlan 302
```

步驟4.將中繼介面配置為新交換機。

```
config t
interface GigabitEthernet1/0/5
  description PnP_Trunk
  switchport mode trunk
  switchport trunk allowed vlan 302
```

步驟5.驗證交換器是否顯示在Catalyst Center的「Provision > Plug and Play」頁面上。



3.使用管理埠的板載交換機

此方法利用交換器的管理介面。

需求

- 在上游交換機上配置的自定義VLAN SVI
- 配置了選項43的DHCP伺服器
- Catalyst Center FQDN的DNS解析

上游交換機上的過程。

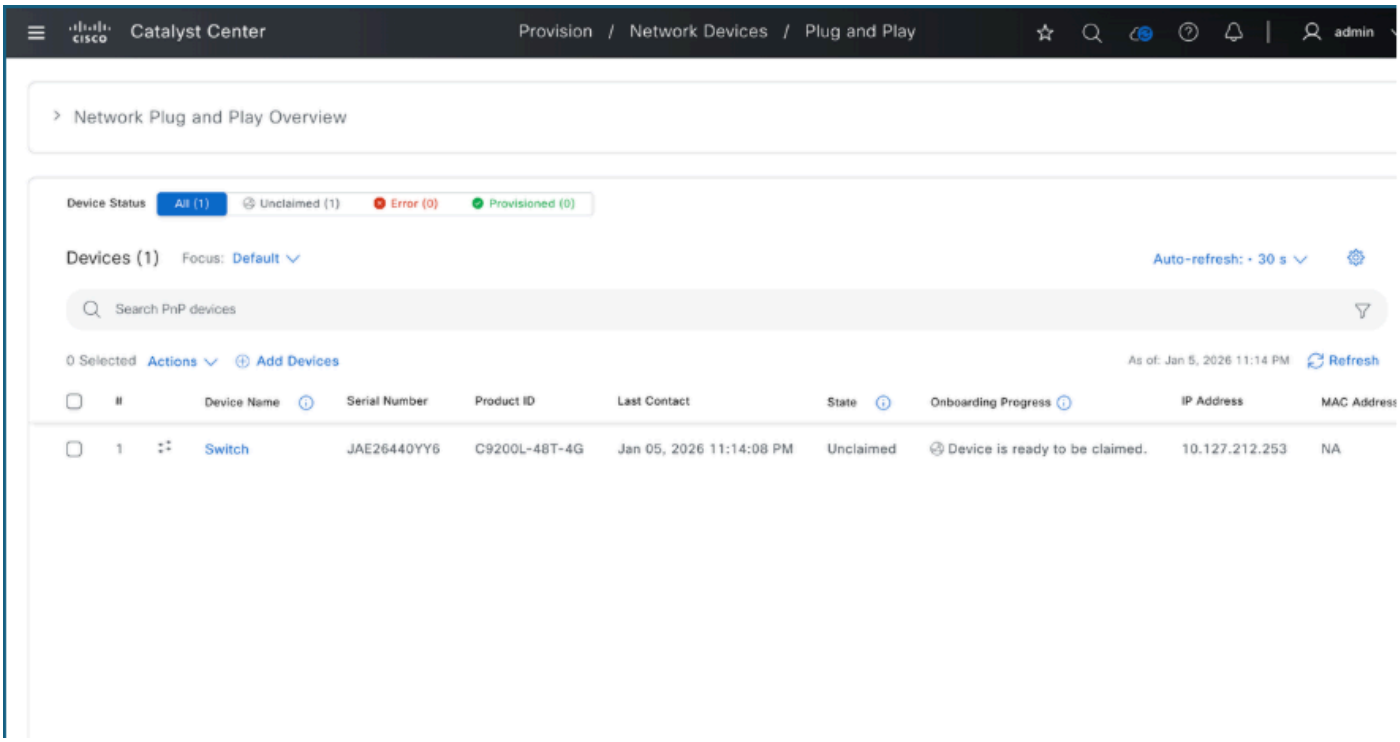
步驟1.配置VLAN的SVI。

