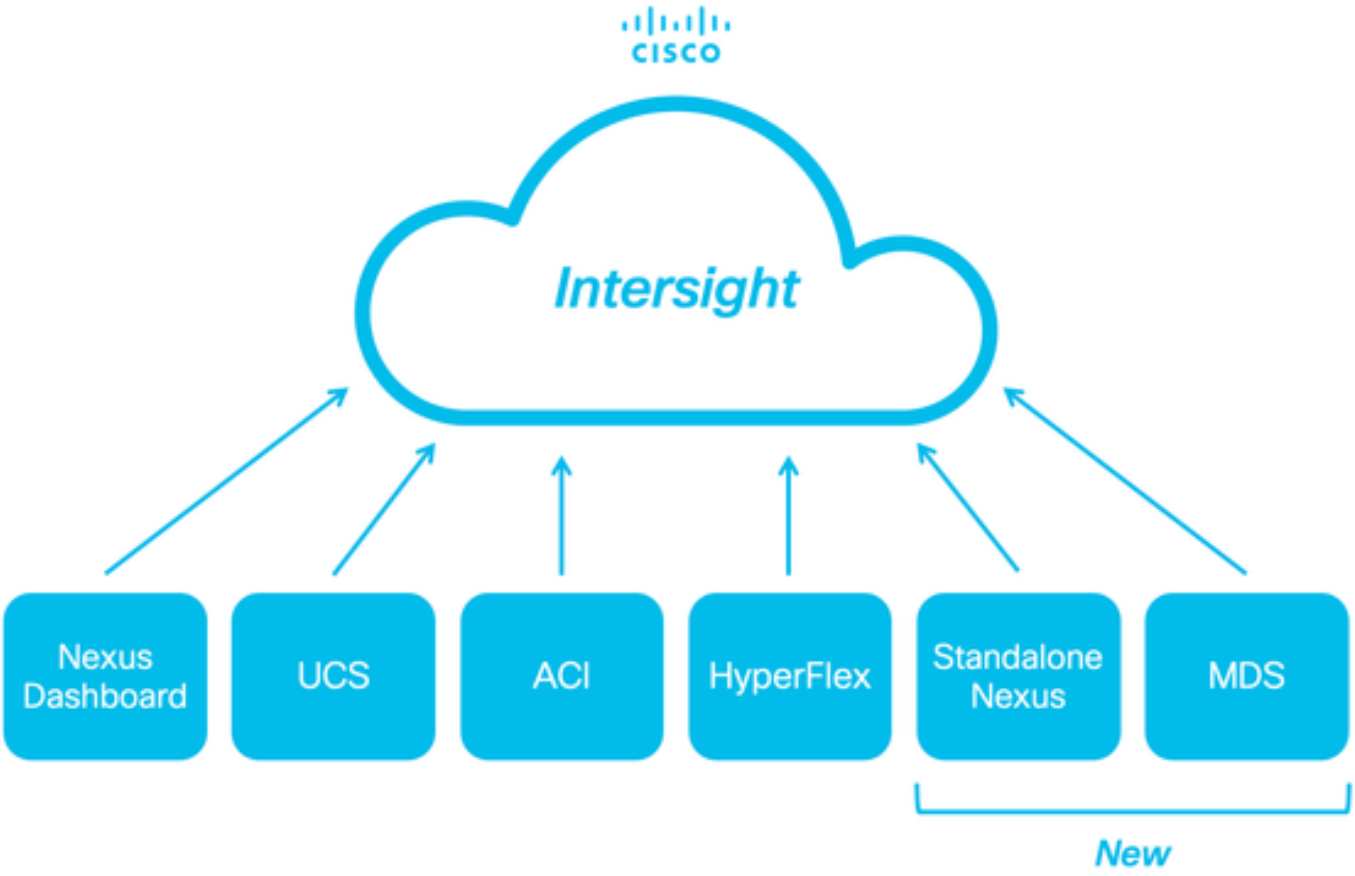
# Configure e reivindique o Nexus independente para a conectividade da Intersight

## Contents



## 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 comopensslcurl. As solicitações do Internet Control Message Protocol (ICMP) são ignoradas.
- Se um proxy for necessário para uma conexão HTTPS com osvc.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

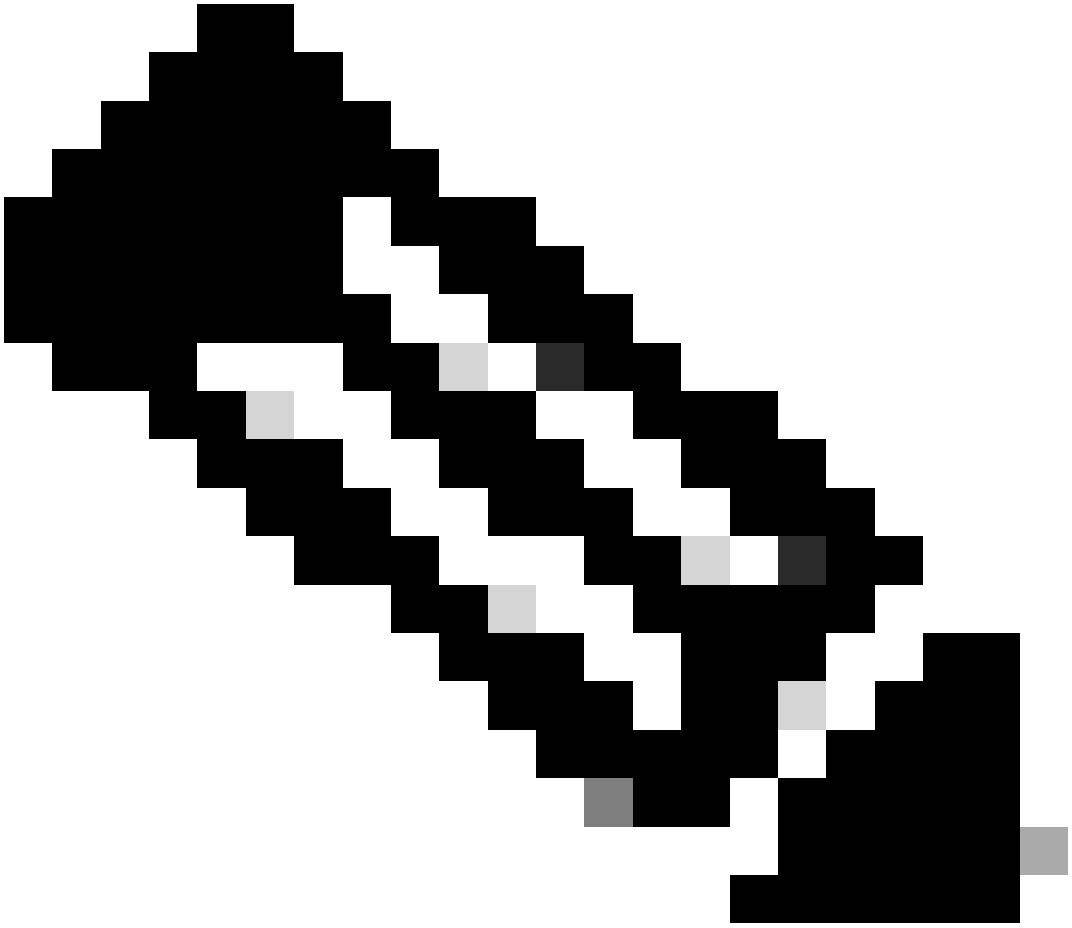
A conectividade da Intersight fornece estes recursos e benefícios para as plataformas baseadas no Cisco NX-OS:

- 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).

---

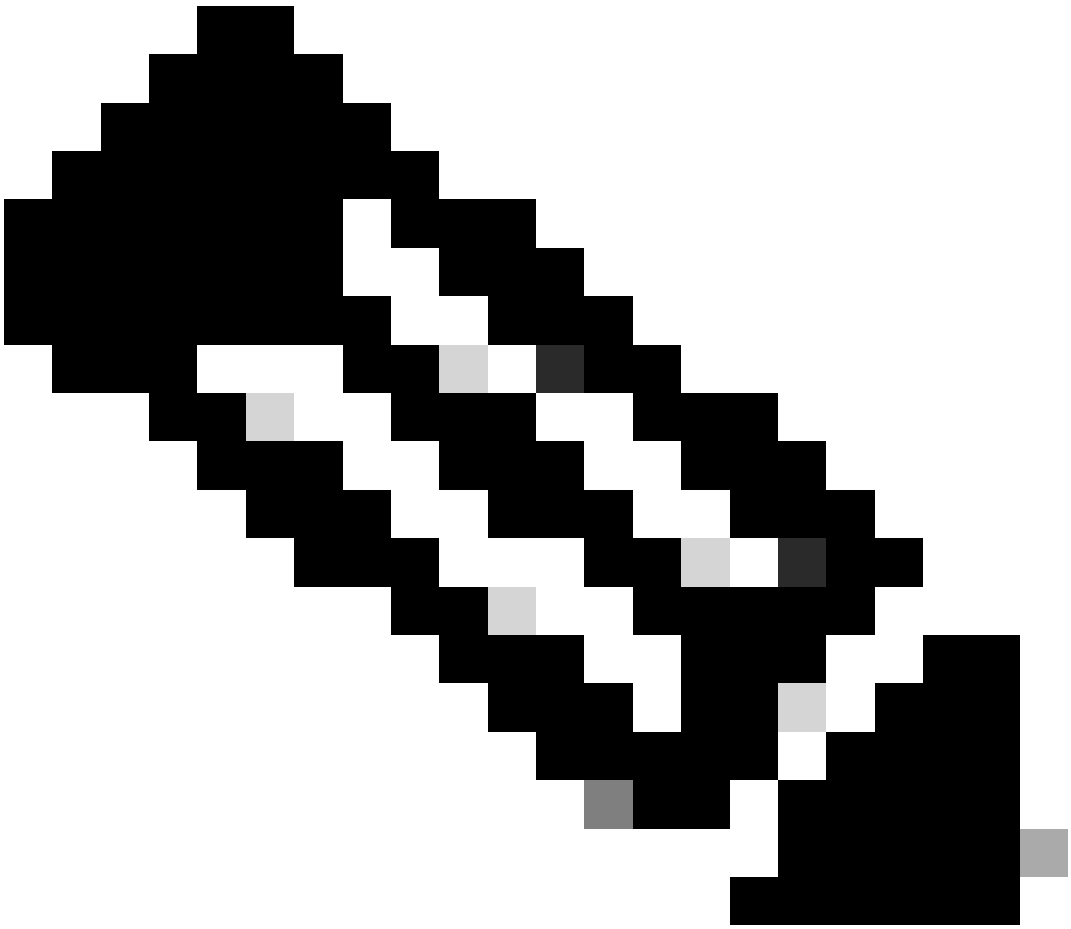
Para verificar a conectividade do Transport Layer Security (TLS) e HTTPS, habilite o bash e a execução `openssl` e `curl` no VRF desejado (`ip netns exec` ) é recomendado.

```
! 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://
```

