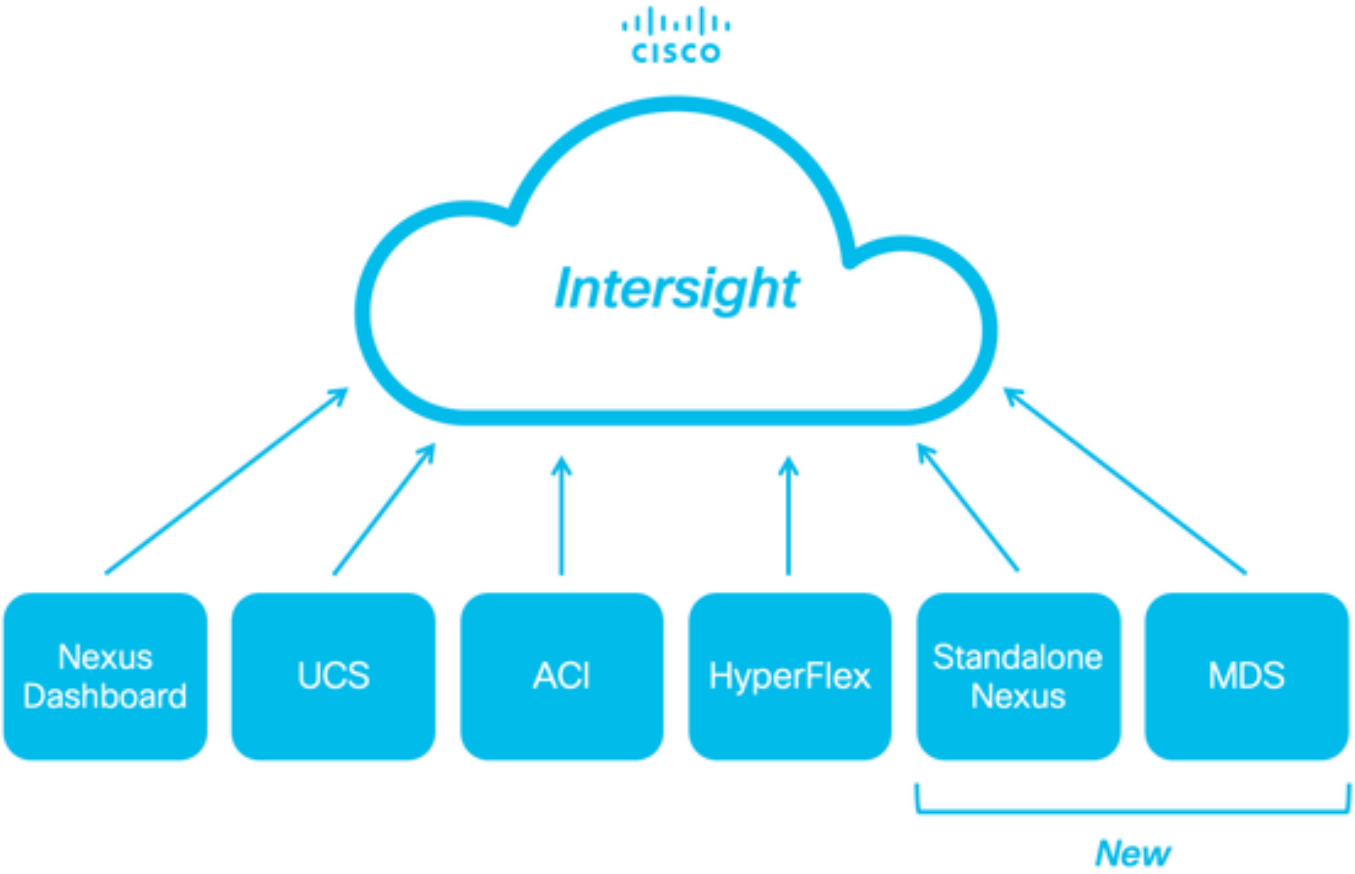
配置并声明独立Nexus用于Intersight连接

目录

简介

本文档介绍在Intersight中启用和声明独立Nexus交换机以获得增强的Cisco TAC支持所需的步骤。



先决条件

您必须在Intersight.com上拥有帐户，Cisco NX-OS®申请无需许可证。如果需要创建新的Intersight帐户，请参阅帐户创建。

要求

Cisco 建议您了解以下主题：

在独立Nexus交换机上，NXDC具有以下准则和限制：

- Cisco NX-OS必须运行版本10.2(3)F或更高版本
- 必须在正确的虚拟路由和转发(VRF)下配置DNS
- svc.intersight.com 必须解析并允许端口443上的出站发起HTTPS连接。可以通过openssl和**curl**进行查看这个值。Internet控制消息协议(ICMP)请求会被忽略。

    - 如果HTTPS连接需要代理svc.intersight.com，可在Nexus交换机设备连接器(NXDC)配置中配置代理。有关代理配置，请参阅配置NXDC。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Nexus N9K-C93240YC-FX2

- 思科NX-OS 10.3(4a)M

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco Intersight是一个云操作平台，由高级基础设施、工作负载优化和Kubernetes服务的可选模块化功能组成。有关详细信息，请访问Intersight概述。

设备通过嵌入在每个系统的Cisco NX-OS映像中的NXDC连接到Intersight门户。从Cisco NX-OS版本10.2(3)F开始，支持设备连接器功能，为连接的设备提供安全的方式，使用安全的互联网连接从Cisco Intersight门户发送信息和接收控制指令。

连接优势

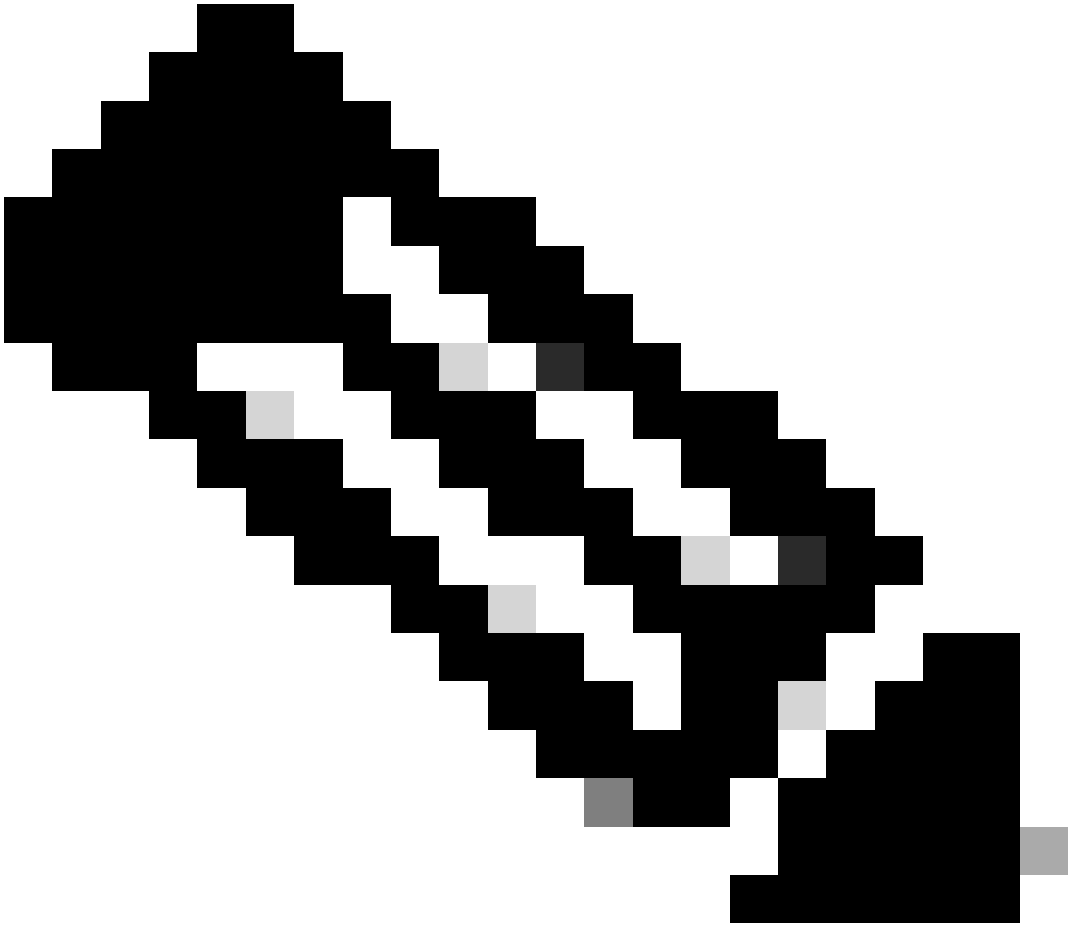
Intersight连接为基于Cisco NX-OS的平台提供以下功能和优势：

- 通过快速问题解决自动收集show tech-support details(RPR for the TAC Service Requests open)
- 远程按需收集 show tech-support details
- 未来的功能包括：
    - 根据遥测或硬件故障打开主动TAC服务请求
    - 单个show命令的远程按需收集及其他

