通过Catalyst Center即插即用了解交换机自注册

目录

简介

本文档介绍用于自动交换机自注册的Catalyst Center即插即用、完整生命周期、发现方法和故障排除。

描述

Catalyst Center Plug and Play(PnP)通过Cisco IOS® XE嵌入式PnP代理实现Cisco Catalyst交换机自注册。此流程能够以最少的人工操作实现安全发现、身份验证和初始调配，从而显着加快部署速度并提高配置一致性。PnP通过标准化设置和可选的0天模板支持可扩展的部署，可确保大规模可靠部署。

本文档概述了完整的自注册生命周期，包括PnP工作流程、发现方法、自注册选项和证书验证。它还提供有关设备申请、验证、故障排除和行业最佳实践的详细指导。

受众

本文档面向通过Catalyst Center部署和管理Cisco Catalyst交换机的网络管理员、部署工程师和系统集成商。

要求

本文档的读者最好具备以下主题的基本工作知识：

- Catalyst中心
- Cisco Catalyst 交换机
- 网络自动化和调配
- DHCP和DNS基本原理

先决条件

在开始自注册流程之前，请确保满足以下前提条件：

- Catalyst Center 2.3.7.9或更高版本已安装并正常运行。
- Cisco Catalyst交换机运行支持的Cisco IOS XE版本16.12.x或更高版本。
- Catalyst交换机和Catalyst Center之间提供网络连接。
- 使用指向Catalyst Center的企业接口IP地址或FQDN的选项43配置DHCP服务器。
- 交换机处于出厂默认（开箱即用）状态，IOS XE 16.12.1及更高版本上提供的pnpa service reset命令可用于将交换机重置为此状态。

即插即用概念概述

复习这些解释如何使用Catalyst Center Plug and Play安装新交换机的关键概念。

1. PnP服务器的DHCP发现

当出厂默认的Cisco Catalyst交换机通电时，PnP代理会尝试使用DHCP发现即插即用控制器（如Catalyst Center）。

发现过程使用标准DHCP交换：

- DHCP 发现
- DHCP 提供
- DHCP 请求
- DHCP 确认

如果配置正确，DHCP服务器包括选项43，为交换机提供PnP服务器的连接详细信息。

2. DHCP选项43格式

DHCP Option 43值是一个分号分隔的ASCII字符串，指定交换机如何连接到PnP服务器。

示例：

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

选项43字段定义

- 5A1N
  - 5 - PnP子选项
  - A — 主用模式（设备发起通信）
  - 1 - PnP代理模板版本
  - N — 禁用调试（D启用调试）
- B2 - PnP服务器IP地址类型
  - 1 — 主机名
  - 2 - IPv4地址
  - 3 - IPv6地址
- K4 — 传输协议

    - 4 - HTTP
    - 5 - HTTPS
- I - PnP服务器IP地址或FQDN
- J - TCP端口号

可选参数包括：

- T - Trustpool证书捆绑包URL（对于HTTPS为必填项）
- Z - NTP服务器IP地址（使用Trustpool安全时必需）

3. DHCP选项43配置示例

- 示例 1：选项43 IPv4配置：10.127.212.43 [Catalyst Center企业接口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
```

- 示例 2：选项43主机名配置：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
```

- 示例 3：选项43 IPv6配置:2001:60:60:60::133 [Catalyst Center企业接口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启动VLAN行为

默认情况下，出厂重置交换机使用VLAN 1进行PnP管理。思科建议在生产环境中使用专用管理VLAN。 这是配置自定义PnP启动VLAN的命令：

```
pnp startup-vlan
```

必须在上游交换机上配置此命令。上游交换机使用Cisco发现协议(CDP)将PnP启动VLAN传送到新交换机。 然后，下游交换机：

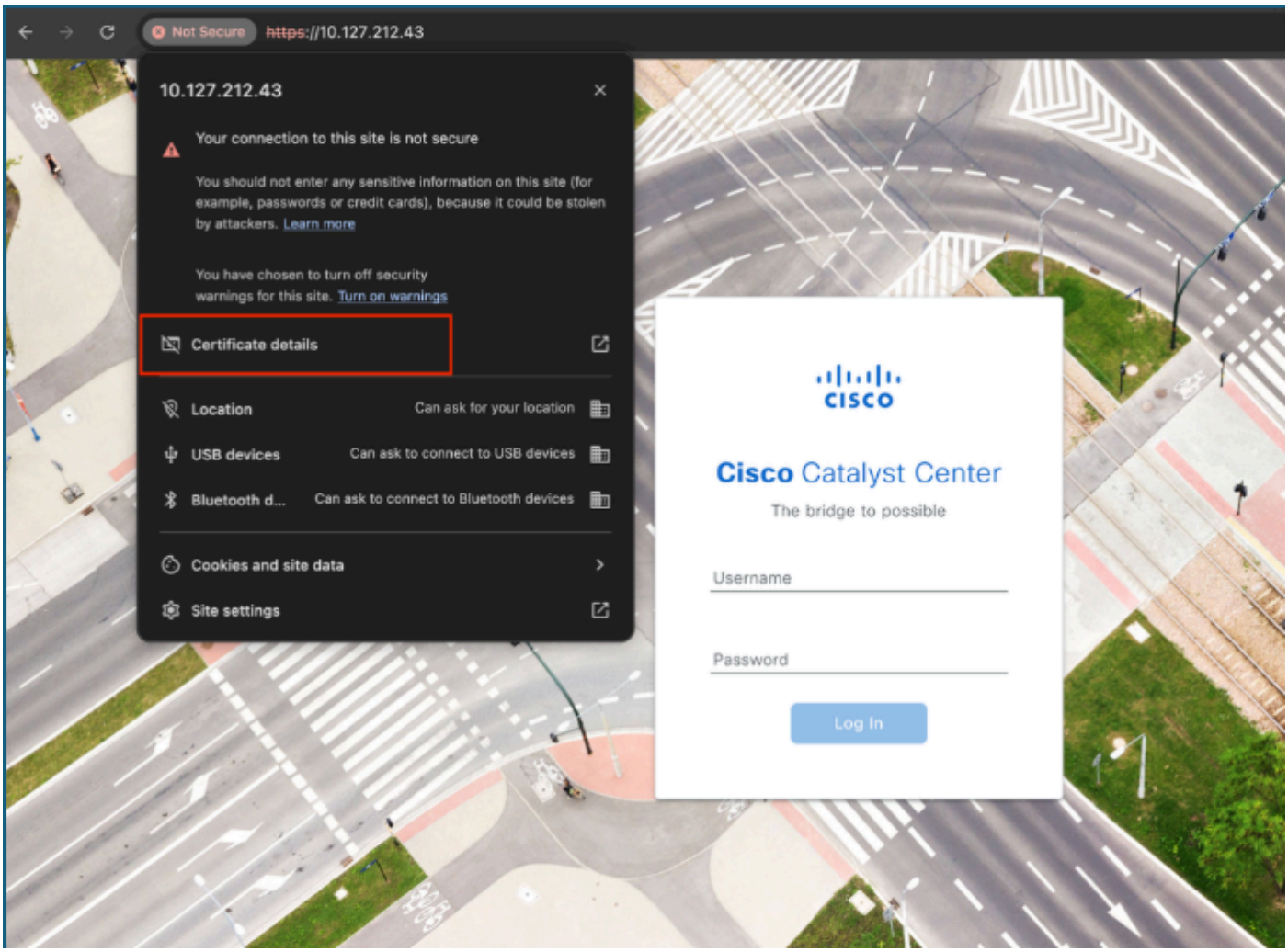
- 禁用VLAN 1上的DHCP
- 在已配置的启动VLAN上启用DHCP
- 更新TRUNK以允许新的VLAN

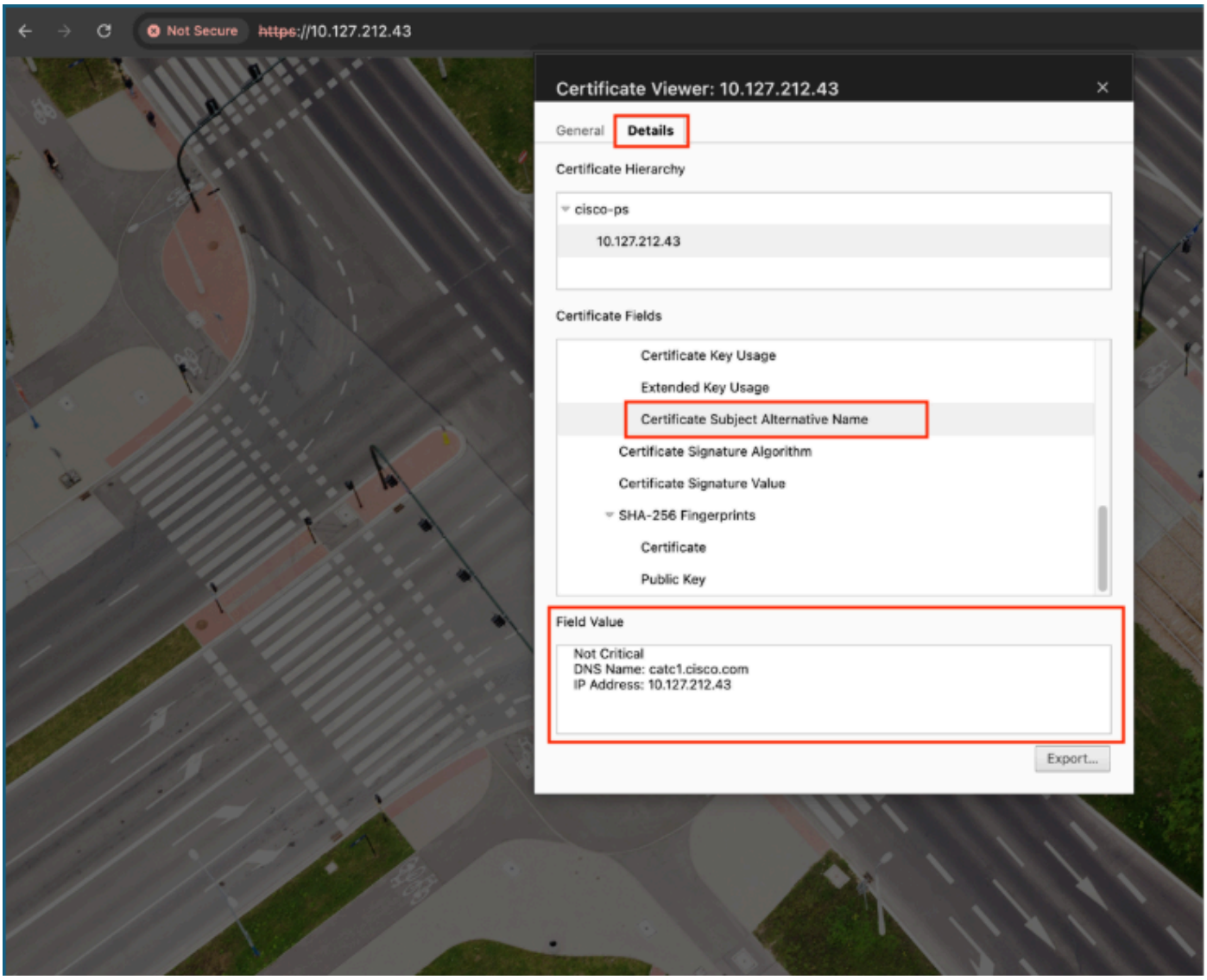
Catalyst Center证书验证

安全自注册要求Catalyst Center SSL证书在Subject Alternative Name(SAN)字段中包含交换机使用的IP地址或FQDN。

GUI验证

1. 在浏览器中打开Catalyst Center登录页面
2. 查看站点信息
3. 打开证书详细信息
4. 验证Extensions（扩展）下的SAN条目


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



注意：如果SAN或主题备用名称字段包含：

- 仅DNS名称 — 在选项43字符串中配置DNS名称。
- 仅IP地址 — 在选项43字符串中配置IP地址。
- IP地址和DNS名称 — 在选项43字符串中配置IP地址。

CLI验证

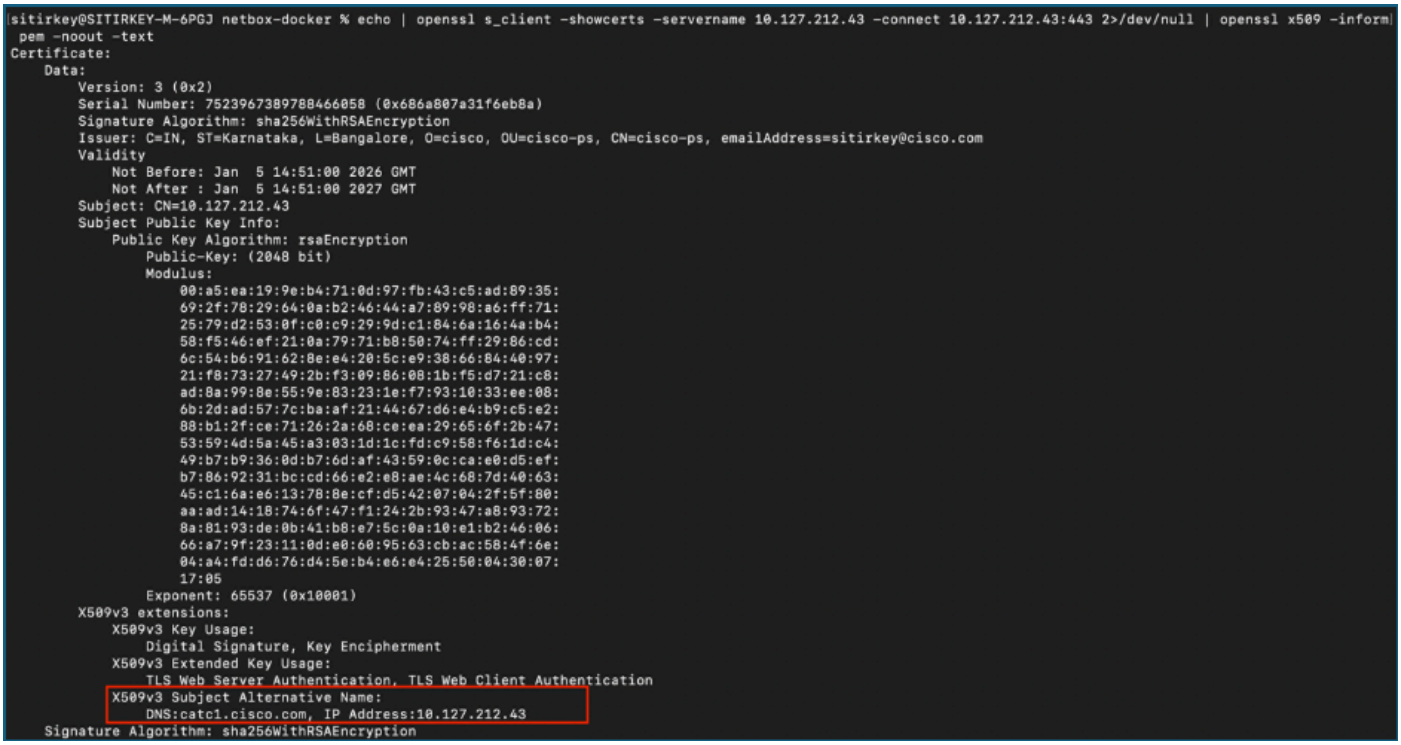
要验证这一点，我们需要一个Catalyst Center IP地址和一个可以到达Catalyst Center服务器的计算机。在终端或命令提示符下运行此命令。

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

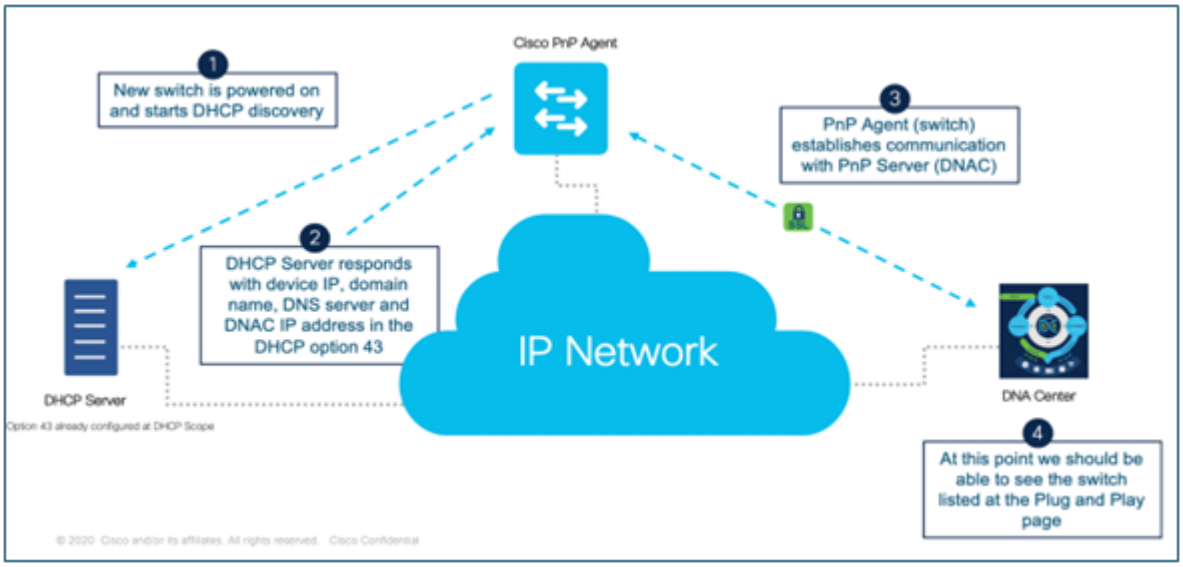
```
-connect

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

验证SAN字段包含适当的IP地址或FQDN。



网络图



Cisco PnP通过实现发现、配置和管理功能，以最少的人工干预实现新设备自注册自动化。当新交换机启动时，它会发送DHCP发现请求，并且DHCP服务器返回网络详细信息，包括通过DHCP选项43的Catalyst Center（PnP服务器）IP地址。使用此信息，交换机的PnP代理通过IP网络安全地连接到PnP服务器。建立连接后，对设备进行身份验证和识别，然后将其添加到即插即用资产，管理员可以在其中快速一致地应用配置和完成调配。

交换机自注册方法

复习本部分介绍的各种入网方法，通过这些方法可将交换机入网Catalyst Center的即插即用清单。

1.使用VLAN1入网

此方法使用默认VLAN 1进行PnP管理

要求

- 在上游交换机上配置了VLAN 1 SVI。
- 配置了选项43的DHCP服务器
- Catalyst Center FQDN的DNS解析

上游交换机上的过程

步骤1.配置VLAN 1的SVI。

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

步骤2.使用选项43配置DHCP池（注意：我们可以将选项43参数与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;
```