## 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` construção.

---

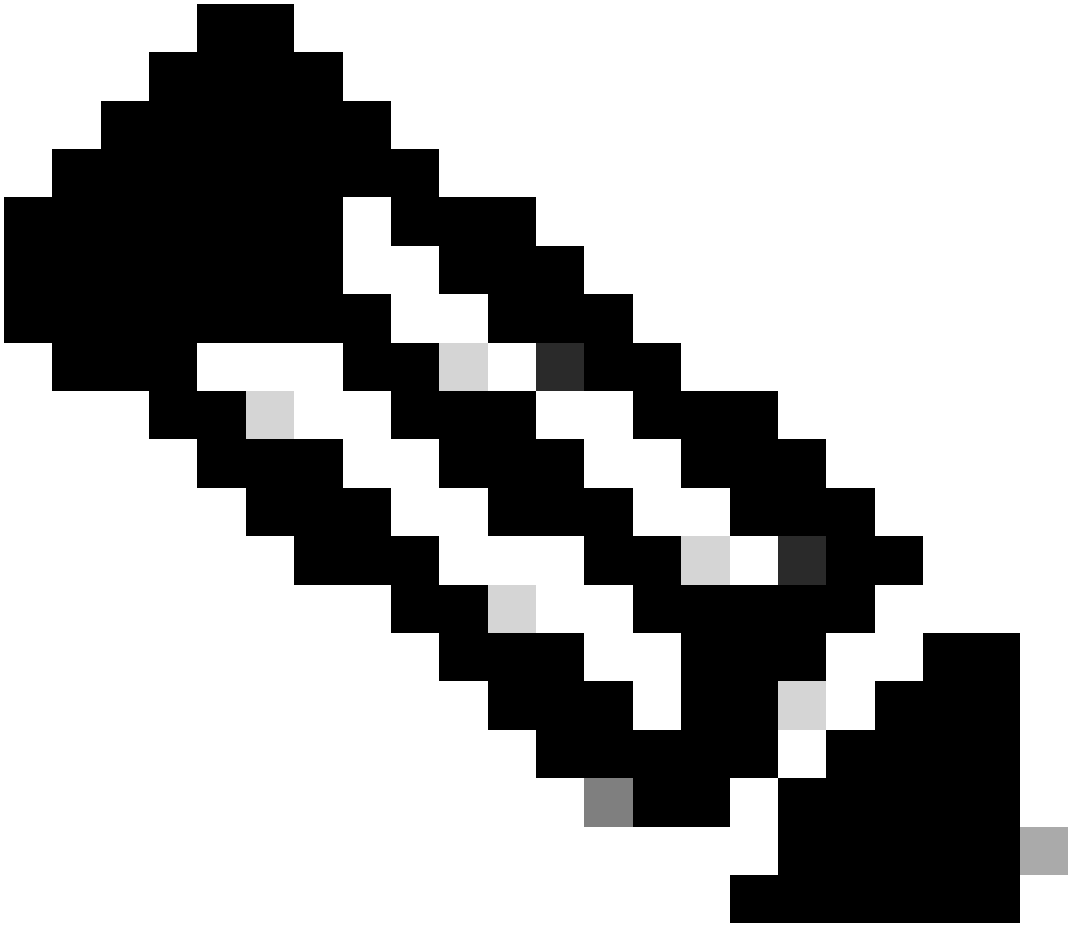
```
Switch# run bash ip netns exec management openssl s_client -connect svc.intersight.com:443
CONNECTED(00000004)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, CN = Amazon RSA 2048 M01
```

```
verify return:1
depth=0 CN = us-east-1.intersight.com
verify return:1
---
Certificate chain
 0 s:CN = us-east-1.intersight.com
   i:C = US, O = Amazon, CN = Amazon RSA 2048 M01
 1 s:C = US, O = Amazon, CN = Amazon RSA 2048 M01
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGfzCCBWegAwIBAgIQD859tBjpT+QUyVOXqkG2pzANBgkqhkiG9w0BAQsFADA8
MoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kg
UlNBIDIwNDggTTAxMB4XDTIzMDQwNTAwMDAwMFoXDTI0MDUwMzIzNTk1OVowIzEh
MB8GA1UEAxMYdXMtZWFzdC0xLmludGVyc2lnaHQuY29tMIIBIjANBgkqhkiG9w0B
AoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kn
BDM+MCNnvmgNDlGnU6/t1jOC78OQpKXr2ksbGC0FzHfMvNjEk9kMCUe179dummrs
pOOFzvIrJGqYvkIXT5WLtiU9aP3+VSEWQO1kTeDHoDfLLJLON42cKjskYt0jCTwE
poKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KI
elf3tYBhuQK3y4DoSqg1/gptnUOlNwSqMu4zXjI7neGyHnzjsPUyI8qilXbPS9tV
KoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kw
HwYDVR0jBBgwFoAUgbgOY4qJEhjl+js7UJWf5uWQE4UwHQYDVR0OBBYEFM7X7s7c
NoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kp
Z2h0LmNvbYIac3ZjLXN0YXRpYzEuaW50ZXJzaWdodC5jb22CGioudXMtZWFzdC0x
LoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K1
Y3MtY29ubmVjdC5jb22CE3N2Yy51Y3MtY29ubmVjdC5jb22CDmludGVyc2lnaHQu
Y29tghJzdmMuaW50ZXJzaWdodC5jb20wDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjA7BgNVHR8ENDAyMDCgLqAshipodHRwOi8v
YoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KI
BgZngQwBAgEwdQYIKwYBBQUHAQEEaTBnMC0GCCsGAQUFBzABhiFodHRwOi8vb2Nz
coKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Ku
cjJtMDEuYW1hem9udHJ1c3QuY29tL3IybTAxLmNlcjAMBgNVHRMBAf8EAjAAMIIB
fgYKKwYBBAHWeQIEAgSCAW4EggFqAWgAdwDuzdBk1dsazsVct52OzROiModGfLzs
3oKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K5
CSFqTpBjlOdOLQ4YuQIhAO1OVDrLJMM+9EtOwmZd8Q1MRHJlOlr2VWmOTF6GGkCV
AHUAc9meiRtMlnigIH1HneayxhzQUV5xGSqMa4AQesF3crUAAAGHUp9iOwAABAMA
RjBEAiAFPPLvt7TN7mTRnQZ+FZLGR/GO4KQqSjYuszDNPArT3wIgf/sQbQqNjCk7
joFUuL9cEPYfNm7n1nZIFIRAK6UqwGOAdgBIsONr2qZHNA/lagL6nTDrHFIBy1bd
LoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K8
MXtts5t/C5lYw5peGAIgKOeFmxTptEfMkBZti39vepUxb5meDvKaZdtXVvFpkCMw
DQYJKoZIhvcNAQELBQADggEBANl6HKZ9P6AIufr7qdNCcW+DXClY6dqX1KNOsCh+
UoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KM
z5R1VV+81gN2HHiuUsEOFwHDbbhiGBJiJteFm0blpruKHennx8HQYfC7bup4N5JH
YoKXXrXrkESkWgbQadlEo3H545Zsix+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kb
LKFl6c+EN0Y76YaCV8doujG3qD/bO9VDx7dhvbSEECYuzbYyPDGnb7Drmhny0Eki
smLUZ3TVcCvPc+1dE/jrbBzPeIY7jGr8eL7masFCuZZn2lM=
-----END CERTIFICATE-----
subject=CN = us-east-1.intersight.com

issuer=C = US, O = Amazon, CN = Amazon RSA 2048 M01

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, P-256, 256 bits
---
```

```
SSL handshake has read 5754 bytes and written 442 bytes
Verification: OK
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 66D0B69FAA7EB69FAA7EC54C9764966ED9A1289650B69FAA7EB69FAA7E9A5FD5ADE
    Session-ID-ctx:
    Master-Key: B69FAA7E45891555D83DFCAEB69FAA7EB69FAA7EA3A99E7689ACFB69FAA7EAD7FD93DB69FAA7EB1AF821
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 86400 (seconds)
    TLS session ticket:
    0000 - 36 12 b2 36 b3 53 07 29-54 ac 56 f0 06 83 4f b1   6..6.S.)T.V...O.
    0010 - 49 35 51 40 22 07 bd 7e-59 d7 7e 44 29 ff c6 2a   I5Q@"..~Y.~D)..*
    0020 - ec bc 11 e1 d3 5d 69 e8-7a d2 f1 c2 08 f6 5b 8f   .....]i.z.....[.
    0030 - 2c 5b 5e 50 e3 e2 8f e7-c4 44 8f e4 6d 45 d2 64   ,[^P.....D..mE.d
    0040 - 93 98 f5 e8 b0 f7 1d 00-26 4b 88 ea 2d 7d 42 58   ........&K..-}BX
    0050 - 05 9f 71 3a fe ac f0 15-a5 5c 1d 74 74 bf 32 1b   ..q:.....\.tt.2.
    0060 - d8 a8 23 84 08 cc f9 3e-54                        ..#....>T

    Start Time: 1707515659
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: yes
---
```