快速入门视频

手动申请NXOS设备

连接验证



注意：抑制Ping响应（丢弃ICMP数据包）。

要检查传输层安全(TLS)和HTTPS连接，建议在所需VRF (ip netns exec <VRF>)中启用bash并执行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

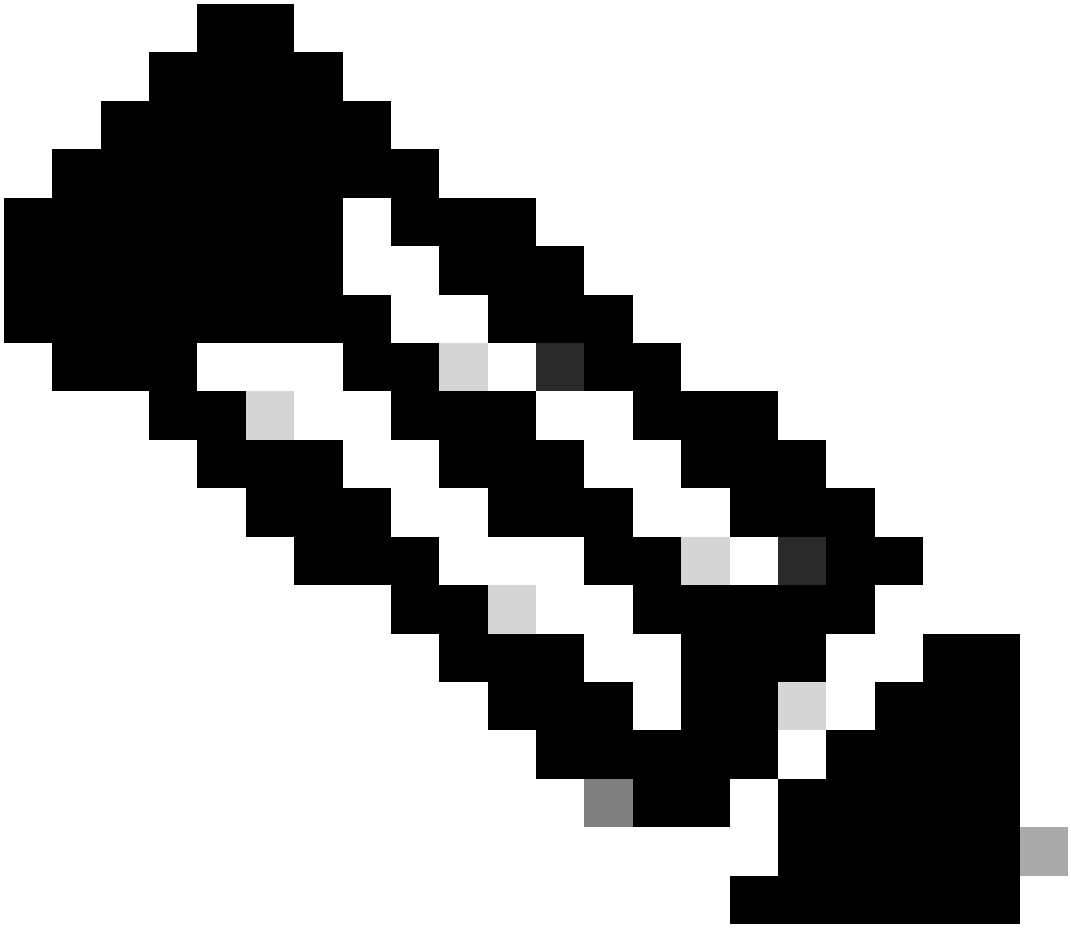
! Verify https

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客户端进行TLS验证

使用OpenSSL，您可以检查与svc.intersight.com:443的TLS连接。成功后，检索服务器的公共签名证书并显示证书颁发机构链。

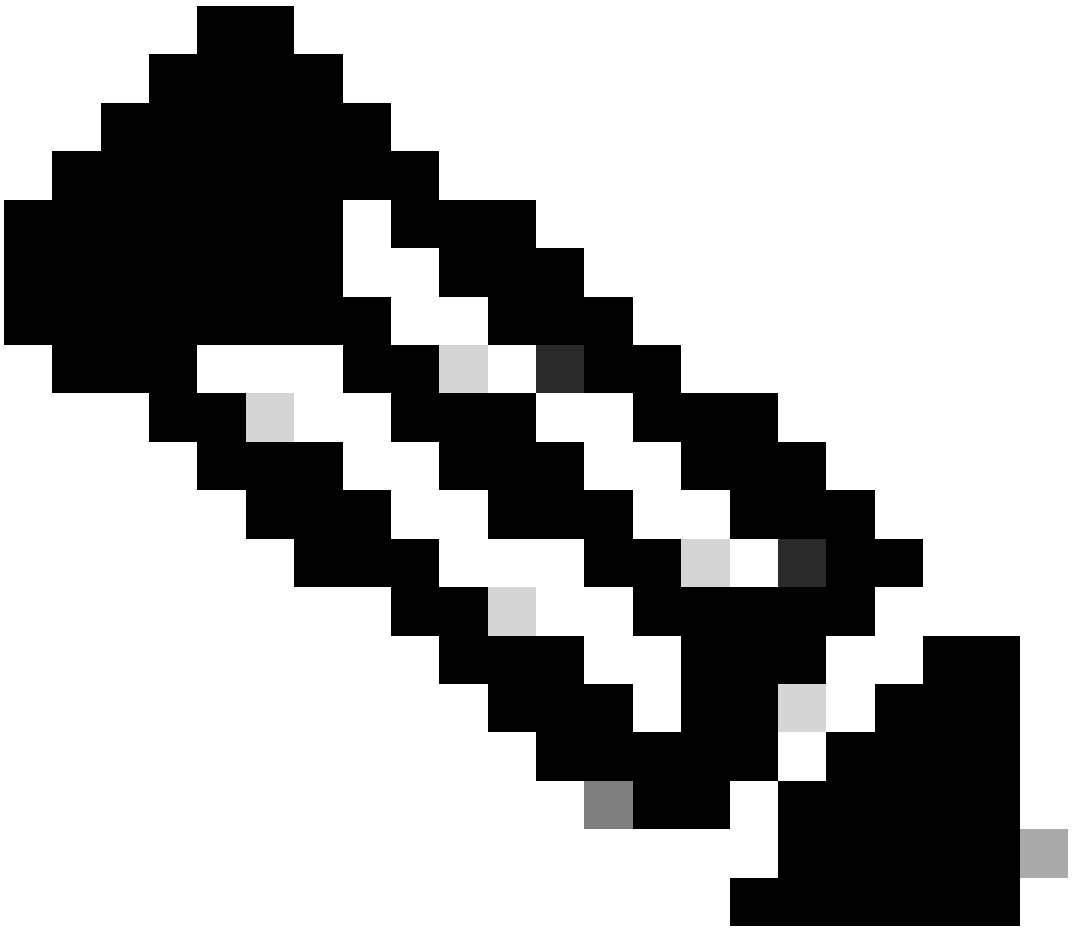


注意：下一个示例在VRF管理中执行openssl s_client命令。 替换ip netns exec <VRF>结构中所需的。

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

HTTPS可达性验证

要检查HTTPS连接，请将**curl**命令与-v verbose flag（显示是否使用代理）一起使用。



注意：为了检查启用或禁用代理的影响，您可以添加选项--proxy [protocol://]host[:port]或--noproxy [protocol://]host[:port]。