```
config t
interface Vlan302
    ip address 10.127.212.49 255.255.255.0
    ip helper-address 10.127.212.1
```

步驟2.配置新交換機的接入介面。

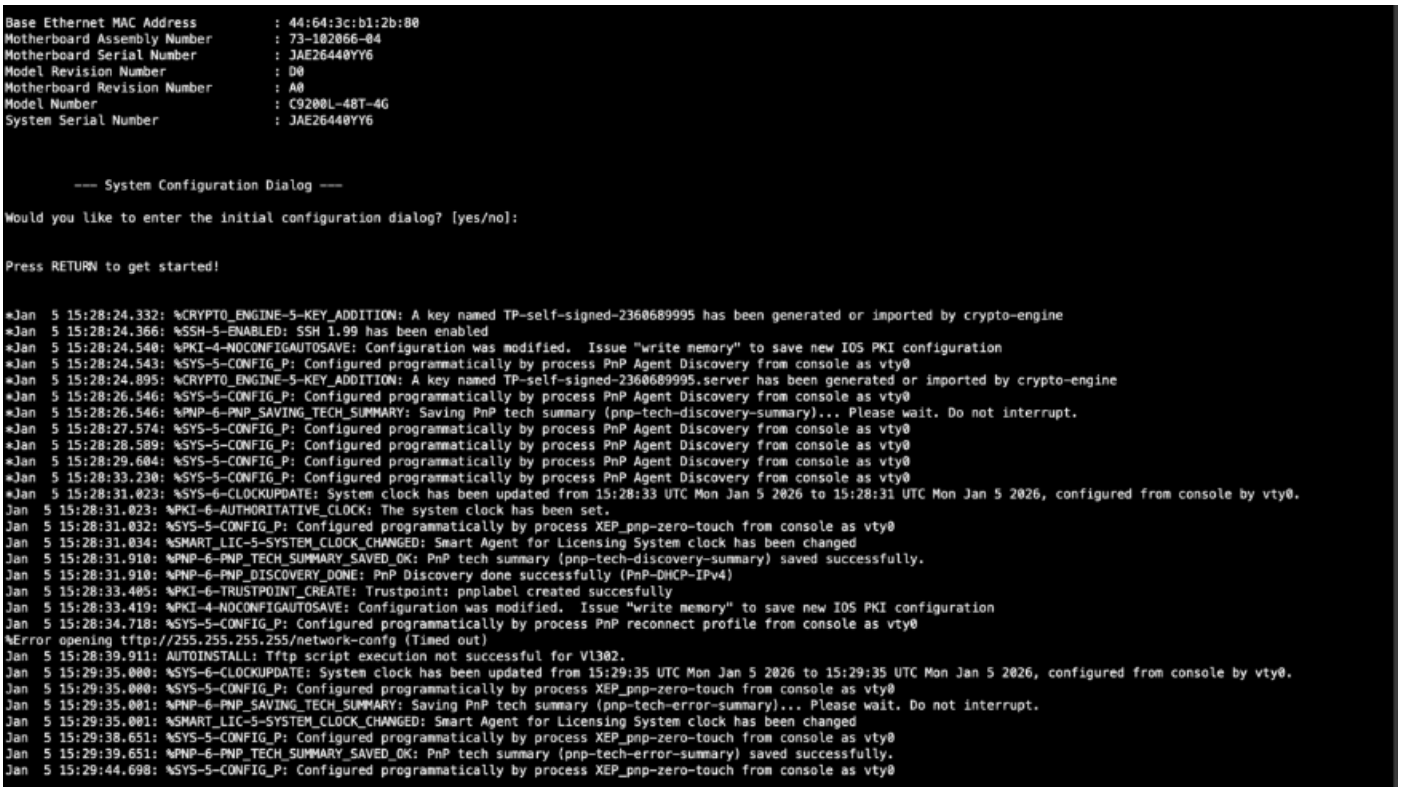
```
config t
interface GigabitEthernet1/0/5
  switchport mode access
  switchport access vlan 302
```

步驟3.驗證交換器是否顯示在Catalyst Center的Provision > Plug and Play頁面上。



4.交換機控制檯日誌

以下是將DHCP用於即插即用時，交換機控制檯上顯示的內容。

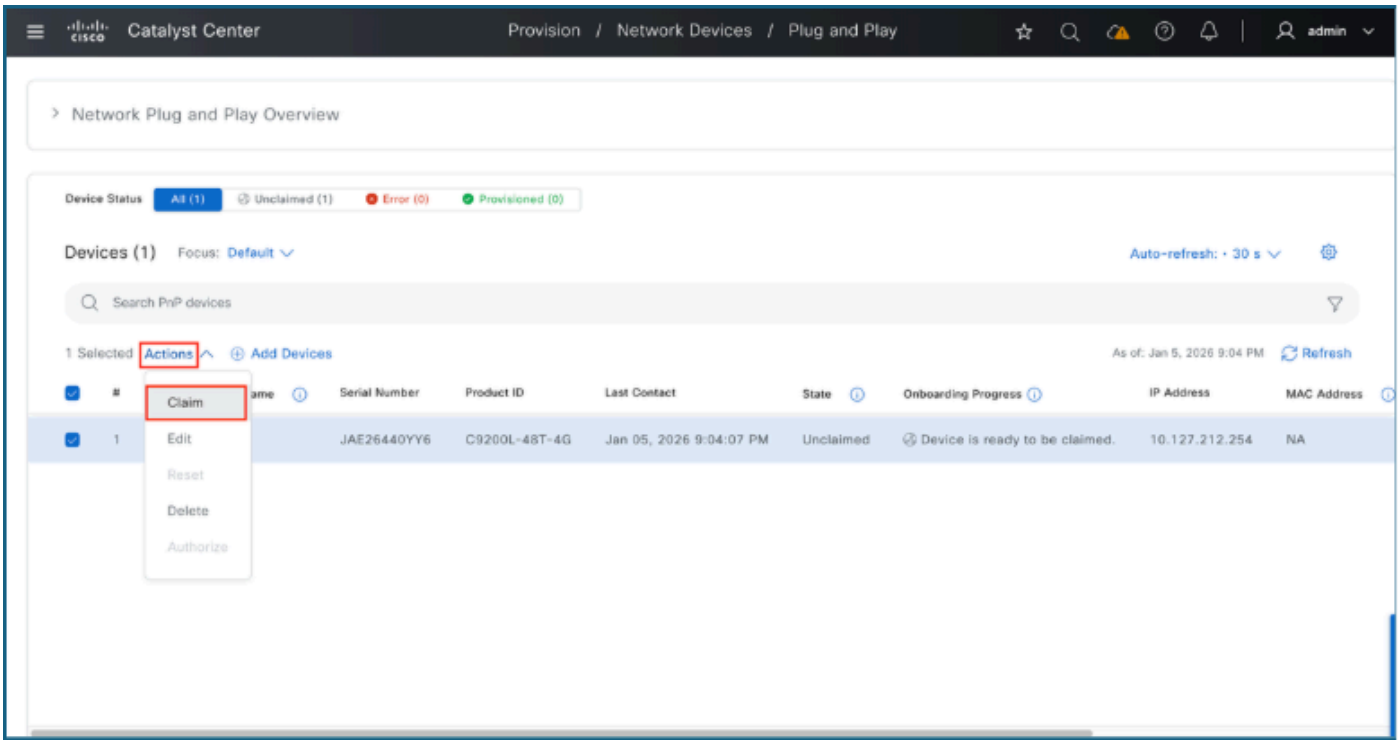


無需第0天模板即可將交換機註冊到Catalyst Center

若要將新交換機安裝到Catalyst Center的資產中，請在裝置在「即插即用」頁面上可見並且可回收時完成這些必要的步驟。

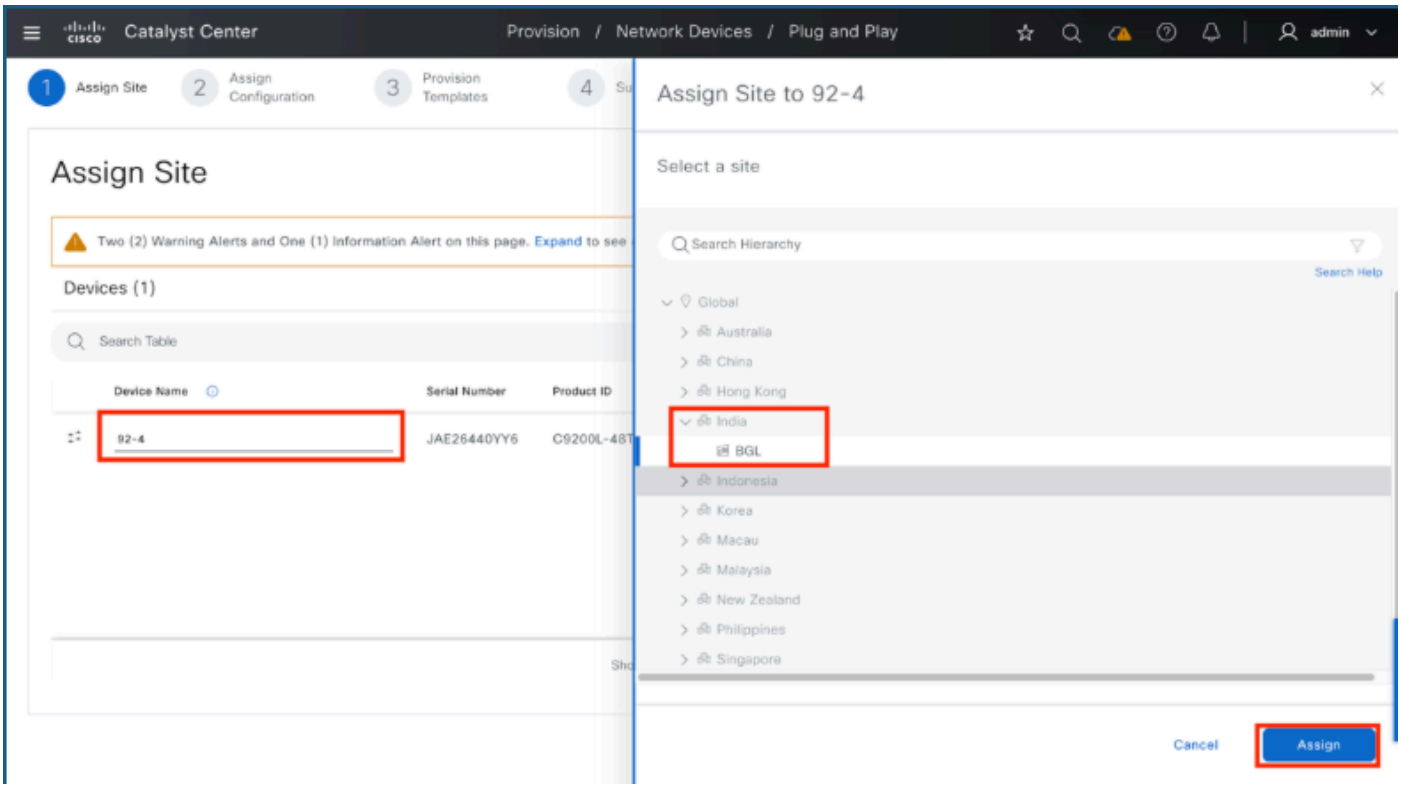
1.要宣告交換機，請執行以下操作：

- 選中要申領的交換機的覈取方塊。
- 定位至「活動」>「索賠」。



2.要命名和對映交換機：

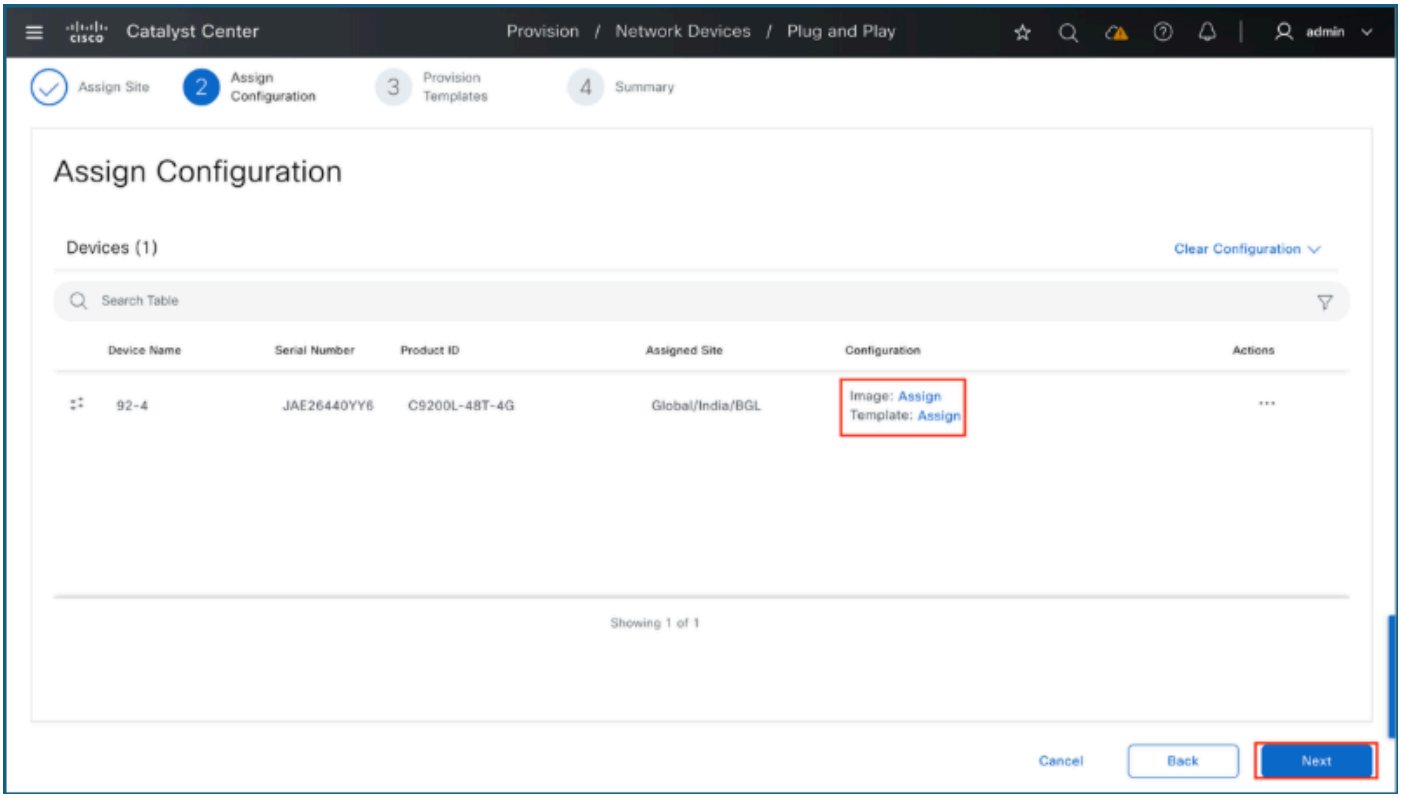
- 在Device Name欄位中輸入名稱，然後按一下Assign。
- 選擇正確的站點或建築，再次按一下Assign，然後按一下Next。



3.分配軟體映像或模板（可選）：

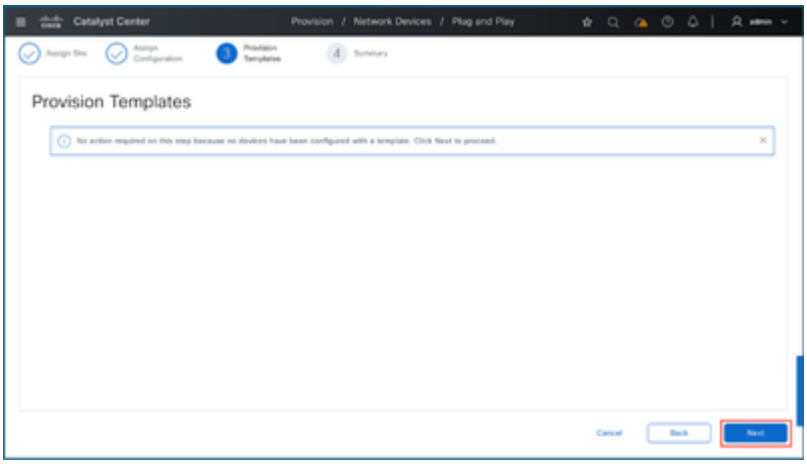
使用此步驟將交換機升級到特定軟體版本或應用第0天配置模板。

- 按一下Image旁邊的Assign以指定軟體版本。
- 按一下Template旁邊的Assign應用模板配置。
- 完成所需的分配後，按一下下一步。



4.調配模板

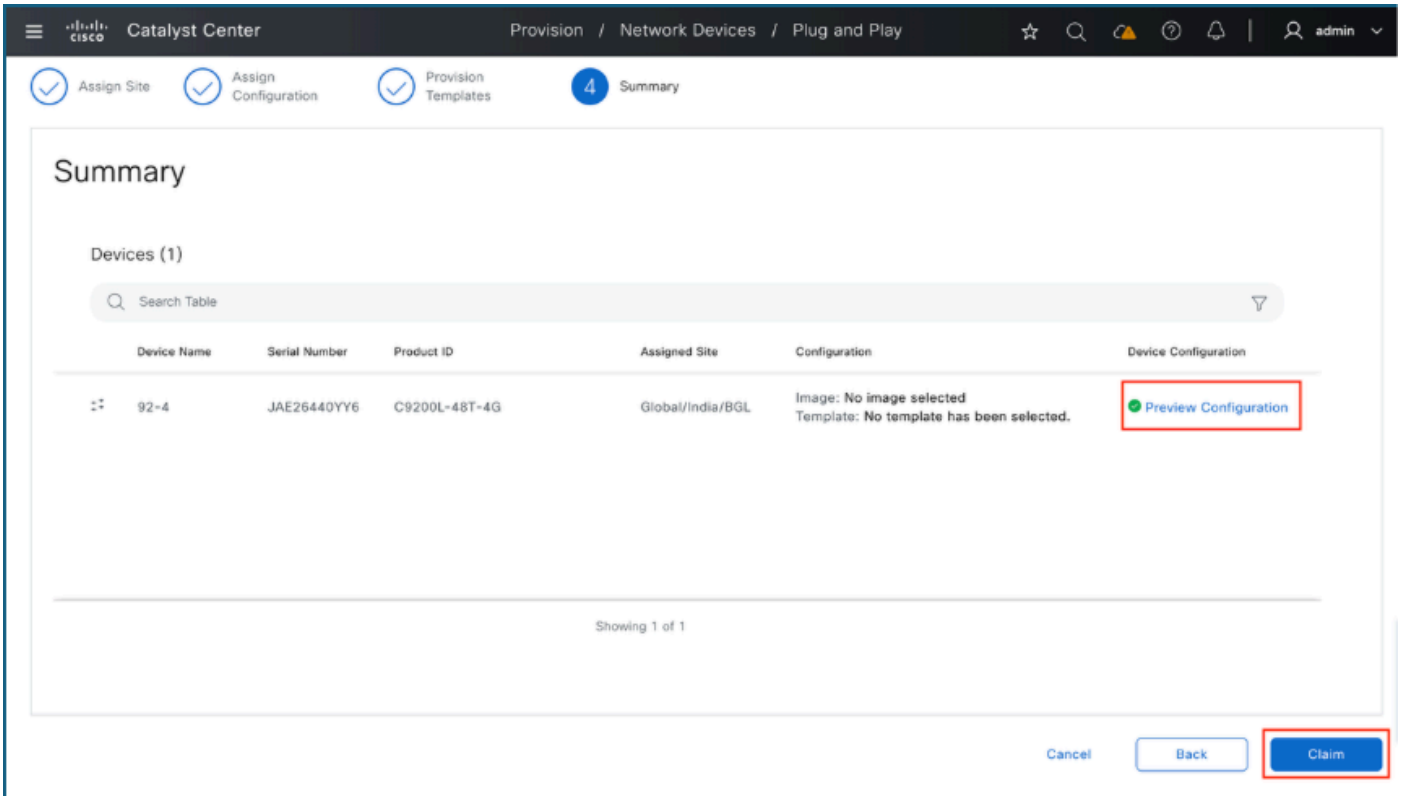
在不使用模板的情況下申請裝置時，請選擇下一步以繞過此配置步驟。

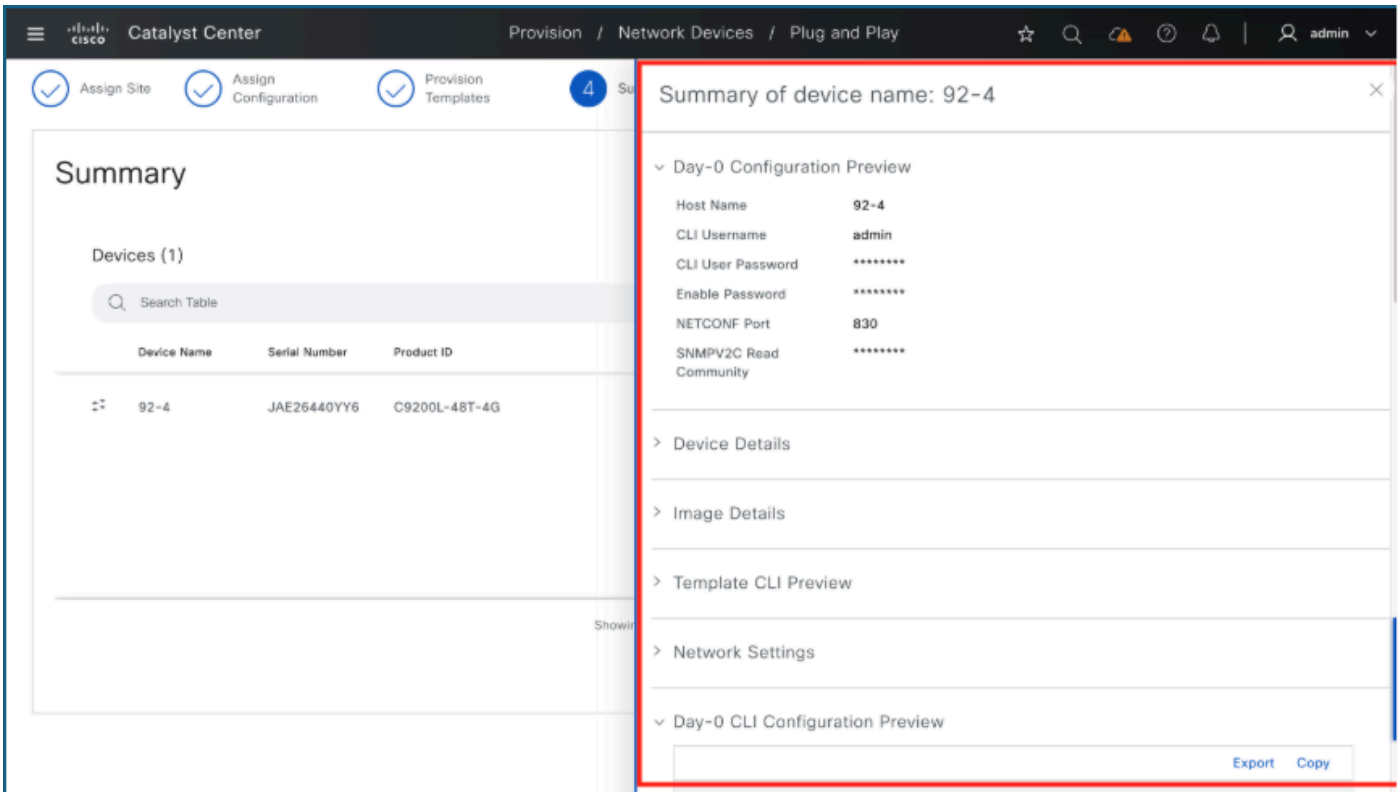


5.摘要

使用「摘要」頁面可在Catalyst Center預配配置之前檢視配置。

