

Configure e reivindique o Nexus independente para a conectividade da Intersight

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Benefícios da conectividade](#)

[Vídeo Quickstart](#)

[Solicitar manualmente um dispositivo NXOS](#)

[Verificação de conectividade](#)

[Verificação TLS com OpenSSL Client](#)

[Verificação de acessibilidade de HTTPS](#)

[Configurar](#)

[Solicite o withinintersight.com do dispositivo](#)

[No dispositivo Nexus](#)

[No portal Intersight](#)

[Reivindique um para muitos dispositivos Nexus independentes em intersight.com usando Ansible@](#)

[Configurar Nexus NXAPI \(usado somente se estiver usando ansible.netcommon.httpapi\)](#)

[Gerar chaves de API de Intersight](#)

[Exemplo: Ansibleinventory.yaml](#)

[Exemplo:playbook.yamlExecution](#)

[Verificar](#)

[No switch Nexus](#)

[Versões anteriores à versão 10.3\(4a\)M](#)

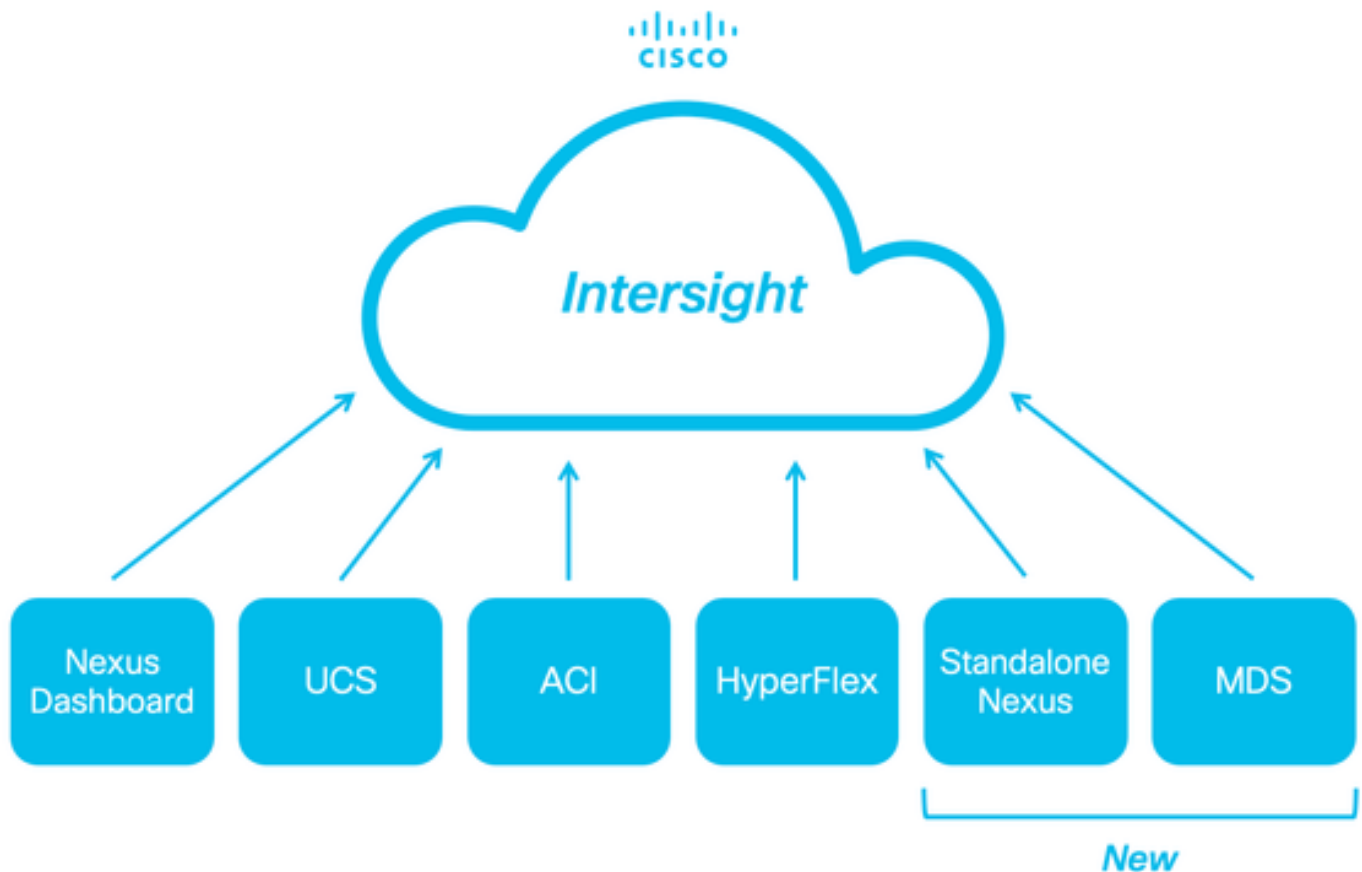
[Versões iniciando com 10.3\(4a\)M](#)

[Ansible](#)

[Desabilitar Conector do Dispositivo](#)

Introdução

Este documento descreve as etapas necessárias para ativar e reivindicar switches Nexus independentes na Intersight para suporte avançado do Cisco TAC.



Pré-requisitos

Você deve ter uma conta no intersight.com, não é necessária licença para a solicitação do Cisco NX-OS®. Se uma nova conta da Intersight precisar ser criada, consulte [Criação de Conta](#).

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

No switch Nexus independente, o NXDC tem estas diretrizes e limitações:

- O Cisco NX-OS deve estar executando a versão 10.2(3)F ou posterior
- [O DNS](#) deve ser configurado no Virtual Routing and Forwarding (VRF) apropriado
- `svc.intersight.com` deve ser resolvido e permitir conexões HTTPS iniciadas na porta 443. Isso pode ser verificado com `openssl` e `curl`.
As solicitações do Internet Control Message Protocol (ICMP) são ignoradas.
- Se um proxy for necessário para uma conexão HTTPS com o `svc.intersight.com`, o proxy poderá ser configurado na configuração do Nexus Switch Device Connector (NXDC). Para a configuração do proxy, consulte [Configuração do NXDC](#).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Intersight é uma plataforma de operações em nuvem que consiste em recursos modulares opcionais de infraestrutura avançada, otimização de carga de trabalho e serviços Kubernetes. Visite [Intersight Overview](#) para obter mais informações.