结构ip netns exec <VRF>用于在所需的VRF中执行curl；例如，ip netns exec management用于VRF管理。

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.esl.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 >

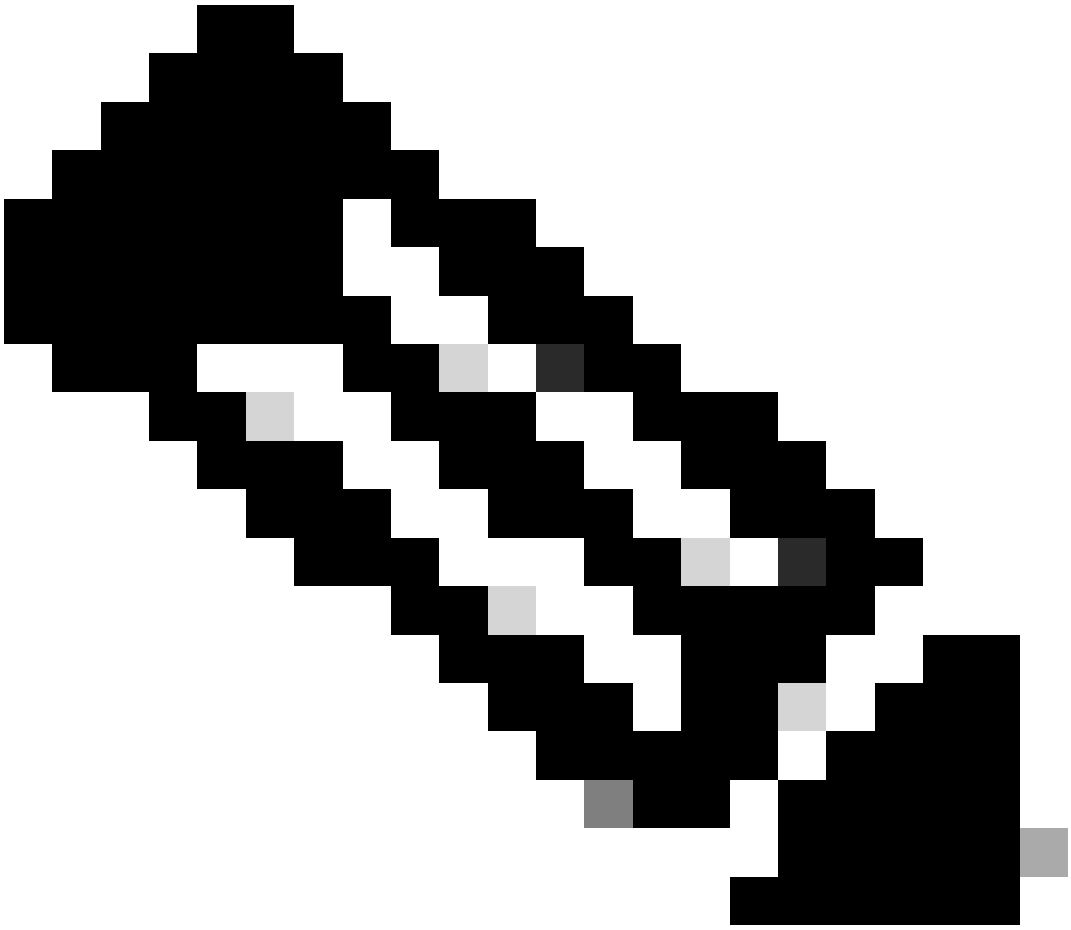
配置

声明设备在 intersight.com

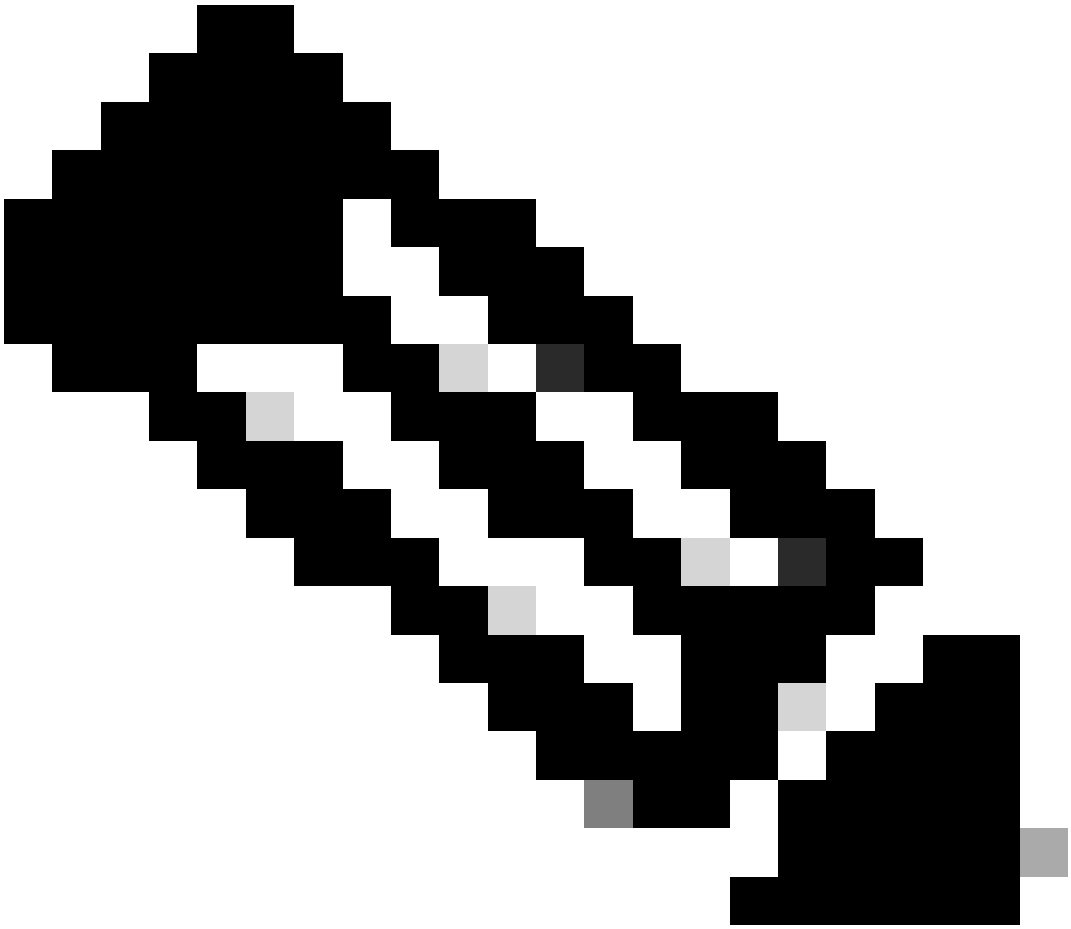
要在Intersight中声明一个新目标，请完成上述步骤。

在Nexus设备上

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



注意：对于NX-OS 10.3(4a)之前的版本，请使用“show intersight claim-info”命令



注意：Nexus生成的声明信息映射到以下Intersight声明字段：

序列号= Intersight领款申请**ID**

Device-ID Security Token = Intersight **Claim Code**

```
# show system device-connector claim-info
SerialNumber: FDO23021ZUJ
SecurityToken: 9FFD4FA94DCD
Duration: 599
Message:
Claim state: Not Claimed
```