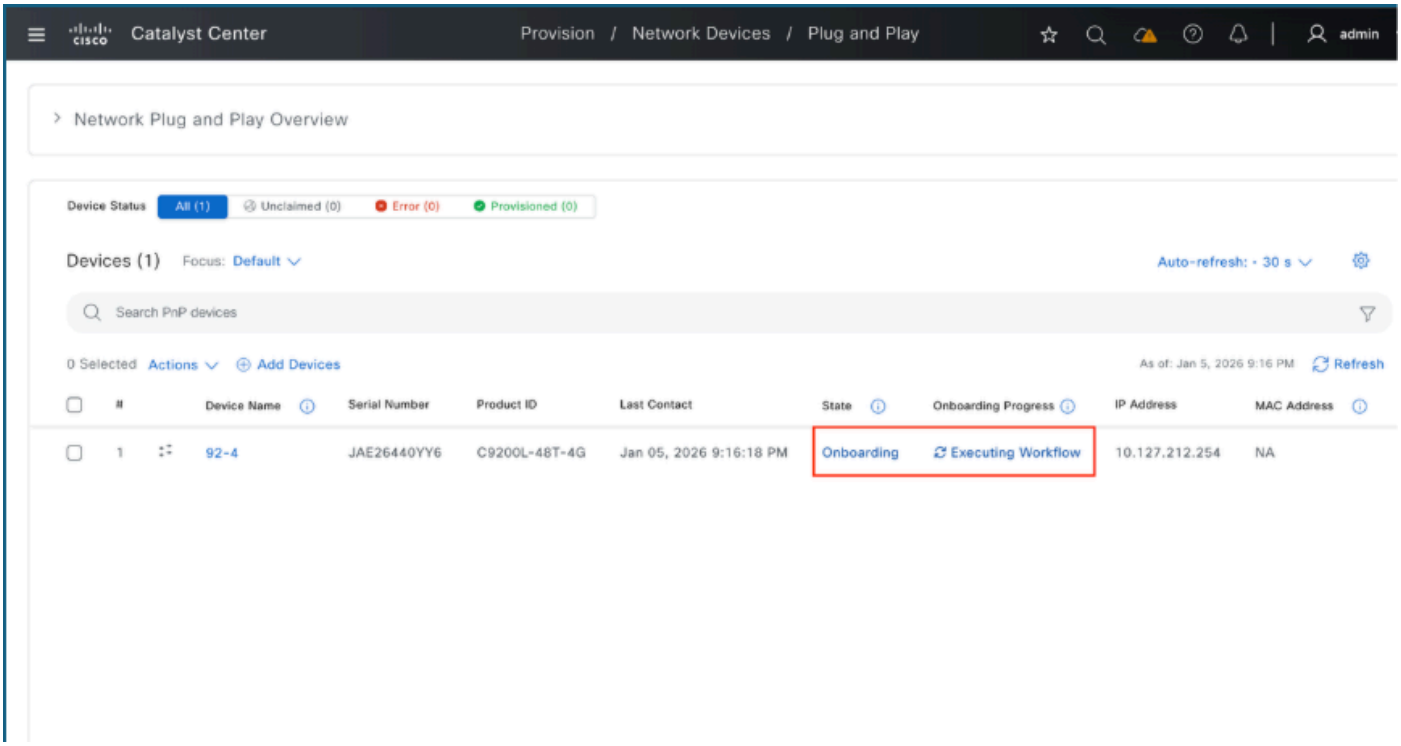
- 按一下「Preview Configuration」。
- 展開各個部分以驗證設定。
- 驗證後，按一下Claim。

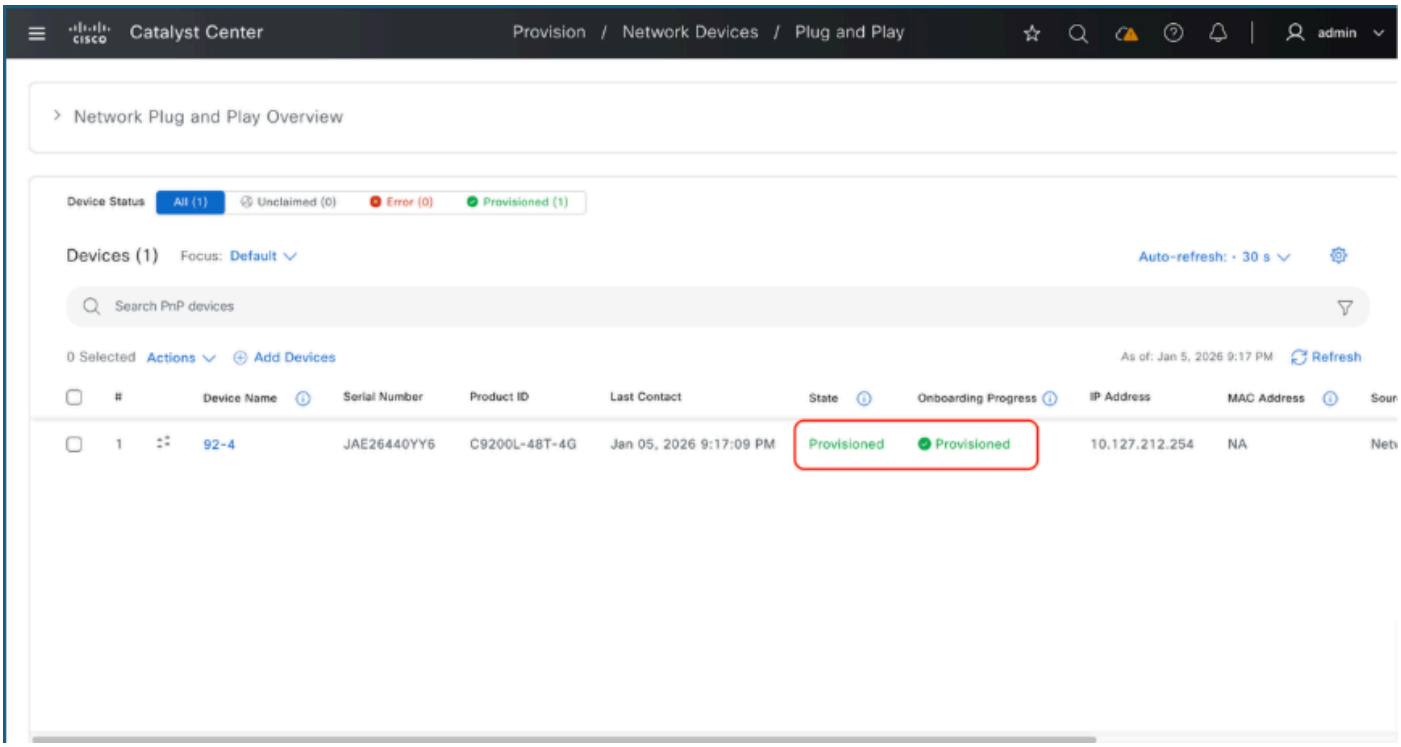




6.監控報銷申請流程

啟動宣告後，該介面會返回到「即插即用」控制面板。監控裝置狀態，如果轉換為已布建，則表示已成功宣告交換器並將其新增到Catalyst Center的清單中。



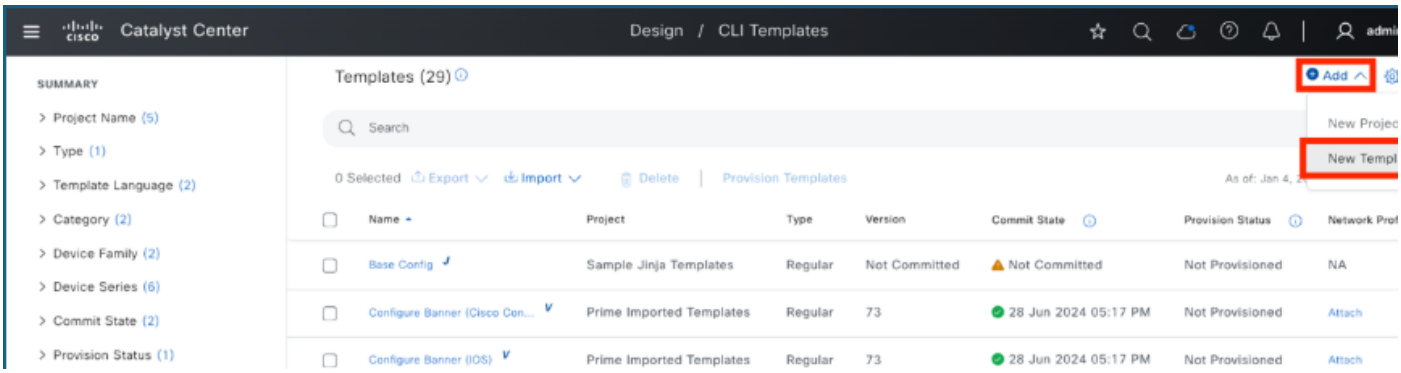


使用第0天模板將交換機註冊到Catalyst Center

在Catalyst Center的「即插即用」頁面上申請新交換機時，應用第0天模板以在申請過程中包括其他配置。

1.建立第0天或入職模板

- 導覽至Design > CLI Templates。
- 選擇Add > New Template。

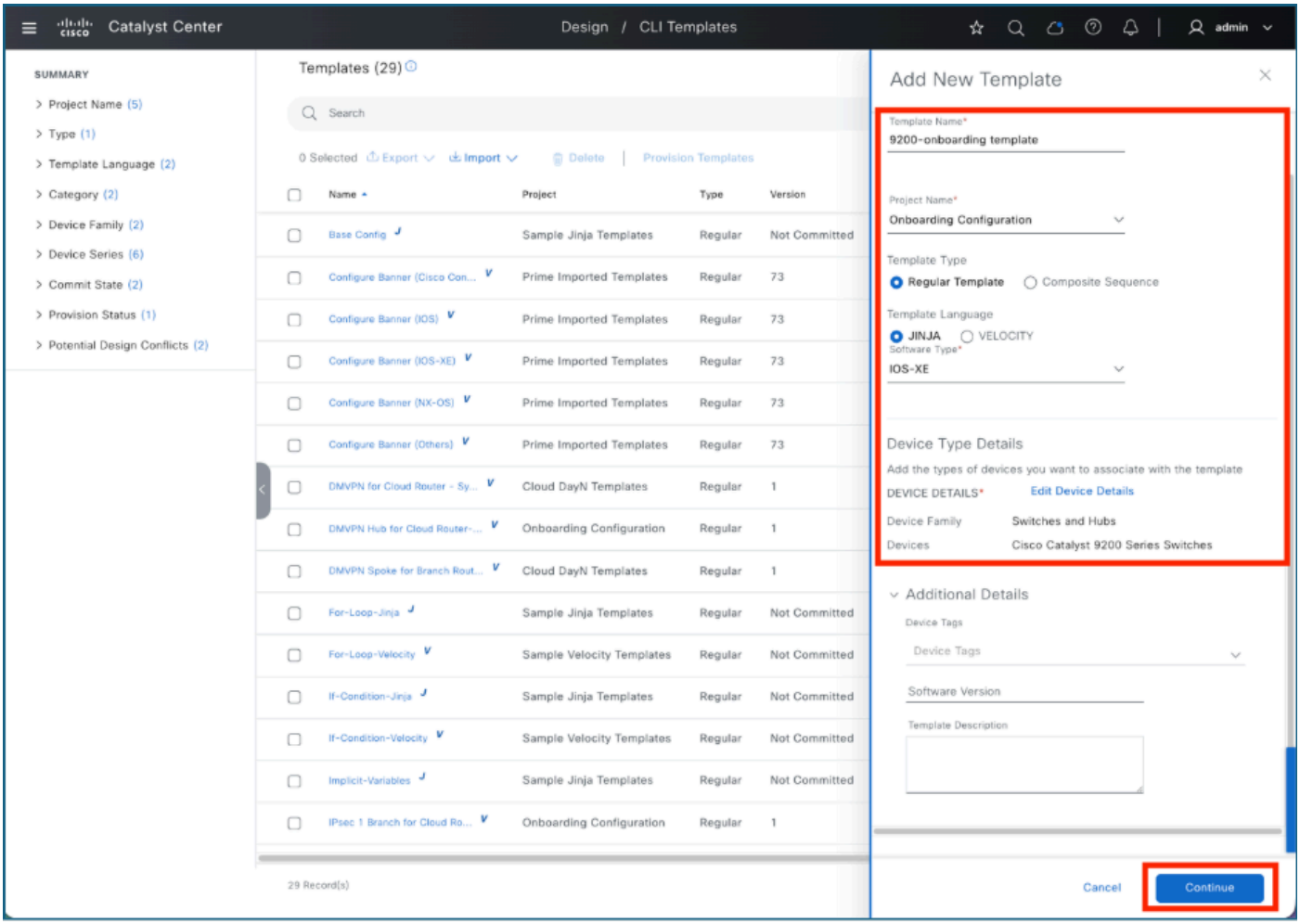


2.新增模板詳細資訊

在側面板中，輸入以下模板規範：

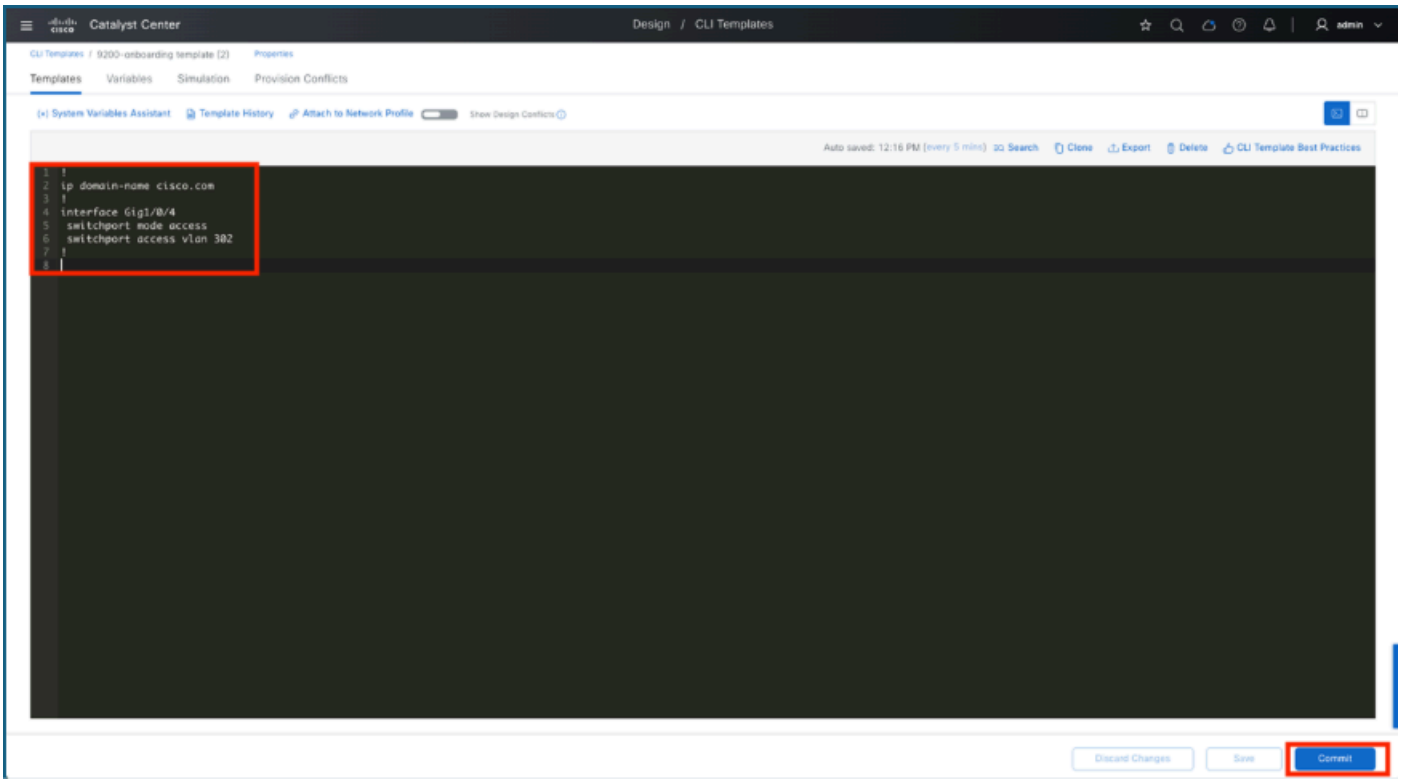
- 模板名稱
- 專案名稱:對於0天模板，請始終選擇Onboarding Configuration。

- 模板型別、語言和軟體型別:從選單中選擇適當的值。
- 按一下Continue以繼續。



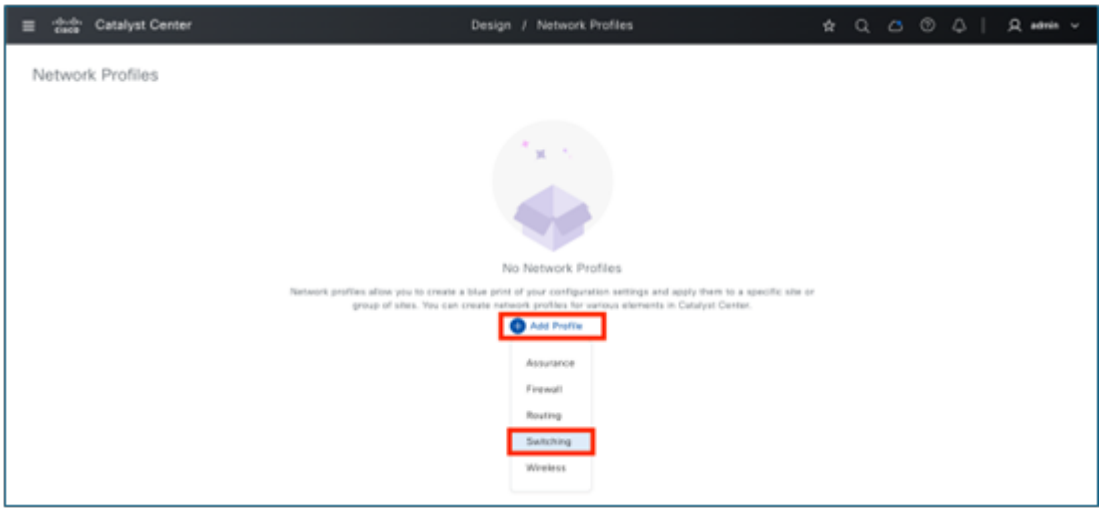
3.編輯模板

在CLI模板編輯器中輸入要部署到交換機的配置。在此示例中，配置了域名和訪問埠。將配置新增到CLI模板編輯器後，按一下Save，然後按一下Commit完成更改。



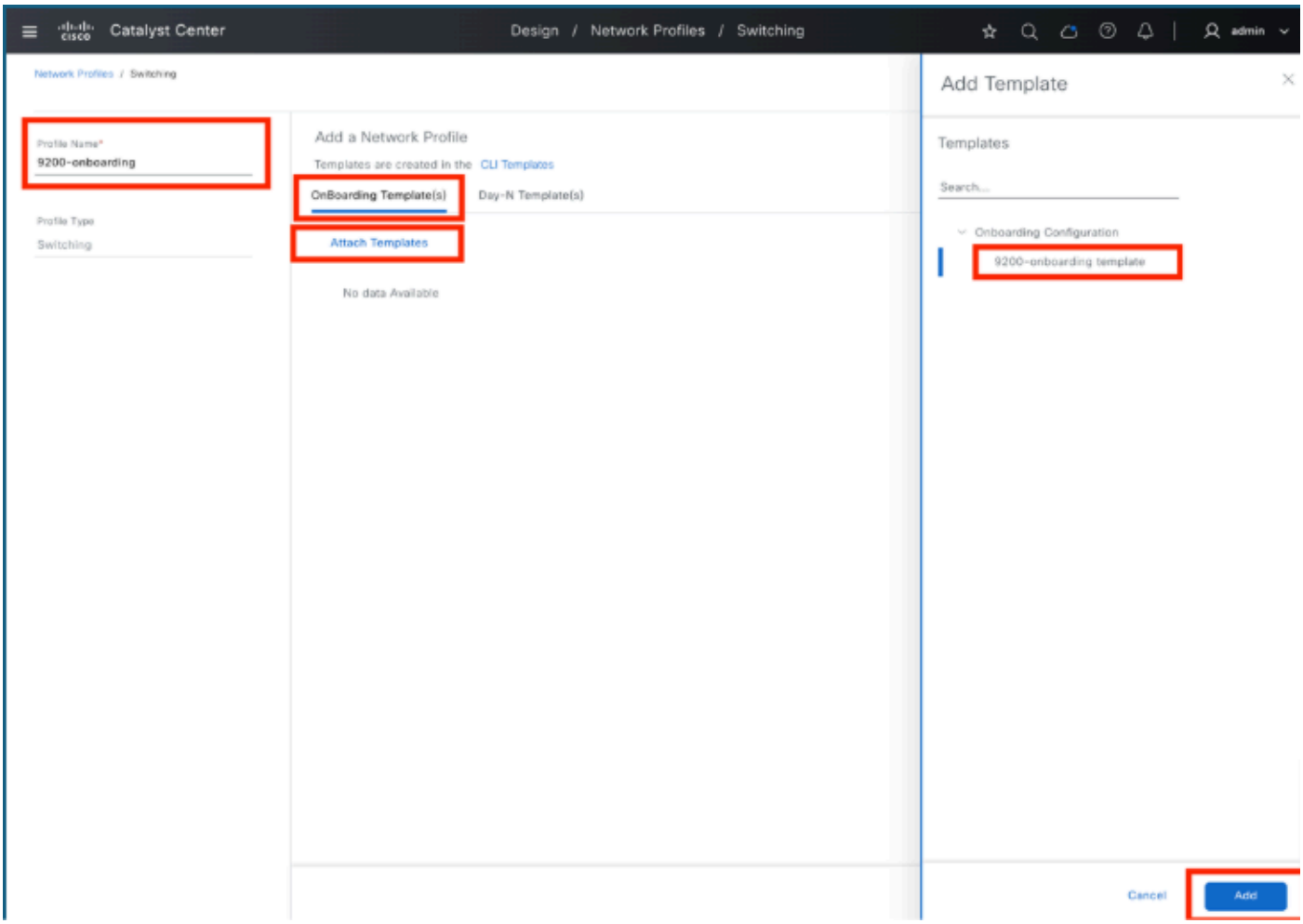
4.建立網路配置檔案

- 導覽至Design功能表，然後選擇Network Profiles。
- 按一下Add Profile 按鈕。
- 從清單中選擇適當的配置檔案型別(例如Switching)。



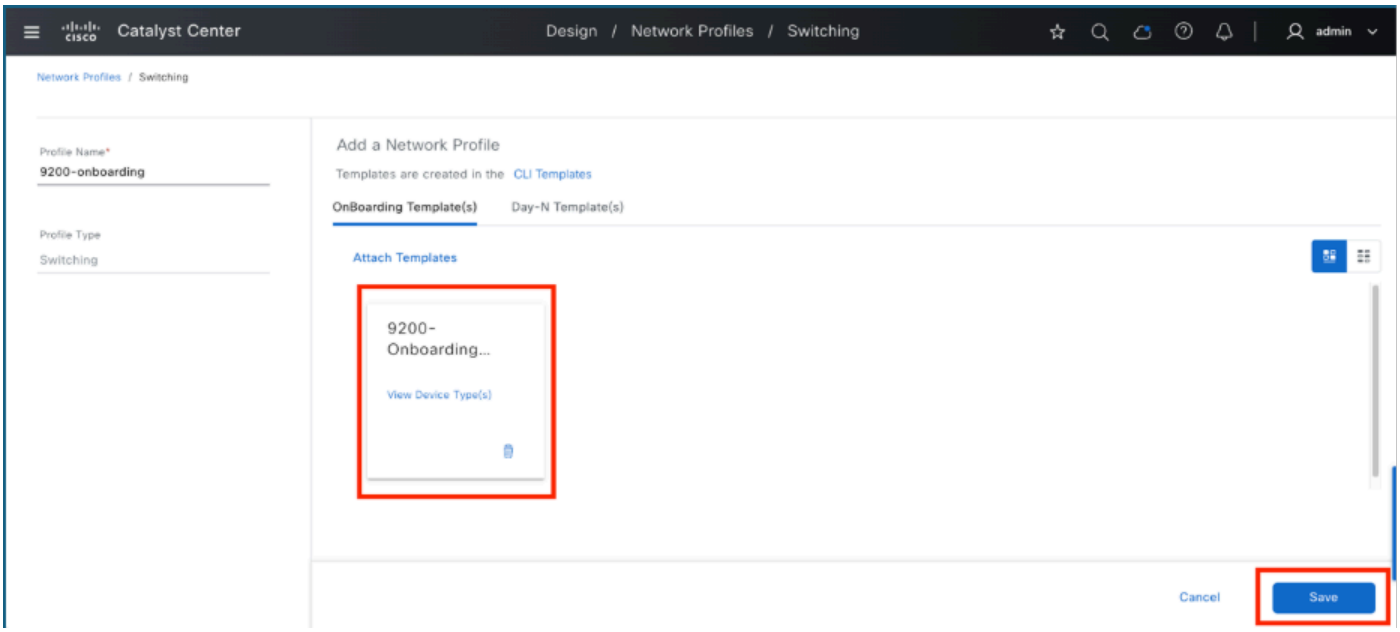
5.新增模板並編輯網路配置檔案設定

- 輸入配置檔名稱：為網路配置檔案提供名稱。
- 訪問模板：點選Onboarding Template(s)，然後選擇Attach Templates。