Os dispositivos são conectados ao portal Intersight por meio de um NXDC que é incorporado à imagem do Cisco NX-OS de cada sistema. Começando com o Cisco NX-OS versão 10.2(3)F, o recurso Conector do dispositivo é suportado, o que fornece uma maneira segura para que os dispositivos conectados enviem informações e recebam instruções de controle do portal Cisco Intersight, usando uma conexão segura com a Internet.

Benefícios da conectividade

A conectividade da Intersight fornece estes recursos e benefícios para as plataformas baseadas no Cisco NX-OS:

- Coleta automatizada de show tech-support details via [resolução rápida de problemas](#) (RPR para solicitações de serviço do TAC abertas)
- Coleta remota sob demanda show tech-support details
- Os recursos futuros incluem:
 - Abertura de TAC SRs proativos com base em telemetria ou falha de hardware
 - Coleta remota sob demanda de comandos show individuais e muito mais

Vídeo Quickstart

Solicitar manualmente um dispositivo NXOS

Verificação de conectividade



Observação: as respostas de ping são suprimidas (os pacotes ICMP são descartados).

Para verificar a conectividade do Transport Layer Security (TLS) e HTTPS, é recomendável ativar o bash e executar os comandos openssl e curl no VRF (ip netns exec <VRF>) desejado.

! Enable bash

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

! Verify TLS

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

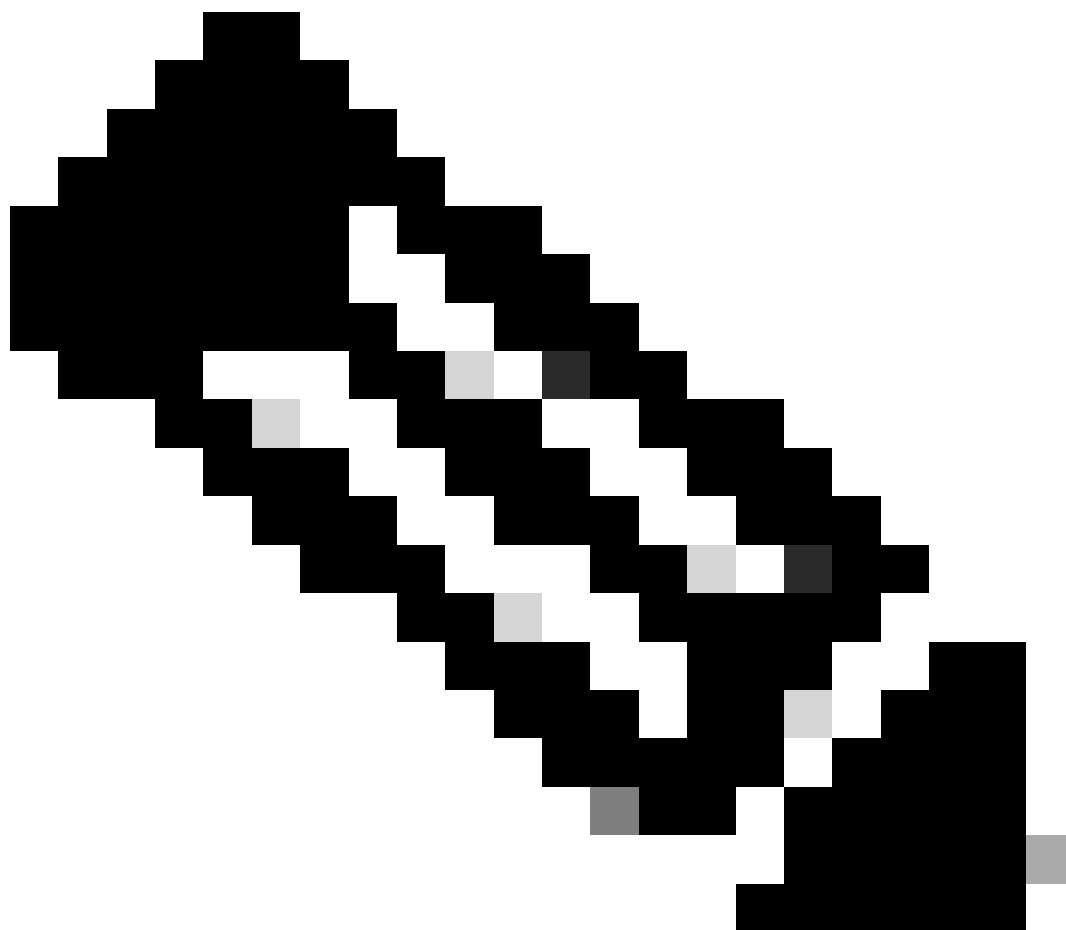
! Verify https

```
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]
```

Verificação TLS com OpenSSL Client

Usando o OpenSSL, você pode verificar a conectividade TLS com o `svc.intersight.com:443`. Quando obtiver êxito, recupere o certificado público assinado pelo servidor e exiba a cadeia da Autoridade de certificação.