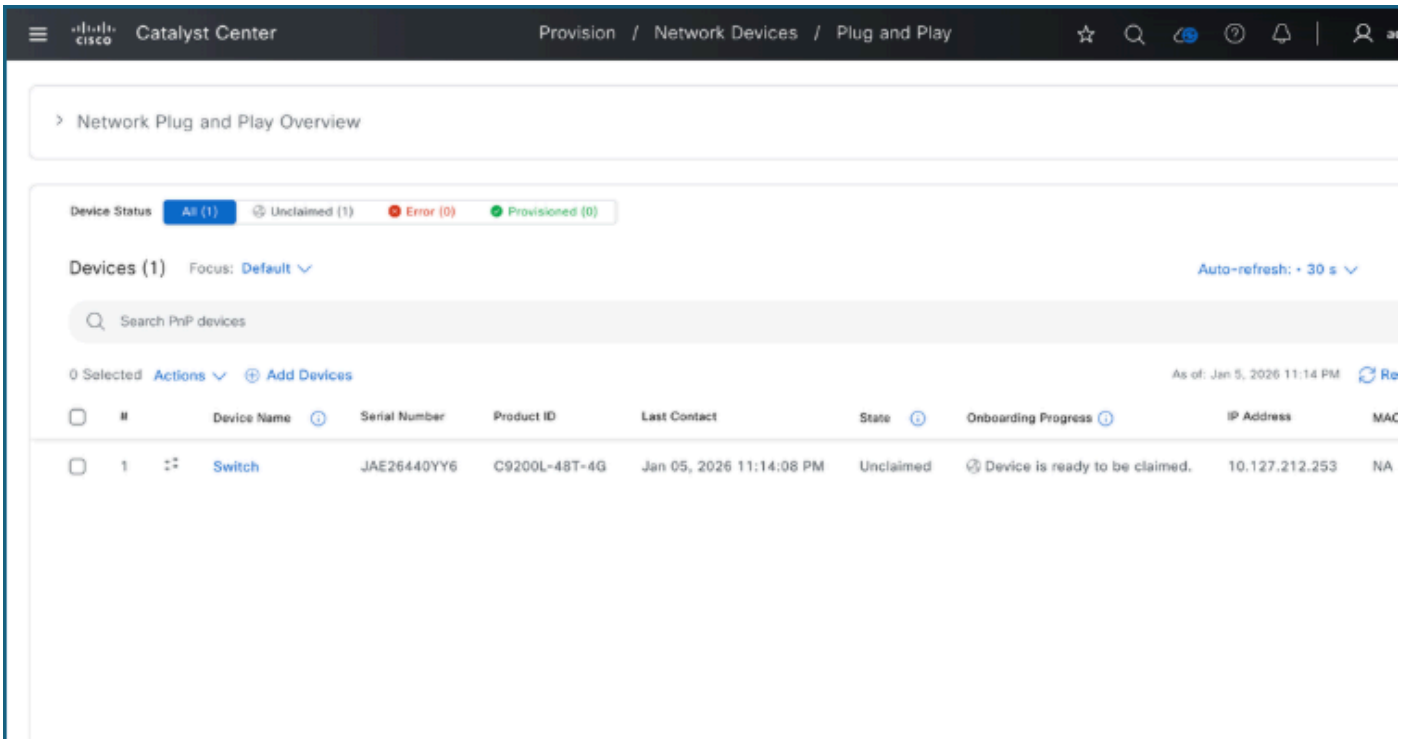
或

```
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
```

步骤3.配置新交换机的TRUNK接口。

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

步骤4.验证交换机是否显示在Catalyst Center的Provision > Plug and Play页面上。



2.使用自定义VLAN入网

此方法使用专用VLAN进行管理。

要求

- 在上游交换机上配置自定义VLAN SVI。
- 配置了选项43的DHCP服务器。
- Catalyst Center FQDN的DNS解析。
- Trunk允许自定义VLAN以及其他流量所需的任何其他VLAN。