## 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 construçãoip netns exec
é usada para executar curl no VRF desejado; por exemplo,ip netns exec managementpara 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://
```

<#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 >
```

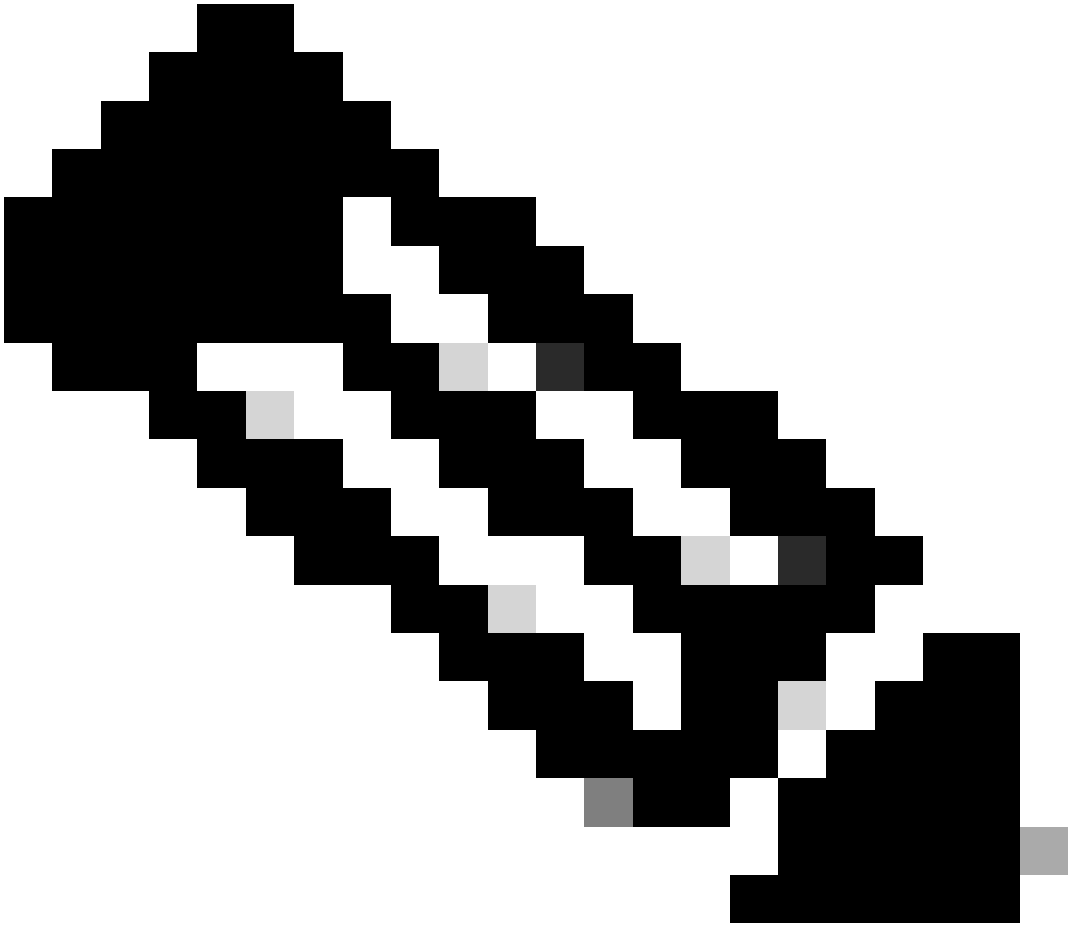
# Configurar

## Reivindique o dispositivo em intersight.com

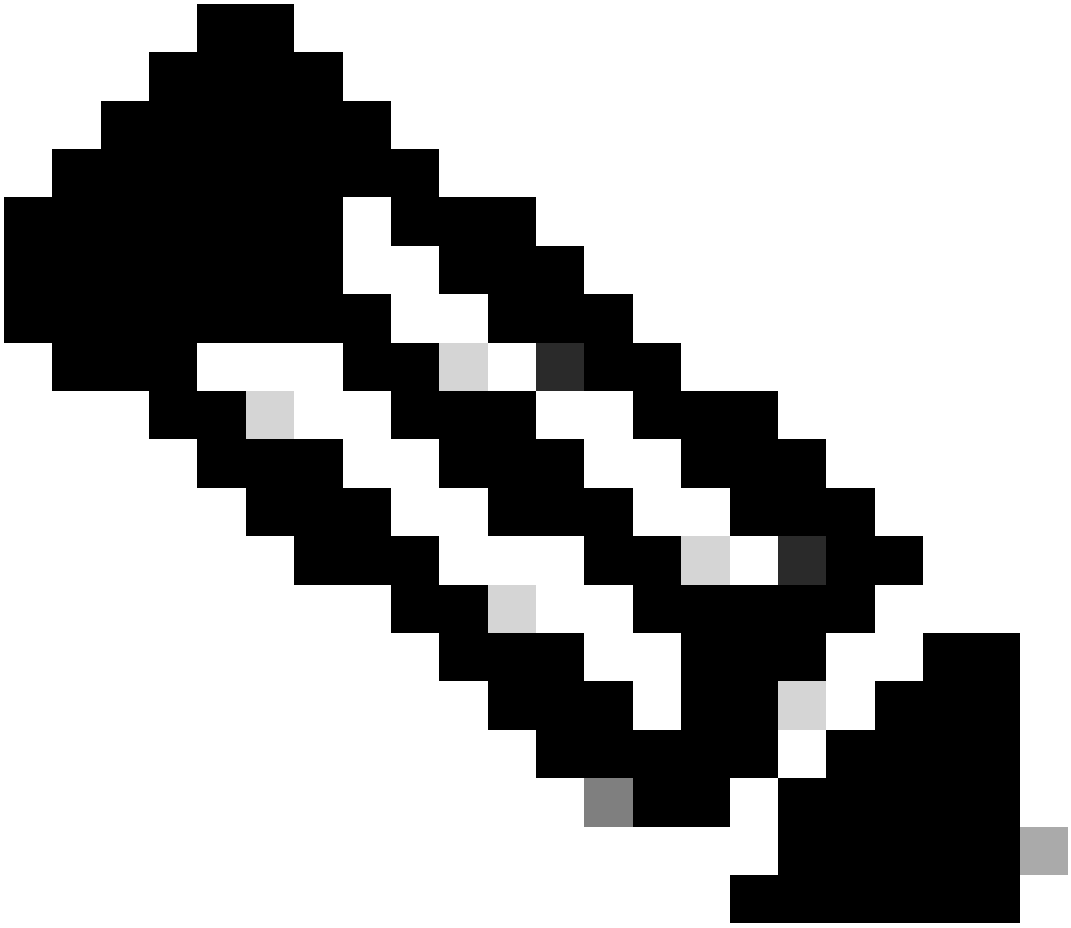
Para solicitar um novo alvo na Intersight, siga as etapas mencionadas.

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:

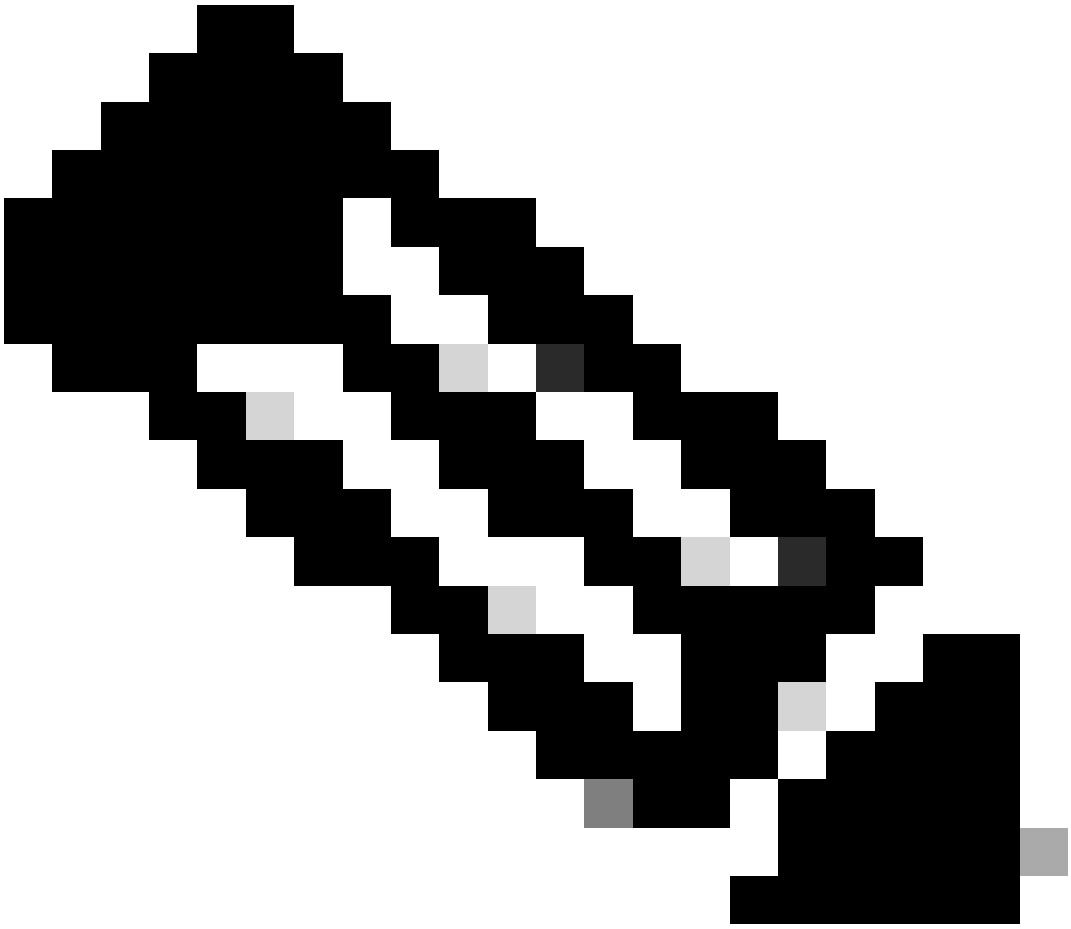
Número de série = ID da reivindicação da Intersight

Token de segurança de ID do dispositivo = Intersight Código da reivindicação

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

A duração relatada aqui é em segundos.