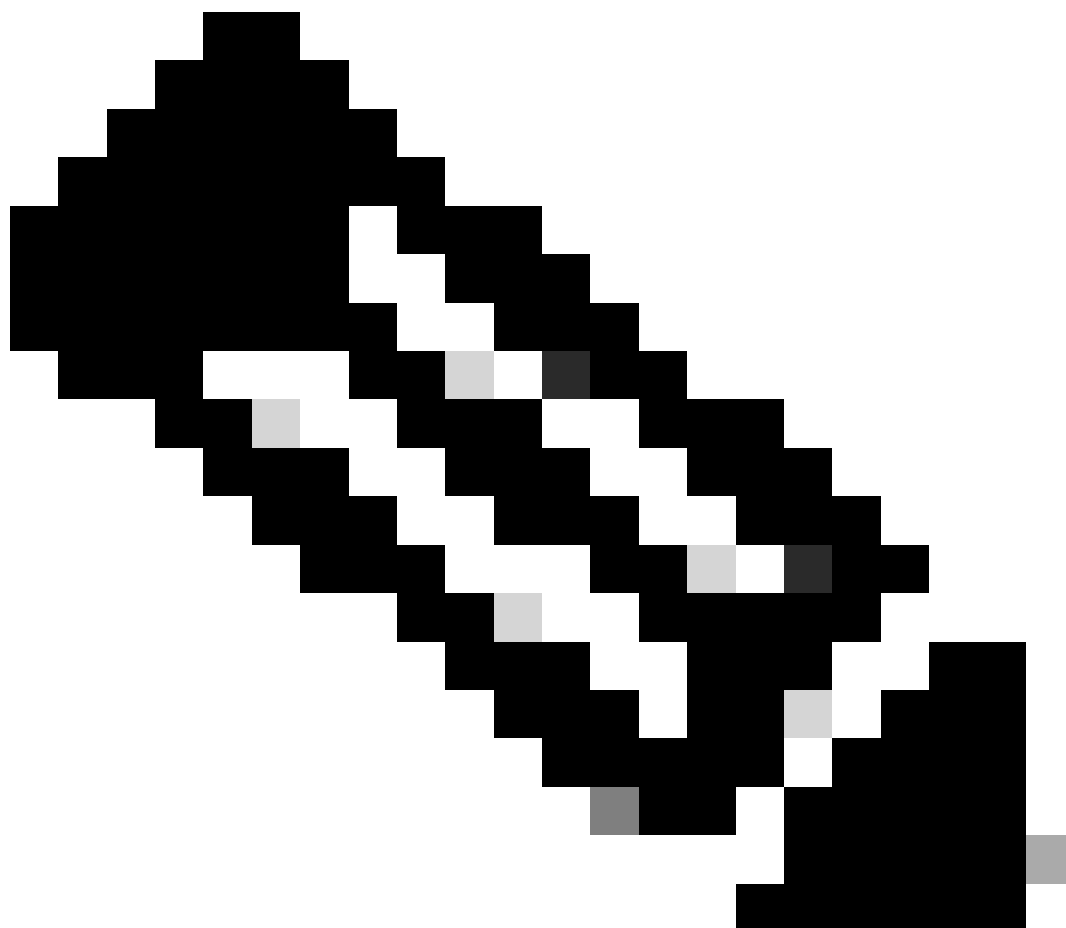


Observação: o próximo exemplo executa o comando `openssl s_client` no gerenciamento do VRF. Substitua o desejado na `ip netns exec <VRF> construção`.

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

Verificação de acessibilidade de HTTPS

Para verificar a conectividade HTTPS, use o comando **curl** com o -v verbose flag (exibe se um proxy é usado ou não).



Observação: para verificar o impacto de ativar ou desativar um proxy, você pode adicionar as opções --proxy [protocol://]host[:port] ou --noproxy [protocol://]host[:port].

A construção `ip netns exec <VRF>` é usada para executar `curl` no VRF desejado; por exemplo, `ip netns exec management` para o gerenciamento do 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 >