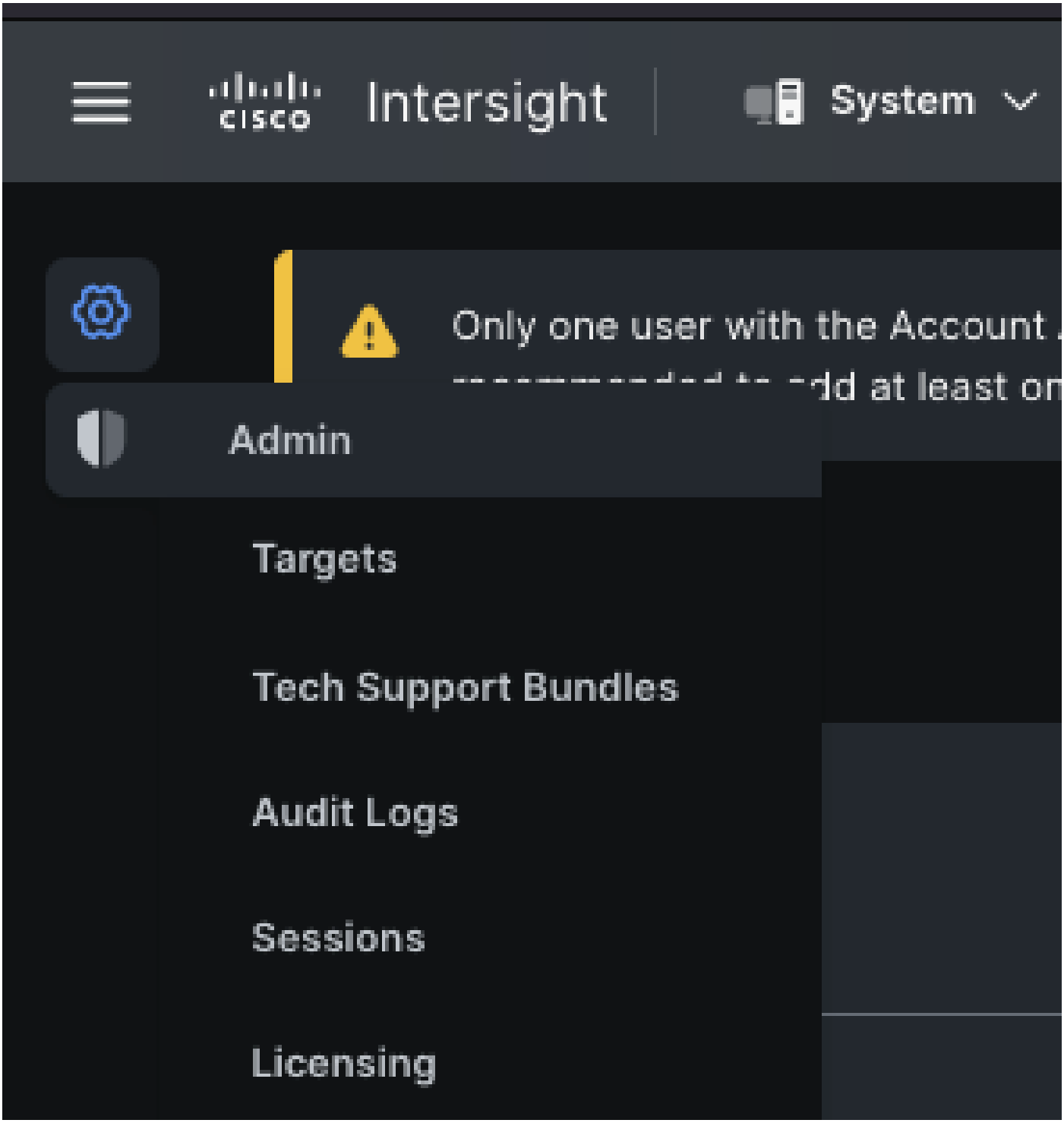
此处报告的持续时间以秒为单位。

在Intersight门户上

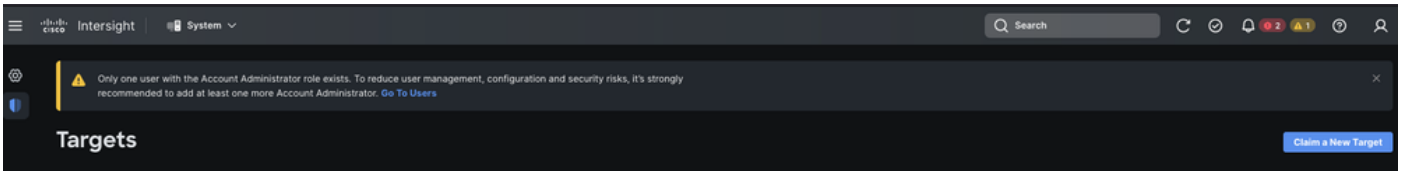
1. 在10分钟内使用帐户管理员、设备管理员或设备技术人员权限登录**Intersight**。

2. 从**Service Selector**下拉列表中选择**System**。

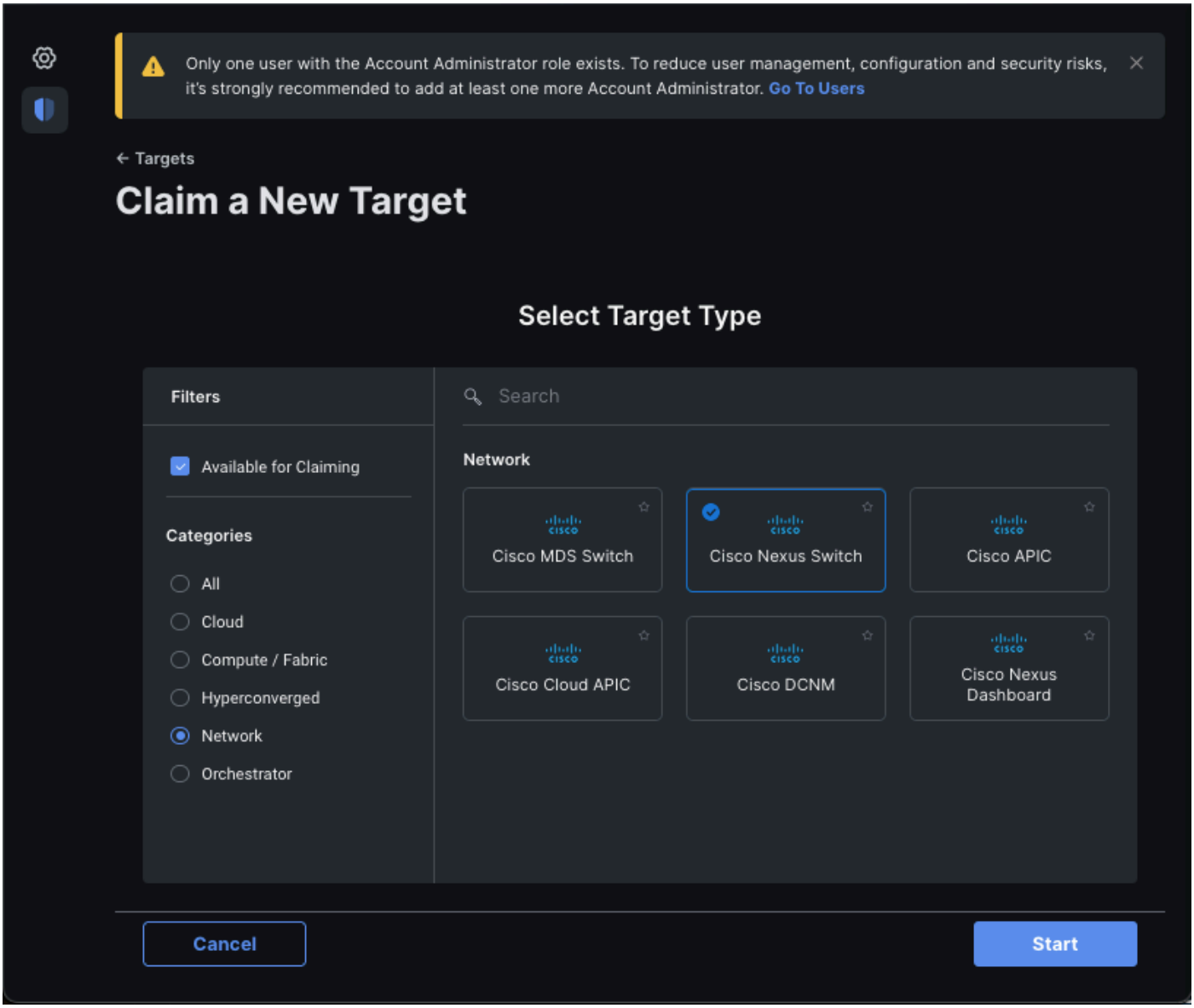
3. 定位至ADMIN > Targets > Claim a New Target。