上游交换机上的过程

步骤1.配置自定义VLAN的SVI。

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

步骤2.使用选项43配置DHCP池（注意：我们可以将选项43参数与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
```

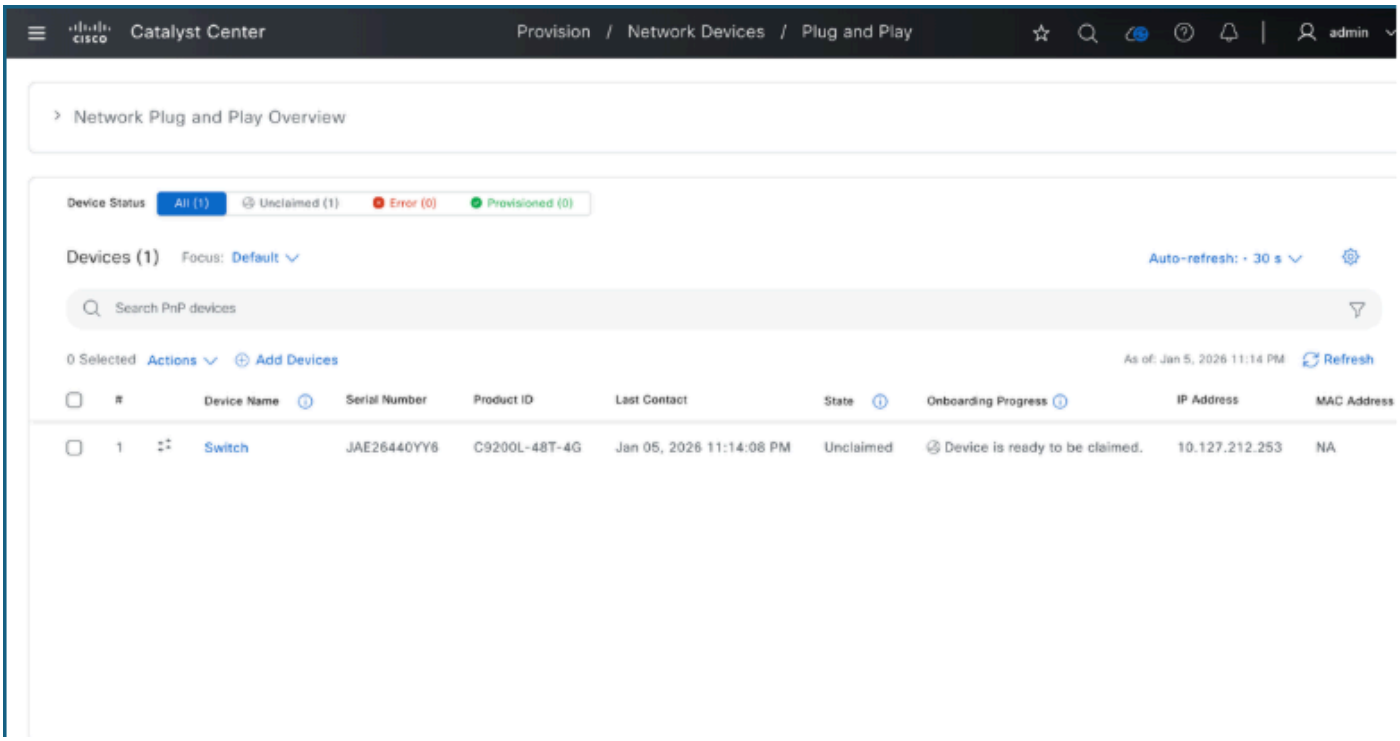
步骤3.将自定义VLAN配置为PnP VLAN。

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

步骤4.将中继接口配置为新交换机。

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

步骤5.验证交换机是否显示在Catalyst Center的Provision > Plug and Play页面。



3.使用管理端口的板载交换机

此方法利用交换机的管理接口。

要求

- 上游交换机上配置的自定义VLAN SVI
- 配置了选项43的DHCP服务器
- Catalyst Center FQDN的DNS解析

上游交换机上的过程。

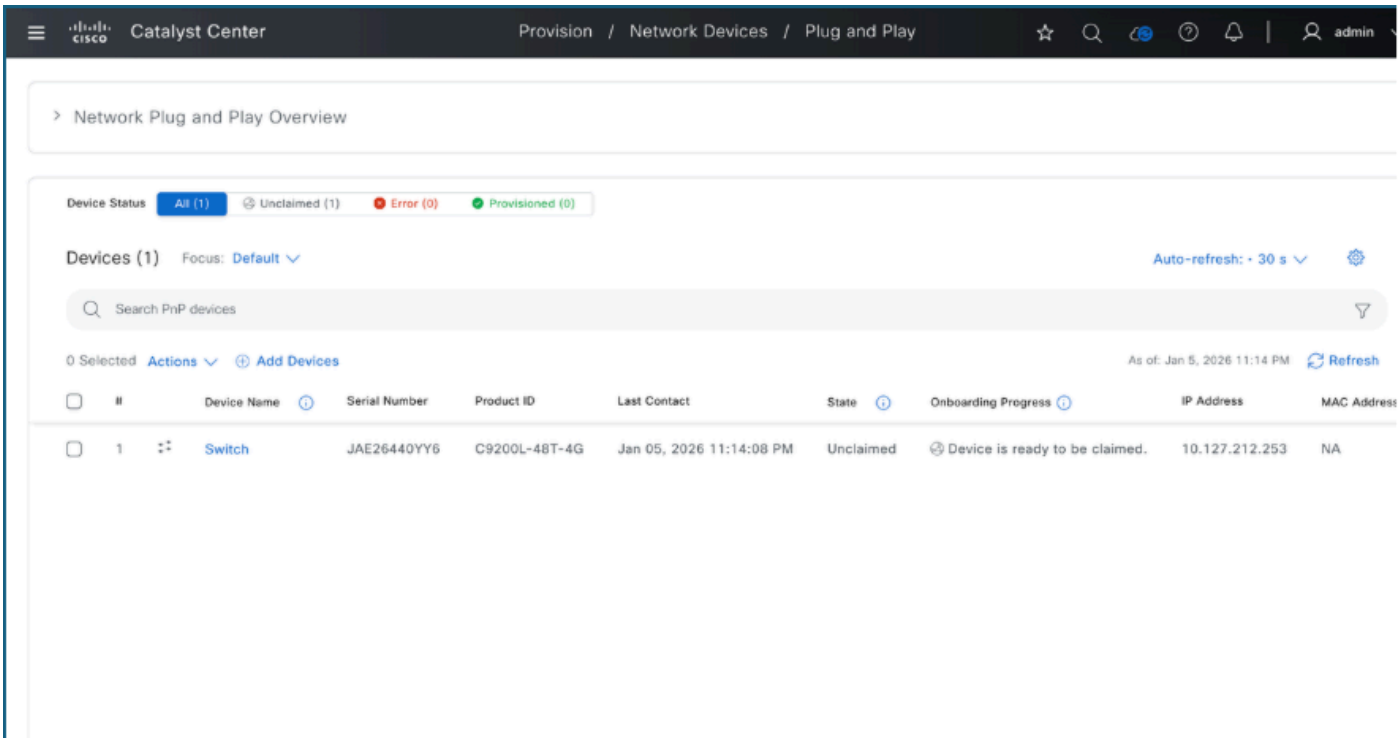
步骤1.配置VLAN的SVI。

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

步骤2.配置新交换机的接入接口。

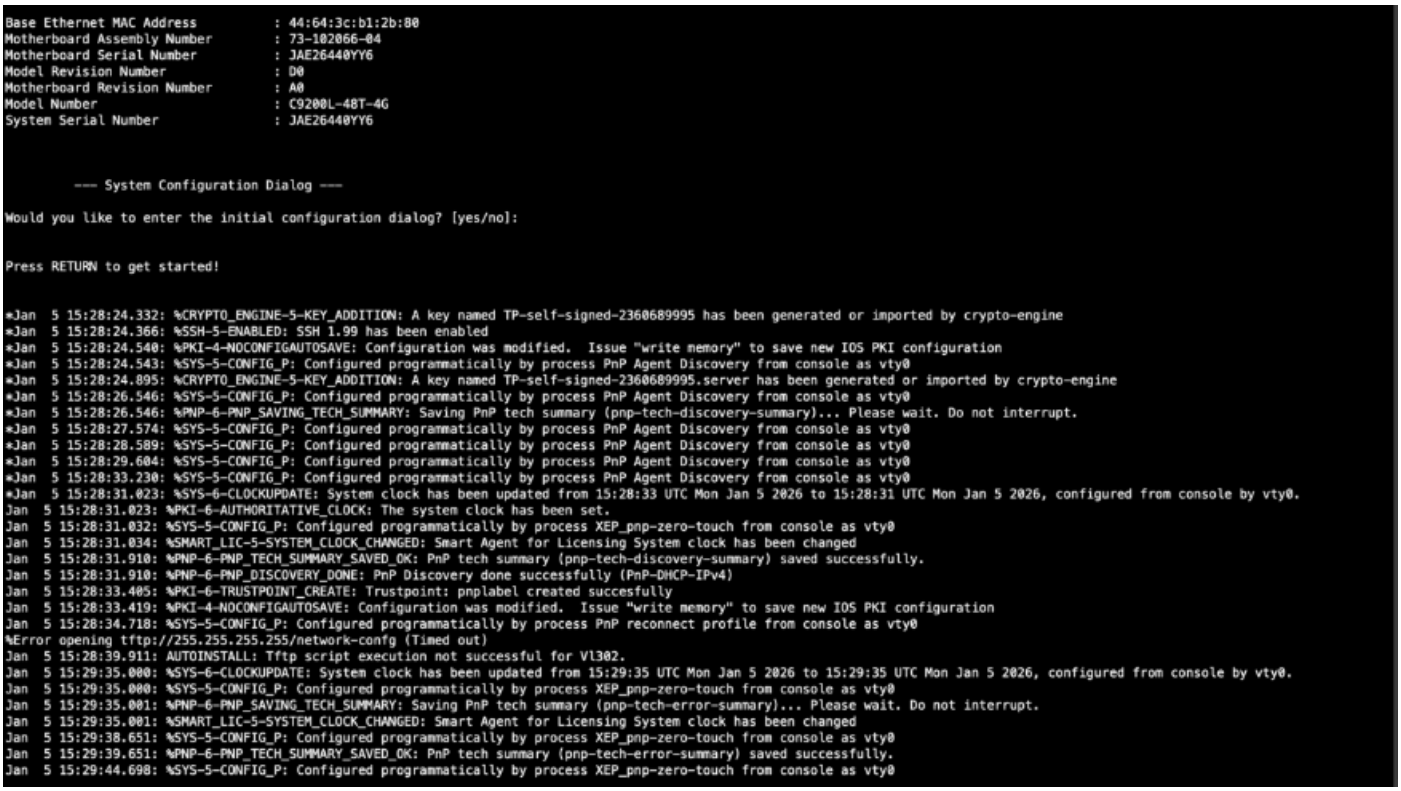
```
config t
interface GigabitEthernet1/0/5
  switchport mode access
  switchport access vlan 302
```

步骤3.检验交换机是否显示在Catalyst Center的Provision > Plug and Play页面上。



4.交换机控制台日志

以下是将DHCP用于即插即用时，交换机控制台上显示的信息。

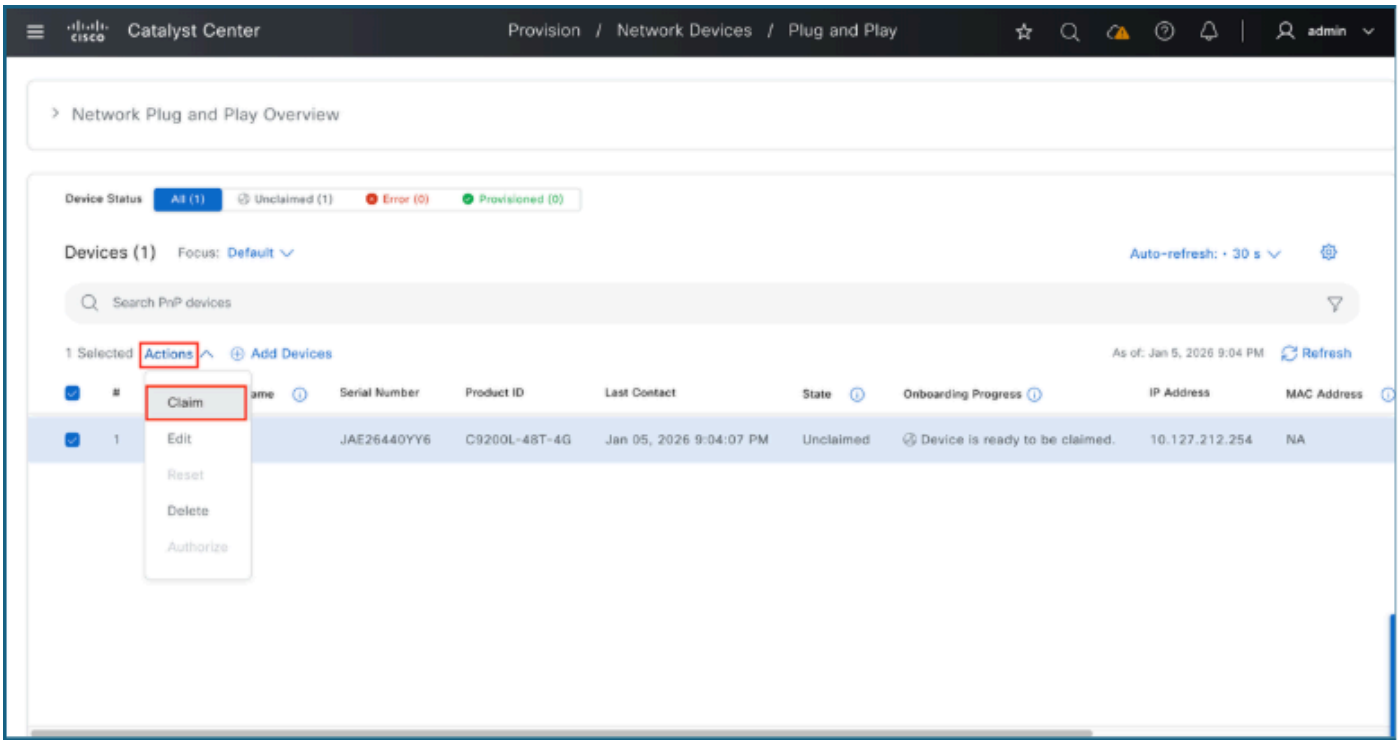


无需第0天模板即可将交换机注册到Catalyst Center

要将新交换机列入Catalyst Center的库存，请在设备在“即插即用”页面上可见并且可申领时完成这些必需步骤。

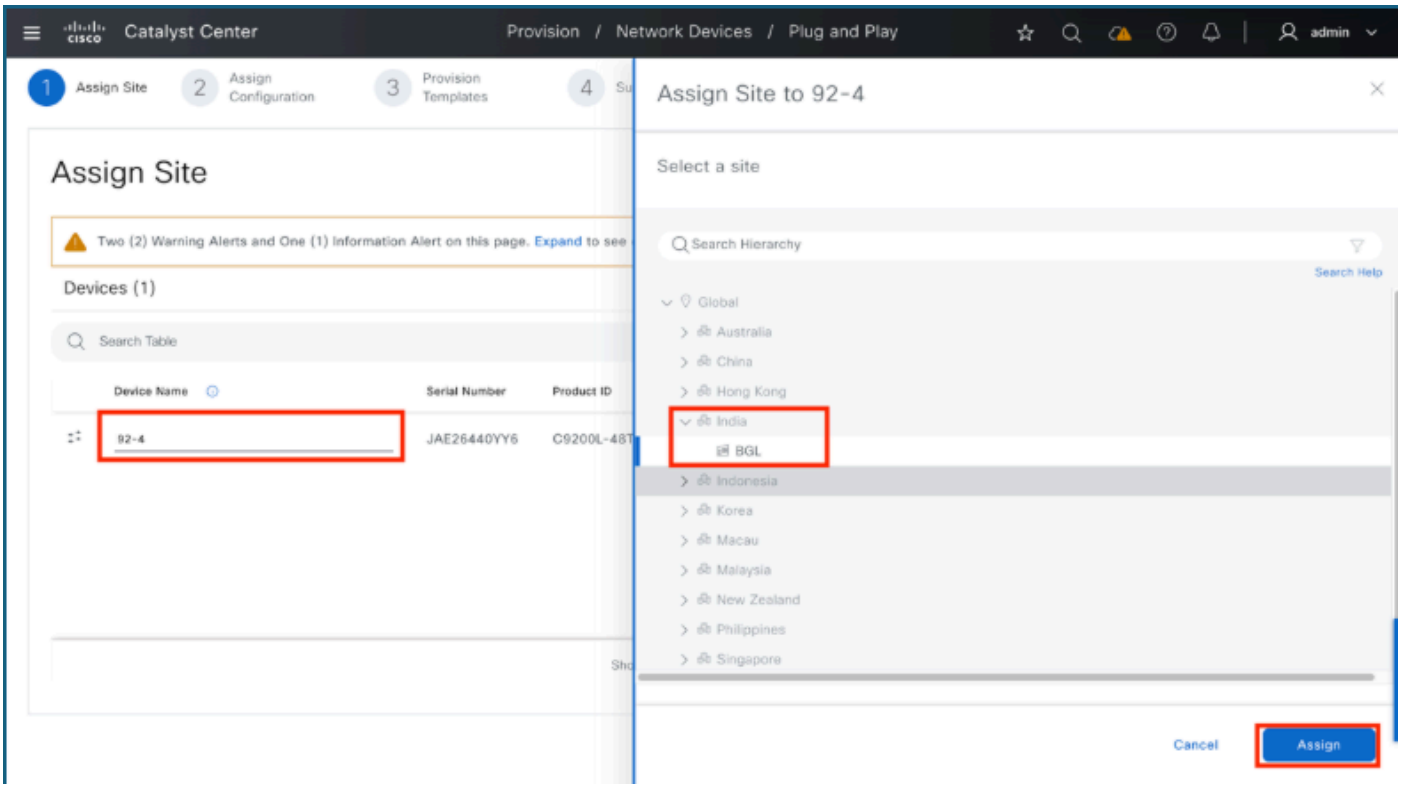
1.要申请开关，请执行以下操作：

- 选中要申领的交换机的复选框。
- 导航至“活动”>“领款申请”。



2.要命名和映射交换机，请执行以下操作：

