

# Configurer et revendiquer la connectivité autonome Nexus pour Intersight

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Avantages de la connectivité](#)

[Vidéo Quickstart](#)

[Demander manuellement un périphérique NXOS](#)

[Vérification de connectivité](#)

[Vérification TLS avec OpenSSL Client](#)

[Vérification de l'accessibilité HTTPS](#)

[Configurer](#)

[Revendication du périphérique `withinintersight.com`](#)

[Sur le périphérique Nexus](#)

[Sur le portail Intersight](#)

[Revendication de un à plusieurs périphériques Nexus autonomes dans `intersight.com` en utilisant `Ansible@`](#)

[Configurez NXAPI Nexus \(utilisé uniquement si vous utilisez `ansible.netcommon.httpapi`\)](#)

[Générer des clés API Intersight](#)

[Exemple : `Ansibleinventory.yaml`](#)

[Exemple : `playbook.yaml`Execution](#)

[Vérifier](#)

[Sur le commutateur Nexus](#)

[Versions antérieures à 10.3\(4a\)M](#)

[Versions commençant par 10.3\(4a\)M](#)

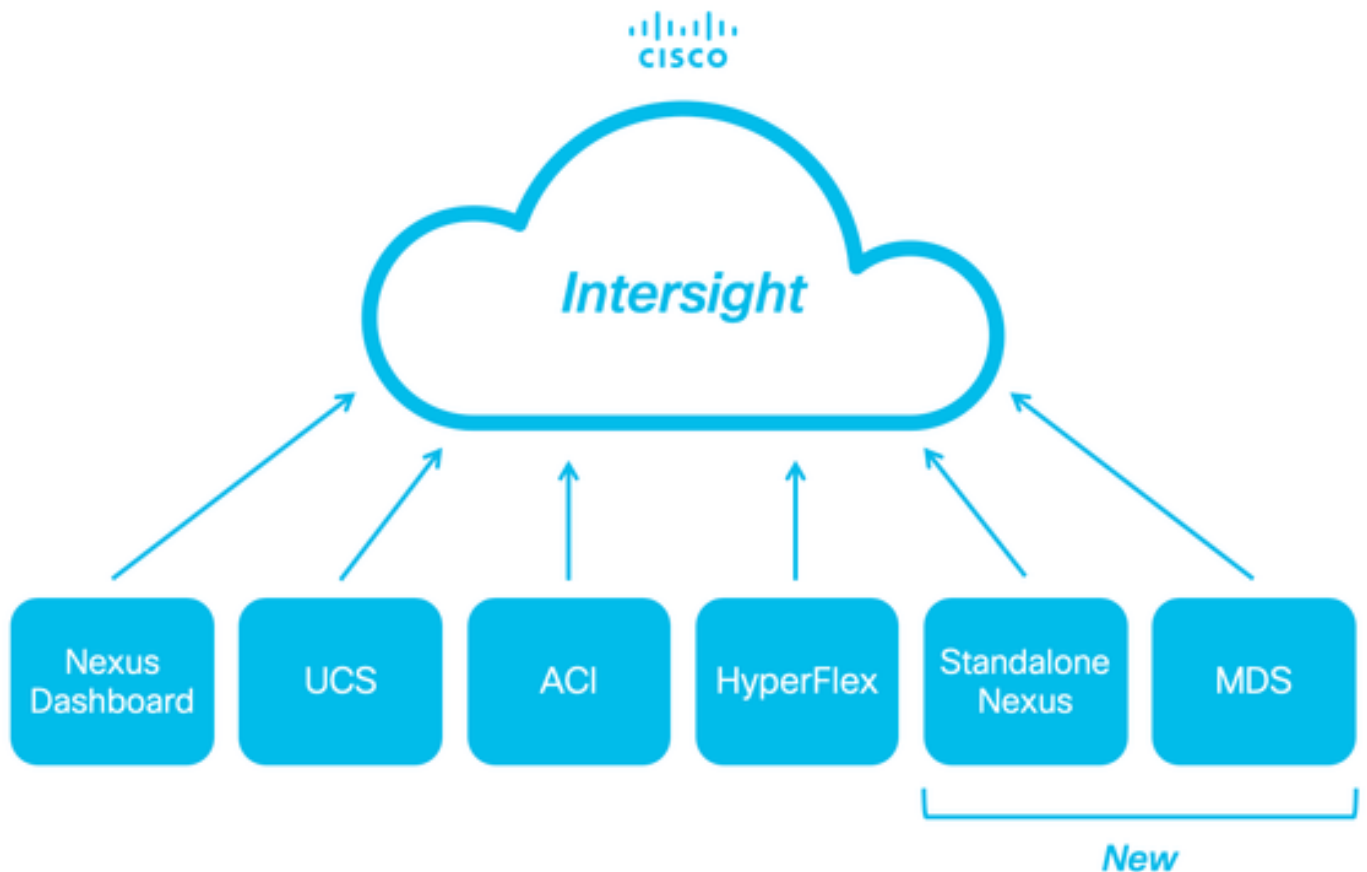
[Ansible](#)