No portal Intersight

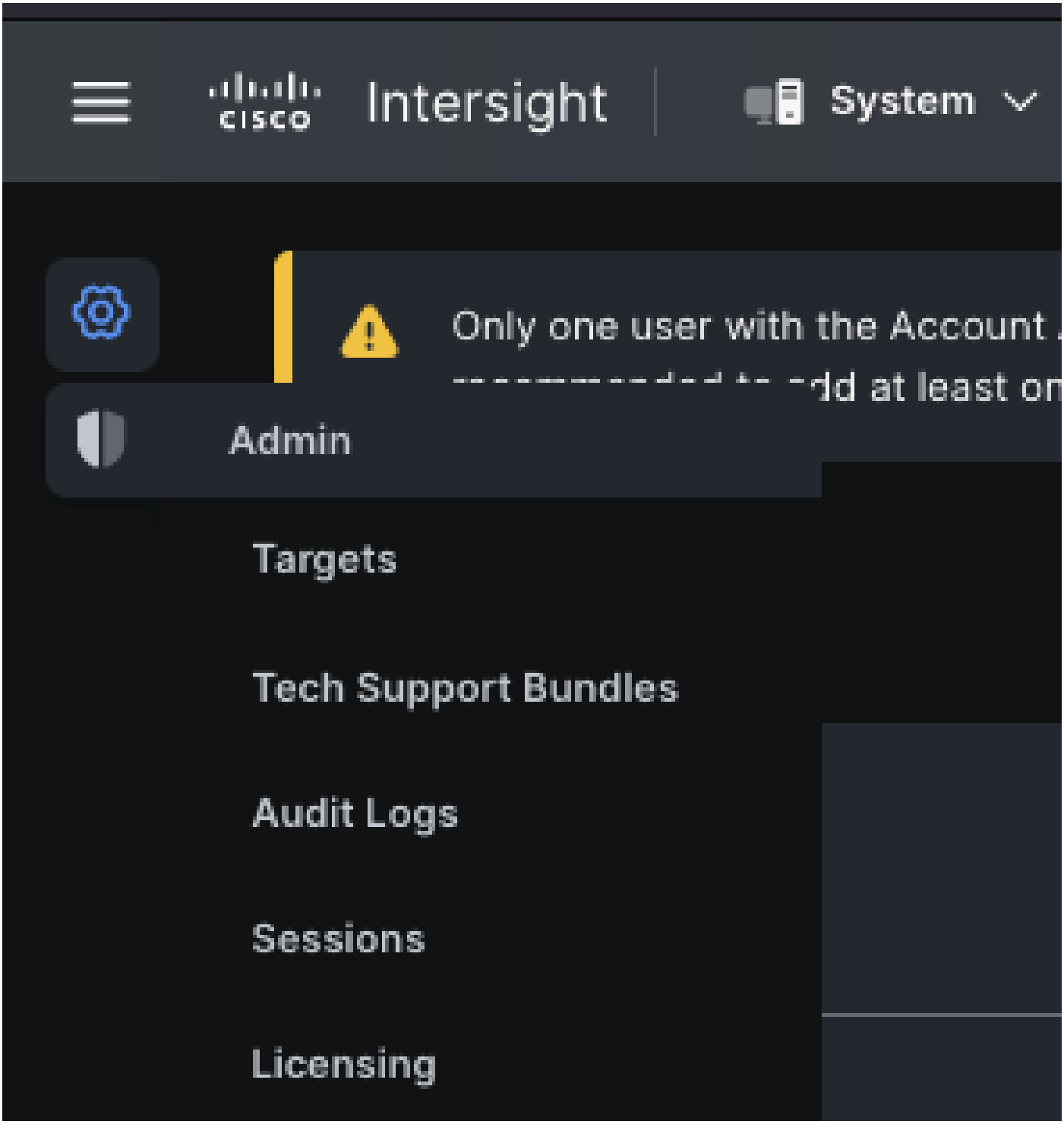


Observação: Observação: a funcionalidade Cisco Intersight Device Claim não está disponível para a região EMEA. Essas etapas só se aplicam à região da América do Norte.

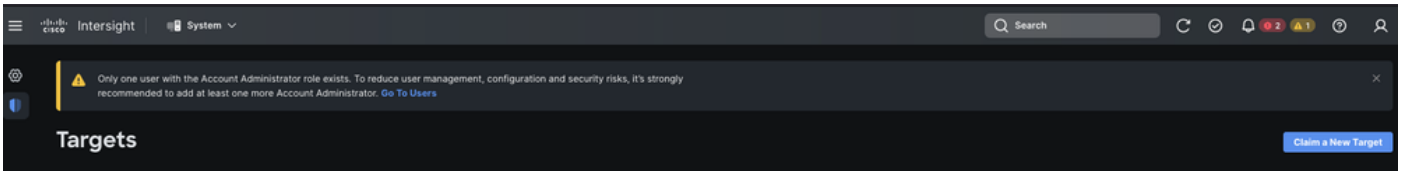
1. Em 10 minutos, efetue login no Intersight com os privilégios de Administrador de Conta, Administrador de Dispositivo ou Técnico de Dispositivo.

2. Na lista suspensa Service Seletor, selecione System.

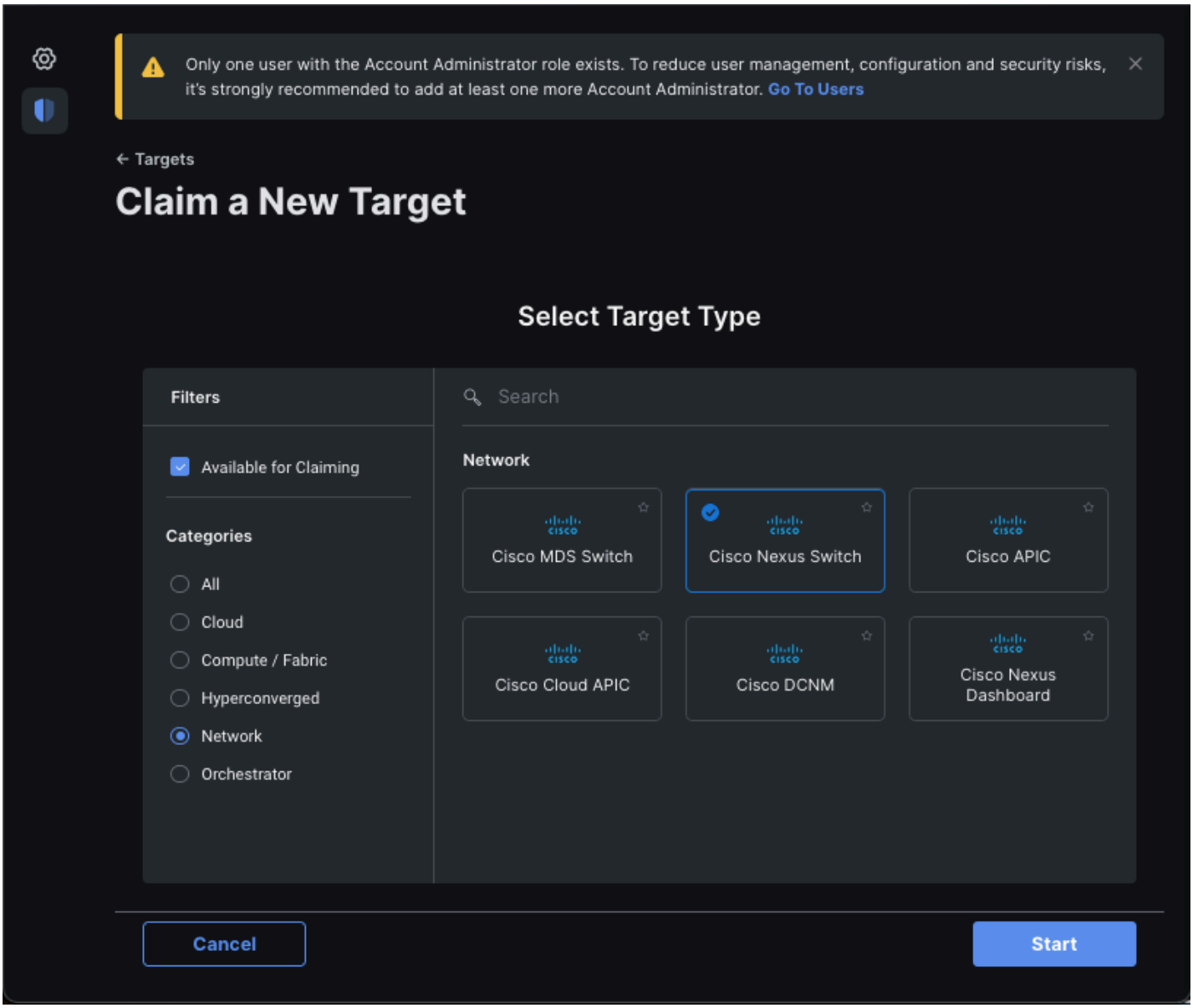
3. Navegue atéADMIN > Targets > Claim a New Target.