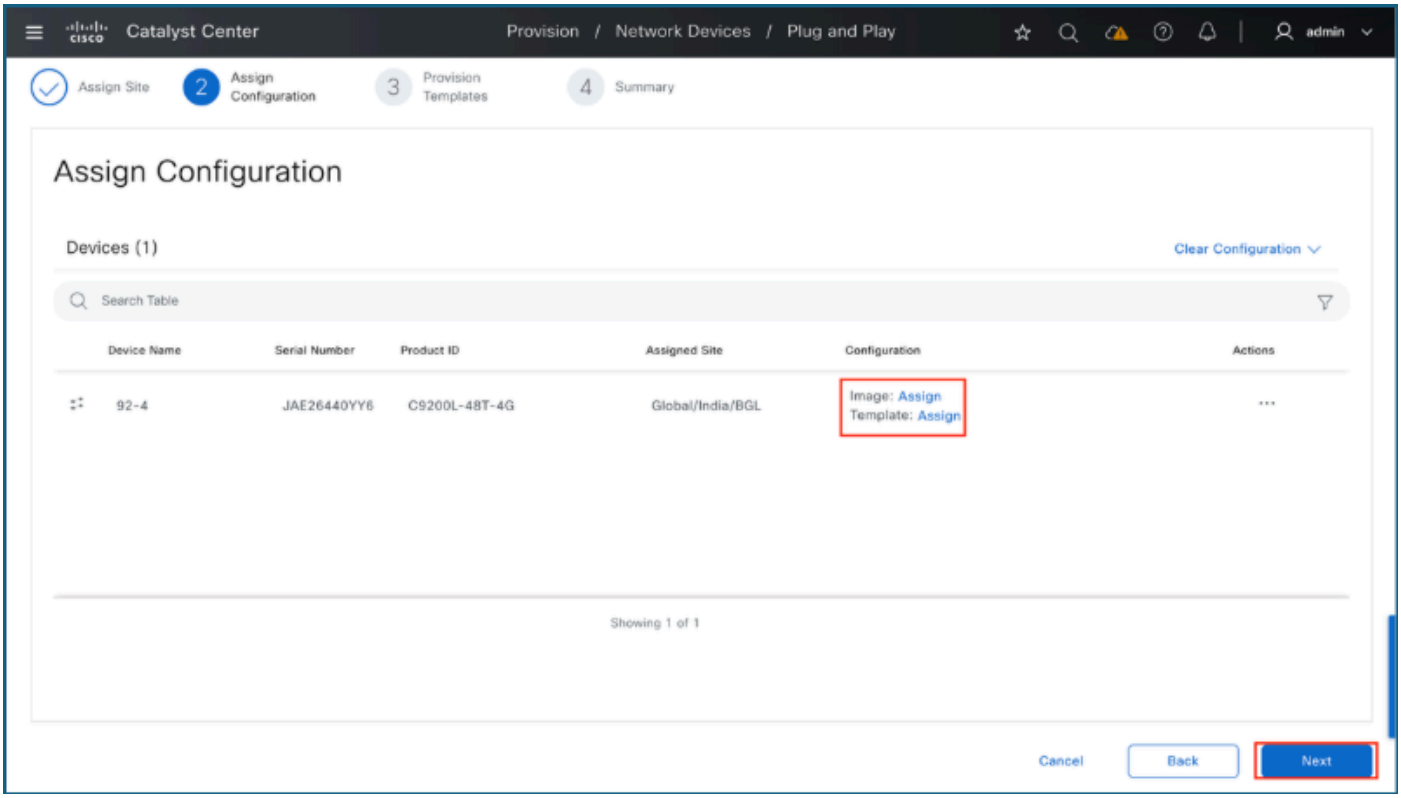
- 在Device Name字段中输入名称，然后单击Assign。
- 选择正确的站点或建筑，再次单击Assign，然后单击Next。



3.分配软件映像或模板（可选）：

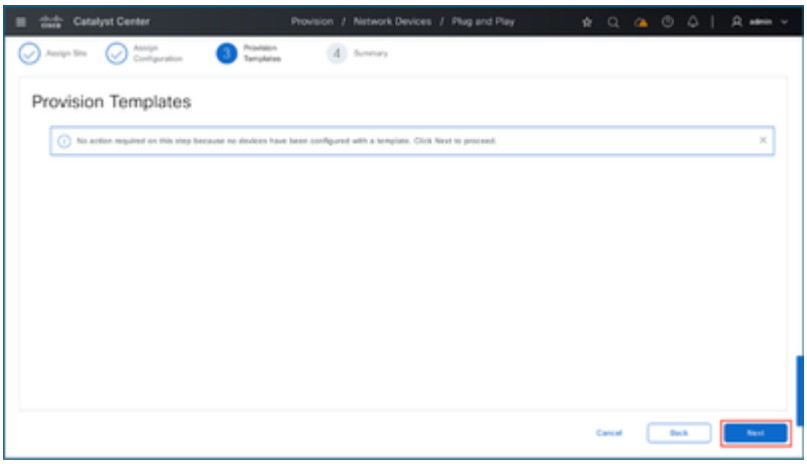
使用此步骤将交换机升级到特定软件版本或应用第0天配置模板。

- 单击Image旁边的Assign以指定软件版本。
- 点击模板旁边的分配以应用模板配置。
- 完成所需的分配后，单击Next。



4.调配模板

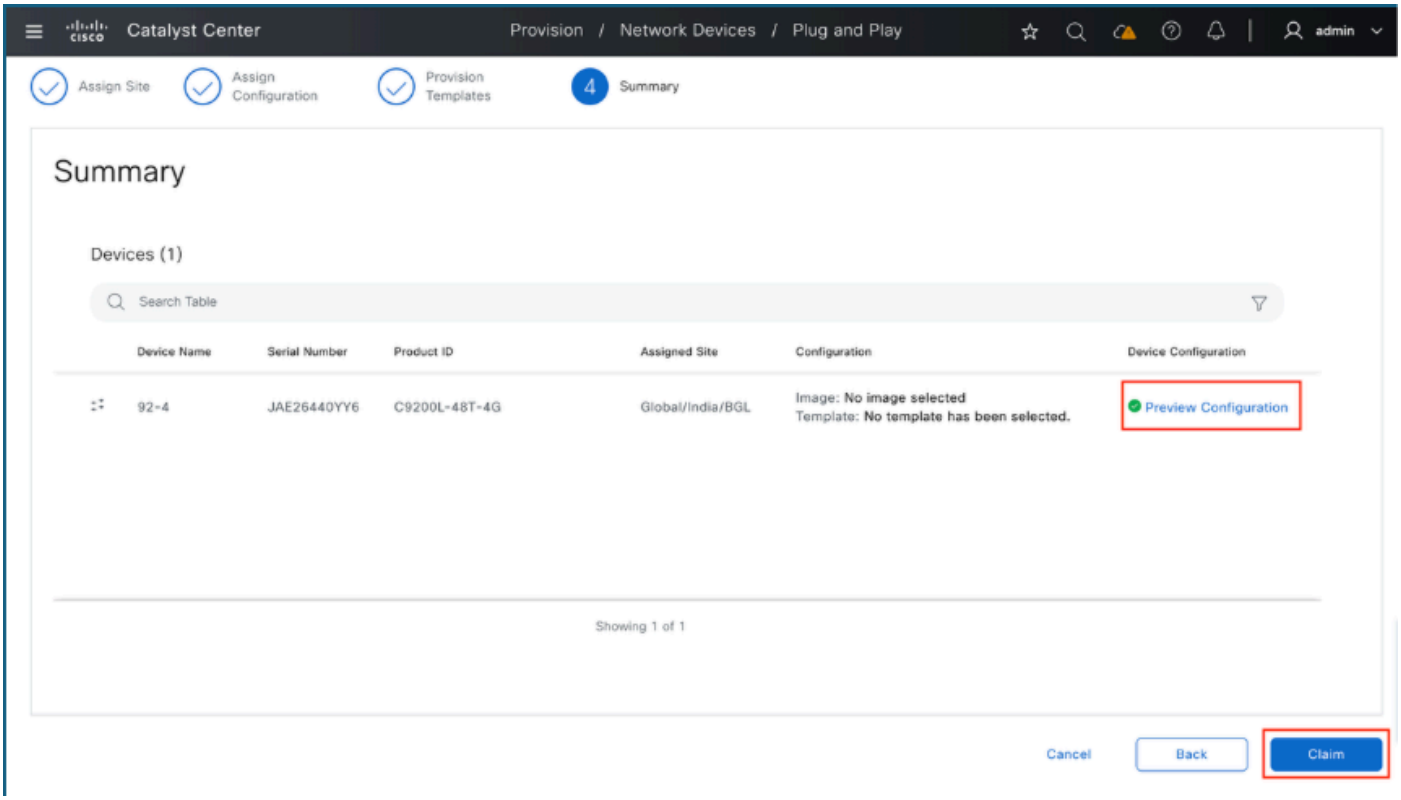
在不使用模板的情况下申请设备时，请选择Next（下一步）绕过此配置步骤。

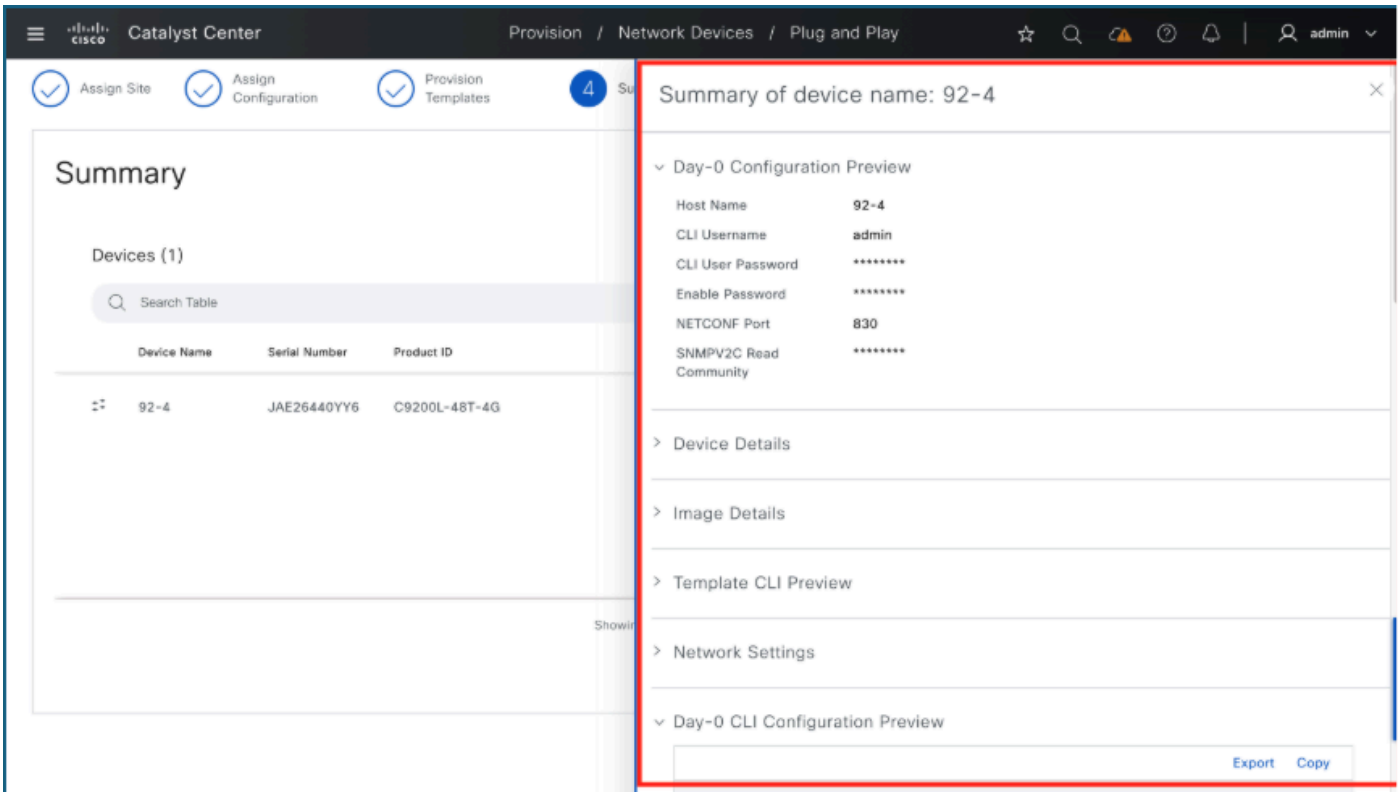


5.总结

使用Summary页面在Catalyst Center调配配置之前查看配置。

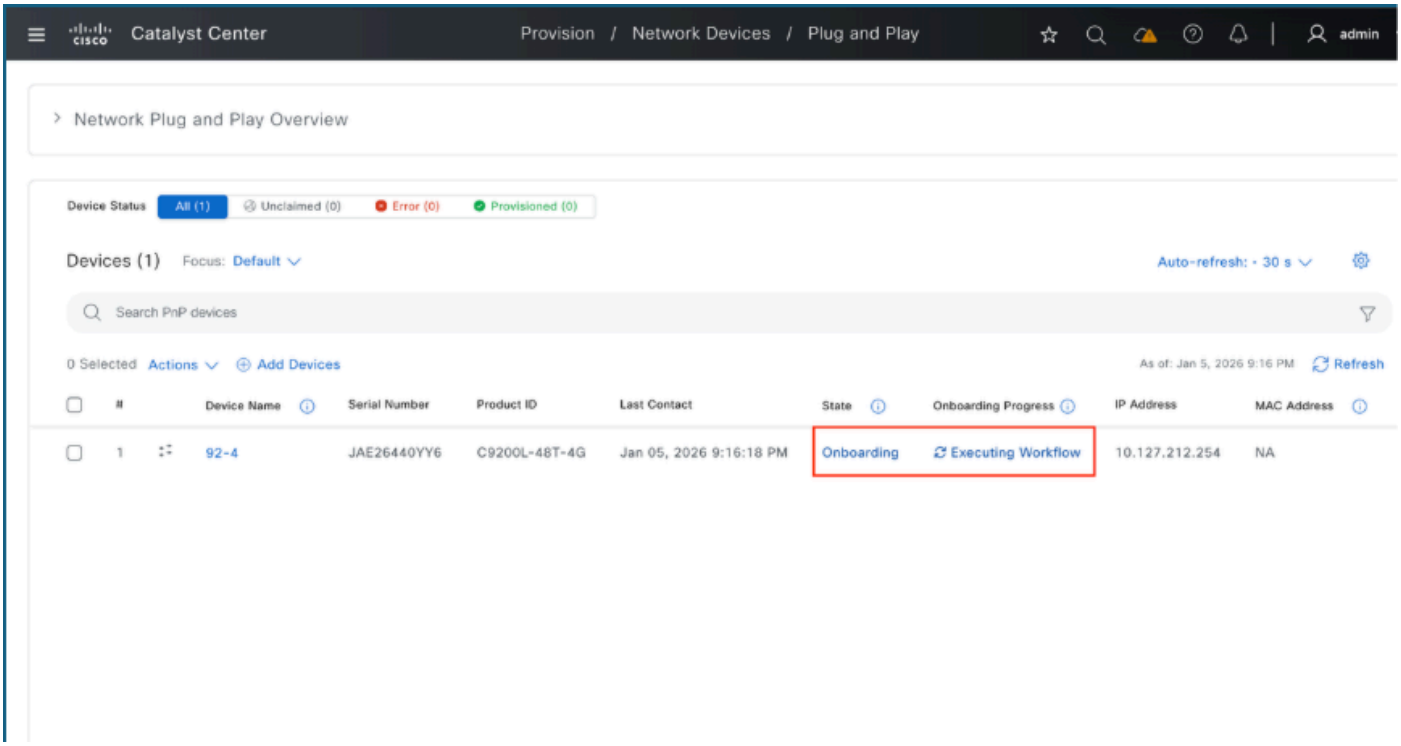
- 单击Preview Configuration。
- 展开各个部分以验证设置。
- 验证后，单击Claim。

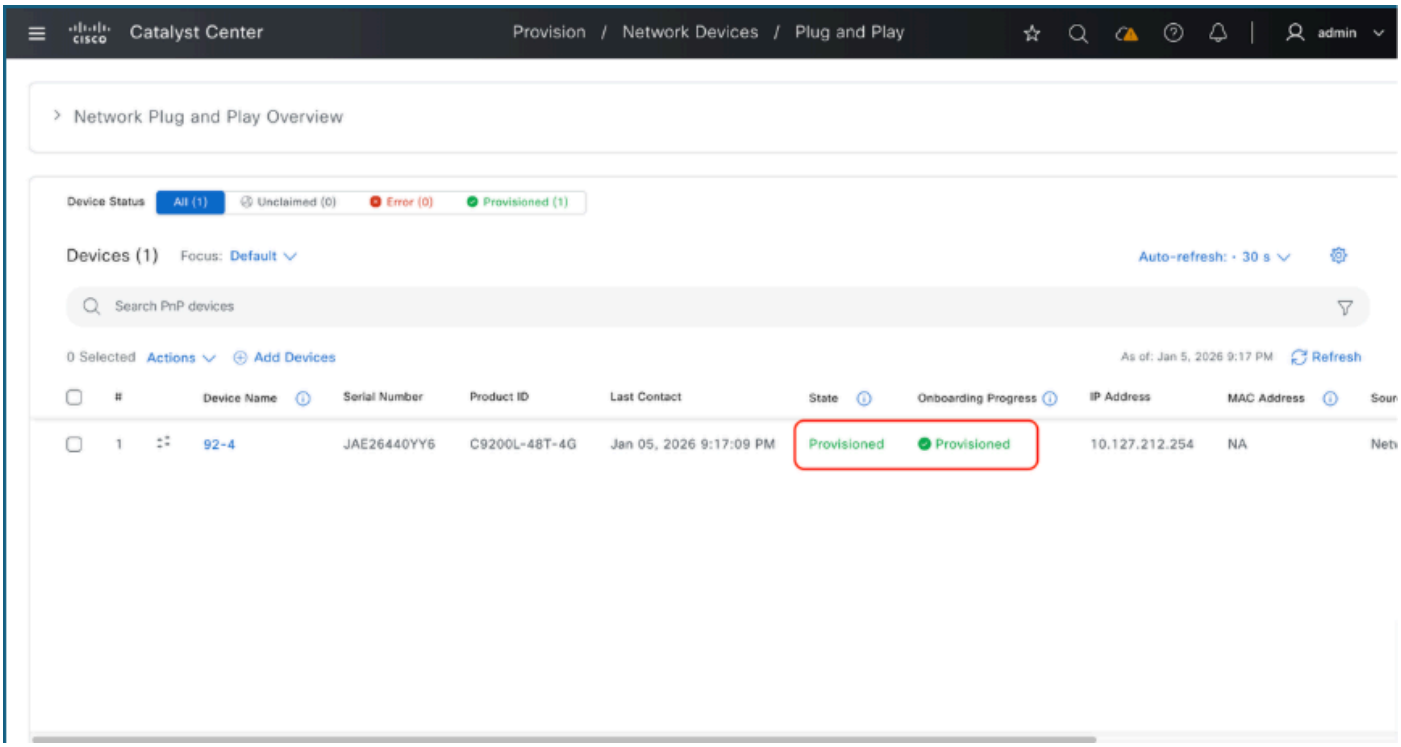




6.监控申请流程

启动申请后，接口会返回到“即插即用”控制面板。监控设备状态，如果转换到Provisioned，则表示交换机已成功申请并添加到Catalyst Center的资产中。



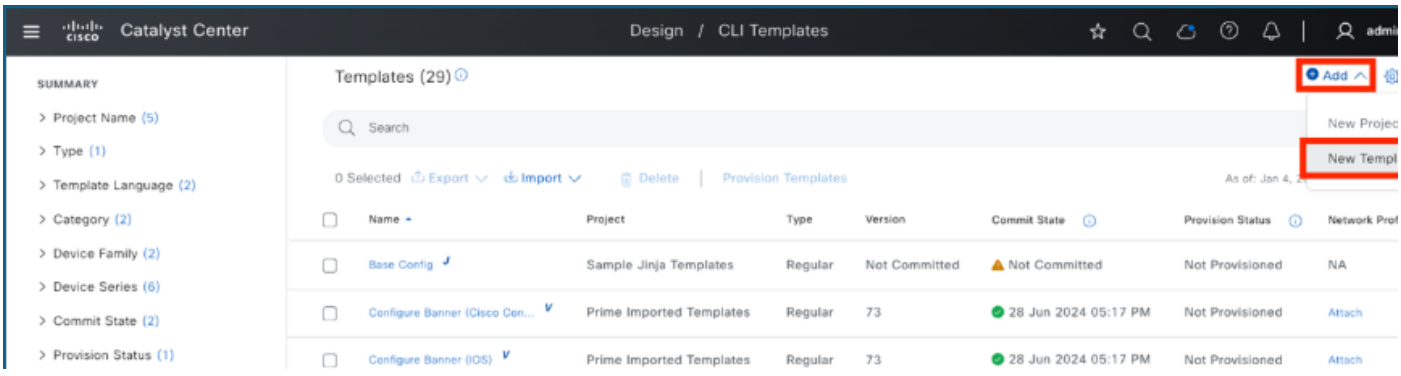


使用第0天模板将交换机注册到Catalyst Center

在Catalyst Center的即插即用页面上准备好新交换机时，应用0天模板以在申请过程中包括其他配置。

1.创建第0天或入职培训模板

- 导航到Design > CLI Templates。
- 选择Add > New Template。

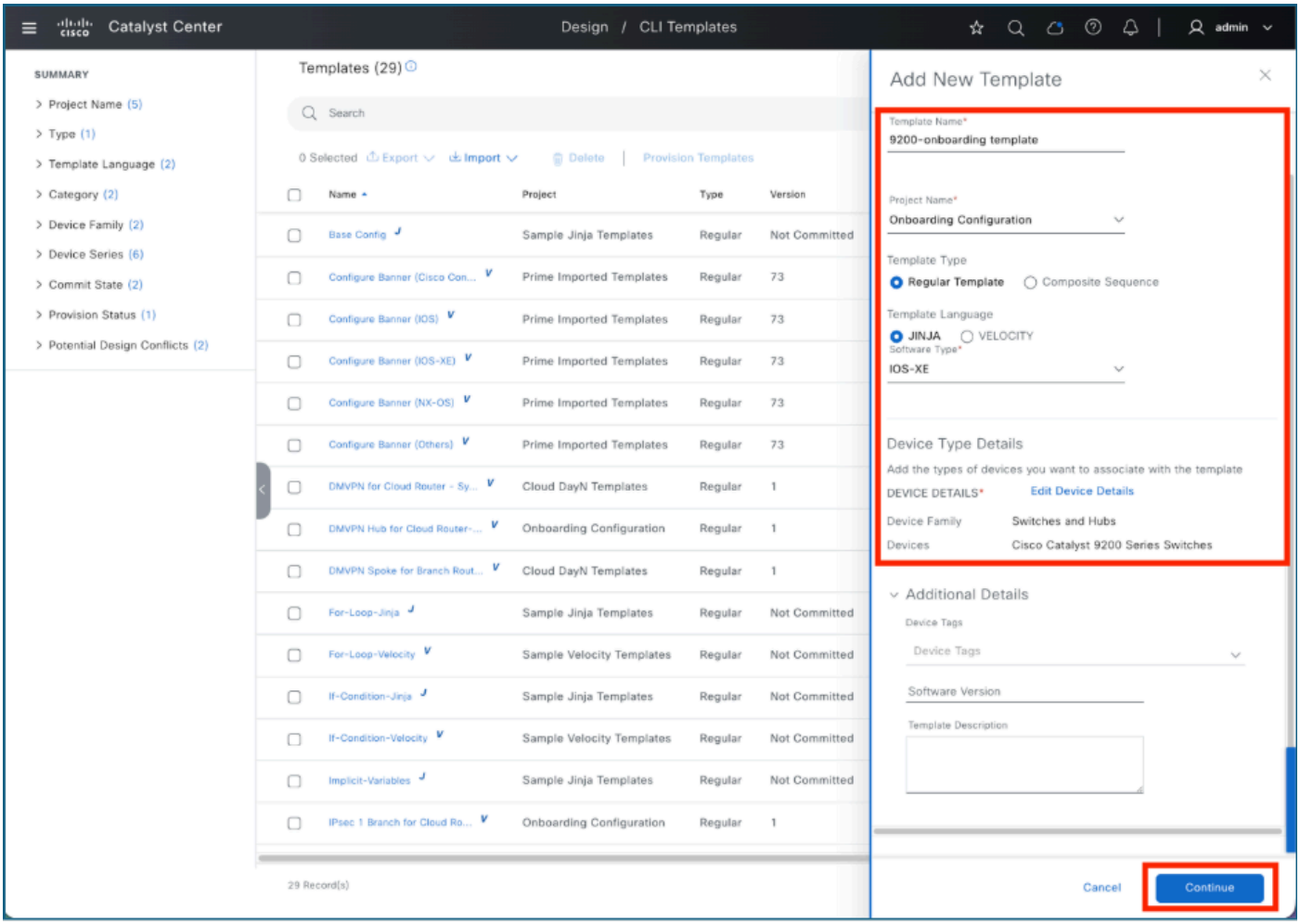


2.添加模板详细信息

在侧面板中，输入以下模板规范：

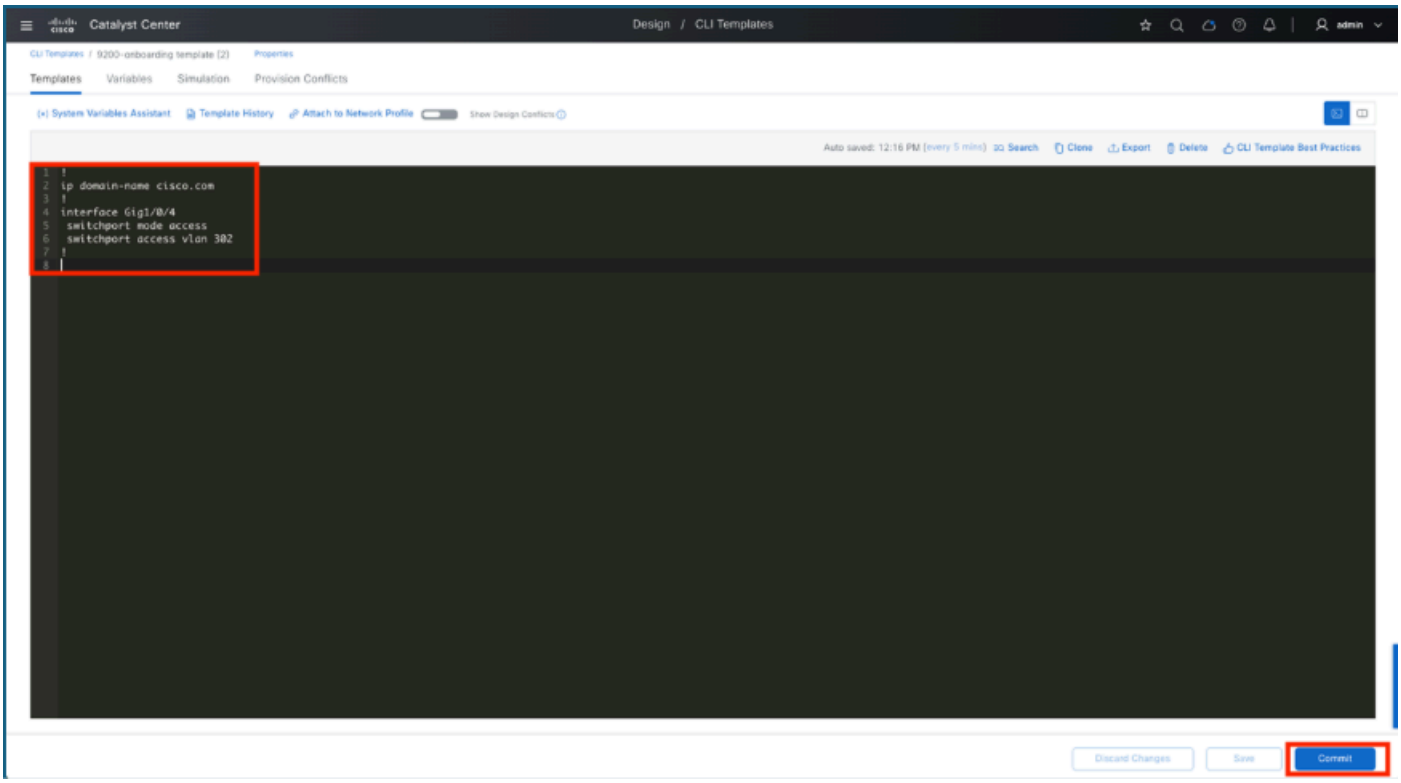
- 模板名称
- 项目名称：对于0天模板，请始终选择Onboarding Configuration。

- 模板类型、语言和软件类型:从菜单中选择适当的值。
- 单击Continue继续。



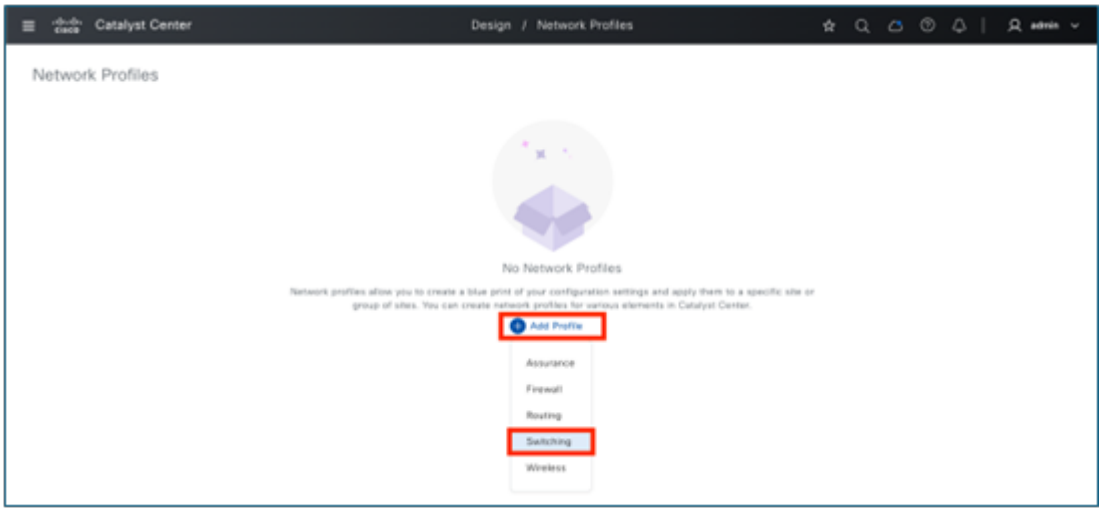
3.编辑模板