[Désactiver le connecteur du périphérique](#)

---

## Introduction

Ce document décrit les étapes requises pour activer et réclamer des commutateurs Nexus autonomes dans Intersight pour une prise en charge améliorée du TAC Cisco.



## Conditions préalables

Vous devez disposer d'un compte sur [intersight.com](https://intersight.com), aucune licence n'est requise pour la demande de licence Cisco NX-OS®. Si un nouveau compte d'aperçu doit être créé, voir [Création de compte](#).

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Sur le commutateur Nexus autonome, NXDC présente les consignes et limitations suivantes :

- Cisco NX-OS doit exécuter la version 10.2(3)F ou ultérieure
- [DNS](#) doit être configuré sous le VRF (Virtual Routing and Forwarding) approprié
- `svc.intersight.com` doit être résolu et autoriser les connexions HTTPS lancées en sortie sur le port 443. Ceci peut être vérifié avec `curl`. Les requêtes ICMP (Internet Control Message Protocol) sont ignorées.
- Si un proxy est requis pour une connexion HTTPS à `svc.intersight.com`, le proxy peut être configuré dans la configuration NXDC (Nexus Switch Device Connector). Pour la configuration du proxy, référez-vous à [Configuration de NXDC](#).

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Cisco Intersight est une plate-forme d'opérations cloud qui comprend des fonctionnalités modulaires en option d'infrastructure avancée, d'optimisation de la charge de travail et de services Kubernetes. Visitez [Aperçu de l'aperçu](#) pour plus d'informations.

Les périphériques sont connectés au portail Intersight via un NXDC intégré à l'image Cisco NX-OS de chaque système. À partir de la version 10.2(3)F de Cisco NX-OS, la fonctionnalité Connecteur de périphérique est prise en charge. Elle permet aux périphériques connectés d'envoyer des informations et de recevoir des instructions de contrôle depuis le portail Cisco Intersight, via une connexion Internet sécurisée.

## Avantages de la connectivité

La connectivité Intersight offre les fonctionnalités et les avantages suivants aux plates-formes basées sur Cisco NX-OS :

- Collecte automatisée des données `show tech-support details` via la [résolution rapide des problèmes](#) (RPR pour les demandes de service TAC ouvertes)
- Collecte à la demande à distance des `show tech-support details`
- Fonctionnalités futures :
  - Ouverture de demandes de service TAC proactives basées sur la télémétrie ou une panne matérielle
  - Collecte à distance à la demande de commandes `show` individuelles et plus encore

## Vidéo Quickstart

Demander manuellement un périphérique NXOS

## Vérification de connectivité



Remarque : les réponses ping sont supprimées (les paquets ICMP sont abandonnés).

---

Afin de vérifier la connectivité TLS (Transport Layer Security) et HTTPS, activer bash et exécuter `openssl` et `curl` dans le VRF souhaité (`ip netns exec`) est recommandé.