- 選擇Template:從Onboarding Configuration目錄中查詢並選擇所需的模板。
- 完成：按一下Add按鈕完成該過程。



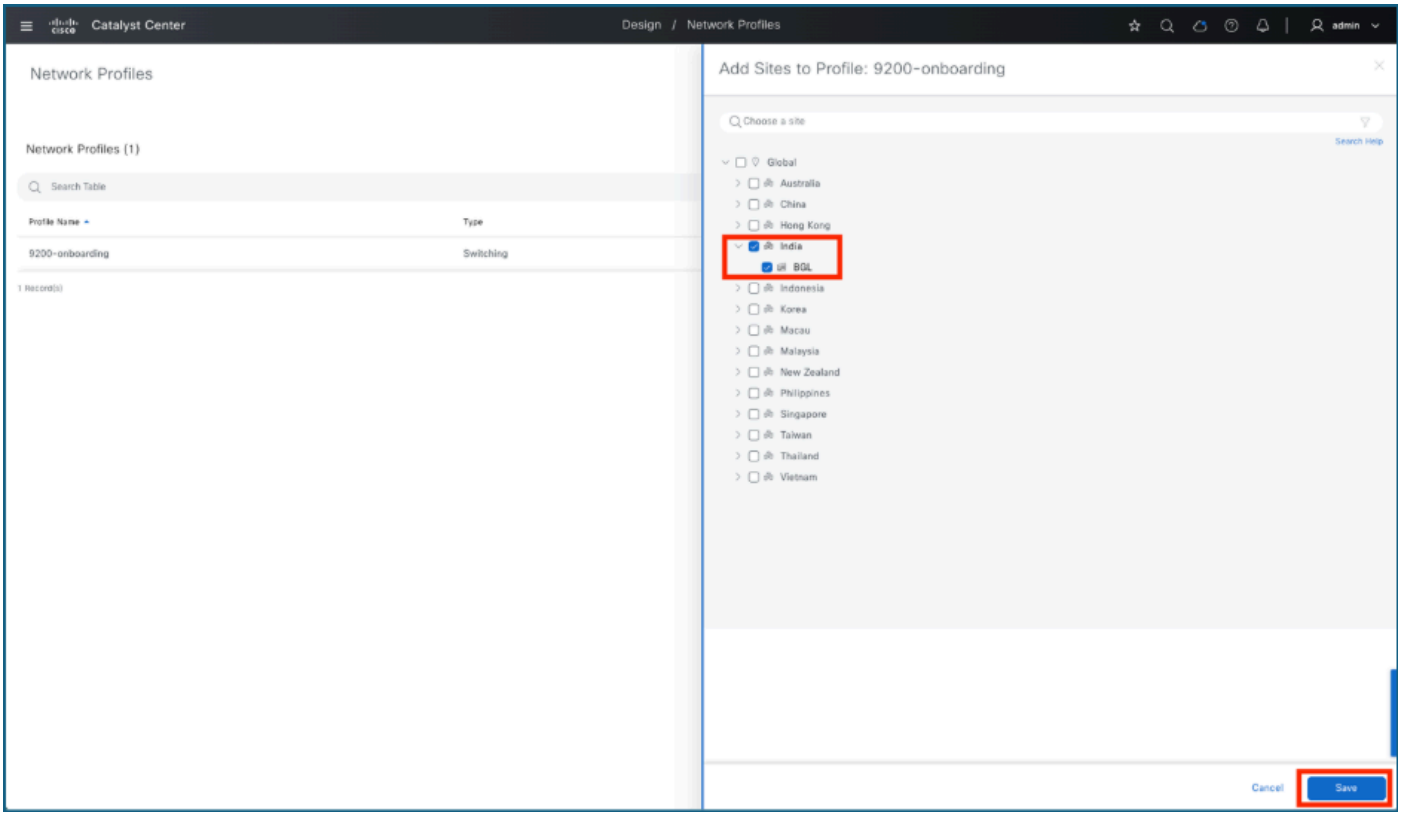
6.儲存配置檔案

- 驗證模板：新增模板後，確保該模板出現在「Onboarding Template(s)（入職模板）」下的清單中。
- 儲存Profile: 按一下儲存按鈕完成並儲存配置檔案設定。



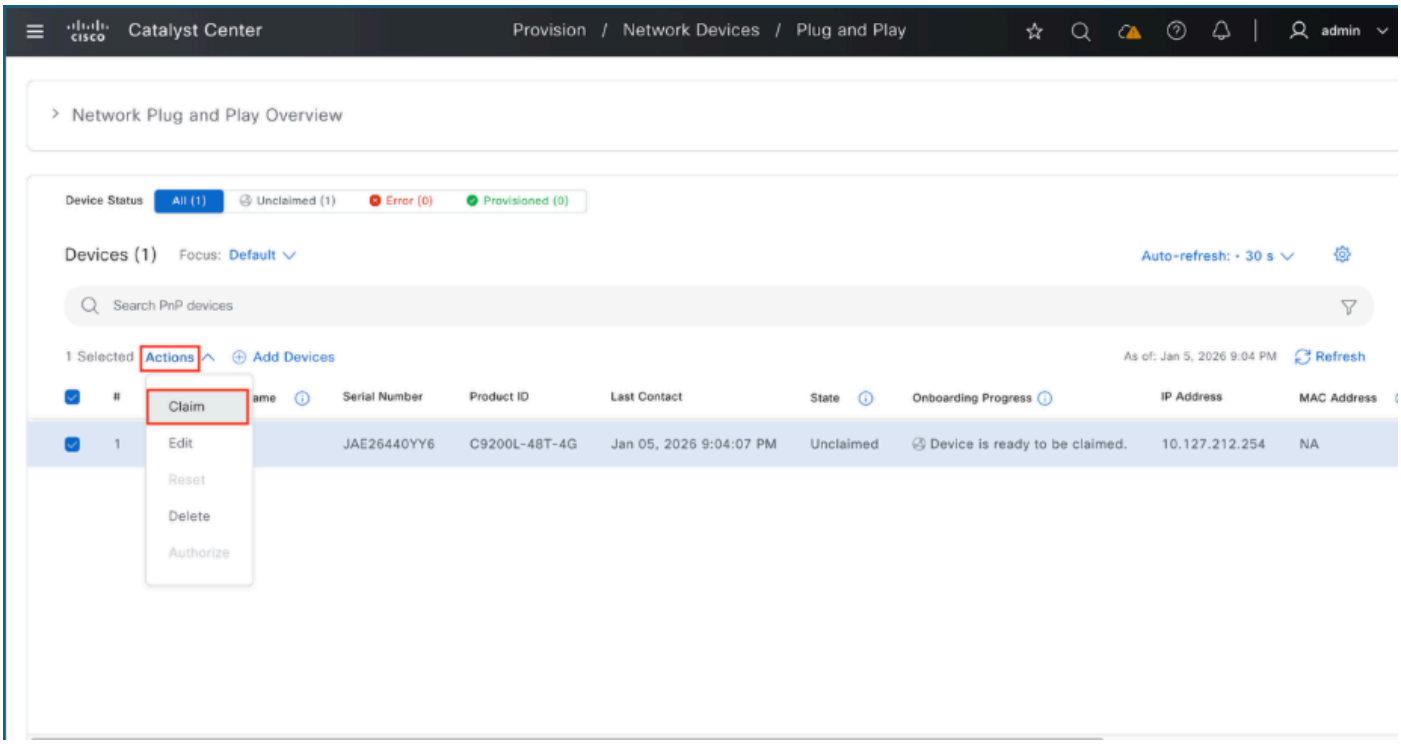
7.將網路配置檔案分配給要安裝交換機/交換機的站點

- 啟動分配：按一下剛建立的網路配置檔案的Assign Site選項。
- 選擇站點：選擇要安裝交換機的特定站點。
- 確認：按一下儲存完成分配。



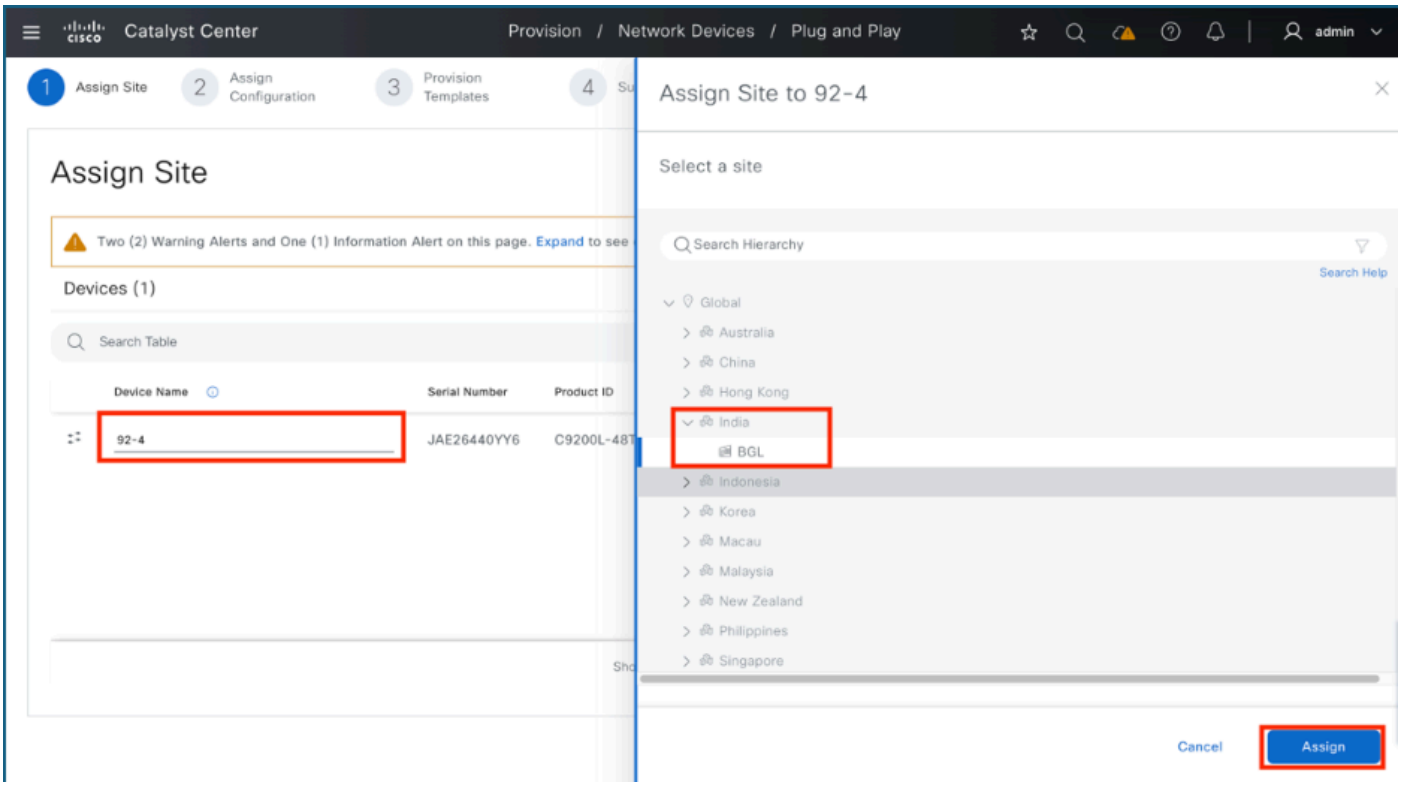
8.索賠開關

- 導航到Plug and Play: Go to Provision 選單，然後選擇Plug and Play。
- 選擇Devices:找到要宣告的一個或多個交換機，然後按一下每個交換機名稱旁邊的覈取方塊。
- 起動索賠：導航至「活動」選單，然後選擇「索賠」。



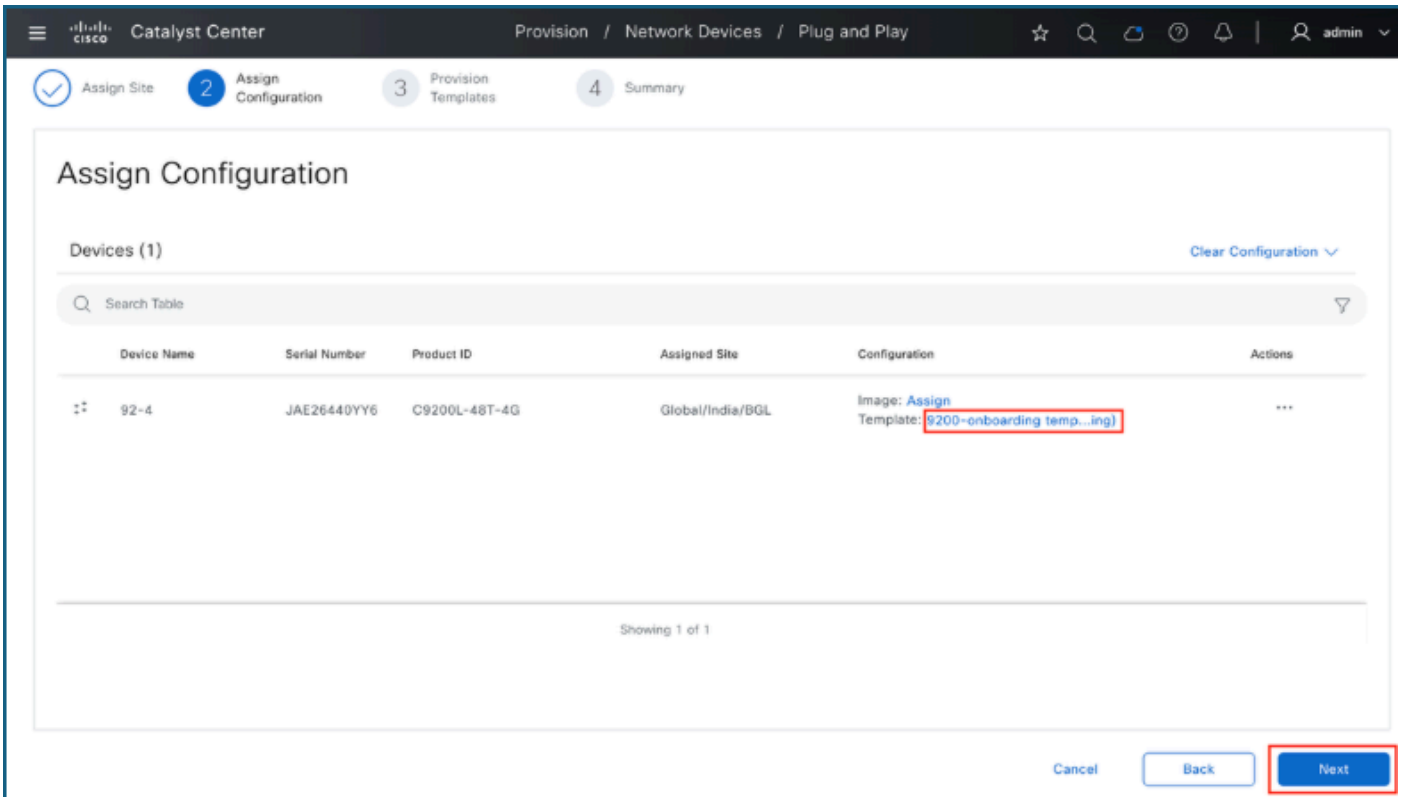
9.為交換機指定名稱並分配給站點

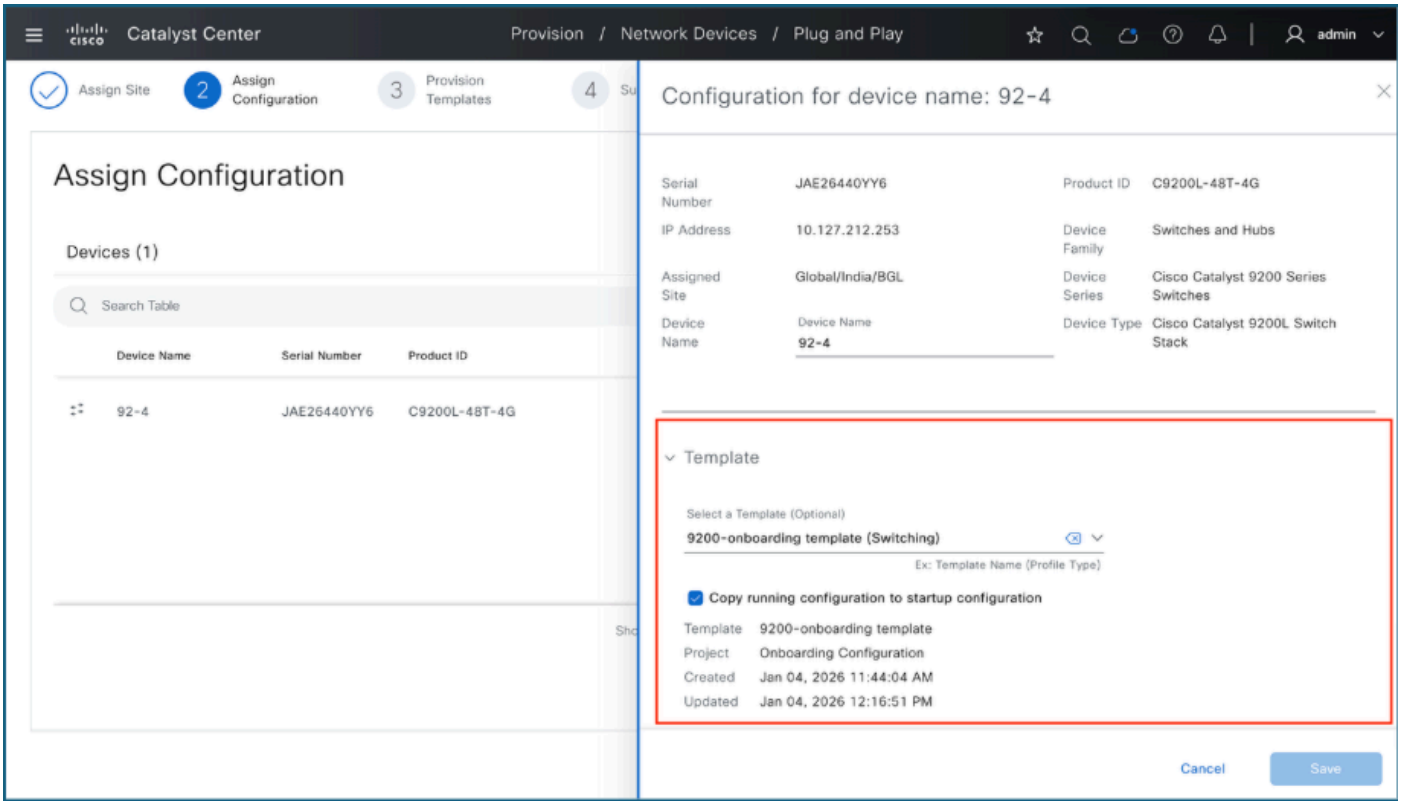
- 為裝置命名：在Device Name（裝置名稱）欄位中輸入交換機所需的名稱。
- 起動分配：按一下分配按鈕。
- 選擇位置：選擇適當的站點或建築物，再次按一下Assign，然後按一下Next繼續。



10.分配第0天模板

- 選擇模板：單擊「模板」選項旁邊自動選擇的模板。
- 檢視詳細資訊：仔細驗證分配的模板的配置詳細資訊。
- 繼續：確認模板分配後，按一下「下一步」。

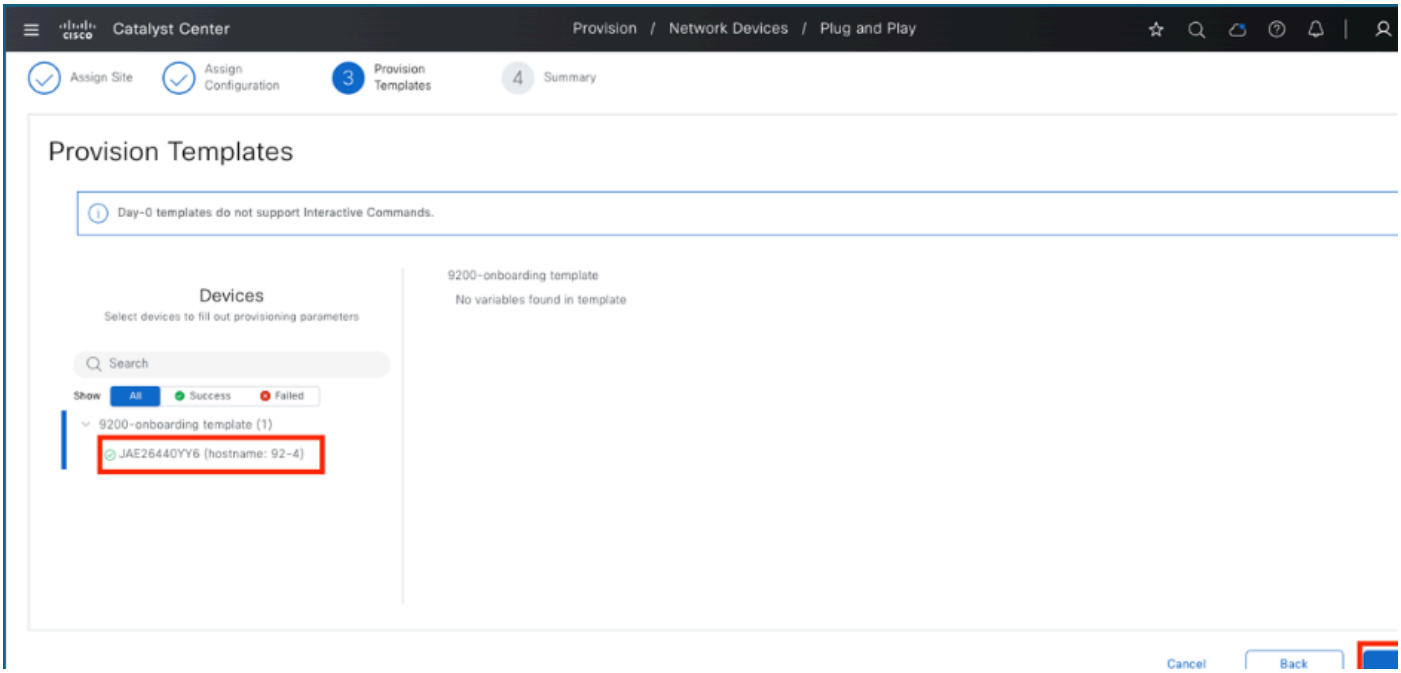




11.調配模板

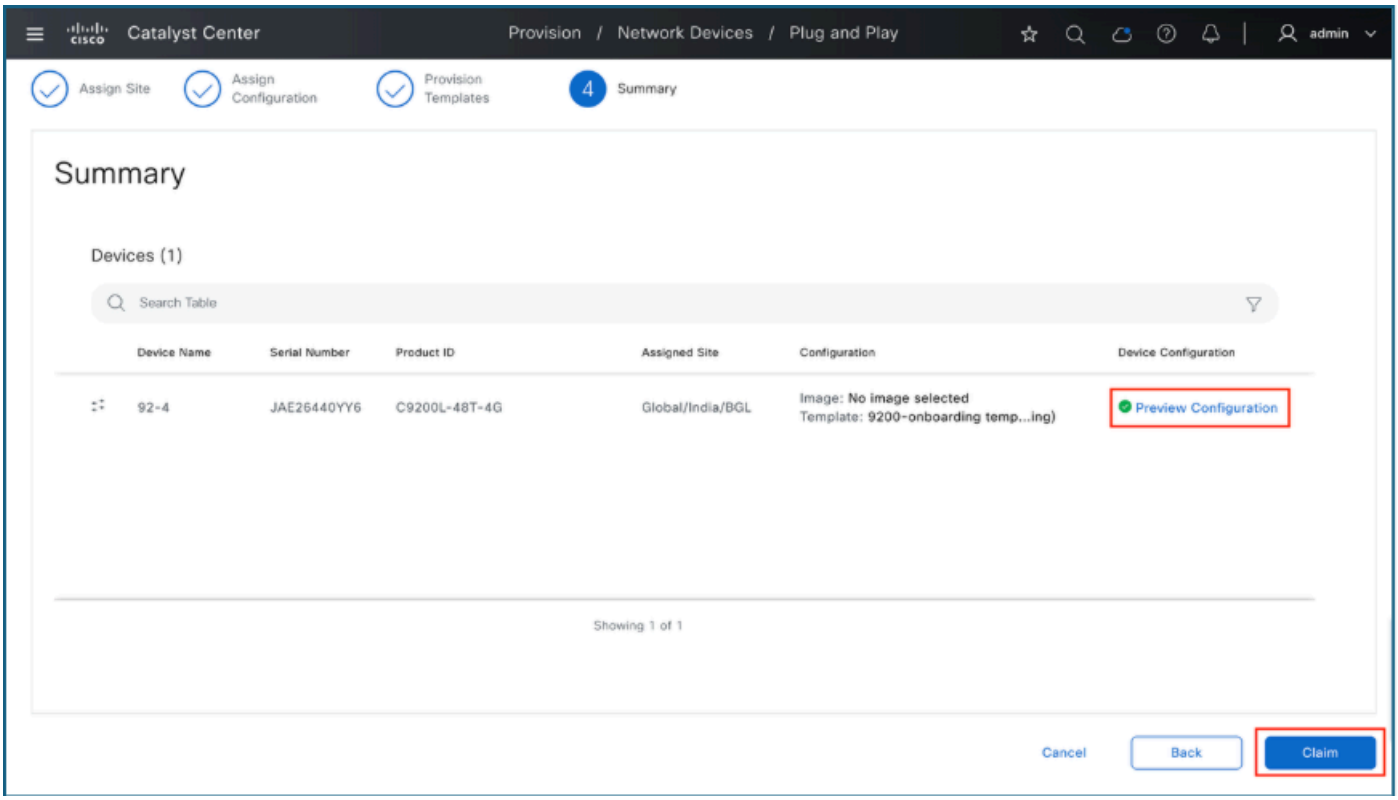
- 選擇裝置：在模板部分下，按一下要配置的特定裝置。

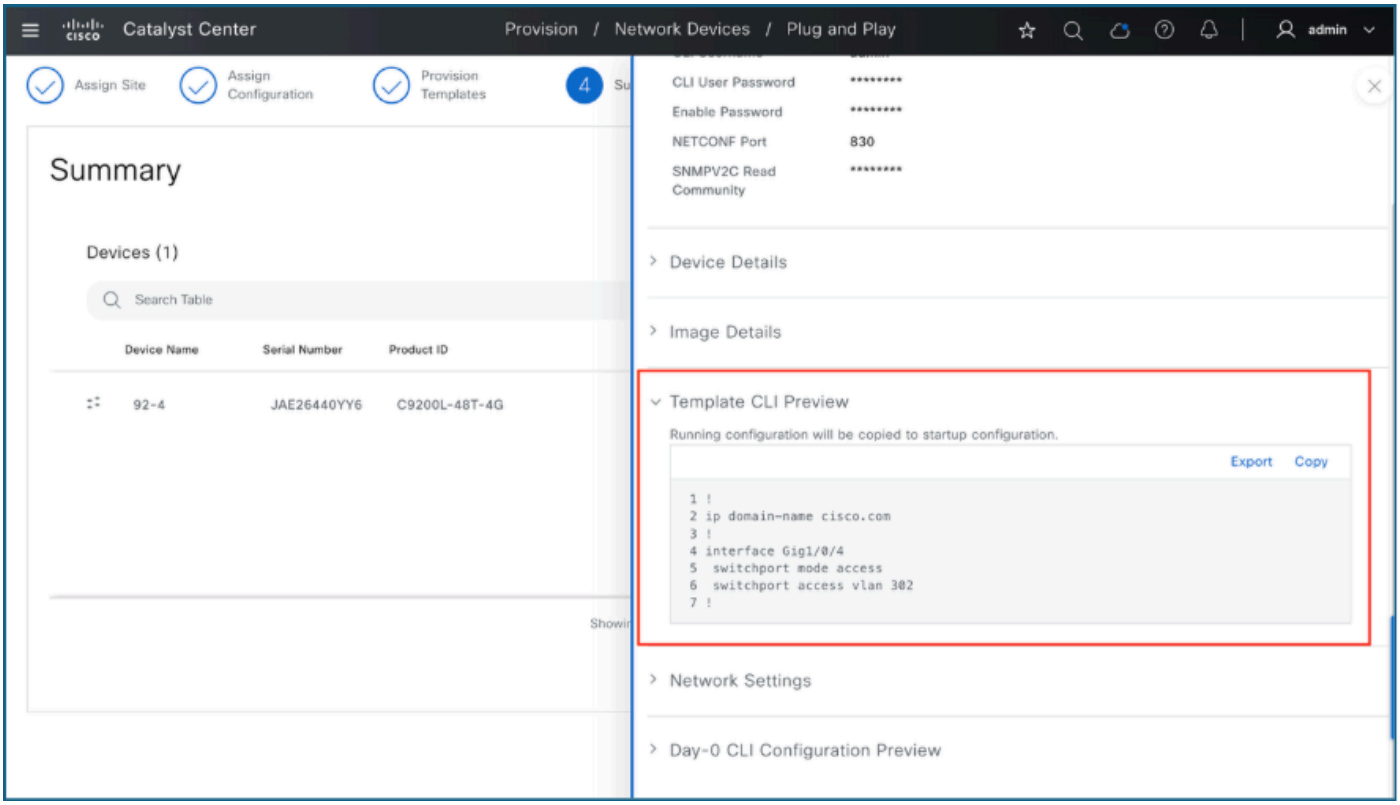
- 標識變數：檢查與模板關聯的任何必需變數值。
- 輸入值：如果任何變數是必需的，請填寫必需的值。
- 繼續：按一下下一步轉到下一步。