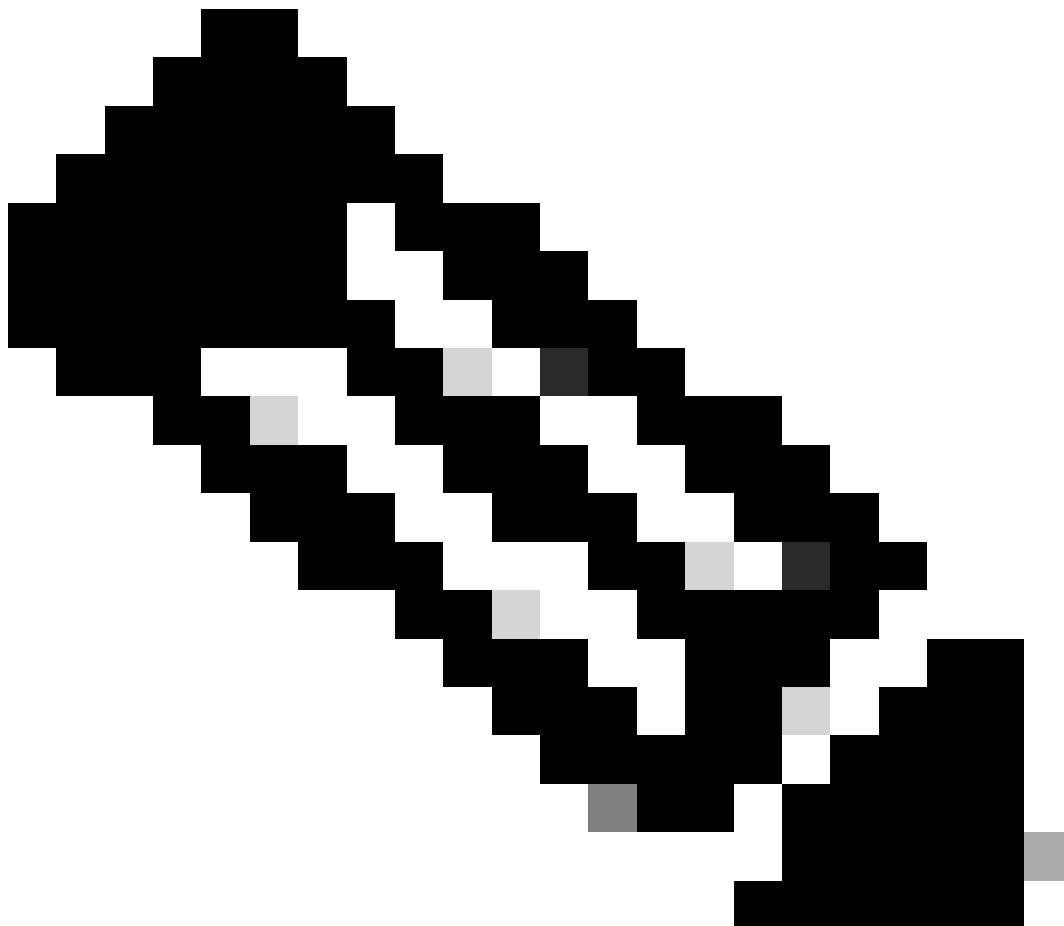
Configurar

Reivindique o dispositivo em intersight.com

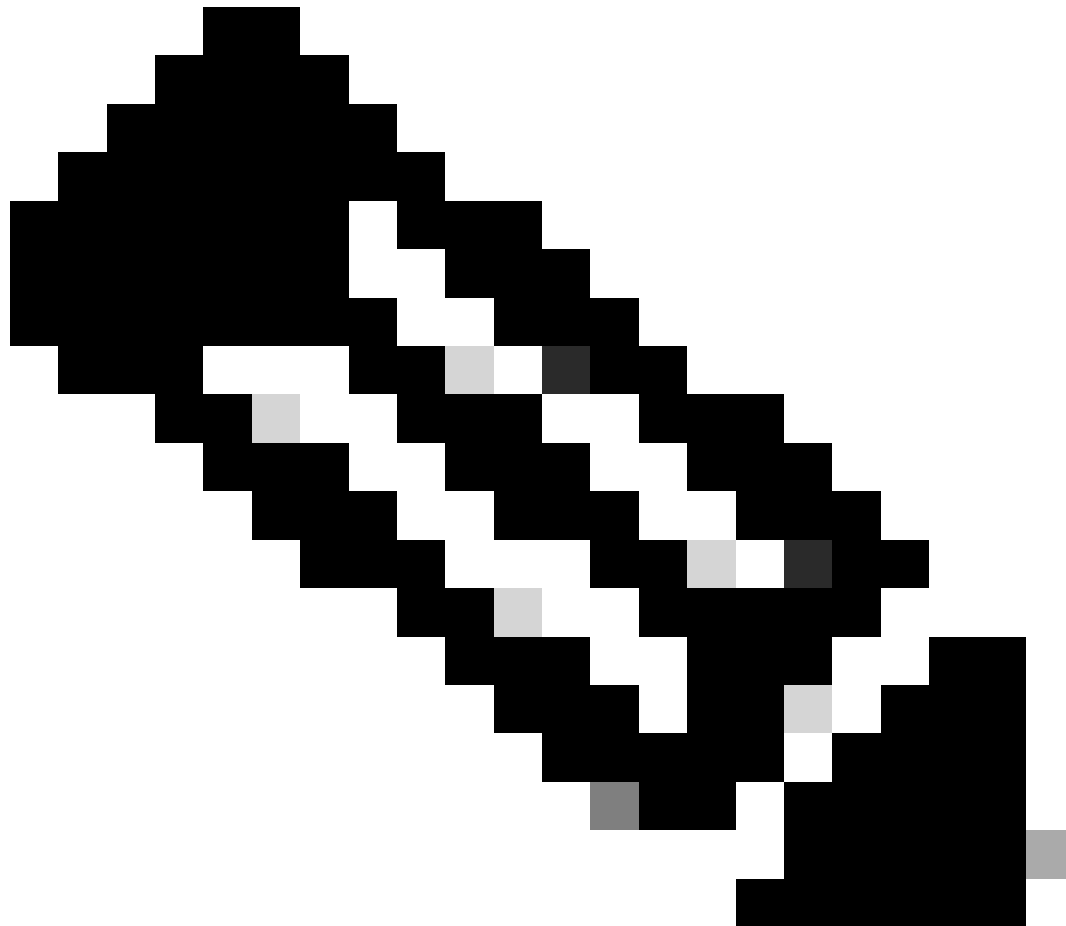
Para solicitar um novo alvo na Intersight, siga as etapas mencionadas.

No dispositivo Nexus

Emita o comando `show system device-connector claim-info` Cisco NX-OS.



Observação: para versões anteriores ao NX-OS 10.3(4a), use o comando "show intersight claim-info"



Observação: o Nexus gerou mapas de informações de solicitação para estes campos de solicitação da Intersight:

Número de série = **ID da reivindicação da Intersight**

Token de segurança da ID do dispositivo = **Código de solicitação da Intersight**