! 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

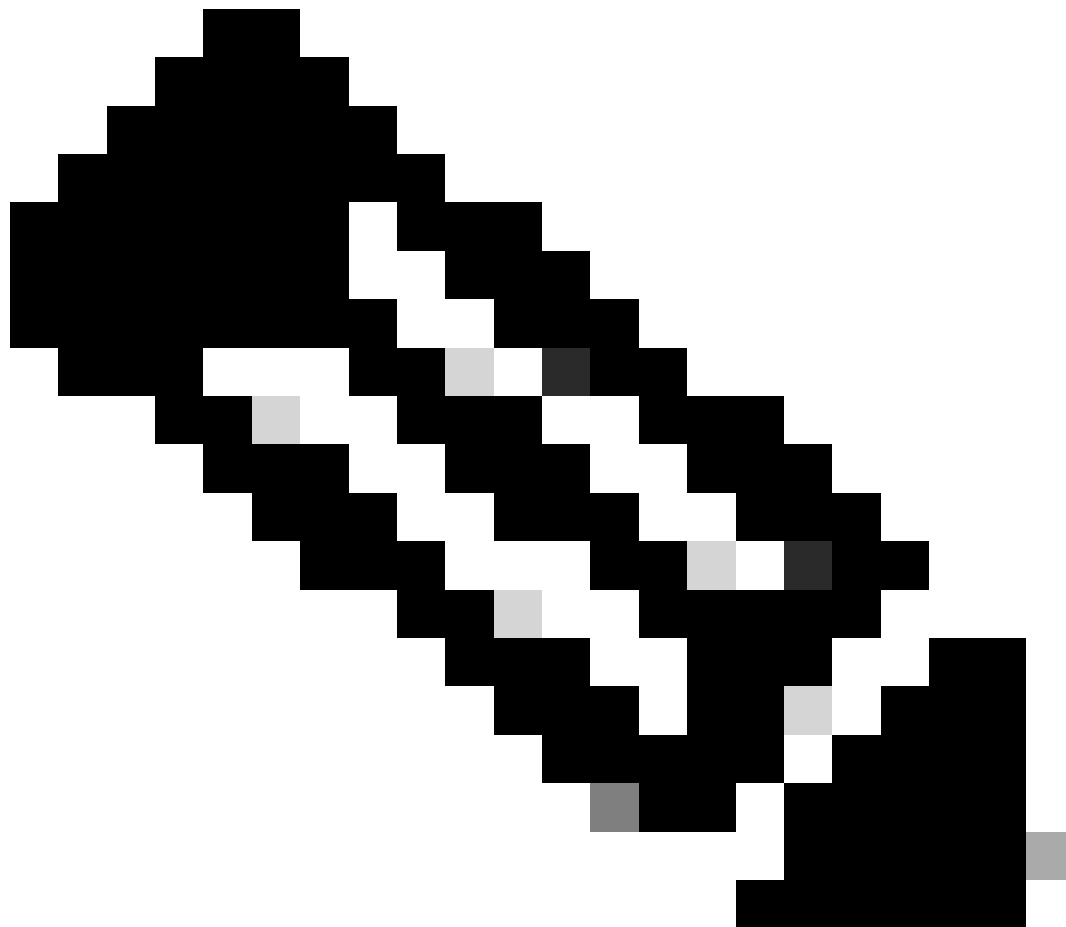
```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443 --proxy [protocol://
```

## Vérification TLS avec OpenSSL Client

Grâce à OpenSSL, vous pouvez vérifier la connectivité TLS avec `svc.intersight.com:443`. Une fois l'opération terminée, récupérez le certificat public signé par le serveur et affichez la chaîne de l'autorité de certification.