在CLI模板编辑器中输入要部署到交换机的配置。在此示例中，配置了域名和访问端口。将配置添加到CLI模板编辑器后，单击Save，然后单击Commit完成更改。



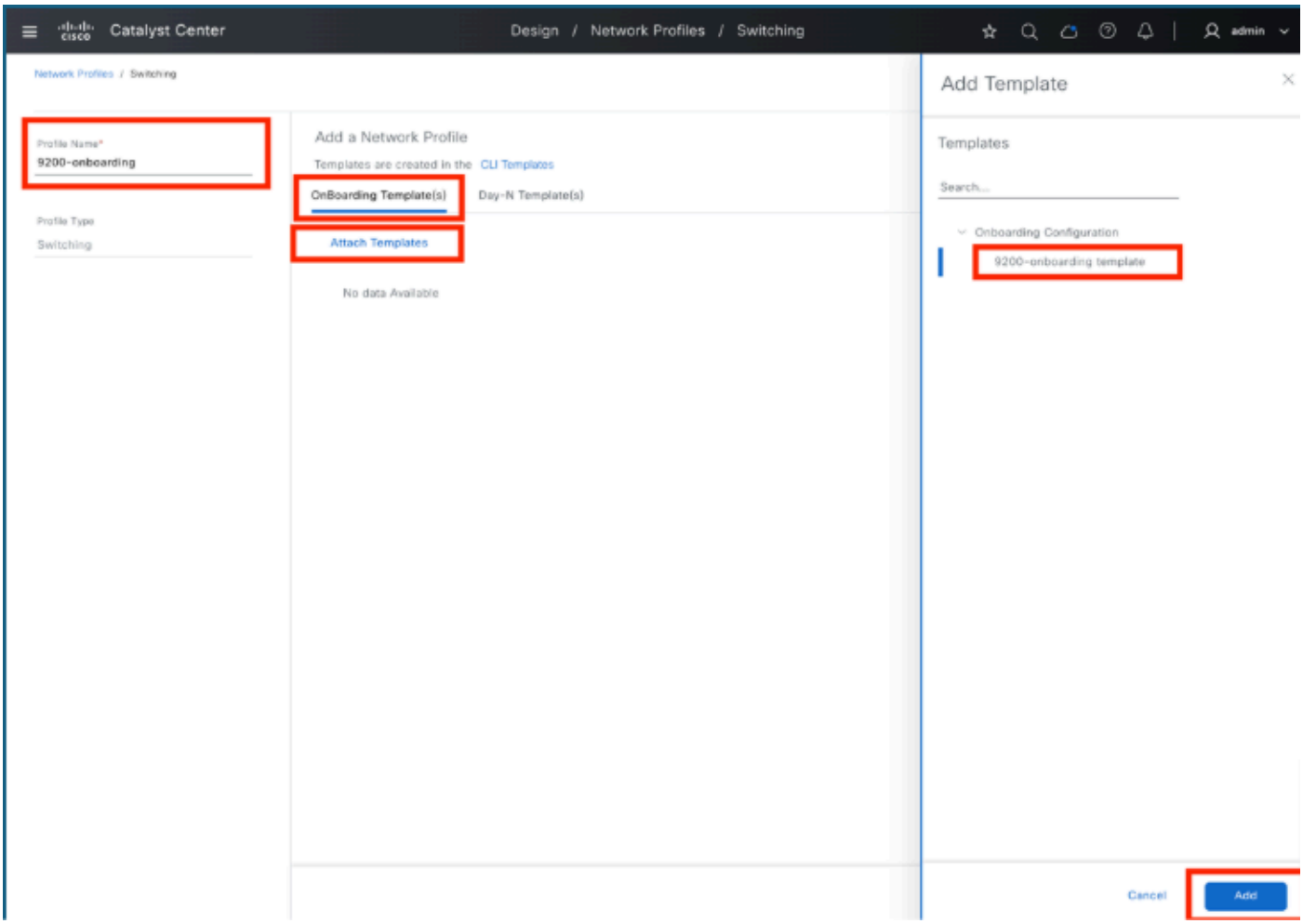
4.创建网络配置文件

- 导航到Design菜单并选择Network Profiles。
- 单击Add Profile按钮。
- 从列表中选择适当的配置文件类型(例如Switching)。



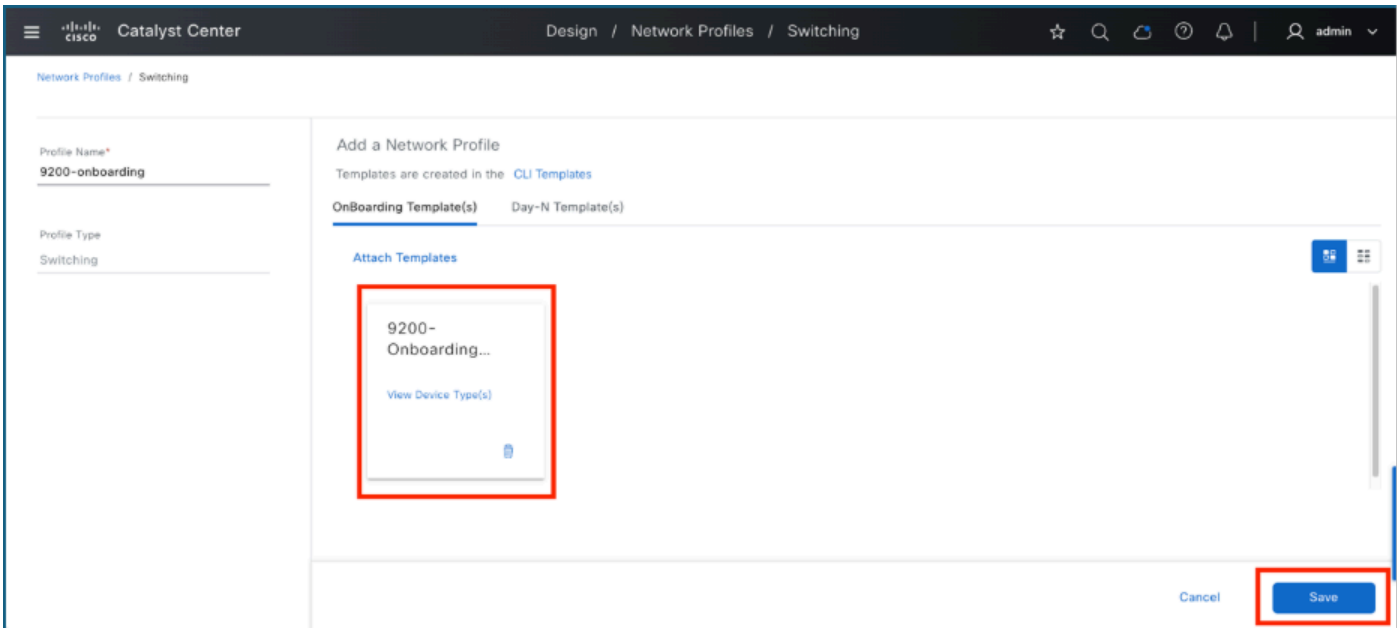
5.添加模板并编辑网络配置文件设置

- 输入配置文件名称：提供网络配置文件的名称。
- 访问模板：点击Onboarding Template(s)，然后选择Attach Templates。
- 选择Template:从Onboarding Configuration目录查找并选择所需的模板。
- 完成：点击Add按钮完成该过程。



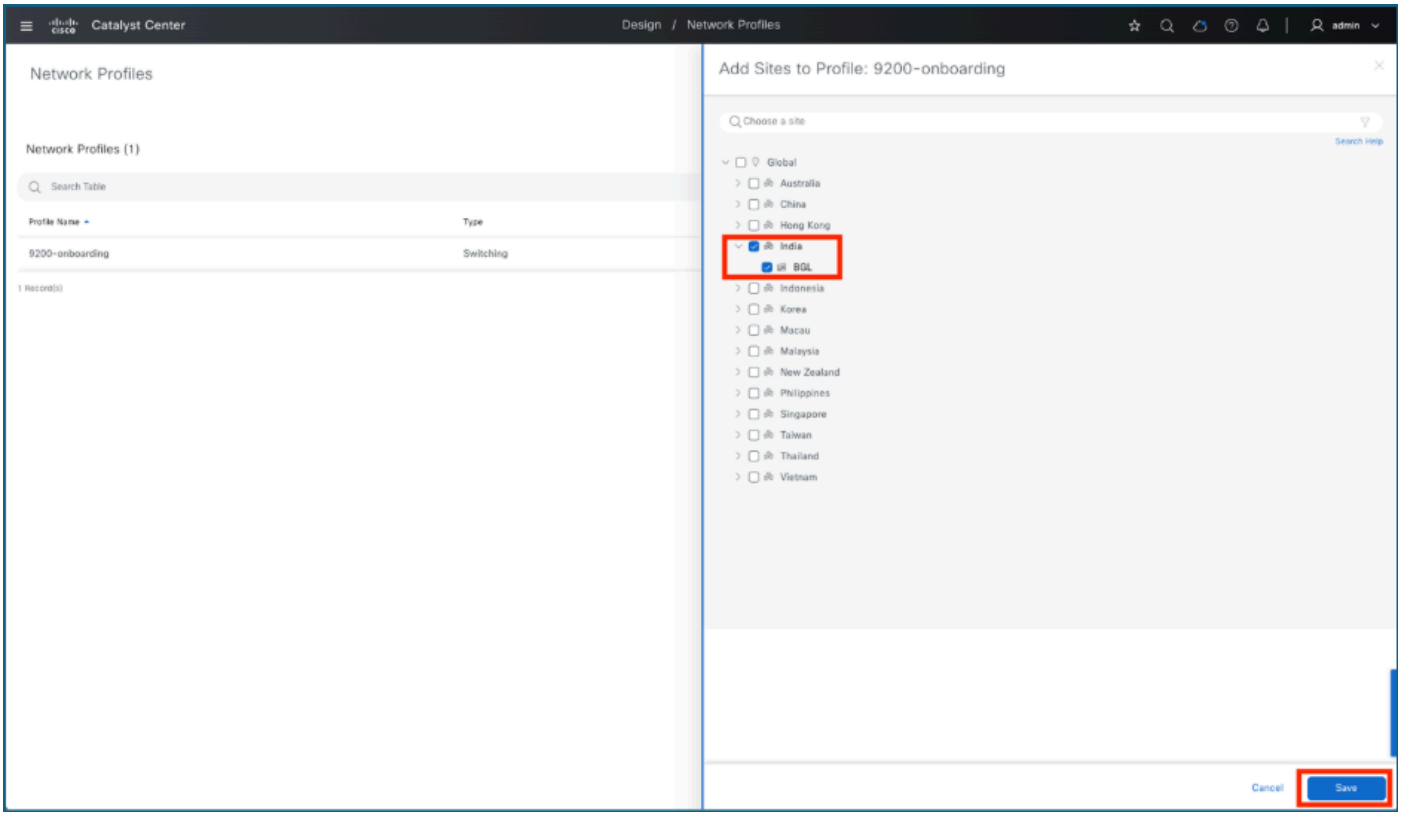
6.保存配置文件

- 验证模板：添加模板后，确保该模板显示在“Onboarding Template(s)（自行激活模板）”下的列表中。
- 保存Profile: 点击保存按钮以最终确认并存储配置文件设置。



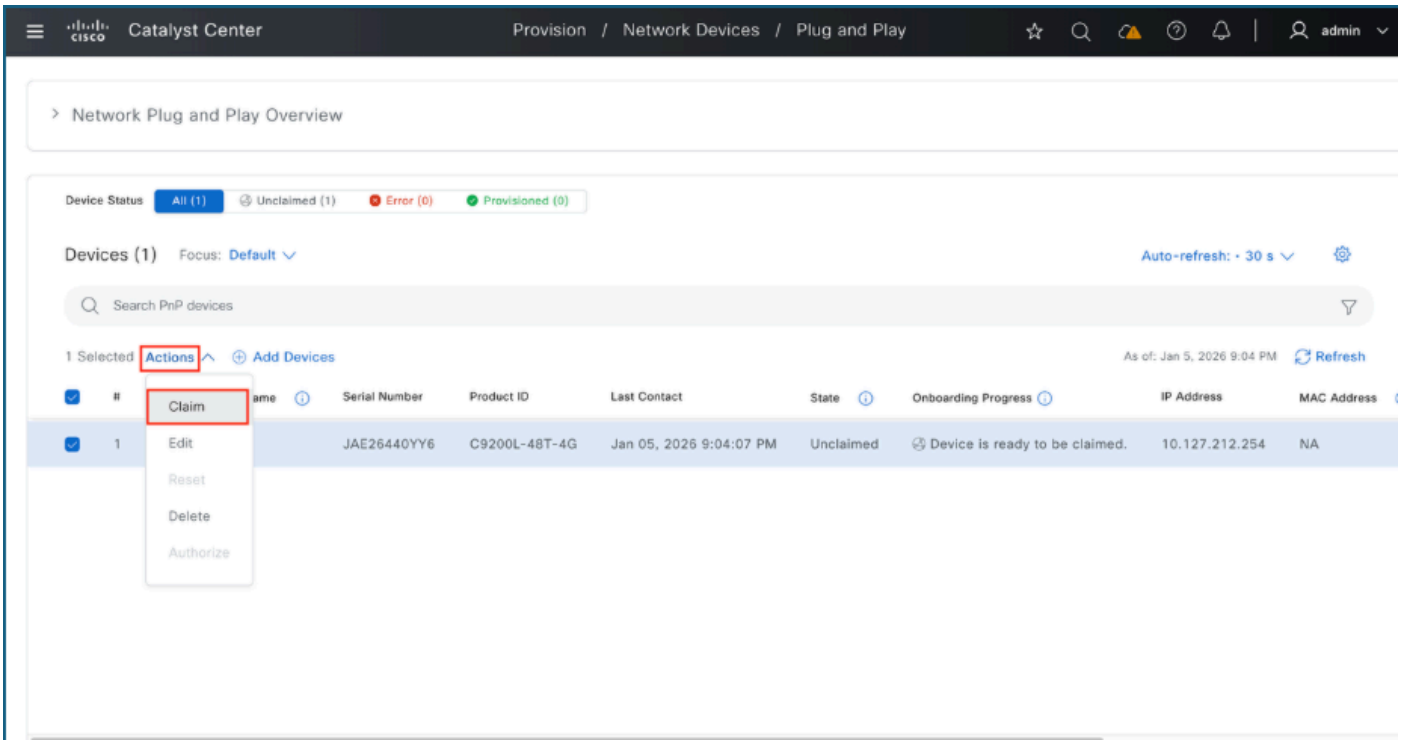
7.将网络配置文件分配到要安装交换机/交换机的站点

- Initiate Assignment：单击刚创建的网络配置文件的Assign Site选项。
- 选择站点：选择交换机将入网的特定站点。
- 确认：单击保存完成分配。



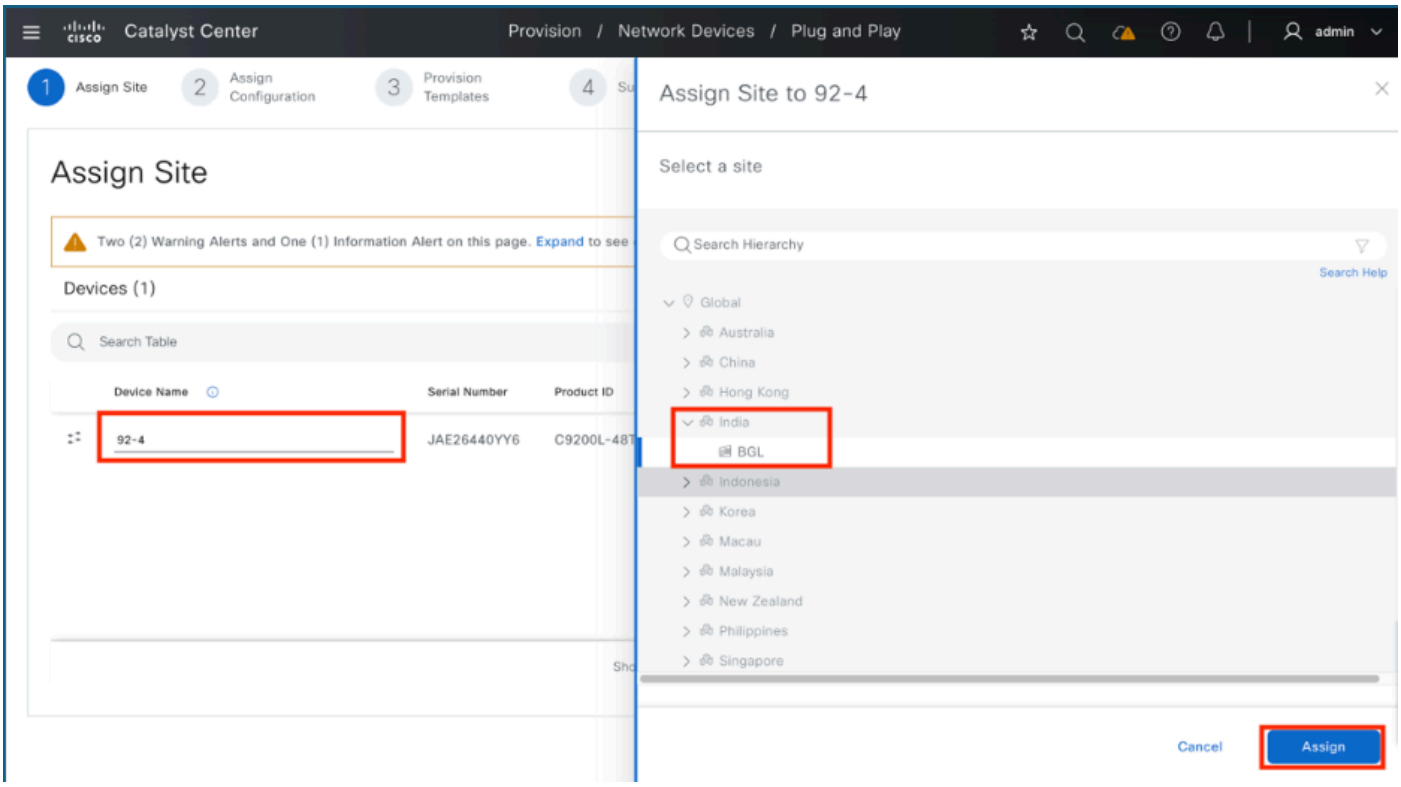
8.索赔开关

- 导航到Plug and Play:转到Provision菜单，然后选择Plug and Play。
- 选择Devices:找到要申领的一个或多个交换机，然后点击每个交换机名称旁边的复选框。
- 启动申请：导航至“Actions”菜单，然后选择“Claim”。



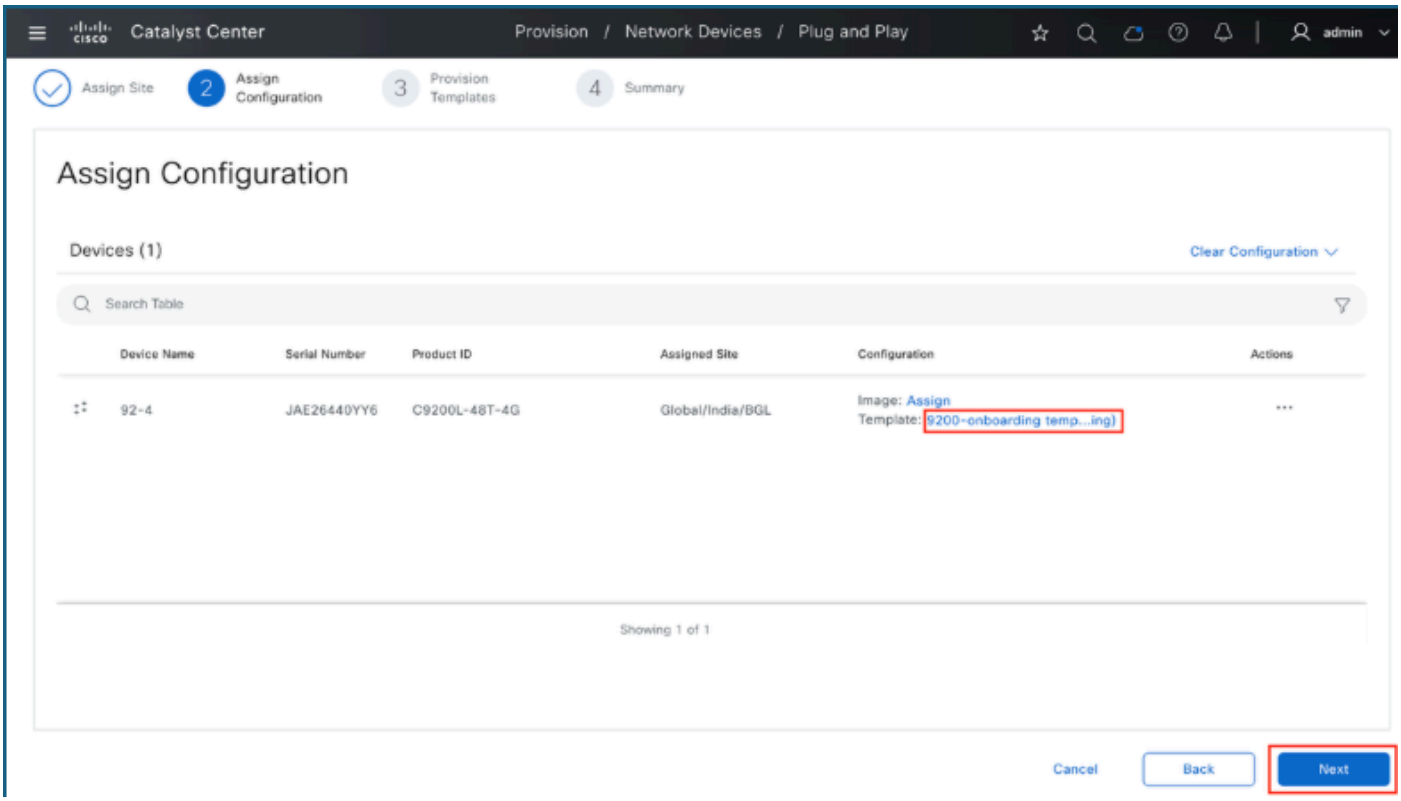
9.为交换机指定名称并分配给站点

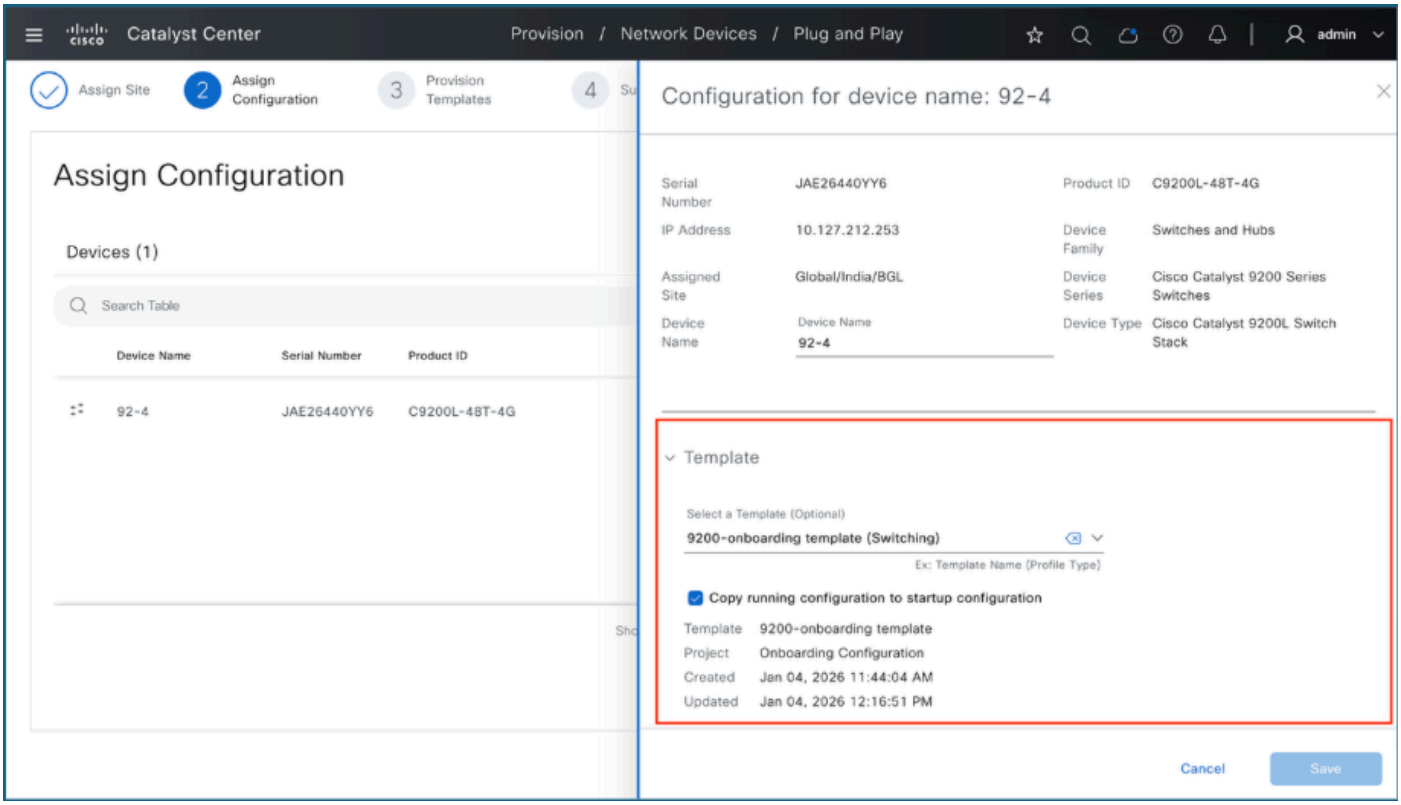
- 命名设备：在设备名称(Device Name)字段中输入交换机的所需名称。
- Initiate Assignment：单击Assign按钮。
- 选择Location：选择适当的站点或建筑，再次单击Assign，然后点击Next以继续。



10.分配第0天模板

- 选择模板(Template)：点击在“模板”(Template)选项旁边自动选择的模板。