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

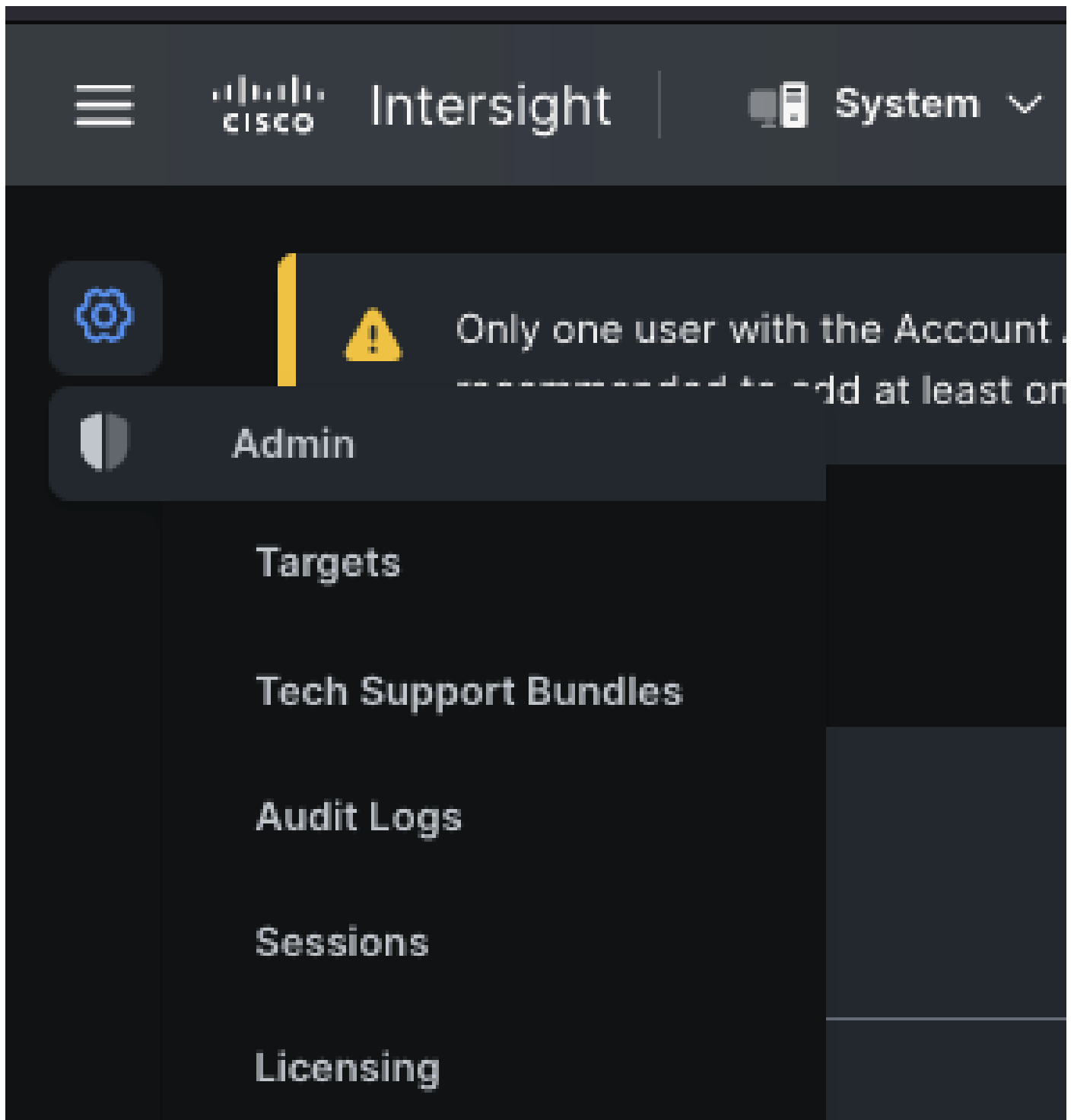
A **duração** relatada aqui é em segundos.

No portal Intersight

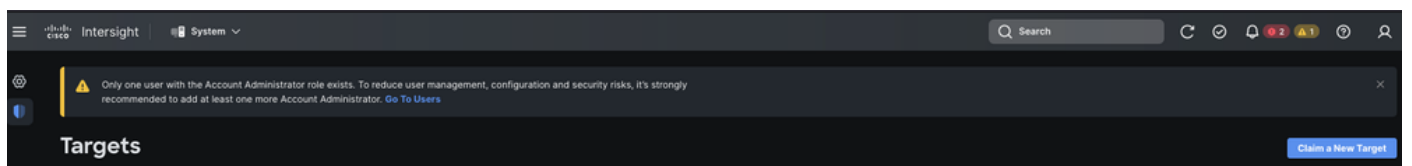
1. Em 10 minutos, efetue login no **Intersight** com os privilégios de Administrador de Conta, Administrador de Dispositivo ou Técnico de Dispositivo.
2. Na lista suspensa **Service Seletor**, selecione **System**.



3. Navegue até ADMIN > Targets > Claim a New Target.



3.1. Clique em **Reivindicar um novo destino** como mostrado na imagem.



4. Escolha **Disponível para Reivindicação** e escolha o **tipo de alvo** (por exemplo, Rede) que deseja reivindicar. Clique em Iniciar.