---



Remarque : l'exemple suivant exécute la commande `openssl s_client` dans la gestion VRF.  
Remplacez la valeur souhaitée dans la construction `ip netns exec`

---

```
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
MoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kg
U1NBIDiWnDggTTAxMB4XDTIzMDQwNTAwMDAwMFOXDTI0MDUwMzIzNTk10VowIzEh
MB8GA1UEAxMYdXMtZWZzdC0xLm1udGVyc21naHQuY29tMIIBIjANBgkqhkiG9w0B
AoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kn
BDM+MCNnmvgND1GnU6/t1jOC780QpKXr2ksbGC0FzHfMvNjEk9kMCUe179dummrs
p00FzvIrJGqYvkIXT5WLtiU9aP3+VSEWQ01kTeDHoDfLLJLON42cKjSkYt0jCTwE
poXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KI
e1f3tYBhuQK3y4DoSgg1/gptnU01NwSqMu4zXjI7neGyHnzjsPUyI8qi1XbPS9tV
KoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kw
HwYDVR0jBBgwFoAUUgbyOY4qJEhj1+js7UJWf5uWQE4UwHQYDVR0OBBYEFM7X7s7c
NoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kp
Z2h0LmNvbYIac3ZjLXN0YXRpYzEuaW50ZXJzaWdodC5jb22CGioudXMtZWZzdC0x
LoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K1
Y3MtY29ubmVjdC5jb22CE3N2Yy51Y3MtY29ubmVjdC5jb22CDm1udGVyc21naHQu
Y29tghJzdmMuaW50ZXJzaWdodC5jb20wDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjA7BgNVHR8ENDAyMDCGqLqAshipodHRwOi8v
YoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KI
BgZngQwBAGewdQYIKwYBBQUHAQEETBnMC0GCCsGAQUFBzABhiFodHRwOi8vb2Nz
coXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Ku
cjJtMDEuYw1hem9udHJ1c3QuY29tL3IybTAXLmN1cjAMBGNVHRMBAf8EAJAAMIIB
fgYKKwYBBAHweQIEAgSCAW4EggFqAwGAdwDuzdBk1dsaszVct520zR0iModGfLzs
3oXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K5
CSFqTpBj1Od0LQ4YuQIhA010VDrLJMM+9EtOwmZd8Q1MRHJ101r2VWmOTF6GGkCV
AHUAc9meiRtM1nigIH1HneayxhzQUV5xGSqMa4AQesF3crUAAAGHUp9i0wAABAMA
RjBEAiAFpPLvt7TN7mTRnQZ+FZLGR/G04KQqSjYuszDNPArt3wIgf/sQbQqNjCk7
joFuU9cEPYfNm7n1nZIFIRAK6UqG0AdgBIs0Nr2qZHNA/lagL6nTDrHFIBY1bd
LoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0K8
MXtts5t/C51Yw5peGAIGk0eFmxTptEfMkBTzi39vepUxb5meDvKaZdtXVvFpkCMw
DQYJKoZIhvcNAQELBQADggEBAN16HKZ9P6AIufr7qdNCcw+DXC1Y6dqX1KN0sCh+
UoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0KM
z5R1VV+81gN2HHiuUsEOFWHDbbhijGBjiJteFm0b1pruKHennx8HQYfC7bup4N5JH
YoXXXrXrkESkWgbQad1Eo3H545ZsIx+mu83r7Gmv5L3+WFKzfUmLgeB2+z1Dk0Kb
LKF16c+EN0Y76YaCV8dougjG3qD/b09VDx7dhvbSEECYuzbYyPDGnb7Drmhny0Eki
smLUZ3TVcCvPc+1dE/jrbBzPeIY7jGr8eL7masFCuZzn21M=
```

-----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...0.
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
---

```

## Vérification de l'accessibilité HTTPS

Afin de vérifier la connectivité HTTPS, utilisez la commande curl avec le -v verbose flag (affiche si un proxy est utilisé ou non).

---

Remarque : pour vérifier l'impact de l'activation ou de la désactivation d'un proxy, vous pouvez ajouter les options `--proxy [protocol://]host[:port]` OU `--no-proxy [protocol://]host[:port]`.

---

La construction `ip netns exec`

est utilisée pour exécuter une commande dans le VRF souhaité ; par exemple, pour la gestion du VRF `ip netns exec management`.