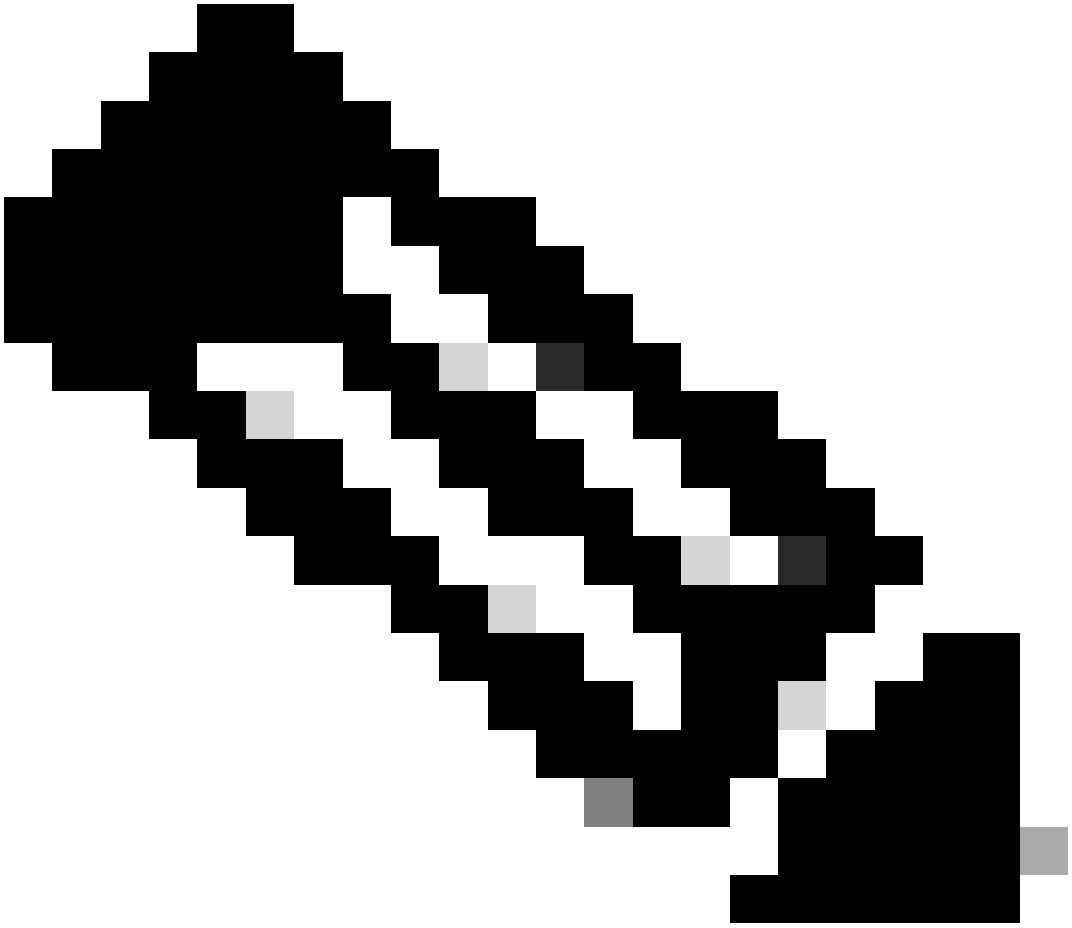

3.1. Clique em Reivindicar um novo destino como mostrado na imagem.



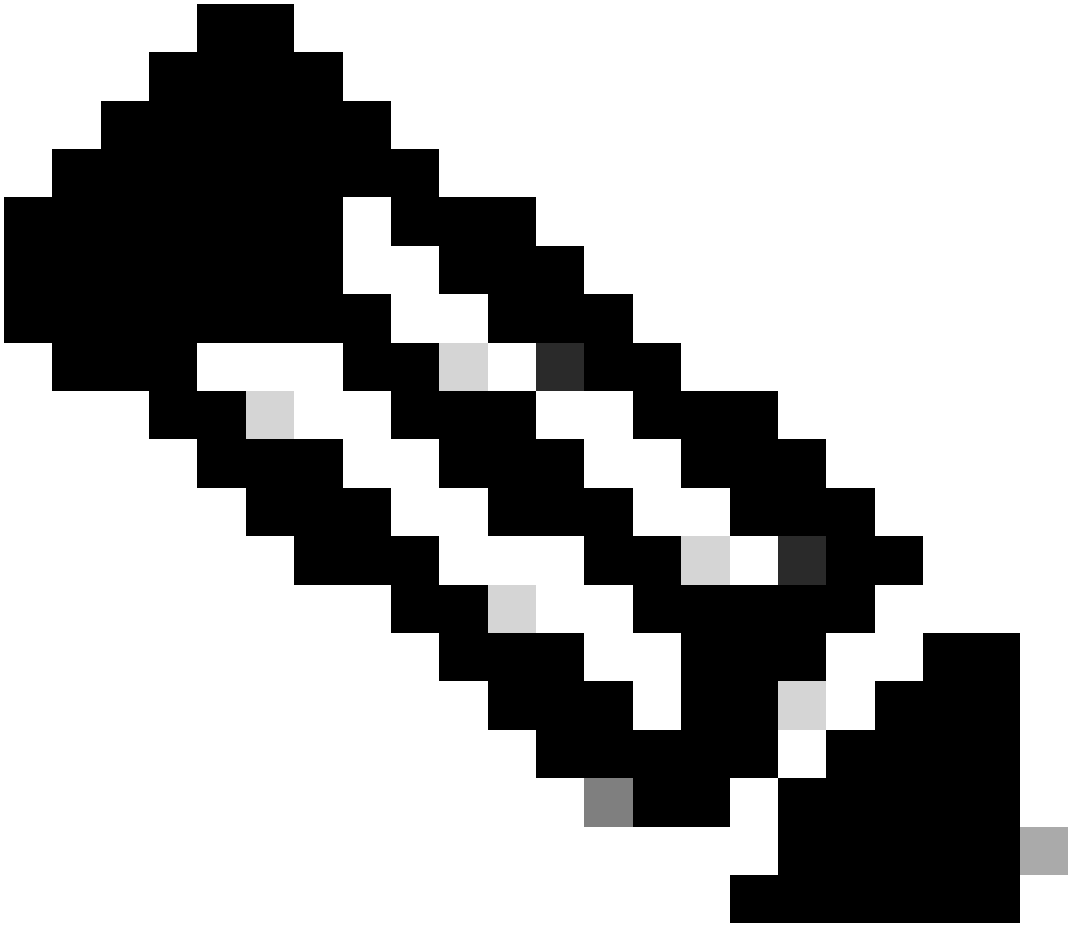

4. Escolha Disponível para Reivindicação e escolha o tipo de alvo (por exemplo, Rede) que deseja reivindicar. Clique em Iniciar.




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

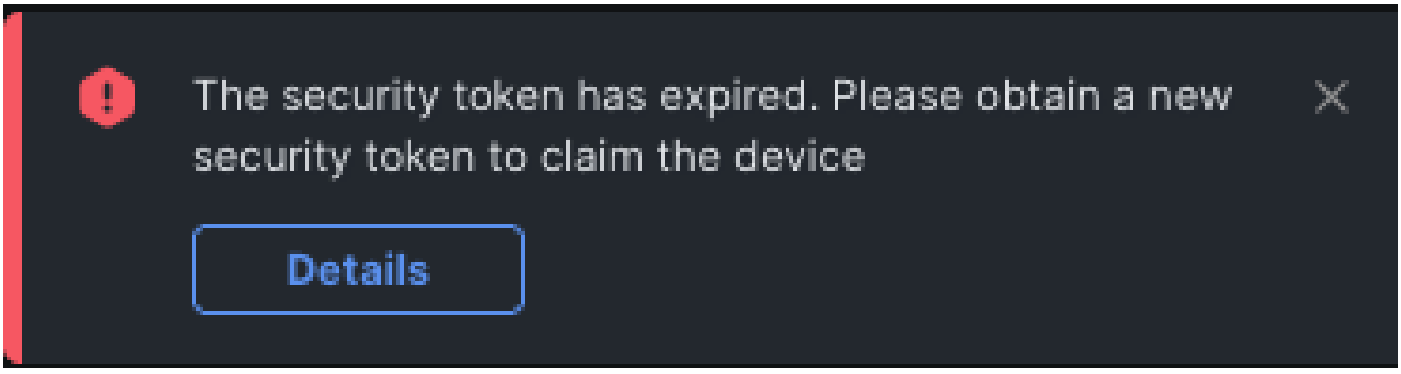


Observação: o token de segurança no switch é usado como o código de declaração e o número de série do switch é a ID do dispositivo.



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

---




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

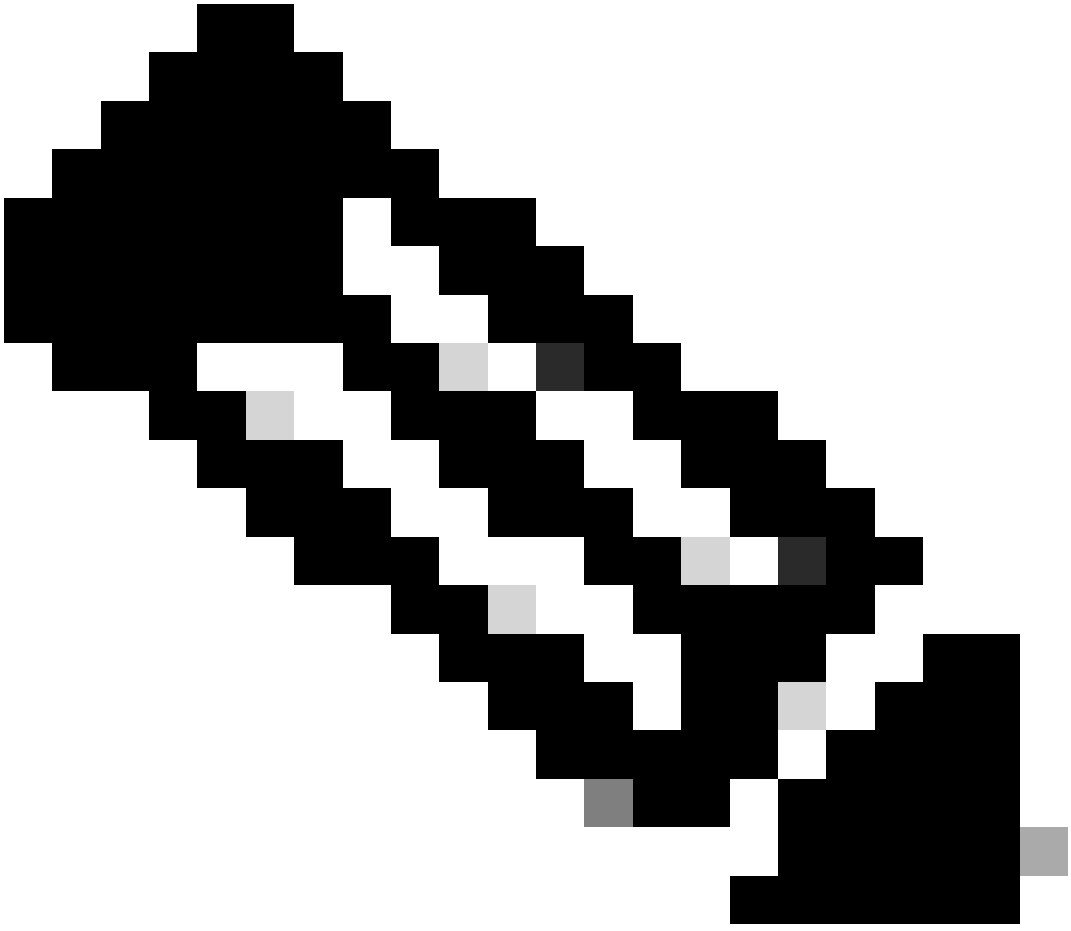
Para reivindicar um para muitos dispositivos Nexus, um manual de atividades Ansible pode ser

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_httpapi_use_proxy: False`(o padrão é True).