⚙️

⚠️ 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

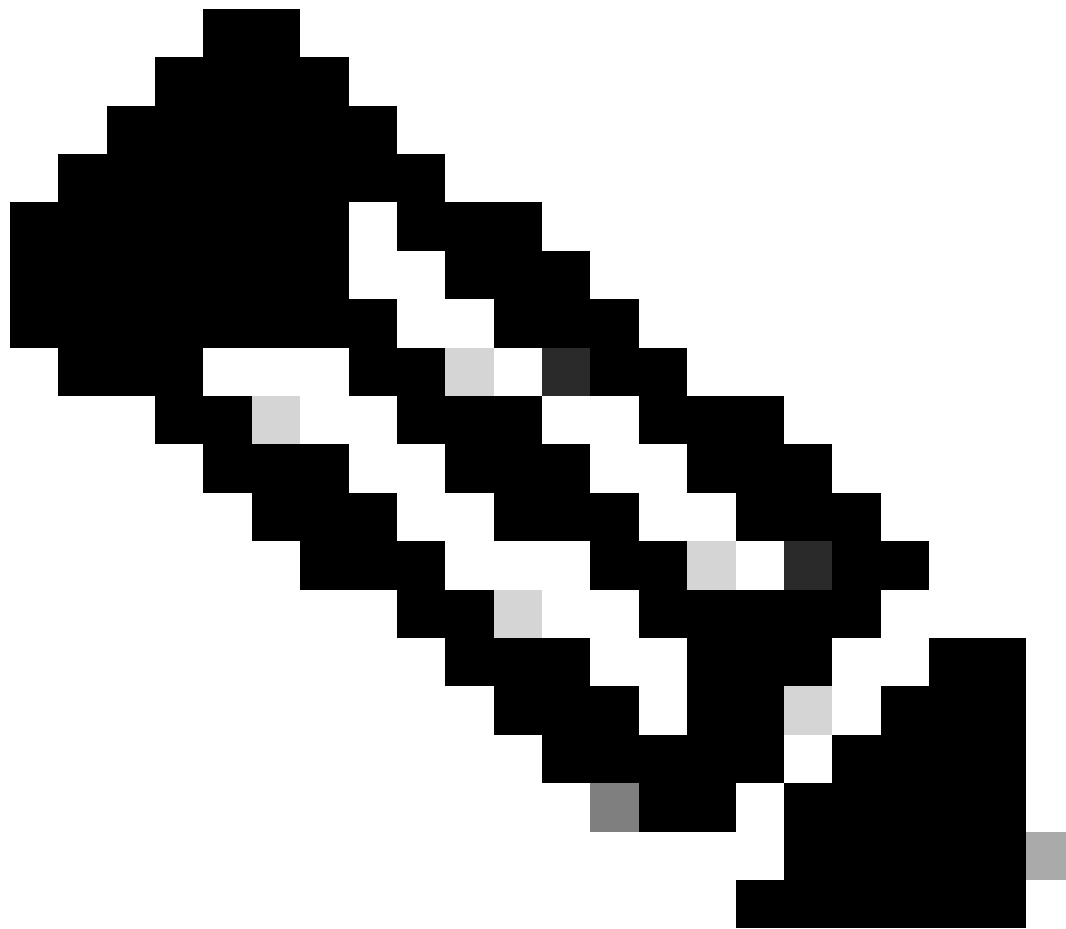
🔍 Search

Network

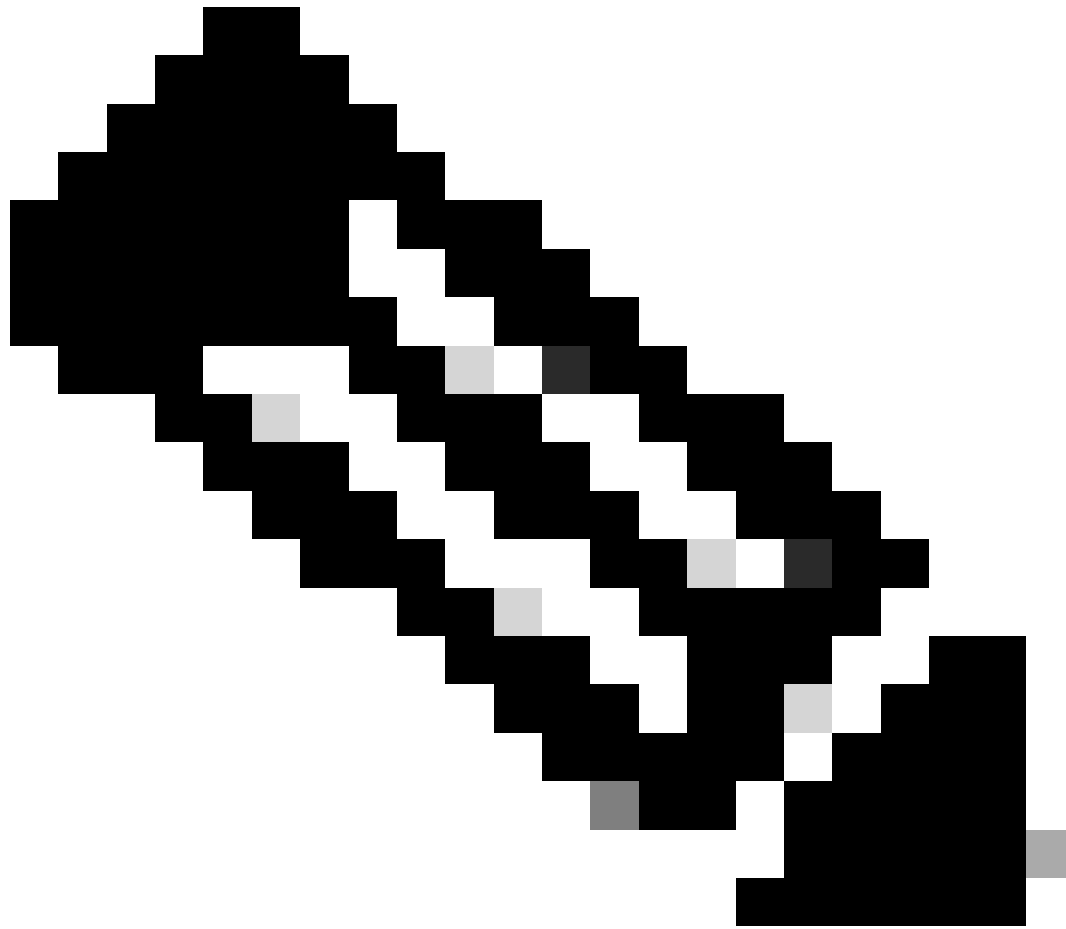
 Cisco MDS Switch	<input checked="" type="checkbox"/>  Cisco Nexus Switch	 Cisco APIC
 Cisco Cloud APIC	 Cisco DCNM	 Cisco Nexus Dashboard

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

5. Insira os detalhes necessários e clique em **Reivindicação** para concluir o processo de reivindicação.



Observação: o **token de segurança** no switch é usado como o código de declaração e o **número de série** do switch é a ID do dispositivo.



Observação: o token de segurança expira. Você deve concluir a reivindicação antes ou o sistema solicitará que você gere novamente uma.