12.摘要

- 稽核配置：在Summary頁面上，稽核由Catalyst Center準備的配置設定。
- 預覽詳細資訊：點選預覽配置(Preview Configuration)以檢視掛起的更改。
- 驗證部分：展開每個部分檢查特定配置詳細資訊。
- 完成：驗證設定後，按一下Claim繼續。

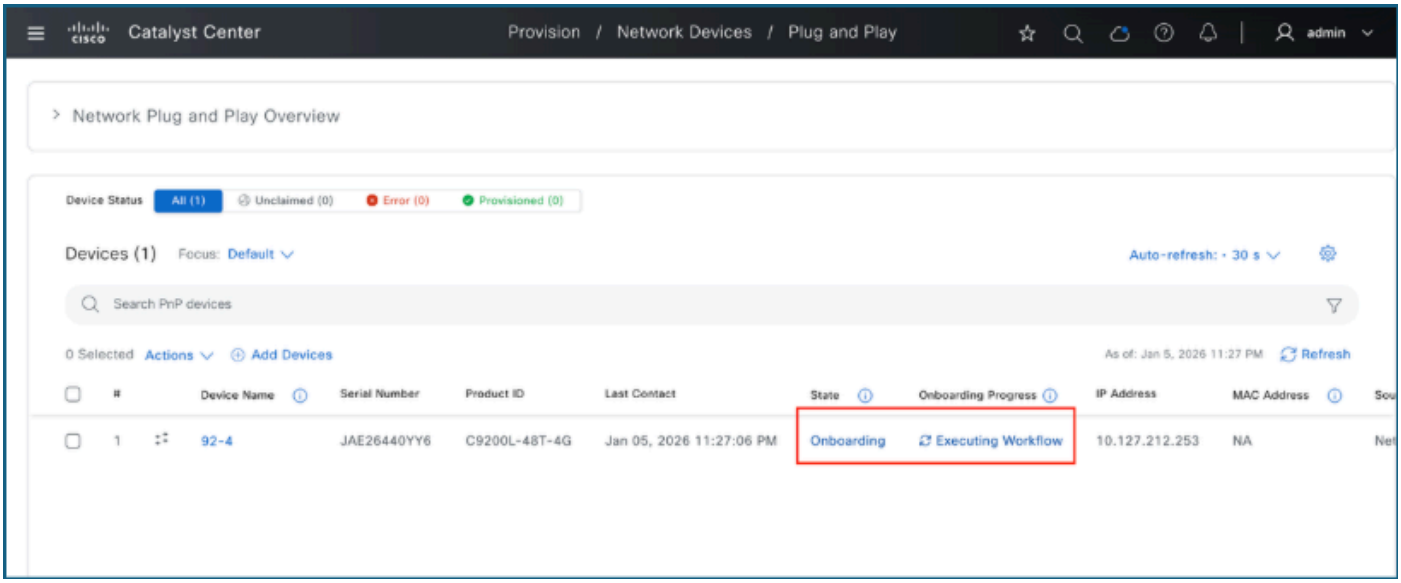


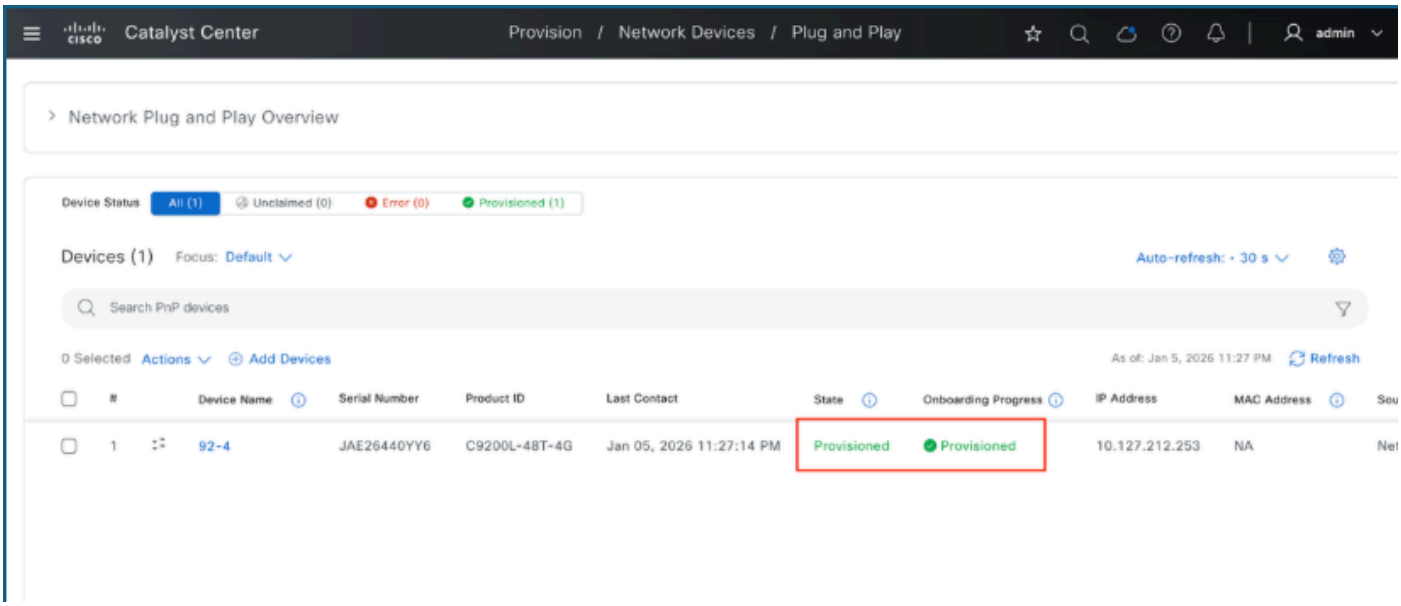


13.監測索賠進度

您將重定向到即插即用頁面以跟蹤裝置進度。

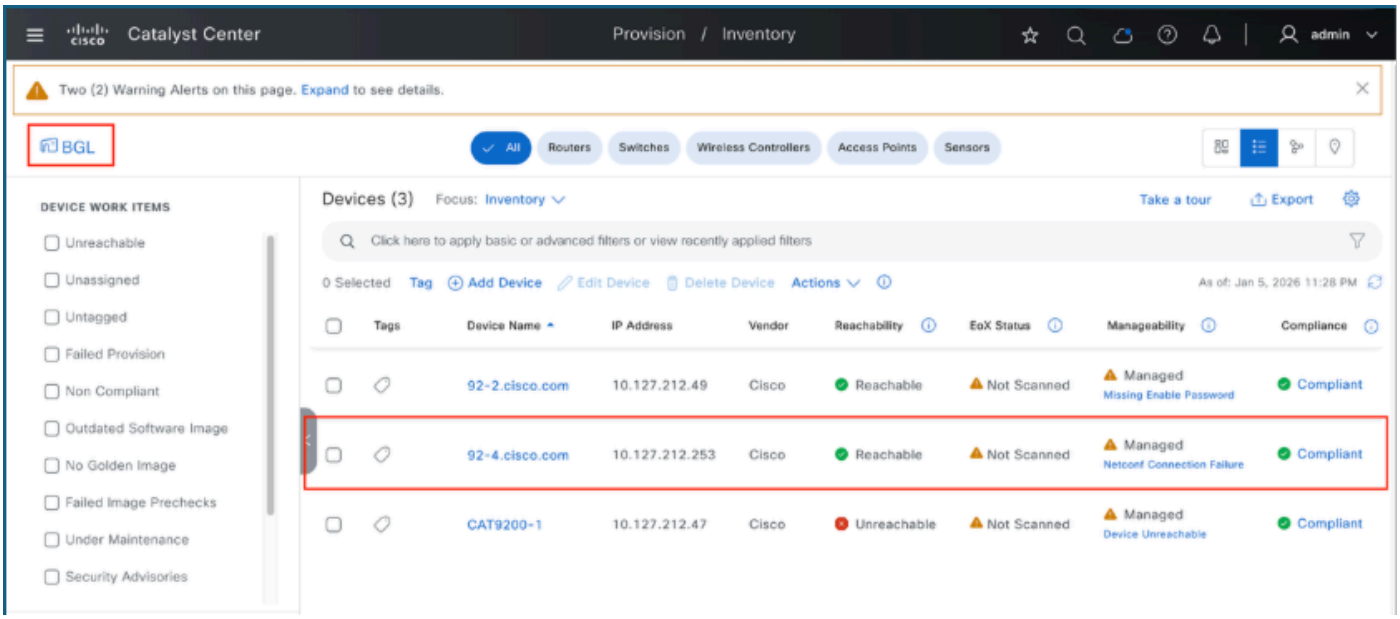
- Monitor Status:在申請流程進行時觀察裝置狀態。
- 確認完成：當狀態更新為Provisioned時，已成功宣告交換機並將其整合到Catalyst Center資產中。





驗證

- 訪問Provision選單：在首頁中開啟Provision頁籤。
- 檢視庫存：選擇庫存選項。
- 驗證狀態：檢查清單以確認交換機已成功調配。



將裝置批次匯入到Catalyst Center即插即用清單

為了簡化大型網路的部署，Catalyst Center支援提前批次匯入裝置轉移方法。此過程包括上傳裝置識別符號（如PID、序列號和可選站點或模板資料），使系統能夠在裝置通電和連線後立即自動加入裝置。

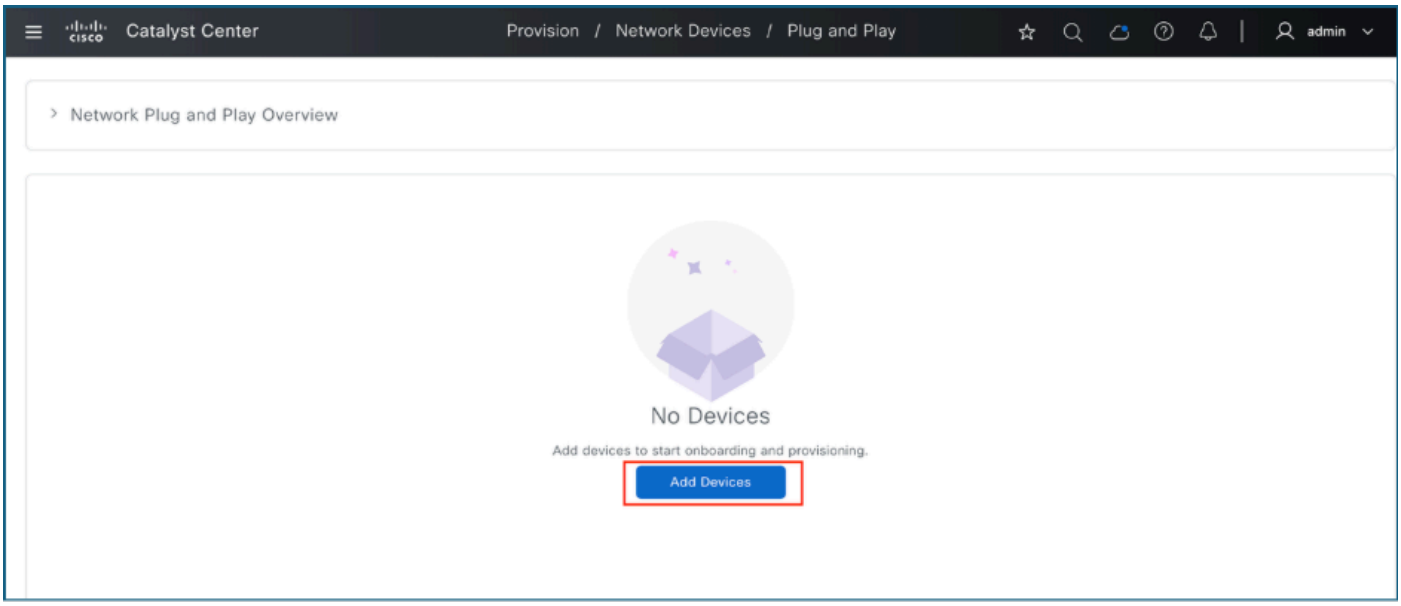
1.必要條件

為確保成功批次匯入，必須滿足以下要求：

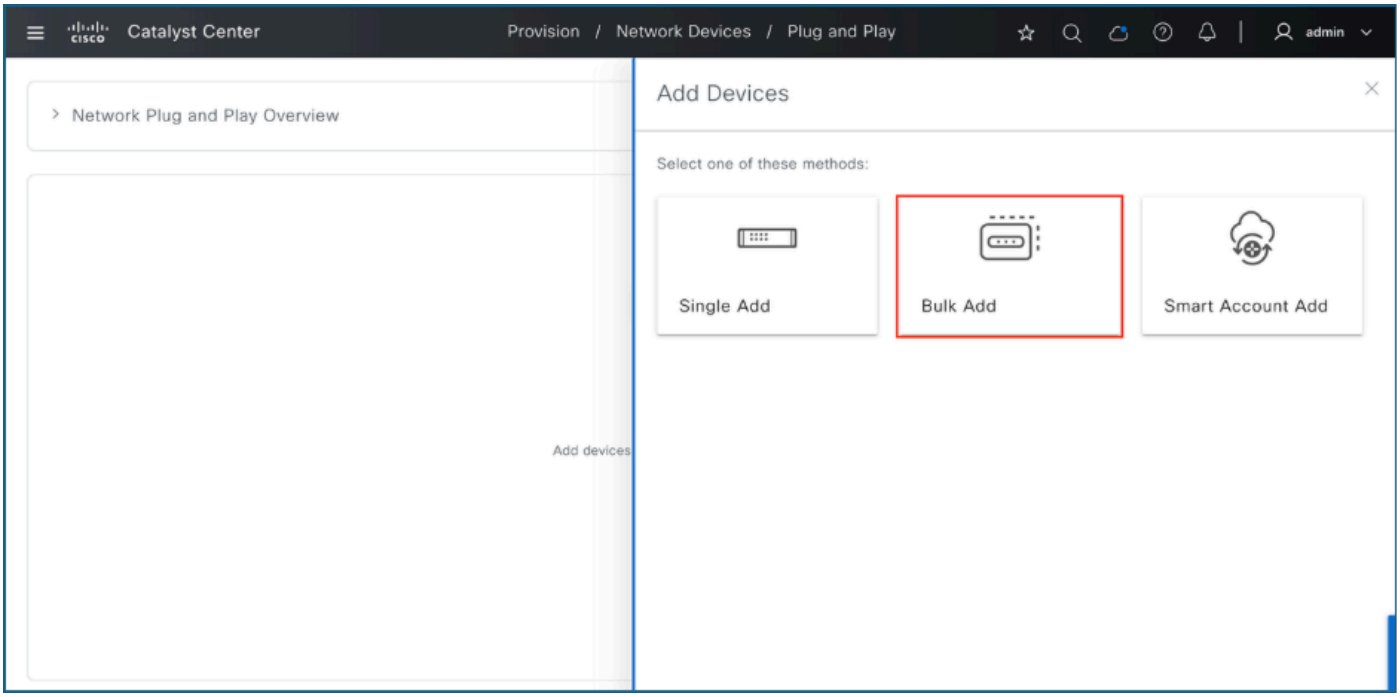
- Catalyst Center例項必須可訪問且運行正常。
- 硬體必須獲得思科即插即用服務的正式支援。
- 必須能夠訪問裝置序列號和PID。
- 必須在Catalyst Center環境中預配置目標站點層次結構。

二、批次進口工序

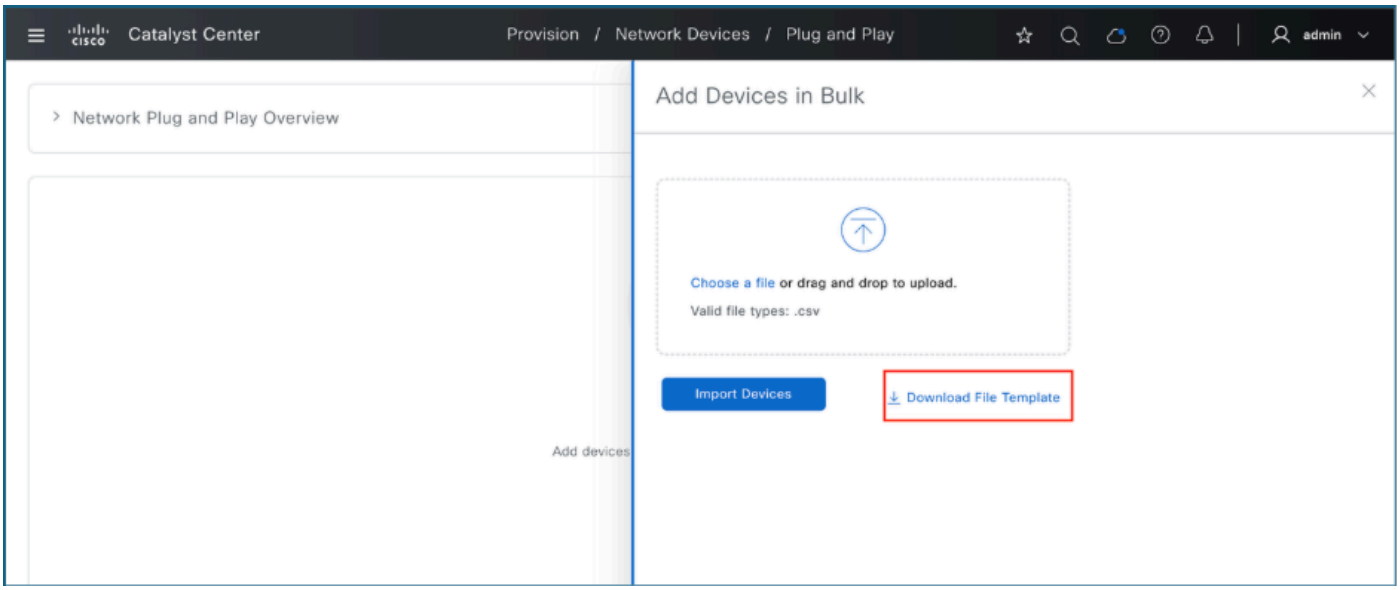
1. 登入Catalyst Center
2. 導覽至Provision > Plug and Play
3. 按一下Add Devices



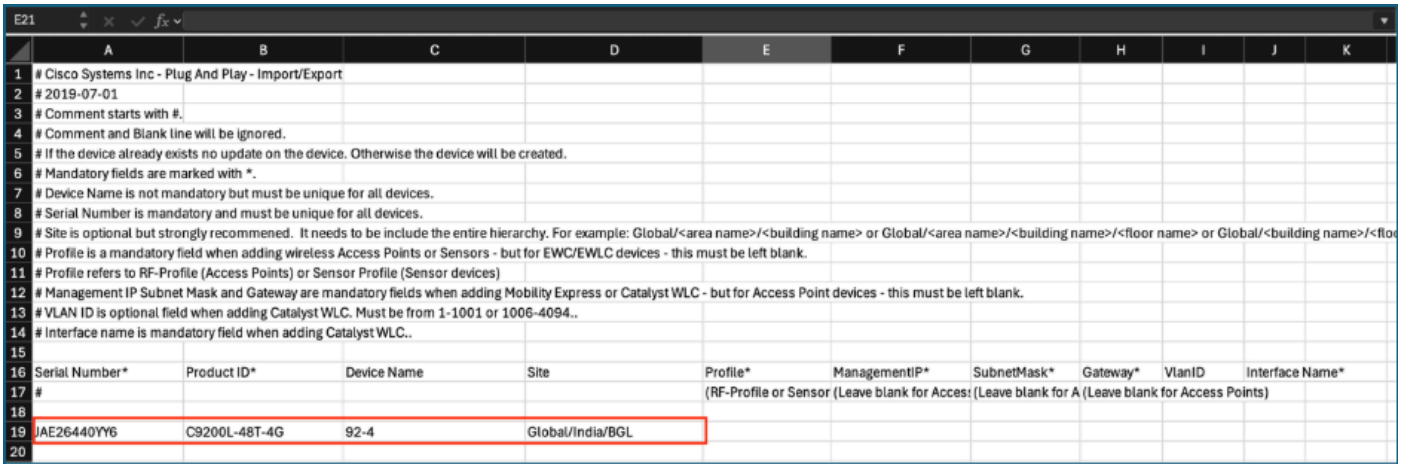
4.按一下Bulk Add



5.按一下Download File Template，下載範例CSV檔案