- 查看详细信息：仔细验证已分配模板的配置详细信息。
- 继续：确认模板分配后，单击“下一步”。

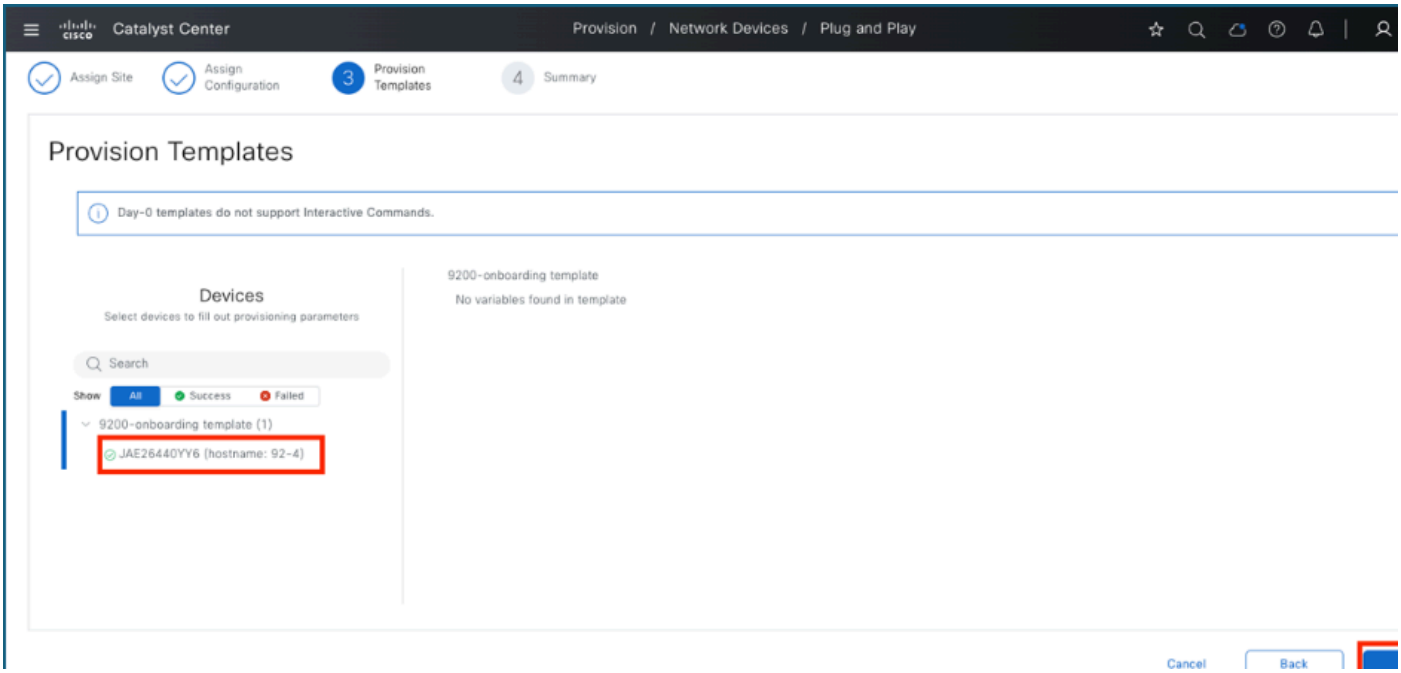




11.调配模板

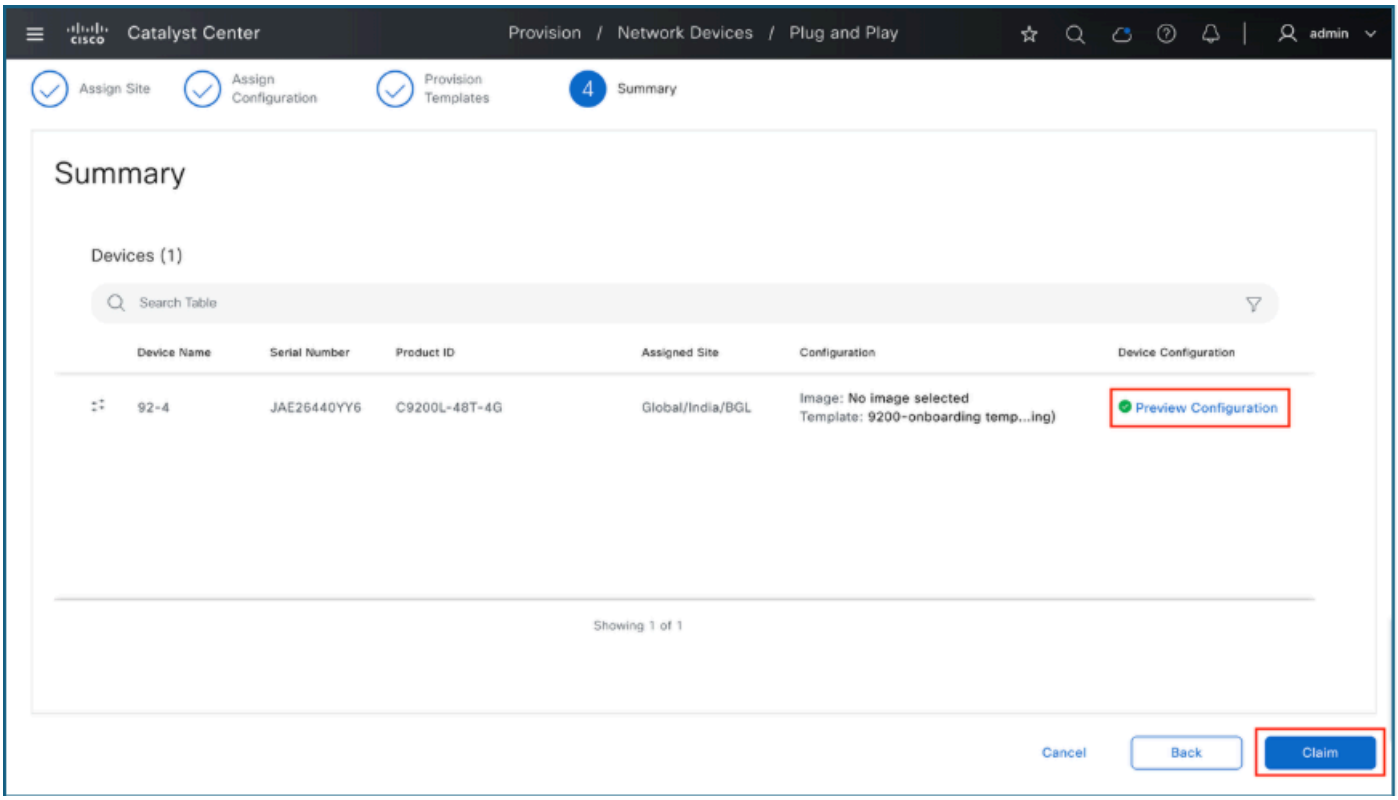
- 选择Device:在模板部分下，点击要配置的特定设备。

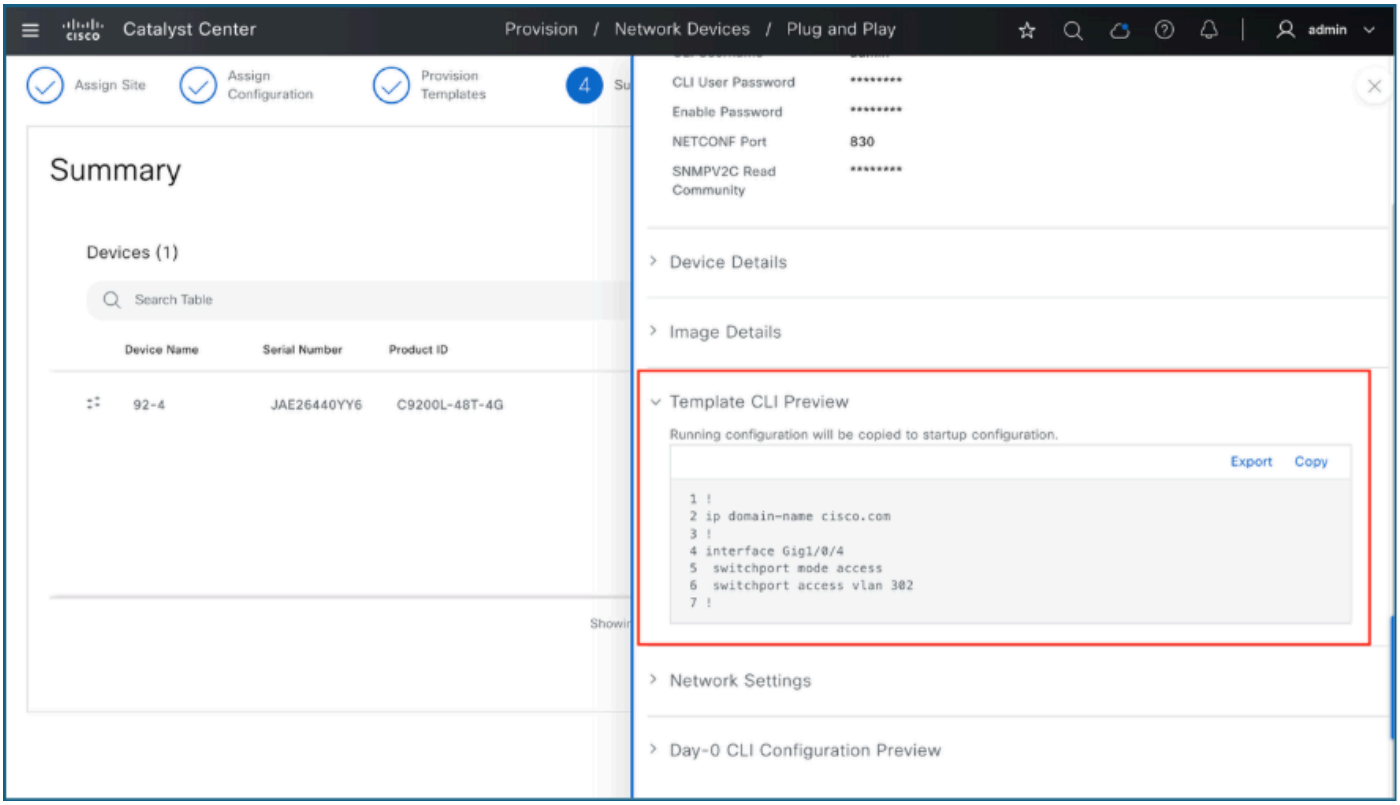
- 标识变量：检查与模板关联的任何必需变量值。
- 输入值：如果任何变量是必需的，请填写必要的值。
- 继续：单击下一步转到下一步。



12.总结

- 审核配置：在摘要页面上，审核由Catalyst Center准备的配置设置。
- Preview Details：单击Preview Configuration查看待决更改。
- 验证部分：展开每个部分以检查特定配置详细信息。
- 完成：验证设置后，单击Claim以继续。

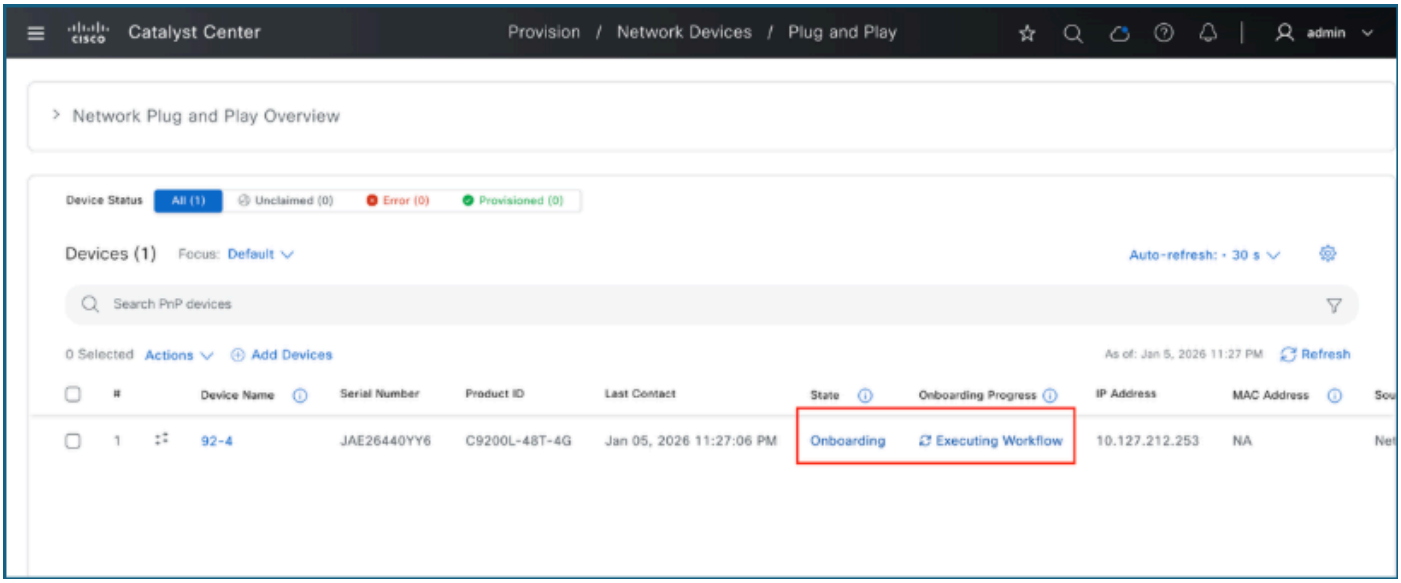


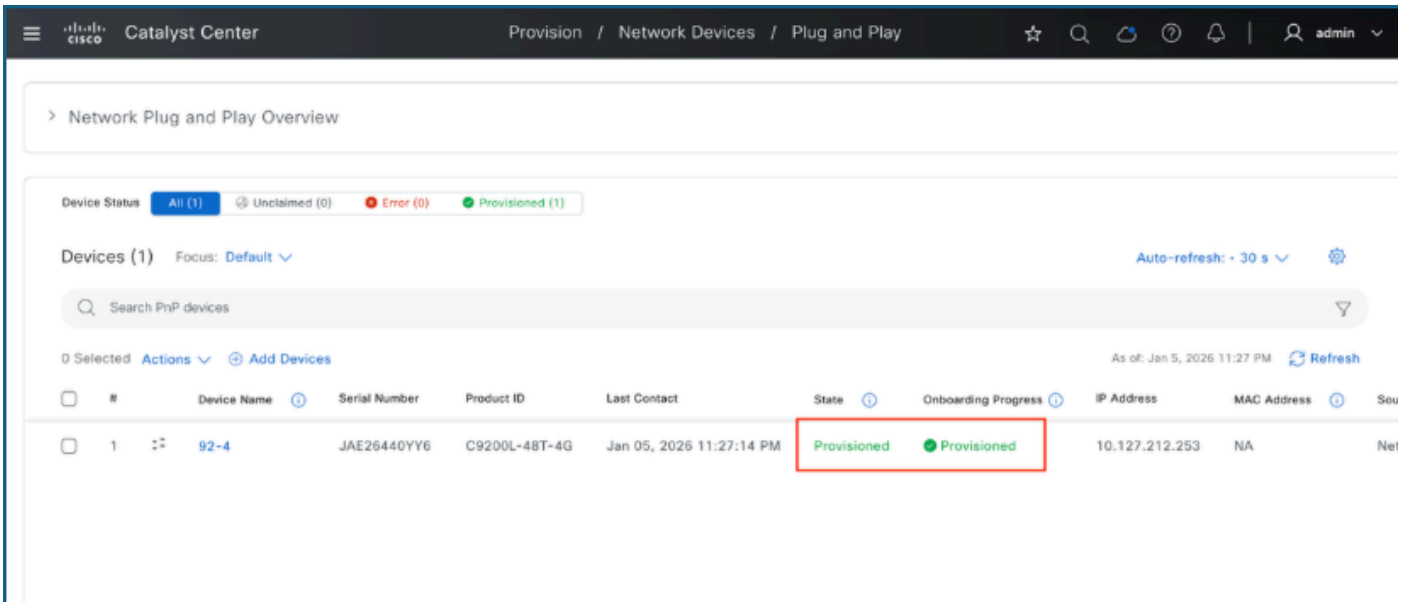


13.监测索赔进度

您将重定向到即插即用页面以跟踪设备进度。

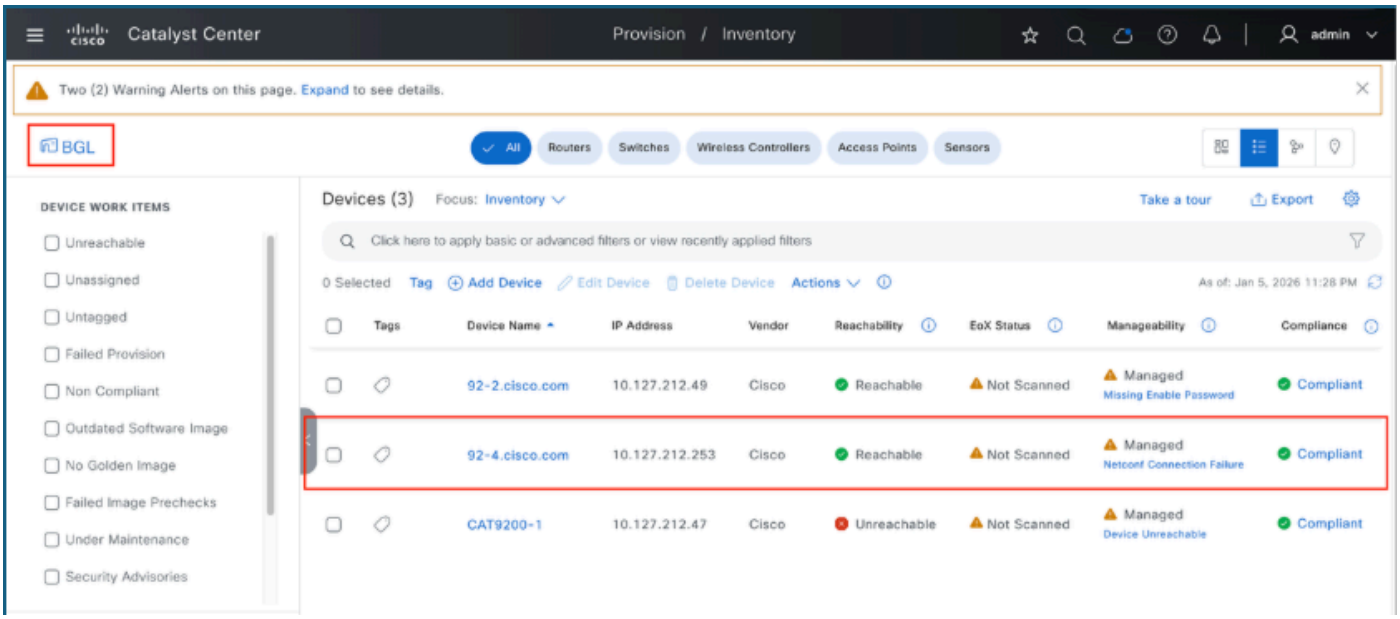
- Monitor Status：在申请流程进行过程中观察设备状态。
- 确认完成：当状态更新为Provisioned时，交换机已成功申请并集成到Catalyst Center资产中。





确认

- 访问Provision Menu：打开主页的Provision选项卡。
- 查看资产：选择资产选项。
- 验证状态：检查列表以确认交换机已成功调配。



将设备批量导入到Catalyst Center即插即用设备库存

为了简化大型网络的部署，Catalyst Center支持提前批量导入设备试运行的方法。此过程包括上传设备标识符（如PID、序列号和可选站点或模板数据），使系统能够在设备通电和连接后立即自动加入设备。

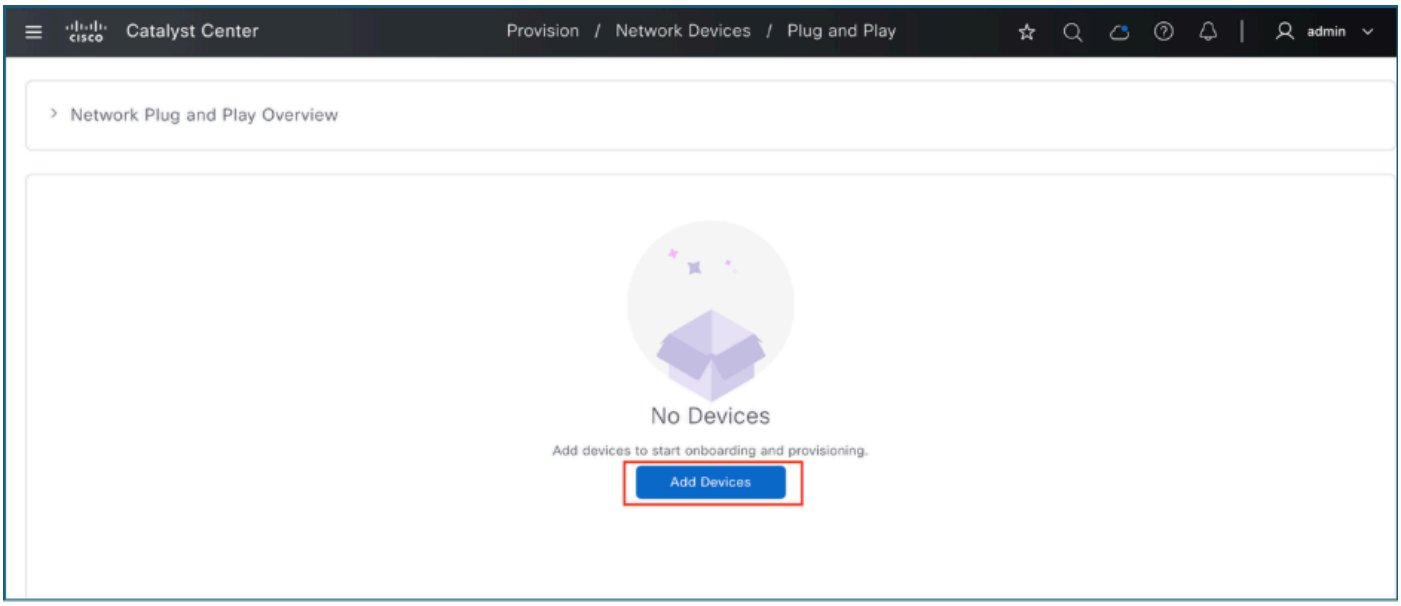
1.先决条件

为确保成功批量导入，必须满足以下要求：

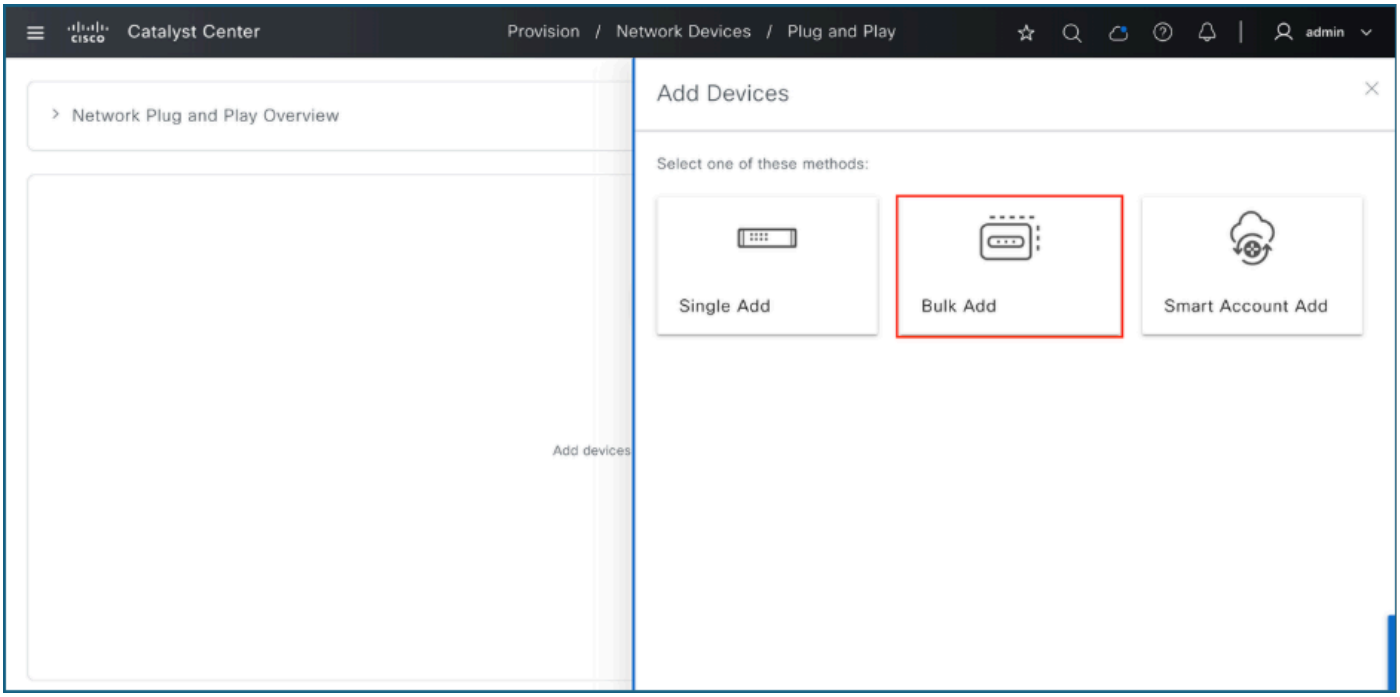
- Catalyst Center实例必须可访问且运行正常。
- 硬件必须获得思科即插即用服务的正式支持。
- 必须能够访问设备序列号和PID。
- 必须在Catalyst Center环境中预配置目标站点层次结构。

2.批量导入程序

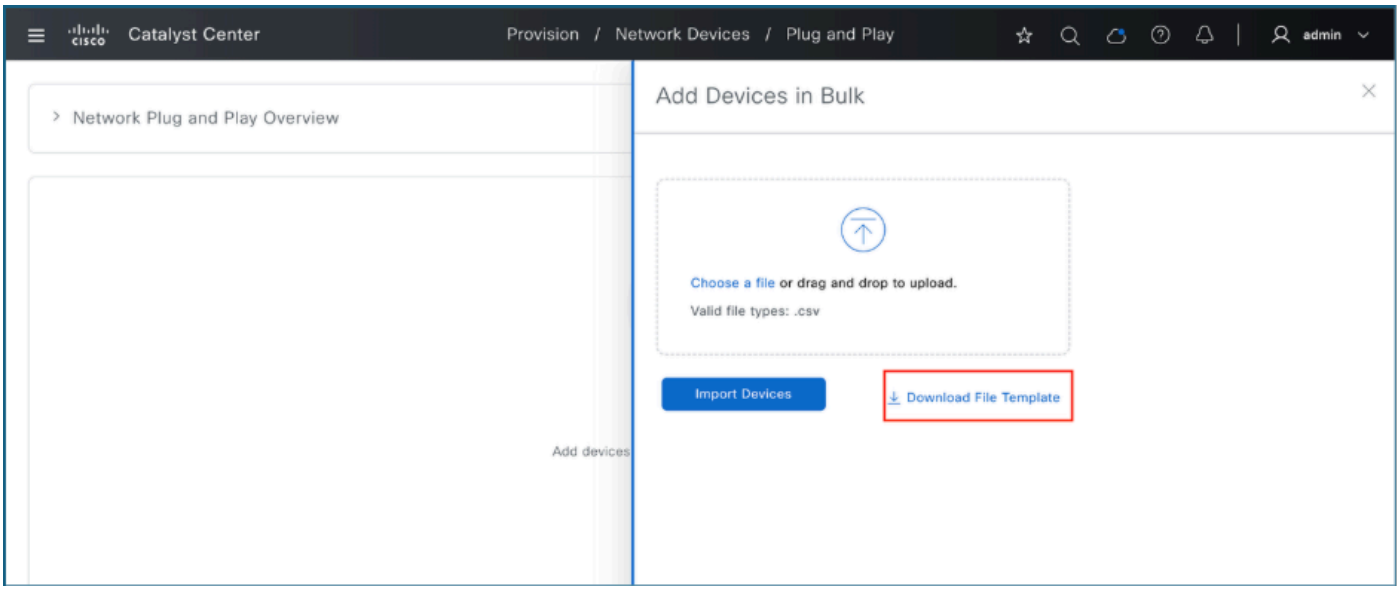