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



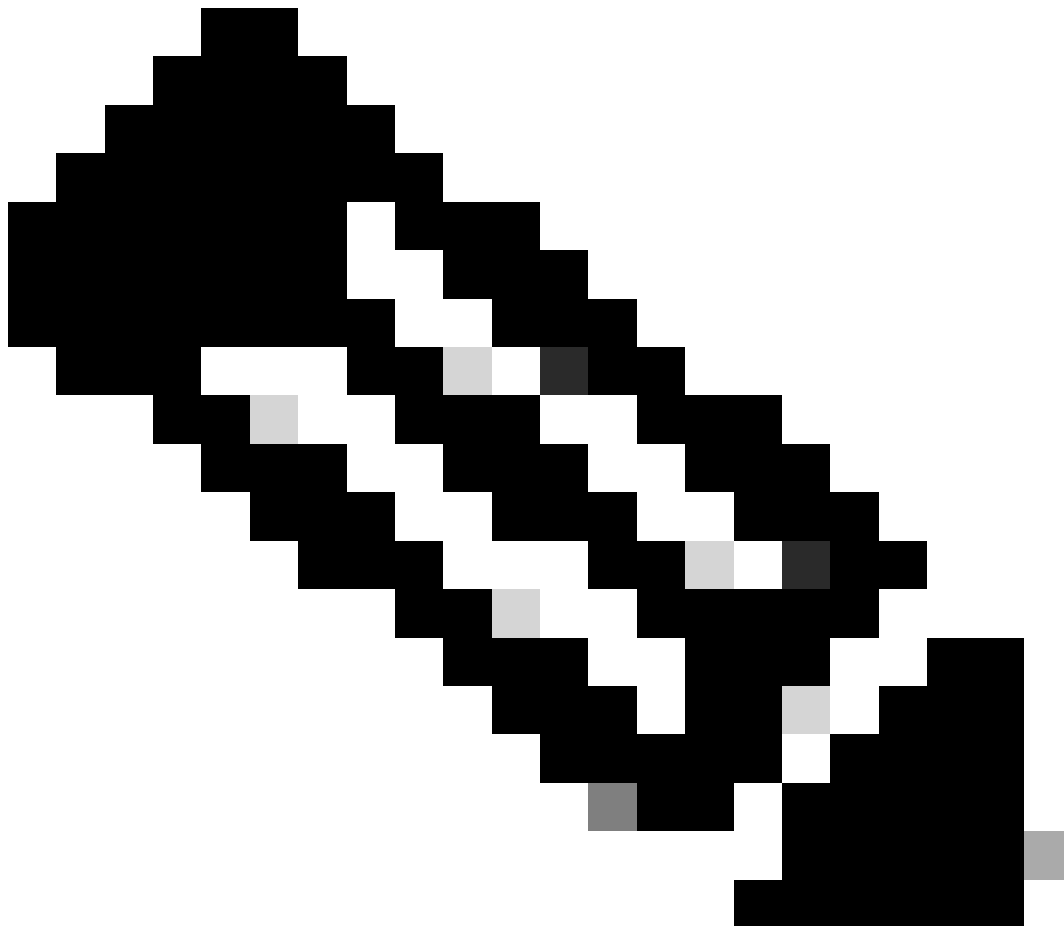
[Details](#)

Reivindique um para muitos dispositivos Nexus independentes em intersight.com usando Ansible®

Para reivindicar um para muitos dispositivos Nexus, um manual de atividades Ansible pode ser executado.

- O inventário e o manual do possível podem ser clonados do git em <https://github.com/datacenter/ansible-intersight-nxos>.
- No Ansible inventory.yaml, o ansible_connection tipo é definido como ansible.netcommon.network_cli para enviar comandos ao switch Nexus. Isso pode ser alterado para ansible.netcommon.httpapi para permitir a conectividade por NXAPI.
- Uma conexão possível com o endpoint Intersight requer uma chave de API, que pode ser gerada a partir da sua conta **intersight.com**.

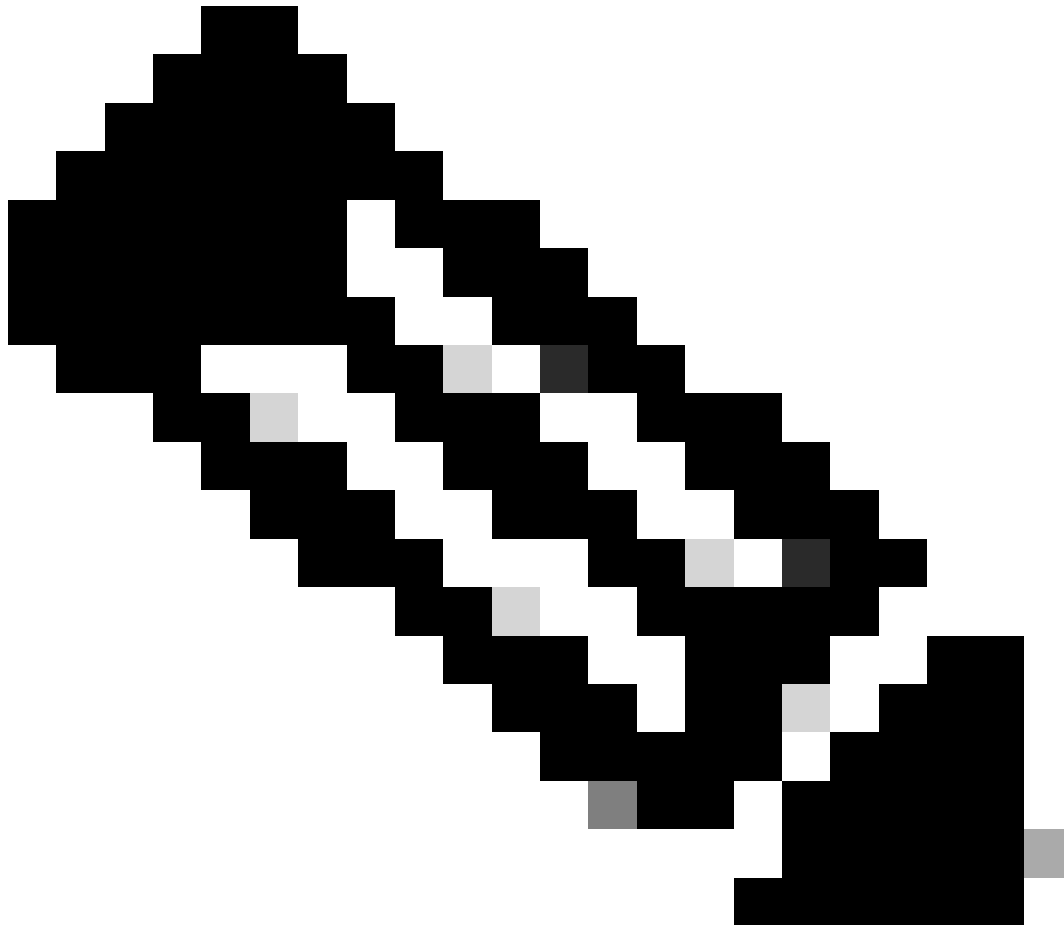
Configurar Nexus NXAPI (usado somente se estiver usando ansible.netcommon.httpapi)



Observação: no caso em que um proxy de nível de sistema é configurado (**HTTP(S)_PROXY**) e o Ansible não deve usar um proxy para se conectar ao endpoint Nexus NXAPI, é desejável definir `ansible_httppapi_use_proxy: False` (o padrão é `True`).