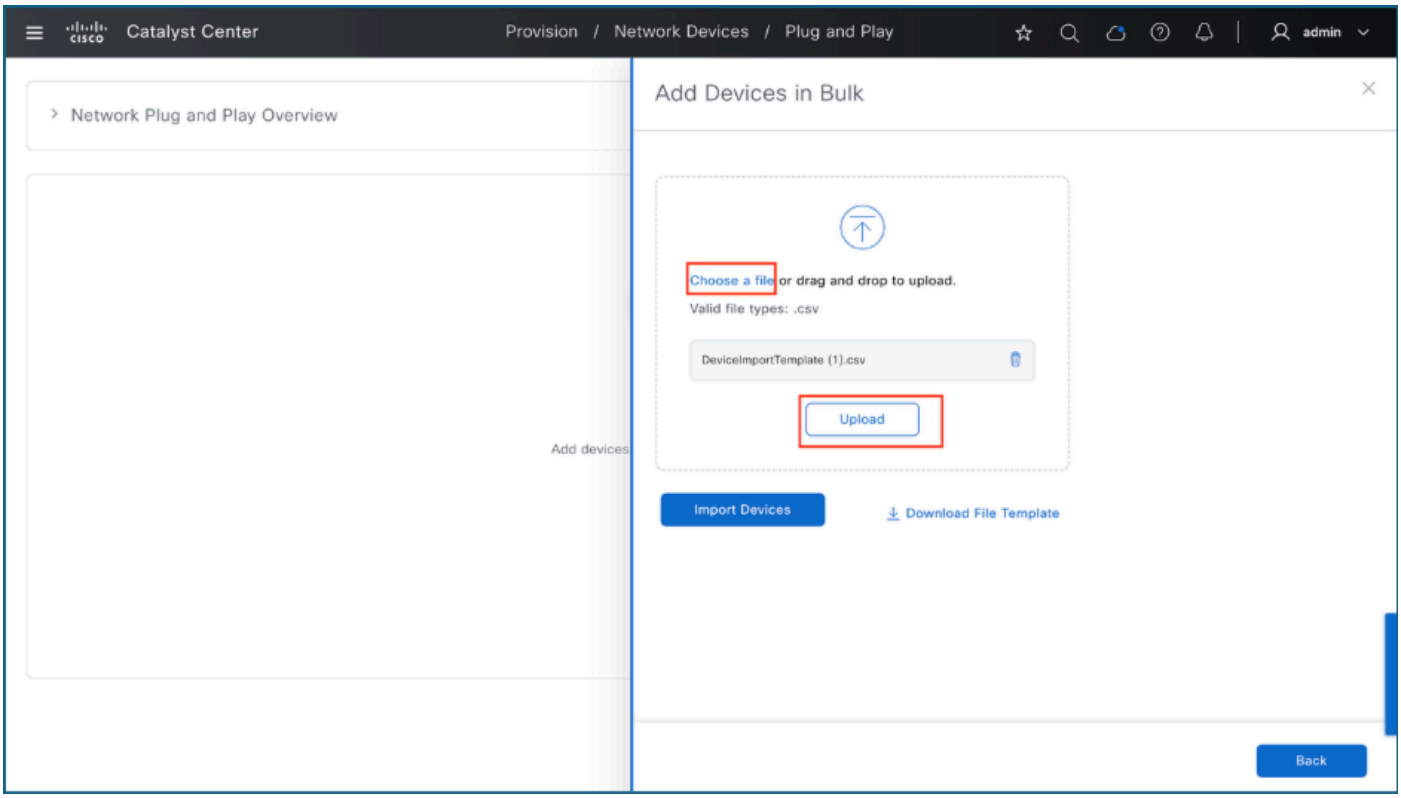


6.使用所需的裝置詳細資訊填充CSV檔案。

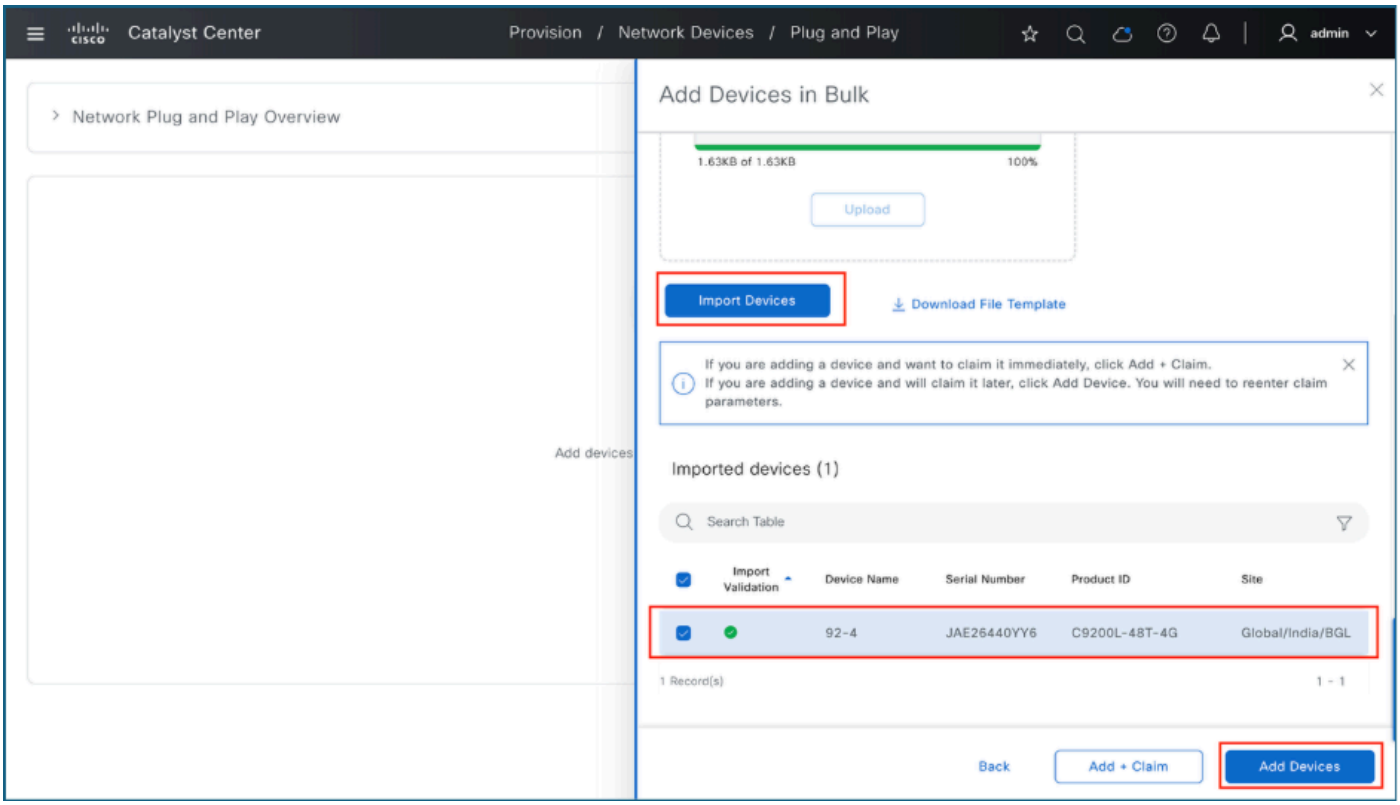


	A	B	C	D	E	F	G	H	I	J	K
1	# Cisco Systems Inc - Plug And Play - Import/Export										
2	# 2019-07-01										
3	# Comment starts with #.										
4	# Comment and Blank line will be ignored.										
5	# If the device already exists no update on the device. Otherwise the device will be created.										
6	# Mandatory fields are marked with *.										
7	# Device Name is not mandatory but must be unique for all devices.										
8	# Serial Number is mandatory and must be unique for all devices.										
9	# Site is optional but strongly recommened. It needs to be include the entire hierarchy. For example: Global/<area name>/<building name> or Global/<area name>/<building name>/<floor name> or Global/<building name>/<flo										
10	# Profile is a mandatory field when adding wireless Access Points or Sensors - but for EWC/EWLC devices - this must be left blank.										
11	# Profile refers to RF-Profile (Access Points) or Sensor Profile (Sensor devices)										