1. 登录到Catalyst Center
2. 导航至调配>即插即用
3. 点击添加设备



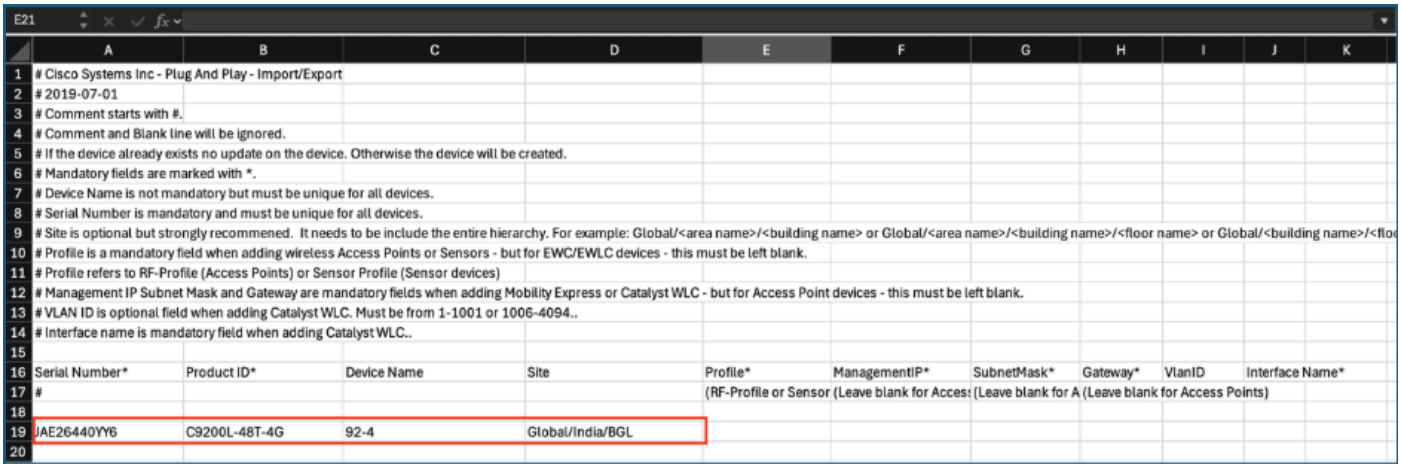
4.单击Bulk Add



5.单击Download File Template下载示例CSV文件

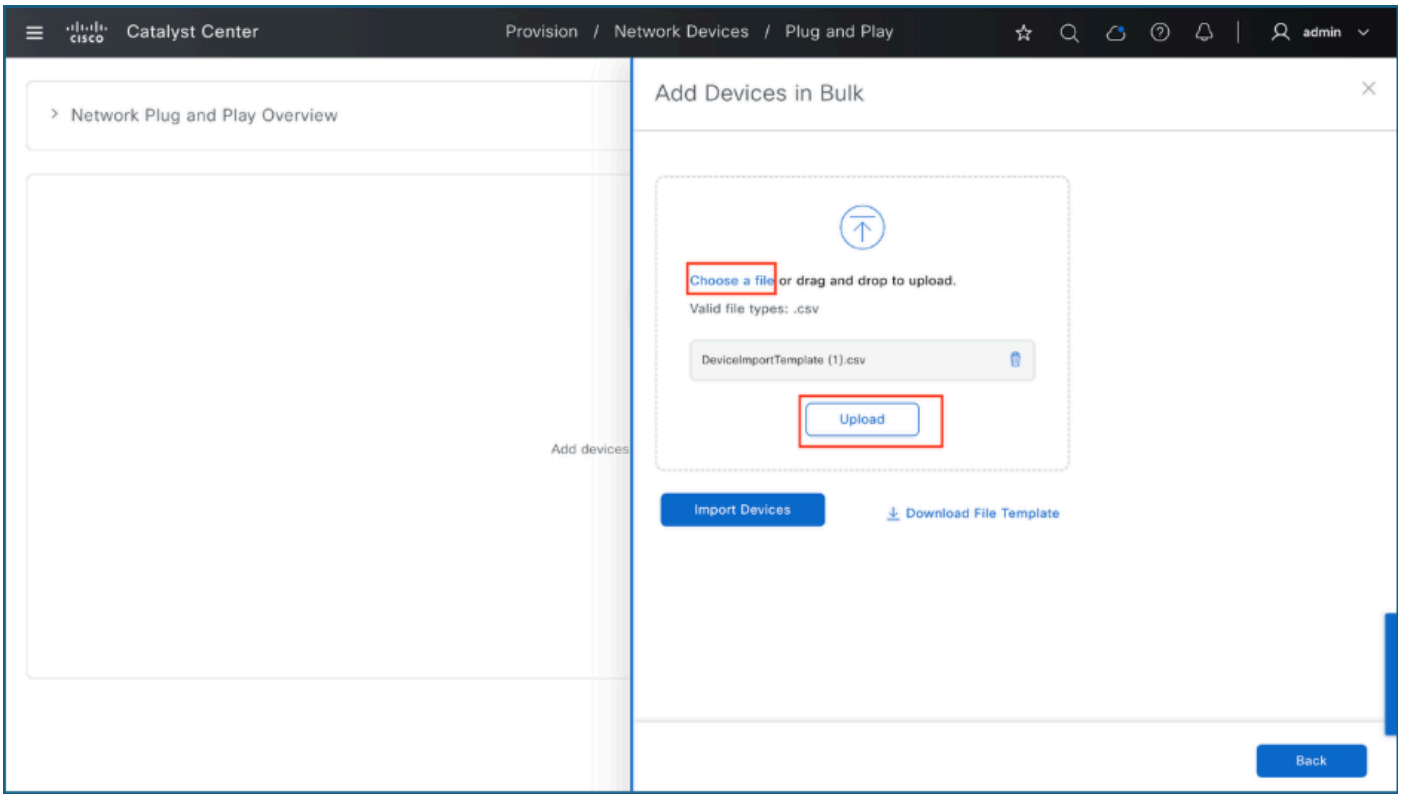


6.使用所需的设备详细信息填充CSV文件。

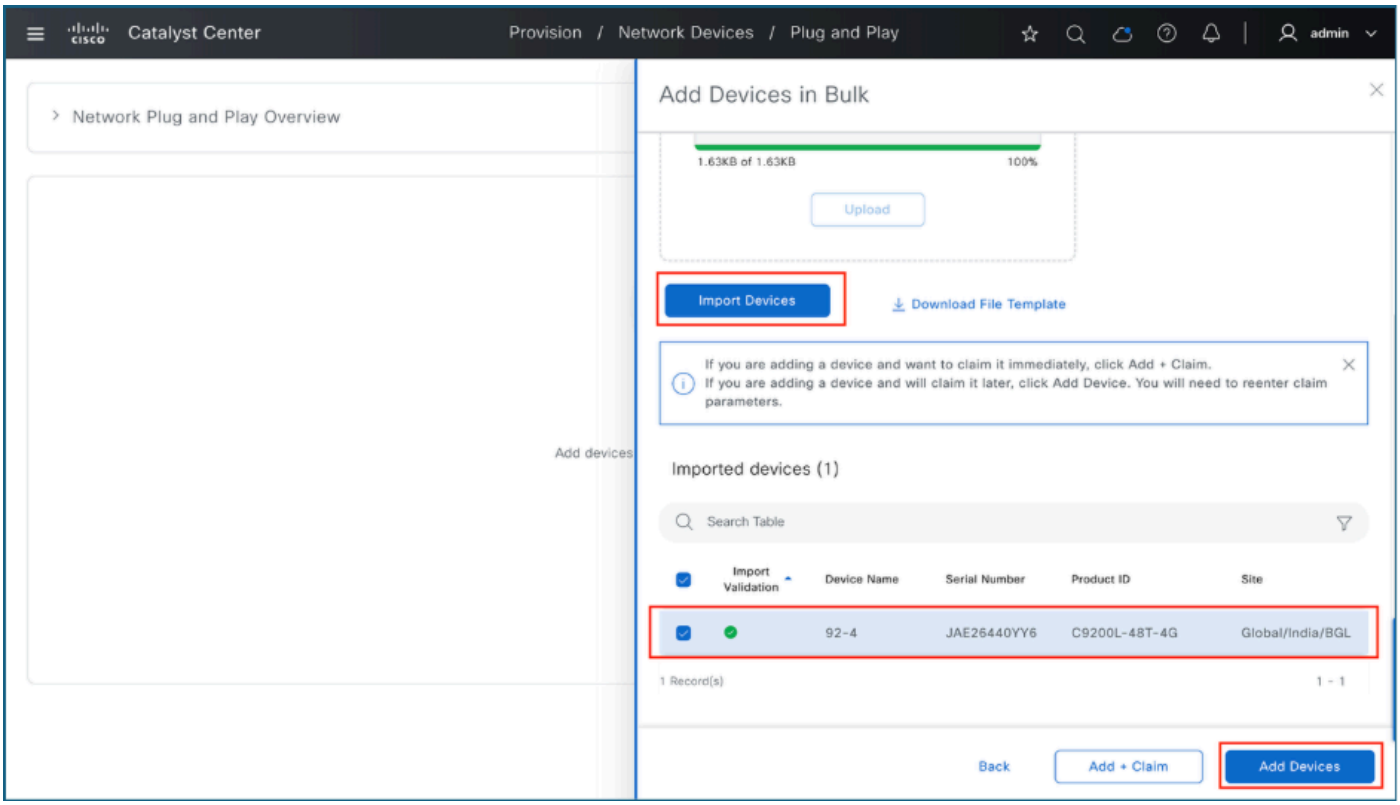


	A	B	C	D	E	F	G	H	I	J	K
1	# Cisco Systems Inc - Plug And Play - Import/Export										
2	# 2019-07-01										
3	# Comment starts with #.										
4	# Comment and Blank line will be ignored.										
5	# If the device already exists no update on the device. Otherwise the device will be created.										
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											

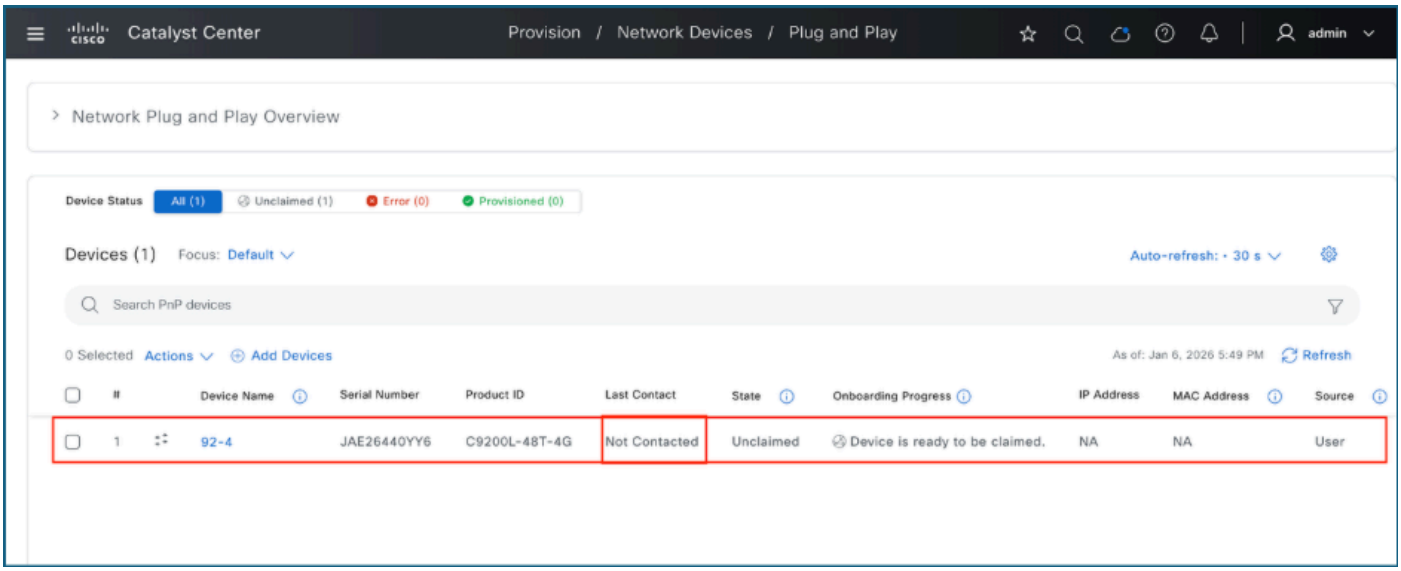
7.上传已完成的CSV文件。



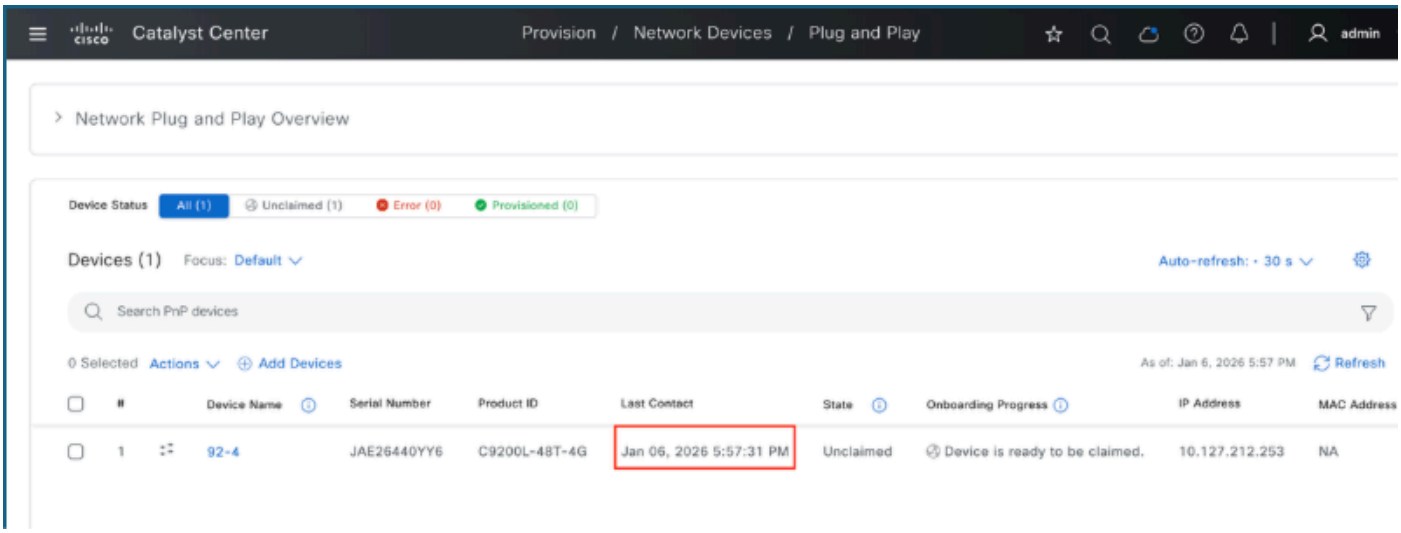
8.从CSV文件导入设备并将其添加到PnP清单



9.设备在资产中显示为“未联系”。



10.设备一旦与Catalyst Center联系，即可申请索赔。



故障排除

如果交换机未显示在Catalyst Center的“即插即用”页面上，以下是识别和解决该问题的步骤。

1. PnP连接验证

这些命令可验证与Catalyst Center的PnP连接。

1.1. ICMP可达性

通过ping Catalyst Center的企业接口IP或虚拟IP(VIP)地址验证ICMP连接。确保可通过ping到达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验证

如果Catalyst Center不响应HELLO验证请求，即插即用(PnP)将失败。要验证连接，请从设备终端或命令提示符运行此命令：curl -v http://<Catalyst Center IP>/pnp/HELLO

确认已收到“HELLO”响应。