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

Para verificar de forma independente a conectividade HTTP para o ponto final NXAPI, você pode tentar enviar um show clock. No próximo exemplo, o switch autentica o cliente usando a autenticação básica. Também é possível configurar o servidor NXAPI para autenticar clientes com base no certificado de usuário X.509.



Observação: o hash de autenticação básica é obtido da codificação base64 de **username:password**. Neste exemplo, a codificação **admin:cisco!123** base64 é YWRtaW46Y2lzY28hMTIz.

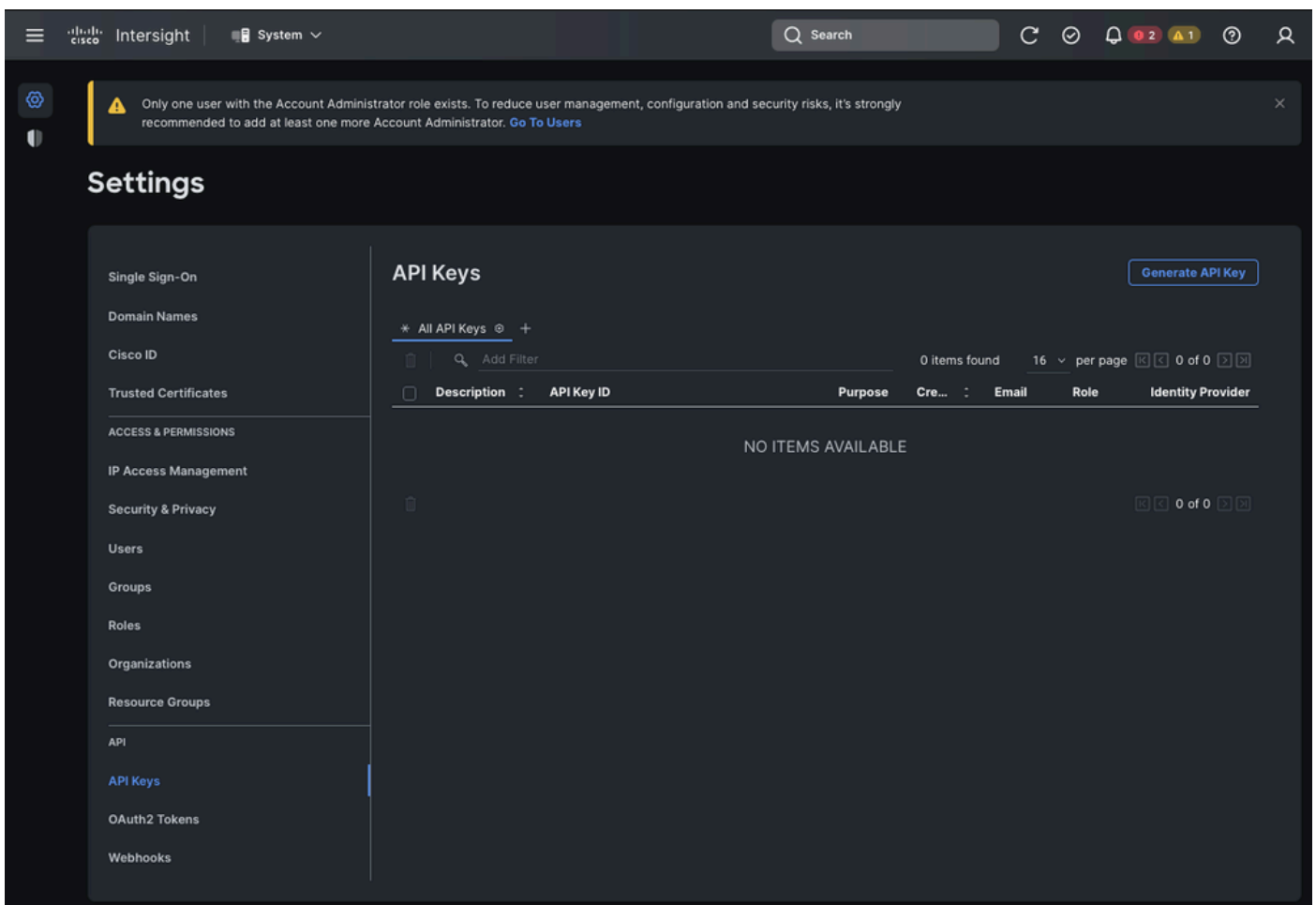
```
curl -v --noproxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

Resposta Curl:

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

Gerar chaves de API de Intersight

Consulte a seção [README.md](#) sobre como obter a chave de API do Intersight System > Settings > API keys > Generate API Key.



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

Exemplo: Ansible inventory.yaml



Observação: no próximo exemplo, o Ansible foi configurado para ignorar as configurações de proxy do sistema operacional com `ansible_httppapi_use_proxy: False`. Se precisar que o servidor Ansible use um proxy para acessar o switch, você poderá remover essa configuração ou defini-la como `True` (padrão).



Observação: a ID da chave de API é uma cadeia de caracteres. A chave privada da API inclui o caminho completo para um arquivo que contém a chave privada. Para o ambiente de produção, é recomendável usar o 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"
...

```

Exemplo: playbook.yaml Execução

Para obter mais informações sobre programação de dispositivos Nexus autônomos com Ansible, consulte a seção Applications/Using Ansible com o Cisco NX-OS do [Guia de Programação do NX-OS do Cisco Nexus 9000 Series](#) para sua versão atual.

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

Verificar

Para verificar a reivindicação de um novo alvo, faça o seguinte:

No switch Nexus

Versões anteriores à versão 10.3(4a)M

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

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

Versões iniciando com 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
```

Ansible

É possível adicionar uma tarefa ao final do `playbook.yml` para obter as informações de interceptação do switch.

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

Aqui está a saída correspondente:

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

Desabilitar Conector do Dispositivo

	Comando ou Ação	Propósito
Passo 1	<code>no feature intersight</code> Exemplo: <code>switch(config)# no feature intersight</code>	Desabilita o processo de interceptação e remove toda a configuração NXDC e o armazenamento de logs.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.