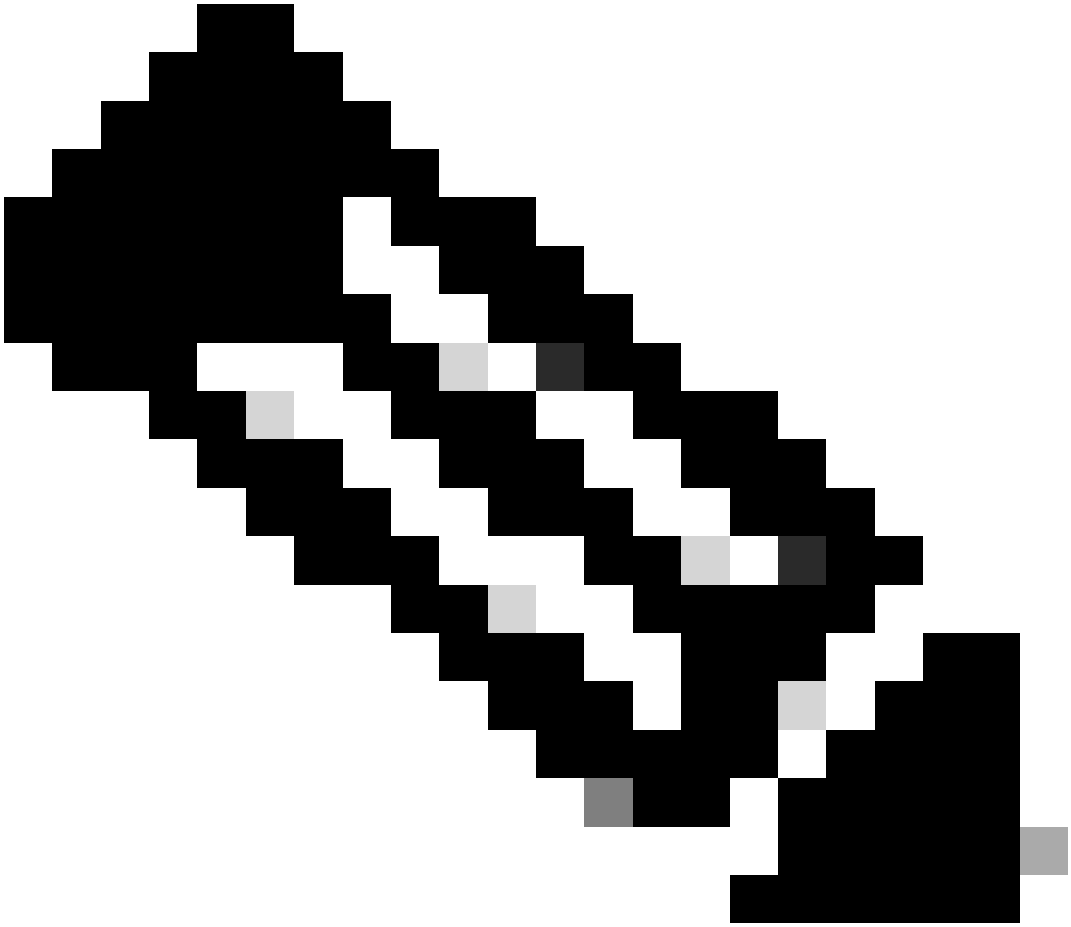
---

```
# configure terminal
```

```
# cfeature nxapi
# nxapi port 80
# no nxapi https port 443
# end

# show nxapi
nxapi enabled
NXAPI timeout 10
NXAPI cmd timeout 300
HTTP Listen on port 80
HTTPS Listen on port 443
Certificate Information:
    Issuer:   issuer=C = US, ST = CA, L = San Jose, O = Cisco Systems Inc., OU = dcnxos, CN = nxos
    Expires:  Feb 10 22:30:38 2024 GMT
```

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 éYWRtaW46Y2lzY28hMTIz.

```
curl -v --noproxy '*' \
     --location 'http://10.1.1.3:80/ins' \
     --header 'Content-Type: application/json' \
     --header 'Authorization: Basic YWRtaW46Y2lzY28hMTIz' \
     --data '{
                "ins_api": {
                    "version": "1.0",
                    "type": "cli_show",
                    "chunk": "0",
                    "sid": "sid",
                    "input": "show clock",
                    "output_format": "json"
                 }
            }'
```

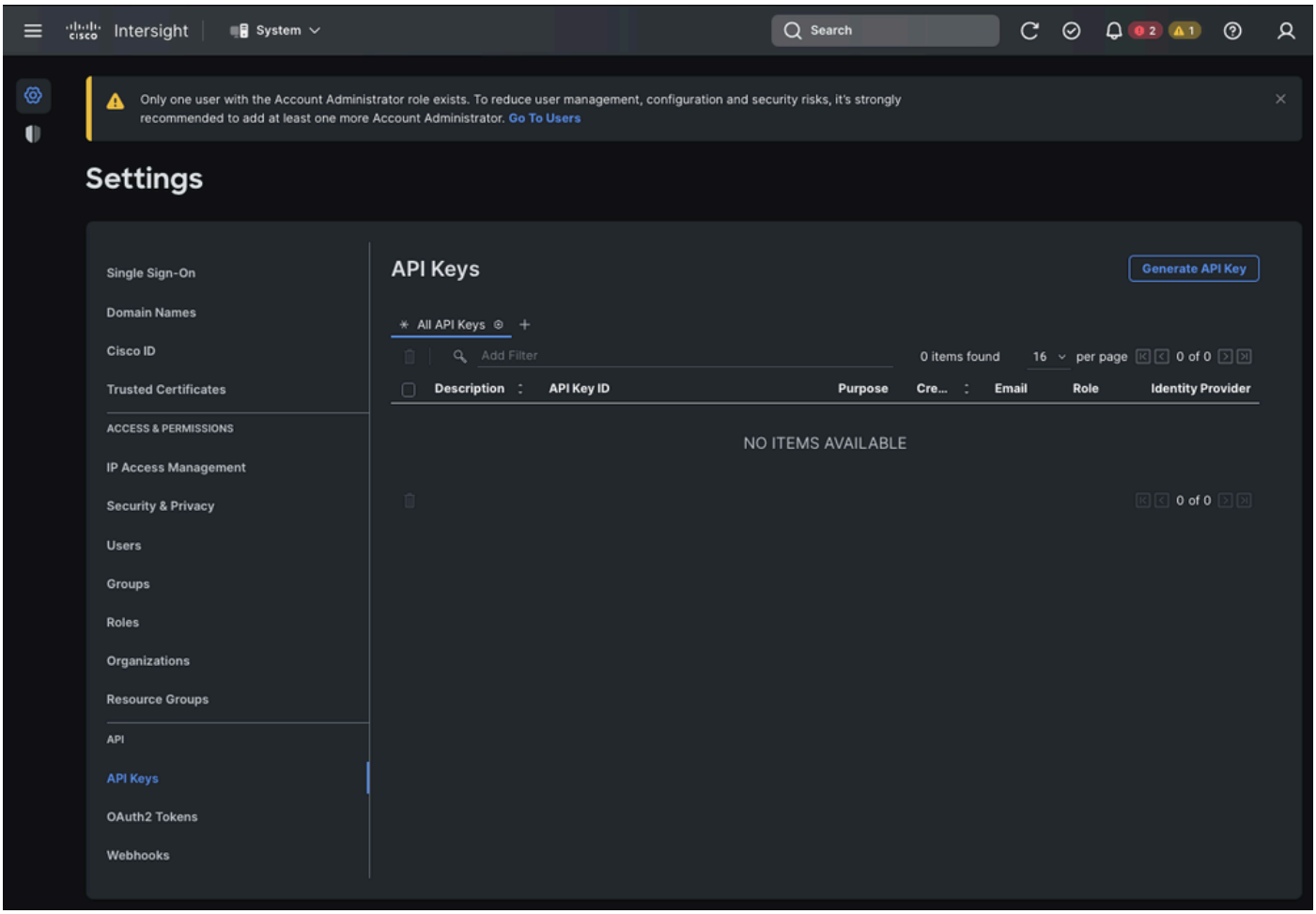
Resposta Curl:

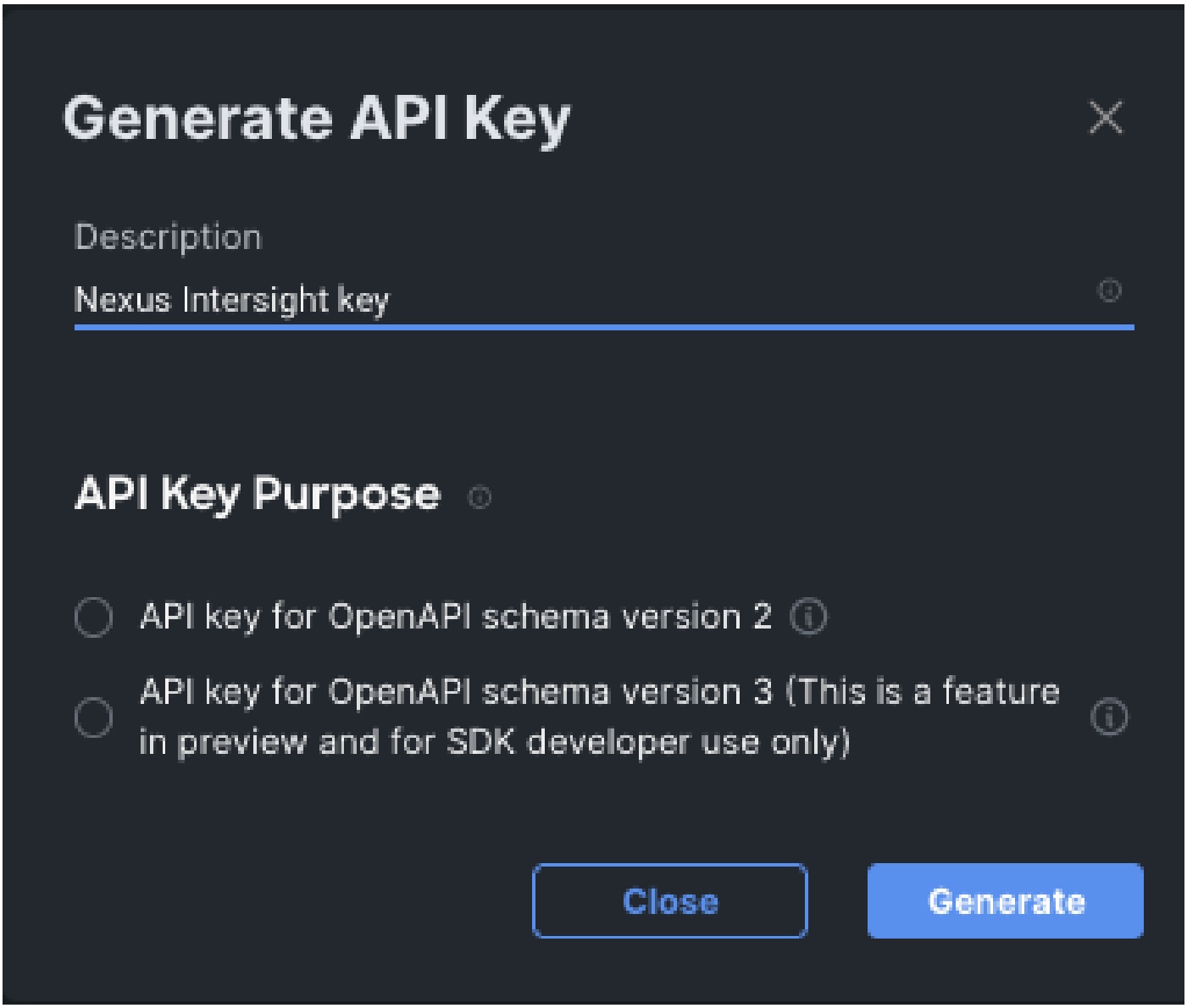
```
* Trying 10.1.1.3...
* TCP_NODELAY set
* Connected to 10.1.1.3 (10.1.1.3) port 80 (#0)
> POST /ins HTTP/1.1
> Host: 10.1.1.3
> User-Agent: curl/7.61.1
> Accept: */*
> Content-Type: application/json
> Authorization: Basic YWRtaW56Y2lzY28hBNIz
> Content-Length: 297
>
* upload completely sent off: 297 out of 297 bytes
< HTTP/1.1 200 OK
< Server: nginx/1.19.6
< Date: Fri, 09 Feb 2024 23:17:10 GMT
< Content-Type: text/json; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< Set-Cookie: nxapi_auth=dzqnf:xRYwROl1Tra64VfOMVuD4oI4=; Secure; HttpOnly;
< anticsrf: /i3vzCvxhOr4w2IrKP+umbDnzHQ=
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< X-Frame-Options: SAMEORIGIN
< X-Content-Type-Options: nosniff
< Content-Security-Policy: block-all-mixed-content; base-uri 'self'; default-src 'self'; script-src 'se
<
{
    "ins_api":    {
        "type":    "cli_show",
        "version":    "1.0",
        "sid":    "eoc",
        "outputs":    {
```

```
            "output":    {
                "input":    "show clock",
                "msg":    "Success",
                "code":    "200",
                "body":    {
                    "simple_time":    "23:17:10.814 UTC Fri Feb 09 2024\n",
                    "time_source":    "NTP"
                }
            }
        }
    }
* Connection #0 to host 10.1.1.3 left intact
}%
```

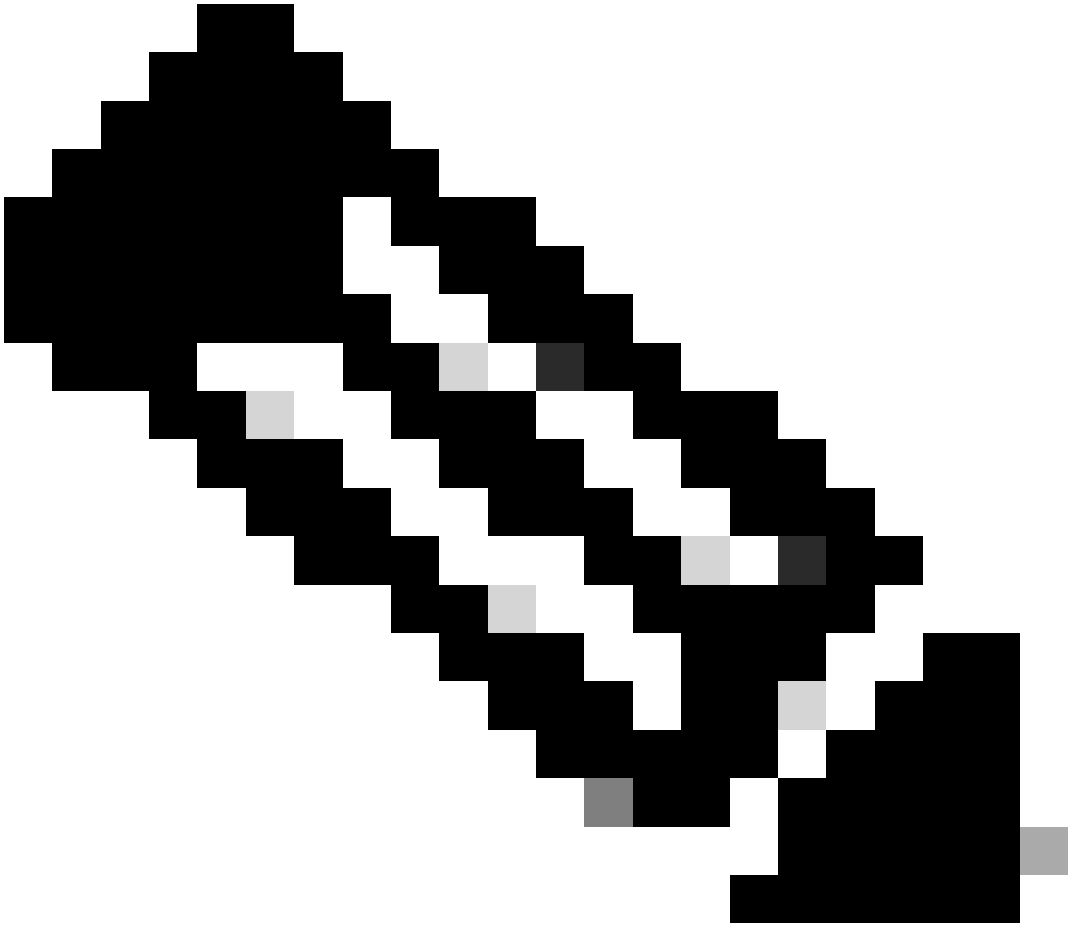

## Gerar chaves de API de Intersight

Consulte a seção README.md sobre como obter a chave de API doIntersight System > Settings > API keys > Generate API Key.