```
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证书检索

如果无法通过HTTPS手动检索Catalyst Center服务器的证书，则PnP功能将失败。要验证这一点，请使用以下命令：copy https://<catc-ip-address>/ca/pem mypem2

确认文件传输已完成，且没有错误。

```
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配置文件状态

如果交换机未显示在Catalyst Center的PnP页面上，请通过执行命令检查PnP HTTP连接show pnp profile

- 验证PnP是否使用正确的Active-URL。

- 确认HTTP统计信息中的“失败计数器”为0。大于0的值表示交换机和Catalyst Center之间的可达性问题。 此图说明了涉及连通性问题的场景。

```
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#
```

此示例说明了一个没有可达性问题的场景。

```
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验证

这些命令有助于验证DHCP配置和连接。

2.1.检验DHCP IP地址分配

执行命令show ip interface brief，以验证PnP VLAN SVI是否已成功从DHCP服务器接收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.确认租用服务器

执行命令show dhcp leaseto验证DHCP租用服务器信息。

```
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.使用调试日志验证选项43

要验证选项43，请使用debug dhcp detail命令启用DHCP调试。启用调试后，请对接口执行shutdown和no shutdown以重新启动DHCP进程。在日志中，找到“DHCP:扫描：供应商特定选项43:"。复制此部分所示的十六进制字符串，使用适当的十六进制到ASCII转换器将其转换为文本，并验证生成的字符串是否正确指向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
```

最佳实践

- 确保交换机处于其出厂默认状态。如果之前调配过交换机，请使用pnpa service reset命令将其重置。
- 避免通过控制台中断PnP进程。

- 在部署之前验证证书和DNS解析。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。