12	# Management IP Subnet Mask and Gateway are mandatory fields when adding Mobility Express or Catalyst WLC - but for Access Point devices - this must be left blank.										
13	# VLAN ID is optional field when adding Catalyst WLC. Must be from 1-1001 or 1006-4094..										
14	# Interface name is mandatory field when adding Catalyst WLC..										
15											
16	Serial Number*	Product ID*	Device Name	Site	Profile*	ManagementIP*	SubnetMask*	Gateway*	VlanID	Interface Name*	
17	#				(RF-Profile or Sensor	(Leave blank for Acces	(Leave blank for A	(Leave blank for Access Points)			
18											
19	JAE26440YY6	C9200L-48T-4G	92-4	Global/India/BGL							
20											

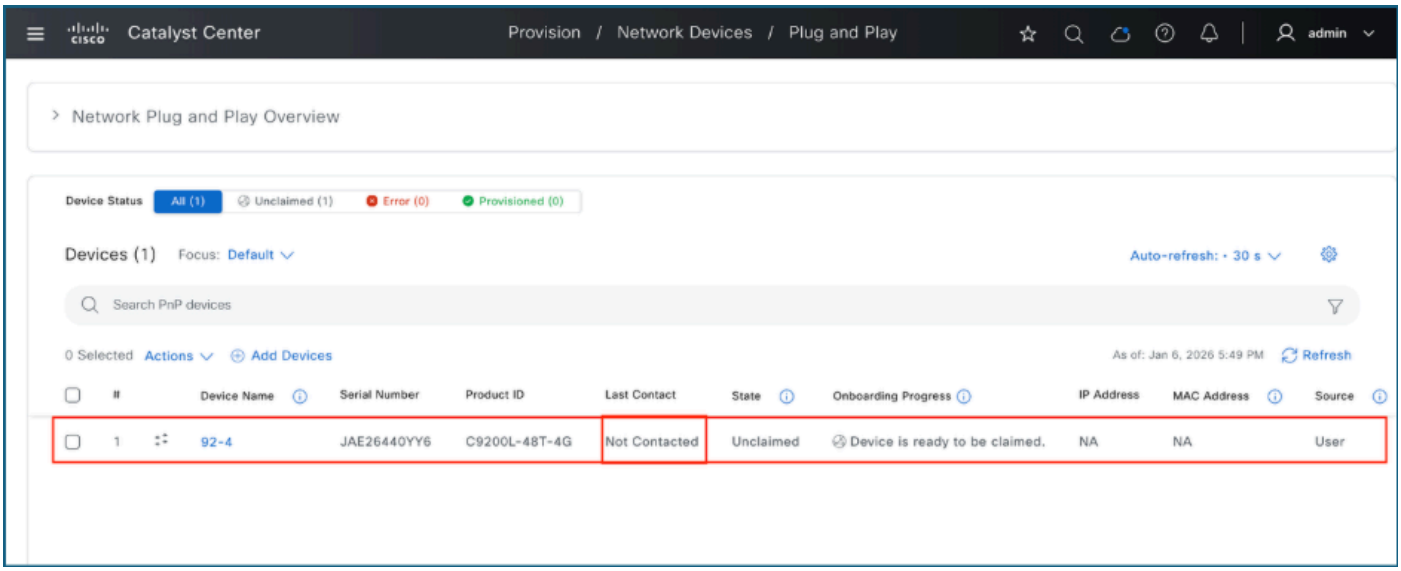
7.上傳已完成的CSV檔案。



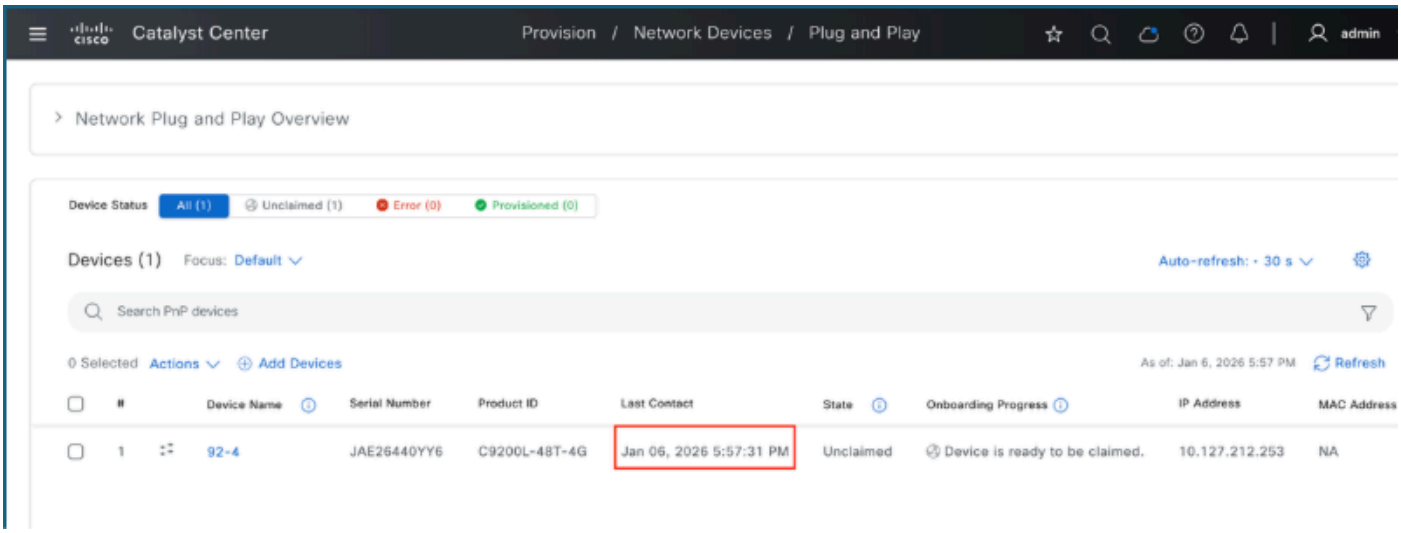
8.從CSV檔案匯入裝置並將其新增到PnP清單



9.設備在資產中顯示為「未聯絡」。



10.一旦裝置與Catalyst Center聯絡，即可申請索賠。



疑難排解

如果交換機未顯示在Catalyst Center的「即插即用」頁面上，以下是識別和解決該問題的步驟。

1. PnP連線驗證

這些命令驗證到Catalyst Center的PnP連線。

1.1. ICMP可達性

通過ping Catalyst Center的企業介面IP或虛擬IP(VIP)地址，驗證ICMP連線。確保可以通過ping訪問Catalyst Center。