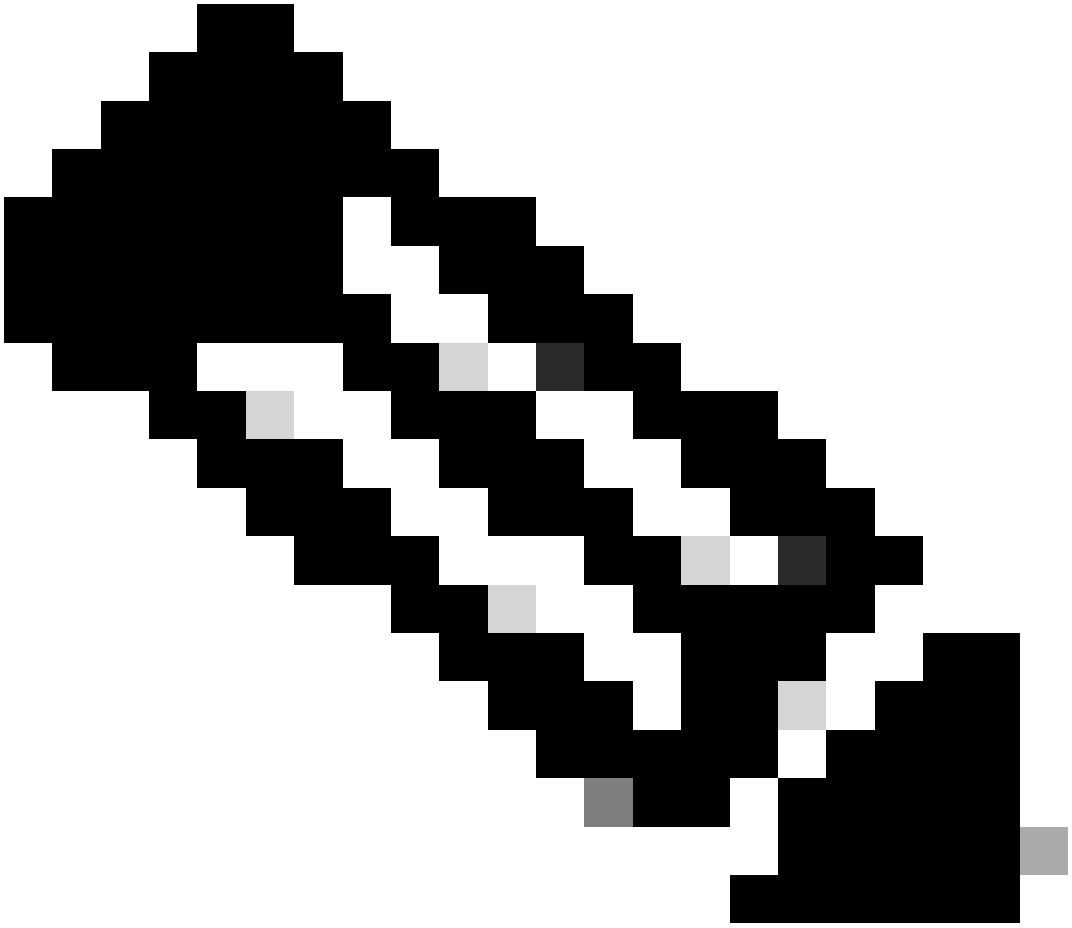
3.1.单击**Claim a New Target**，如图所示。



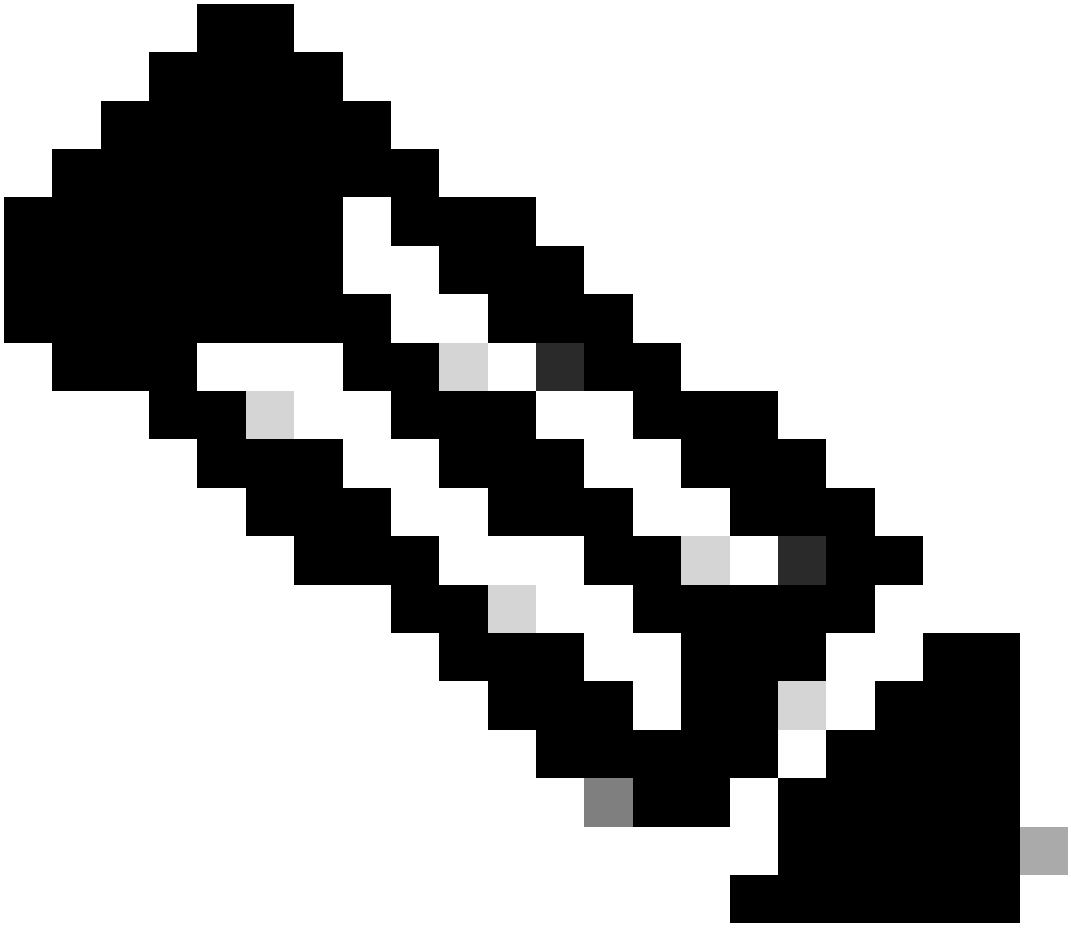
4. 选择**可用于申请**，然后选择您要申请的**目**标类型（例如，网络）。单击开始。