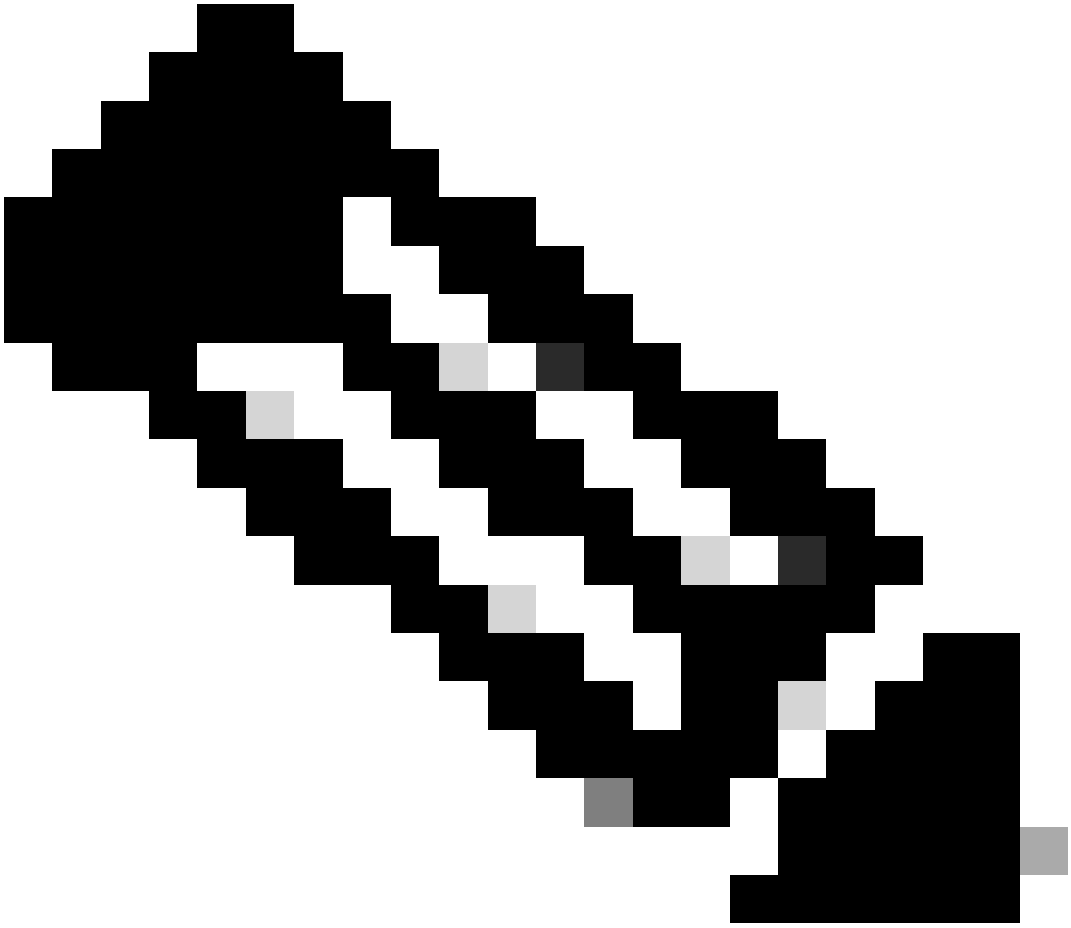





Exemplo: Ansible inventory.yaml



Observação: no próximo exemplo, o Ansible foi configurado para ignorar as configurações de proxy do sistema operacional com`ansible_httpapi_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: "5fcb99d97564612d33fdfcal/5fcb99d97564612d33fdf1b2/65c6c09d756461330198ce7e"
    api_private_key: "/home/admin/ansible-intersight-nxos/my_intersight_private_key.txt"
...
```

Exemplo:playbook.yamlExecução

Para obter mais informações sobre programação de dispositivos Nexus autônomos com Ansible, consulte a seçãoApplications/Using Ansiblecom 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] ********************************************************************************************************************************************************

TASK [Enable feature intersight] **********************************************************************************************************************************
[WARNING]: To ensure idempotency and correct diff the input configuration lines should be similar to how they appear if present in the runni
device
changed: [switch1]

TASK [Configure proxy] ********************************************************************************************************************************************
ok: [switch1]

TASK [Unconfigure proxy] ******************************************************************************************************************************************
skipping: [switch1]

TASK [Configure src interface] ************************************************************************************************************************************
ok: [switch1]

TASK [Unconfigure src interface] **********************************************************************************************************************************
skipping: [switch1]

TASK [Configure src vrf] ******************************************************************************************************************************************
ok: [switch1]

TASK [Unconfigure src vrf] ****************************************************************************************************************************************
skipping: [switch1]

TASK [Await connection to Intersight] *****************************************************************************************************************************
FAILED - RETRYING: [switch1]: Await connection to Intersight (10 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (9 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (8 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (7 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (6 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (5 retries left).
FAILED - RETRYING: [switch1]: Await connection to Intersight (4 retries left).
ok: [switch1]

TASK [Get show system device-connector claim-info] *****************************************************************************************************************
```

```
ok: [switch1]

TASK [Set claiminfoDict] ********************************************************************************************************************************************
ok: [switch1] => (item=SerialNumber: FDO21112E2L)
ok: [switch1] => (item=  SecurityToken: 0A70886FE1B8)
ok: [switch1] => (item=  Duration: 599)
ok: [switch1] => (item=  Message: )
ok: [switch1] => (item=  Claim state: Not Claimed)

TASK [claim device - PROXY] *****************************************************************************************************************************************
skipping: [switch1]

TASK [claim device - NO PROXY] **************************************************************************************************************************************
changed: [switch1]

PLAY RECAP **********************************************************************************************************************************************************
switch1                    : ok=8    changed=2    unreachable=0    failed=0    skipped=4    rescued=0    ignored=0
```

# 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",
  "AccountOwnershipUser": "bpaez@cisco.com",
  "AccountOwnershipTime": "2024-04-25T22:37:25.173Z",
  "AccountOwnershipId": "TAC-DCRS",
  "DomainGroupMoid": "662050327564613301 4ec978",
  "AccountMoid": "662050327564613301 4ec977",
  "CloudDns": "svc.ucs-connect.com",
  "CloudDnsList": [
    "svc.intersight.com",
    "svc-static1.intersight.com",
    "svc.ucs-connect.com",
    "svc-static1.ucs-connect.com"
  ],
  "CloudCert": "",
  "UserCloudCerts": {},
  "Identity": "662adb256f72613901e8bc19",
  "AccessKeyId": "98facfdbf3855bcfd340f2bbb0c388f8",
  "AccessKey": "",
  "PrivateAccessKey": "-----BEGIN RSA PRIVATE KEY-----
-CUT-
5Do\nD18Ta5YvuIYFLZrYlHLyCDOhS5O35AUEGNtEceiPhQjOCvRumyJD\n-----END RSA PRIVATE KEY-----\n",
  "CloudEnabled": true,
  "ReadOnlyMode": false,
  "LocalConfigLockout": false,
```

```
  "TunneledKVM": false,
  "HttpProxy": {
    "ProxyHost": "proxy.cisco.com",
    "ProxyPort": 8080,
    "Preference": 0,
    "ProxyType": "Manual",
    "Targets": [
      {
        "ProxyHost": "proxy.cisco.com",
        "ProxyPort": 8080,
        "Preference": 0
      }
    ]
  },
  "LogLevel": "info",
  "DbVersion": 1,
  "AutoUpgradeAdminState": "Automatic"
```

## Versões iniciando com 10.3(4a)M

# show system device-connector claim-info

```
N9k-Leaf-2# show system device-connector claim-info
  SerialNumber: FDO23021ZUJ
  SecurityToken:
  Duration: 0
  Message: Cannot fetch claim code for already claimed device
  Claim state: Claimed
  Claim time: 2024-02-09T15:38:57.561Z
  Claimed by: brvarney@cisco.com
  Account: ACI-DCRS-TAC
  Site name:
  Site ID:
```

# show system internal intersight info

```
# show system internal intersight info
Intersight connector.db Info:
ConnectionState         :Connected
ConnectionStateQual     :
AccountOwnershipState   :Claimed
AccountOwnershipUser    :brvarney@cisco.com
AccountOwnershipTime    :2024-02-09T15:38:57.561Z
AccountOwnershipId      :ACI-DCRS-TAC
DomainGroupMoid         :5eb2e1e47565612d3079fe9a
AccountMoid             :5eb2e1e47565612d3079fe92
CloudDns                :svc.ucs-connect.com
CloudDnsList:
        1.              :svc.ucs-connect.com
        2.              :svc.intersight.com
        3.              :svc-static1.intersight.com
        4.              :svc-static1.ucs-connect.com
```

```
Identity                :65c647116f72513501e75530
CloudEnabled            :true
ReadOnlyMode            :false
LocalConfigLockout      :false
TunneledKVM             :false
HttpProxy:
        ProxyHost       :proxy.cisco.com
        ProxyPort       :8080
        Preferenc       :0
        ProxyType       :Manual
    Target[1]:
        ProxyHost       :proxy.cisco.com
        ProxyPort       :8080
        Preference      :0
LogLevel                :info
DbVersion               :1
AutoUpgradeAdminState   :Automatic
```

## Ansible

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

```
 - name: Get intersight info
    nxos_command:
      commands:
      - show system internal intersight info
    register: intersightInfo_claimed
    retries: 10
    delay: 10
    until: intersightInfo.stdout is search("Connecte")

  - name: Display intersight info
    vars:
      msg: |-
           output from {{ inventory_hostname }}:
           {{ intersightInfo_claimed.stdout | join("") }}
    debug:
      msg: "{{ msg.split('\n') }}"
```

Aqui está a saída correspondente:

```
TASK [Get intersight info] ********************************************************************************
ok: [switch1]

TASK [Display intersight info] ****************************************************************************
ok: [switch1] => {
    "msg": [
        "output from switch1:",
        "Intersight connector.db Info:",
        "ConnectionState         :Connected",
        "ConnectionStateQual     :",
```

```
        "AccountOwnershipState   :Claimed",
        "AccountOwnershipUser    :vricci@cisco.com",
        "AccountOwnershipTime    :2024-02-10T01:00:28.516Z",
        "AccountOwnershipId      :vricci",
        "DomainGroupMoid         :5fcb98d97565612d33fdf1ae",
        "AccountMoid             :5fcb98d97565612d33fdf1ac",
        "CloudDns                :svc.intersight.com",
        "CloudDnsList:           ",
        "        1.              :svc.intersight.com",
        "        2.              :svc-static1.intersight.com",
        "        3.              :svc.ucs-connect.com",
        "        4.              :svc-static1.ucs-connect.com",
        "Identity                :65c6caac6f72613901f841c1",
        "CloudEnabled            :true",
        "ReadOnlyMode            :false",
        "LocalConfigLockout      :false",
        "TunneledKVM             :false",
        "HttpProxy:              ",
        "        ProxyHost       :proxy.cisco.com",
        "        ProxyPort       :80",
        "        Preferenc       :0",
        "        ProxyType       :Manual",
        "    Target[1]:          ",
        "        ProxyHost       :proxy.cisco.com",
        "        ProxyPort       :80",
        "        Preference      :0",
        "LogLevel                :info",
        "DbVersion               :1",
        "AutoUpgradeAdminState   :Automatic"
    ]
}
```

# Desabilitar Conector do Dispositivo

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | no feature intersight<br><br>Exemplo:<br><br>`switch(config)# no feature intersight` | 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.