```
Switch#ping 10.127.212.43
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.127.212.43, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

1.2. HTTP HELLO驗證

如果Catalyst Center不響應HELLO驗證請求，即插即用(PnP)將失敗。要驗證連線，請從裝置終端或命令提示符運行此命令：curl -v http://<Catalyst Center IP>/pnp/HELLO

確認收到「HELLO」響應。

```
sitirkey@SITIRKEY-M-6PGJ netbox-docker % curl -v http://10.127.212.43/pnp/HE
*   Trying 10.127.212.43:80...
* Connected to 10.127.212.43 (10.127.212.43) port 80
> GET /pnp/HELLO HTTP/1.1
> Host: 10.127.212.43
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 04 Jan 2026 07:51:20 GMT
< Content-Type: text/plain;charset=iso-8859-1
< Content-Length: 5
< Connection: keep-alive
<
* Connection #0 to host 10.127.212.43 left intact
```

1.3. HTTPS證書檢索

如果無法通過HTTPS手動檢索Catalyst Center伺服器的證書，則PnP功能失敗。若要驗證這一點，請使用以下命令：copy https://<catc-ip-address>/ca/pem mypem2

確認檔案傳輸是否完成，沒有錯誤。

```
92-4#copy https://10.127.212.43/ca/pem mypem2
Destination filename [mypem2]?
Accessing https://10.127.212.43/ca/pem...
Loading https://10.127.212.43/ca/pem
1472 bytes copied in 0.060 secs (24533 bytes/sec)
92-4#
```

1.4. PnP配置檔案狀態

如果交換機未顯示在Catalyst Center的PnP頁面上，請通過執行命令檢查PnP HTTP連線show pnp profile

- 驗證PnP是否使用正確的Active-URL。

- 確認HTTP統計資訊中的「失敗計數器」為0。大於0的值表示交換機和Catalyst Center之間的可達性問題。 此圖說明了一個涉及可達性問題的場景。

```
Switch#show pnp profile
PnP Profiles: Active:0, Created:0, Deleted:0, Hidden:0

Name            CBType Node     Primary-Path           Primary-Trans  Backup-Trans

-------------- show pnp http tracking ---------------

PNP-T3-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[PnP-Discovery-Proc]
        Active-URL=[http://10.127.212.43:80/pnp/HELLO], Last-URL=[http://10.127.212.43:80/pnp/HELLO]
        SID=7, Last-SID=6, TID=4294967295, last-TID=4294967295, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=7F6CDC0EF0
        HTTP-Register Stats: Total=3, OK=3, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=2, OK=2, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=6, OK=6, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=6, OK=0, Failed=6, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-HTTP-Tracker: Active-Name=[-], Last-Name=[-]
        Active-URL=[-], Last-URL=[-]
        SID=0, Last-SID=0, TID=0, last-TID=0, Head-Date=[-], Status-Code=0, Get-Status=0, Get-Watch=0
        HTTP-Register Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Alloc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Free Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Resp-Data-Proc Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Watch-Init Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Get-Wait-Complete Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Get Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
        HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
        SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
        Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
Switch#
```

此範例說明了一個沒有可達性問題的情境。

```
PNP-T1-Discovery: Active-Name=[PnP-Discovery-Proc], Last-Name=[-]
       Active-URL=[http://catc1.cisco.com:80/pnp/HELLO], Last-URL=[-]
       SID=5, Last-SID=0, TID=1, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:17 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881114
       HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
       HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
       HTTP-Send-Hello Stats: Total=0, OK=0, Failed=0, Ignored=0
       SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
       Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0

PNP-T1-pnp-zero-touch: Active-Name=[PnP-pnp-zero-touch], Last-Name=[-]
       Active-URL=[https://catc1.cisco.com:443/pnp/HELLO], Last-URL=[-]
       SID=8, Last-SID=0, TID=8, last-TID=0, Head-Date=[Mon, 05 Jan 2026 15:28:34 GMT], Status-Code=200, Get-Status=8, Get-Watch=4B881570
       HTTP-Register Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Unregister Stats: Total=0, OK=0, Failed=0, Ignored=0
       HTTP-Resp-Data-Alloc Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Resp-Data-Free Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Resp-Data-Proc Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Get-Watch-Init Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Get-Wait-Complete Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Send-Get Stats: Total=1, OK=1, Failed=0, Ignored=0
       HTTP-Send-Head Stats: Total=0, OK=0, Failed=0, Ignored=0
       HTTP-Send-Hello Stats: Total=1, OK=1, Failed=0, Ignored=0
       SSL-Handshake Stats: Total=0, OK=0, Failed=0, Ignored=0
       Server-ID-Check Stats: Total=0, OK=0, Failed=0, Ignored=0
```

2. DHCP驗證

這些命令有助於驗證DHCP配置和連線。

2.1.檢驗DHCP IP地址分配

執行命令show ip interface brief 驗證PnP VLAN SVI是否已成功從DHCP伺服器接收IP地址。

```
Switch#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan302                10.127.212.254  YES DHCP   up                    up
GigabitEthernet0/0     unassigned      YES unset  up                    up
```

2.2.確認租用伺服器

執行命令show dhcp lease 以驗證DHCP租用伺服器資訊。

```
Switch#show dhcp lease
Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 10.127.212.49, state: 5 Bound
   DHCP transaction id: 23F1
   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 10.127.212.49
   Next timer fires after: 11:52:27
   Retry count: 0   Client-ID: cisco-4464.3cb1.2bf7-Vl302
   Client-ID hex dump: 636973636F2D343436342E336362312E
                       326266372D566C333032
   Hostname: Switch
```

2.3.使用調試日誌驗證選項43

要驗證選項43，請使用debug dhcp detail命令啟用DHCP調試。啟用調試後，對介面執行關閉和no shutdown以重新啟動DHCP進程。在日誌中，找到「DHCP:掃描：供應商特定選項43:"。複製本節所示的十六進位制字串，使用適當的十六進位制到ASCII轉換器將其轉換為文本，並驗證生成的字串是否正確指向Catalyst Center。

```
000344: Jan  4 08:55:39.247: DHCP Offer Message   Offered Address: 10.127.212.254
000345: Jan  4 08:55:39.247: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000346: Jan  4 08:55:39.247: DHCP: Server ID Option: 10.127.212.49
000347: Jan  4 08:55:39.247: DHCP: offer received from 10.127.212.49
000348: Jan  4 08:55:39.247: DHCP: SRequest attempt # 1 for entry:
000349: Jan  4 08:55:39.247: Temp IP addr: 10.127.212.254  for peer on Interface: Vlan302
000350: Jan  4 08:55:39.247: Temp  sub net mask: 255.255.255.0
000351: Jan  4 08:55:39.247:    DHCP Lease server: 10.127.212.49, state: 4 Requesting
000352: Jan  4 08:55:39.247:    DHCP transaction id: A62
000353: Jan  4 08:55:39.247:    Lease: 86400 secs,  Renewal: 0 secs,  Rebind: 0 secs
000354: Jan  4 08:55:39.247:    Next timer fires after: 00:00:03
000355: Jan  4 08:55:39.247:    Retry count: 1   Client-ID: cisco-4464.3cb1.2bf7-Vl302
000356: Jan  4 08:55:39.247:    Client-ID hex dump: 636973636F2D343436342E336362312E
000357: Jan  4 08:55:39.247:                        326266372D566C333032
000358: Jan  4 08:55:39.248:    Hostname: Switch
000359: Jan  4 08:55:39.248: DHCP: SRequest- Server ID option: 10.127.212.49
000360: Jan  4 08:55:39.248: DHCP: SRequest- Requested IP addr option: 10.127.212.254
000361: Jan  4 08:55:39.248: DHCP: SRequest placed lease len option: 86400
000362: Jan  4 08:55:39.248: DHCP: SRequest placed class-id option: 636973636F706E70
000363: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000364: Jan  4 08:55:39.248: DHCP: SRequest: 323 bytes
000365: Jan  4 08:55:39.248:             B'cast on Vlan302 interface from 0.0.0.0
000366: Jan  4 08:55:39.254: DHCP: Received a BOOTREP pkt
000367: Jan  4 08:55:39.254: DHCP: Scan: Message type: DHCP Ack
000368: Jan  4 08:55:39.254: DHCP: Scan: Client ID: cisco-4464.3cb1.2bf7-Vl302
000369: Jan  4 08:55:39.254: DHCP: Scan: Server ID Option: 10.127.212.49 = A7FD431
000370: Jan  4 08:55:39.254: DHCP: Scan: Lease Time: 86400
000371: Jan  4 08:55:39.254: DHCP: Scan: Renewal time: 43200
000372: Jan  4 08:55:39.254: DHCP: Scan: Rebind time: 75600
000373: Jan  4 08:55:39.254: DHCP: Scan: Subnet Address Option: 255.255.255.0
000374: Jan  4 08:55:39.254: DHCP: Scan: Vendor specific option 43: 3541314E3B42323B4B343B4931302E3132372E3231322E34333B4A38303B
000375: Jan  4 08:55:39.254: DHCP: Scan: Router Option: 10.127.212.49
000376: Jan  4 08:55:39.254: DHCP: rcvd pkt source: 10.127.212.49,  destination:  255.255.255.255
000377: Jan  4 08:55:39.254:    UDP  sport: 43,  dport: 44,  length: 349
000378: Jan  4 08:55:39.255:    DHCP op: 2, htype: 1, hlen: 6, hops: 0
000379: Jan  4 08:55:39.255:    DHCP server identifier: 10.127.212.49
000380: Jan  4 08:55:39.255:         xid: A62, secs: 0, flags: 8000
000381: Jan  4 08:55:39.255:         client: 0.0.0.0, your: 10.127.212.254
000382: Jan  4 08:55:39.255:         srvr:   0.0.0.0, gw: 0.0.0.0
000383: Jan  4 08:55:39.255:         options block length: 101

000384: Jan  4 08:55:39.255: DHCP Ack Message
000385: Jan  4 08:55:39.255: DHCP: Lease Seconds: 86400    Renewal secs:  43200    Rebind secs:   75600
000386: Jan  4 08:55:39.255: DHCP: Server ID Option: 10.127.212.49
000387: Jan  4 08:55:40.232: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan302, changed state to up
000388: Jan  4 08:55:42.256: DHCP: Offered Address has no conflicts
000389: Jan  4 08:55:42.259: DHCP: Releasing ipl options:
000390: Jan  4 08:55:42.259: DHCP: Applying DHCP options:
000391: Jan  4 08:55:42.259:   Setting default_gateway to 10.127.212.49
000392: Jan  4 08:55:42.260:   Adding default route 10.127.212.49
000393: Jan  4 08:55:43.259: DHCPC: Notifying other components about option 43
000394: Jan  4 08:55:43.259: DHCP: Sending notification of ASSIGNMENT:
000395: Jan  4 08:55:43.259:   Address 10.127.212.254 mask 255.255.255.0
```

最佳實踐

- 確保交換器處於其出廠預設狀態。如果之前已布建交換器，請使用pnpa service reset指令重設交換器。
- 避免通過控制檯中斷PnP進程。

- 在部署之前驗證證書和DNS解析。

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）。