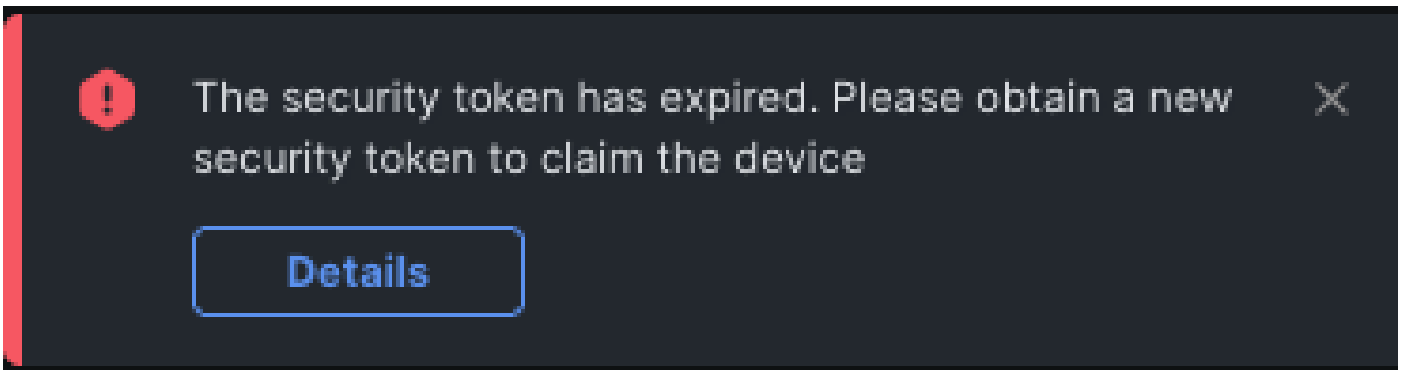
5. 输入所需的详细信息并单击**Claim** 以完成申请流程。



注意：交换机上的**安全令牌**用作声明代码，交换机的**序列号**为设备ID。



注意：安全令牌过期。您必须在之前完成领款申请，否则系统会提示您重新生成领款申请。

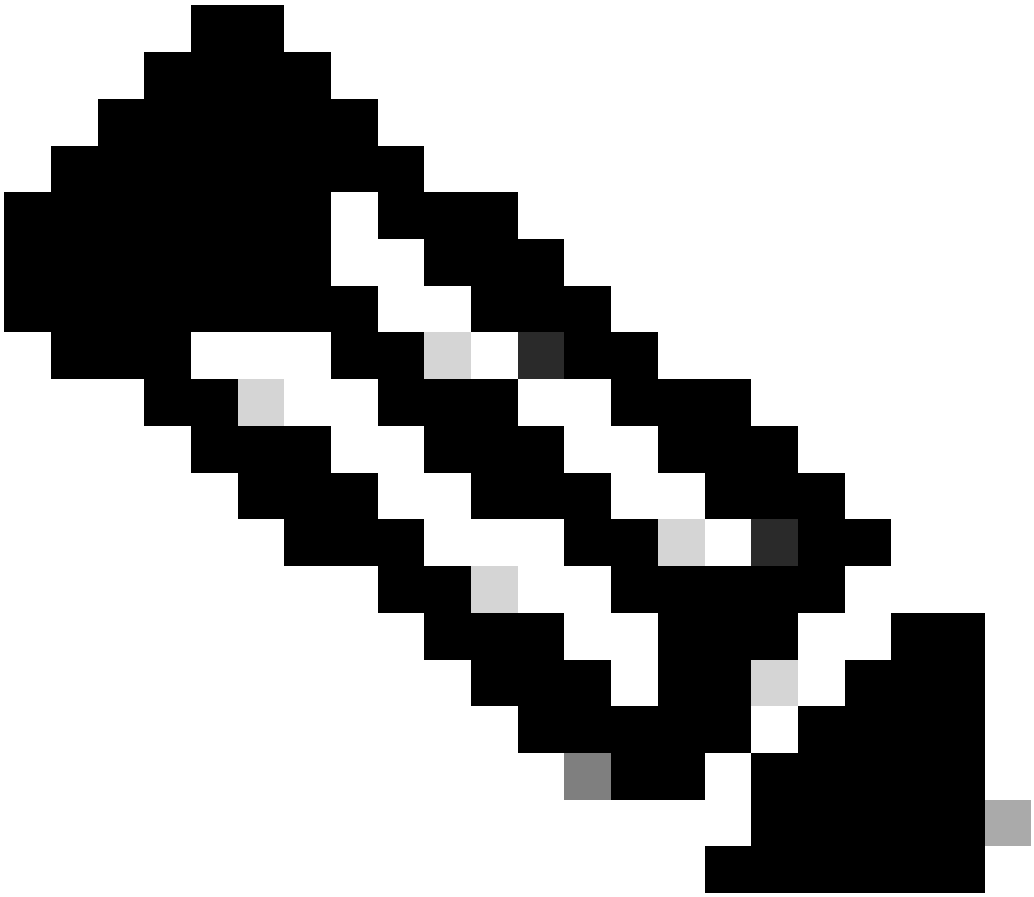


使用Ansible在intersight.com中声明一到多个独立Nexus设备®

为了逐一声明Nexus设备，可以运行Ansible手册。

- ansible资产和攻略可以从https://github.com/datacenter/ansible-intersight-nxos克隆。
- 在Ansibleinventory.yaml中，ansible_connection类型设置为ansible.netcommon.network_cli，以便向Nexus交换机发送命令。可以将其更改为ansible.netcommon.httpapi，以便允许通过NXAPI进行连接。
- 与Intersight终结点的Ansible连接需要API密钥，可通过您的**intersight.com**帐户生成。

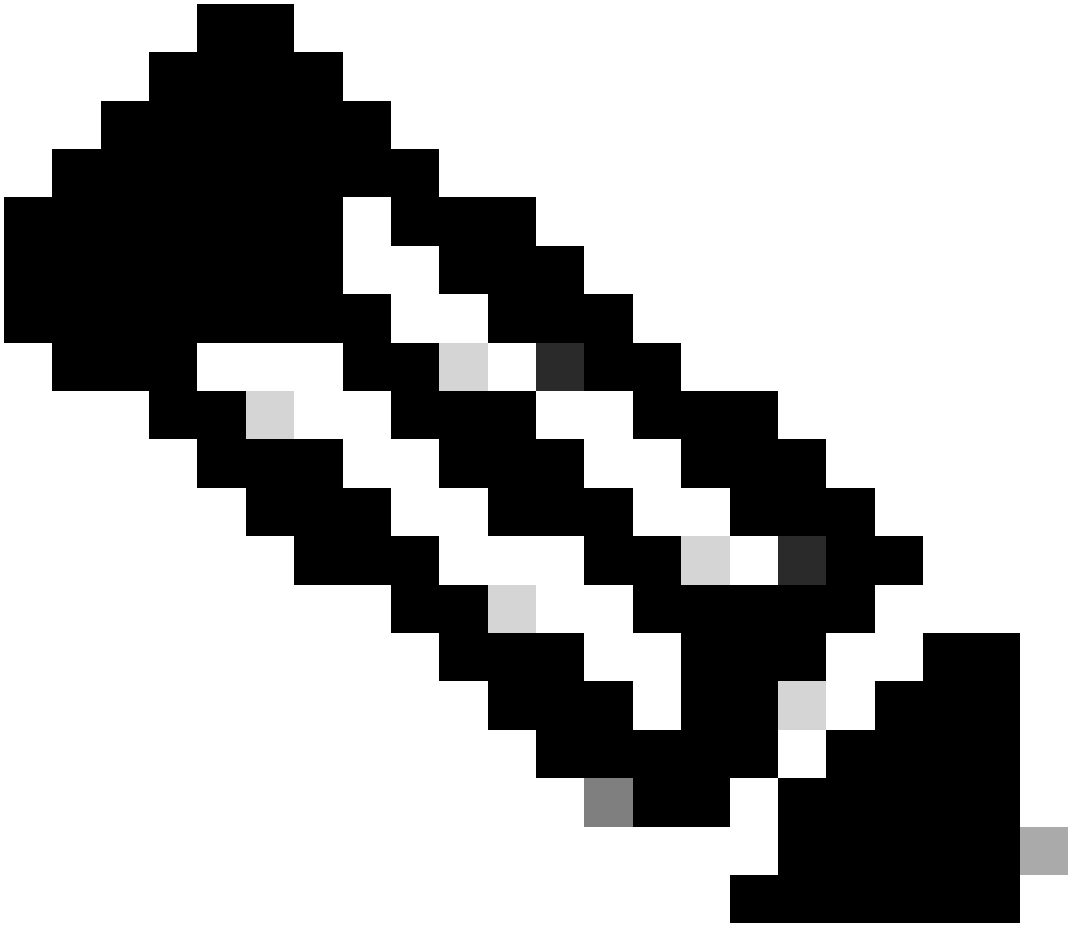
配置Nexus NXAPI(仅在使用ansible.netcommon.httpapi时使用)



注意：如果配置了系统级代理(**HTTP(S)_PROXY**)，并且Ansible不能使用代理连接Nexus NXAPI终端，则需要设置 ansible_httpapi_use_proxy: False（默认为True）。

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

为了独立验证到NXAPI终端的HTTP连接，您可以尝试发送show clock。在下一个示例中，交换机使用基本身份验证对客户端进行身份验证。也可以配置NXAPI服务器以根据X.509用户证书对客户端进行身份验证。



注意：基本身份验证哈希是从**username：password的**base64编码中获取的。在本示例中，**admin：cisco！123** base64编码为YWRtaW46Y2lzY28hMTIz。

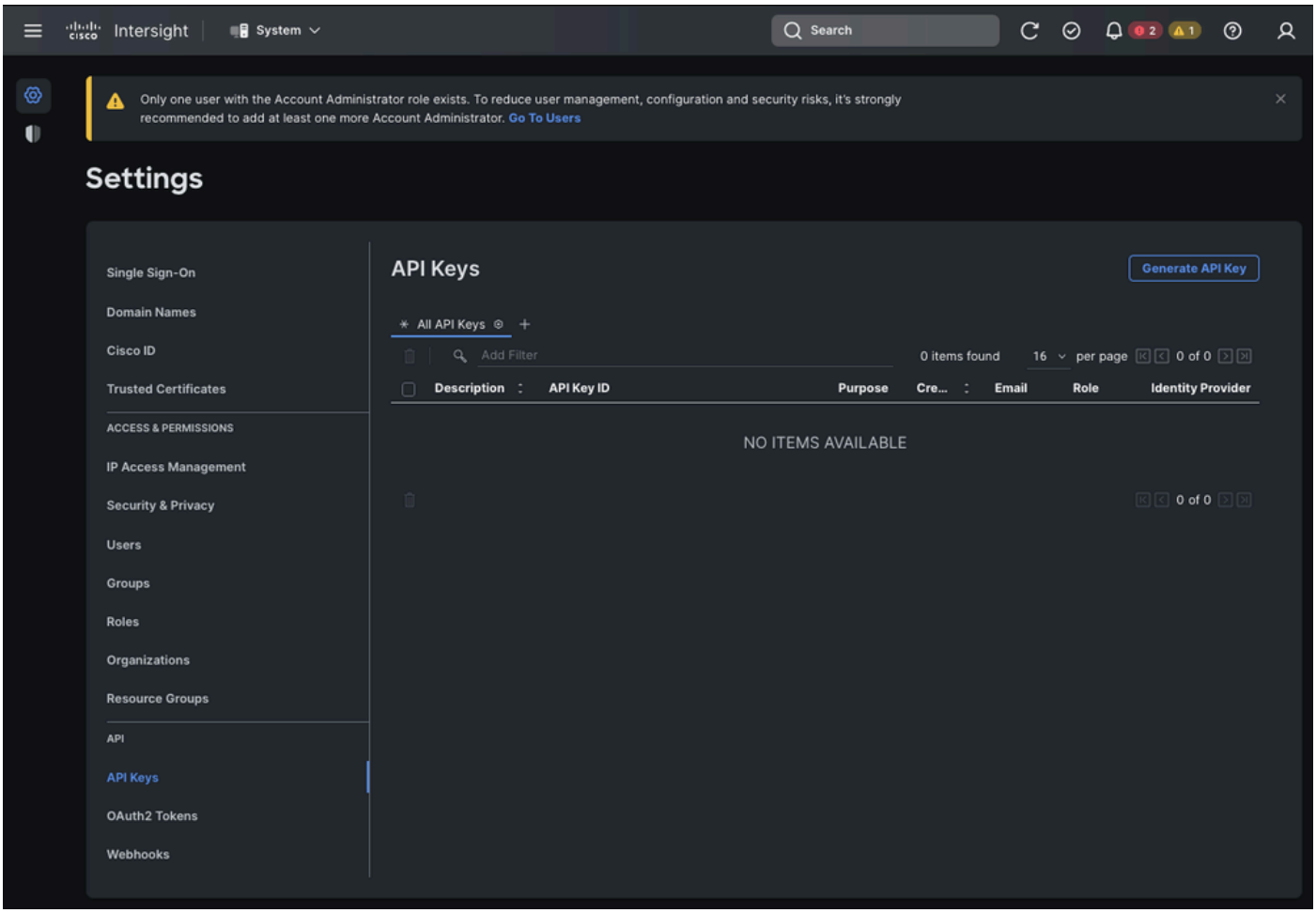
```
curl -v --noproxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

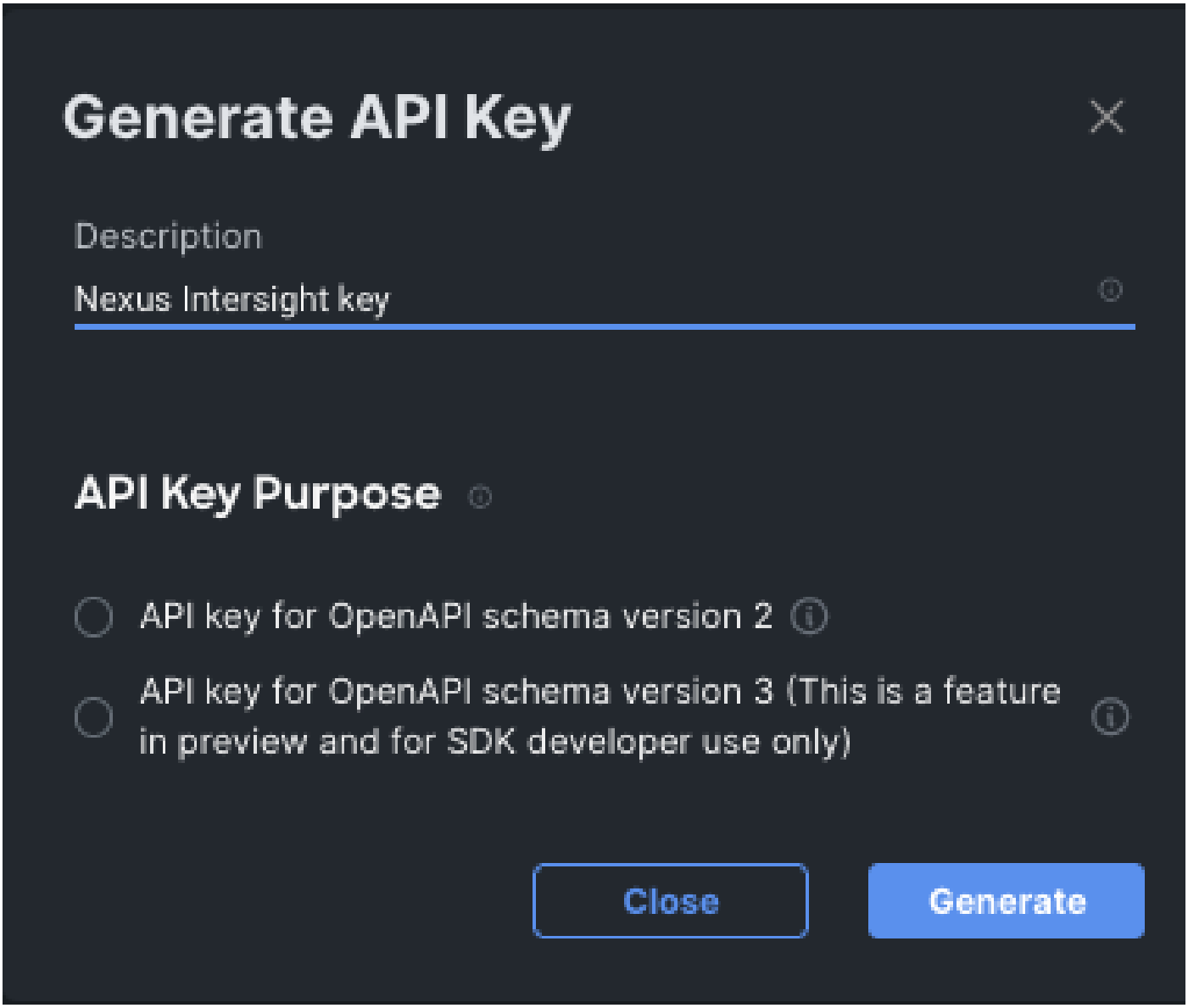
卷曲响应：

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

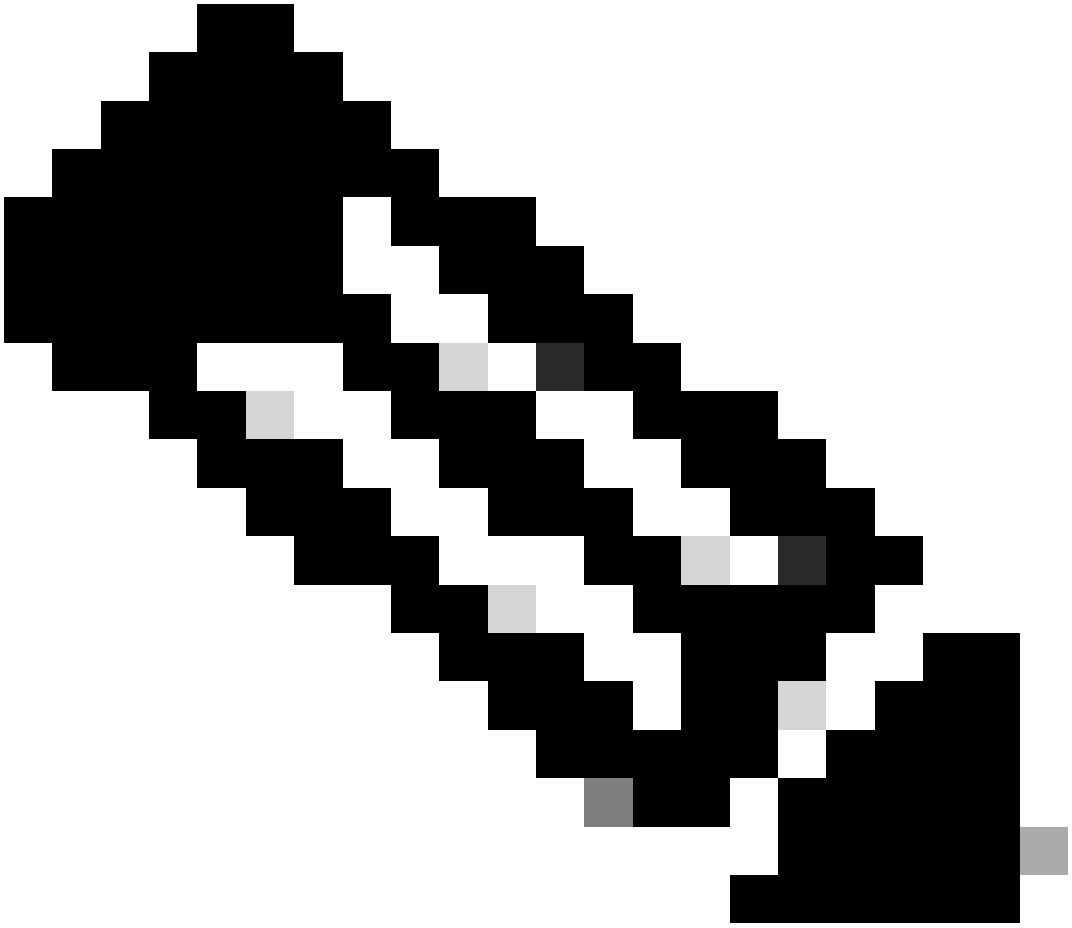
生成Intersight API密钥

有关如何从Intersight System > Settings > API keys > Generate API Key获取API密钥，请参阅README.md部分。

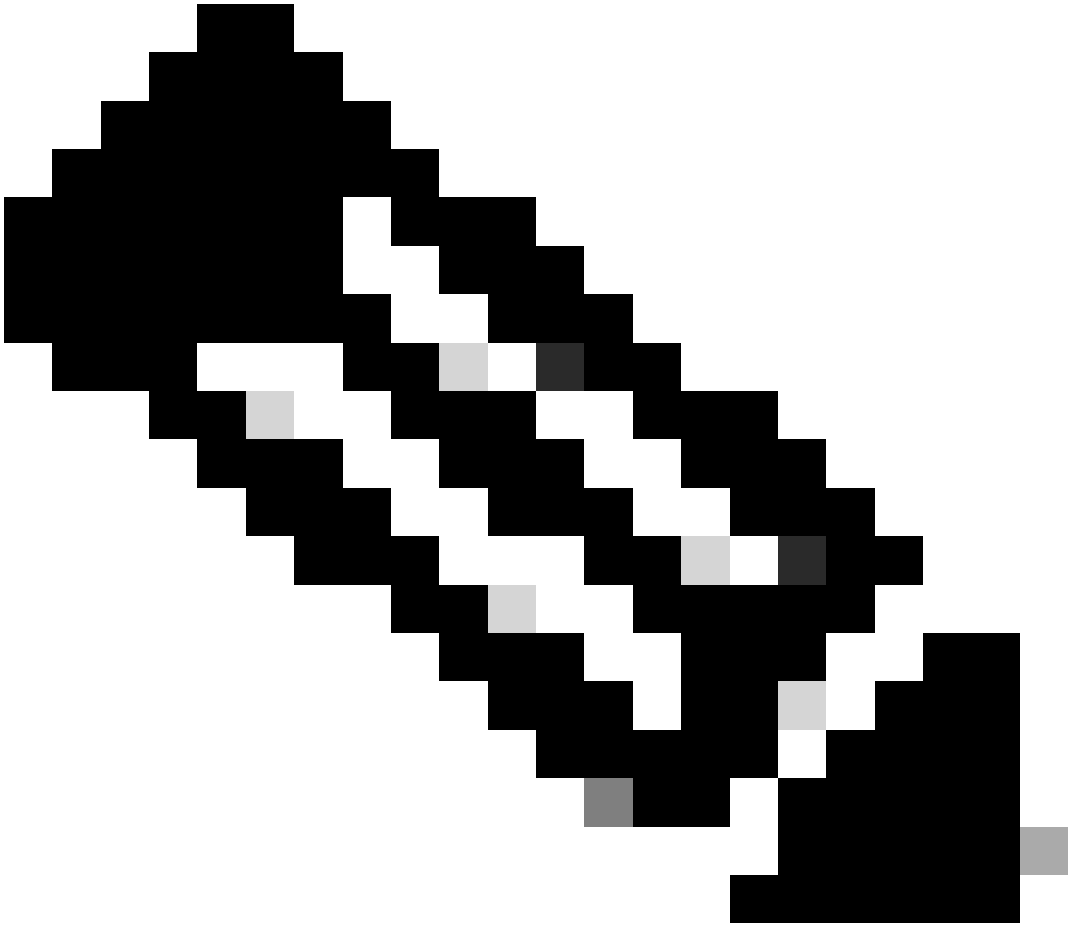




示例：Ansible inventory.yaml



注意：在下一个示例中，配置了ansible以便使用ansible_httpapi_use_proxy: False忽略操作系统代理设置。如果您需要Ansible服务器使用代理才能访问交换机，则可以删除该配置或将其设置为True（默认值）。



注意：API密钥ID是一个字符串。API私钥包括包含私钥的文件的完整路径。对于生产环境，建议使用Ansible保管库。

```
---
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: "5fcb99d97564612d33fdfcal/5fcb99d97564612d33fdf1b2/65c6c09d756461330198ce7e"
      api_private_key: "/home/admin/ansible-intersight-nxos/my_intersight_private_key.txt"
...
```

示例：playbook.yaml执行

有关使用Ansible对独立Nexus设备进行编程的详细信息，请参阅您当前版本的Cisco Nexus 9000系列NX-OS可编程性指南的Applications/Using Ansible使用Cisco NX-OS部分。

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

验证

要验证新目标的声明，请完成以下操作：

在Nexus交换机上

10.3(4a)M之前的版本

#运行bash sudo cat /mnt/pss/connector.db

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

以10.3(4a)M开头的版本

show system device-connector claim-info

```
N9k-Leaf-2# show system device-connector claim-info SerialNumber: FDO23021ZUJ SecurityToken: Duration:
```

show system internal intersight info

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

Ansible

可以在playbook.yaml末尾添加一个任务来获取交换机插入信息。

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

以下是相应的输出：

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

禁用设备连接器

	命令或操作	目的
第 1 步	no feature intersight 示例： `switch(config)# no feature intersight`	禁用intersight进程并删除所有NXDC配置和日志存储。

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）。