```
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 >
```

## Configurer

Demander le périphérique dans [intersight.com](https://intersight.com)

Afin de revendiquer une nouvelle cible dans Intersight, accomplissez les étapes mentionnées.

Sur le périphérique Nexus

Exécutez la commande Cisco NX-OS `show system device-connector claim-info`.



Remarque : pour les versions antérieures à NX-OS 10.3(4a), utilisez la commande « show intersight claim-info »

---



Remarque : les informations de demande générées par Nexus correspondent aux champs de demande Intersight suivants :

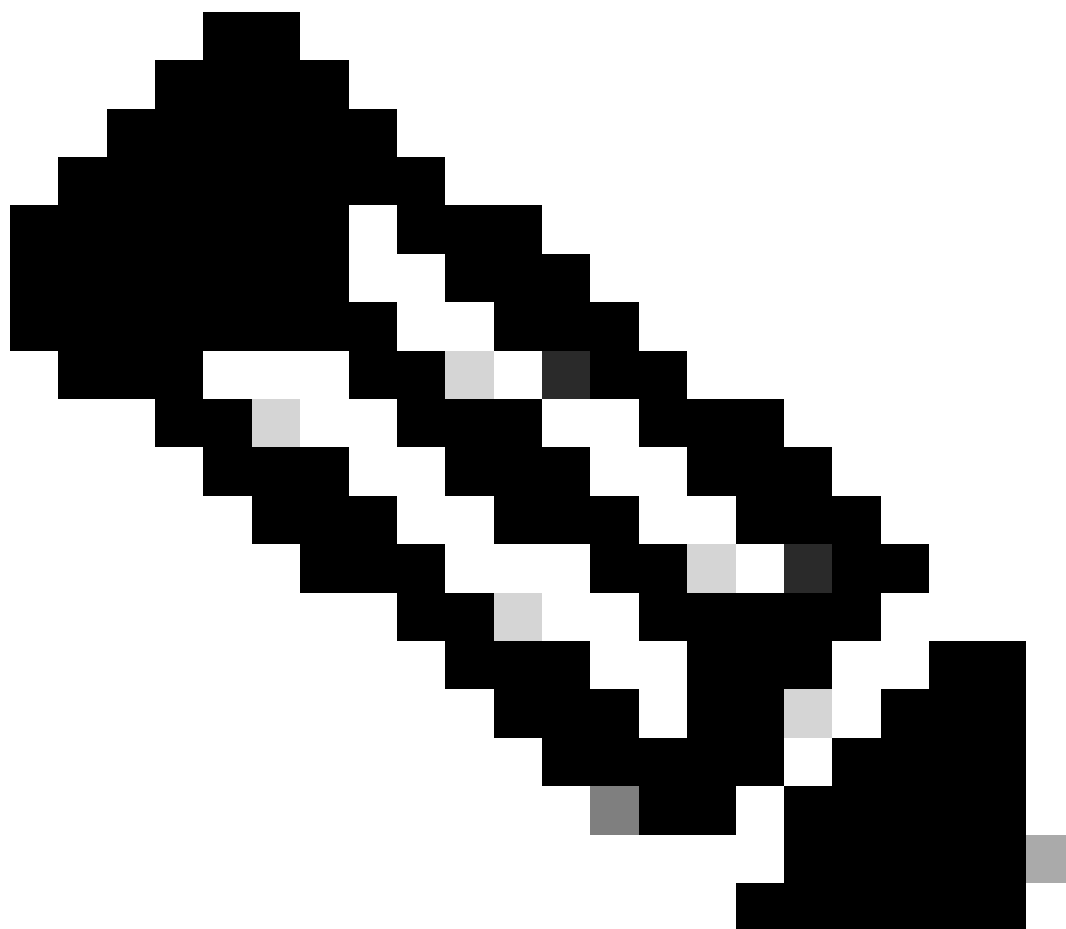
Numéro de série = ID de demande Intersight

Jeton de sécurité Device-ID = Intersight Code de demande

---

```
# show system device-connector claim-info
SerialNumber: F023021ZUJ
SecurityToken: 9FFD4FA94DCD
Duration: 599
Message:
Claim state: Not Claimed
```

La durée indiquée ici est en secondes.

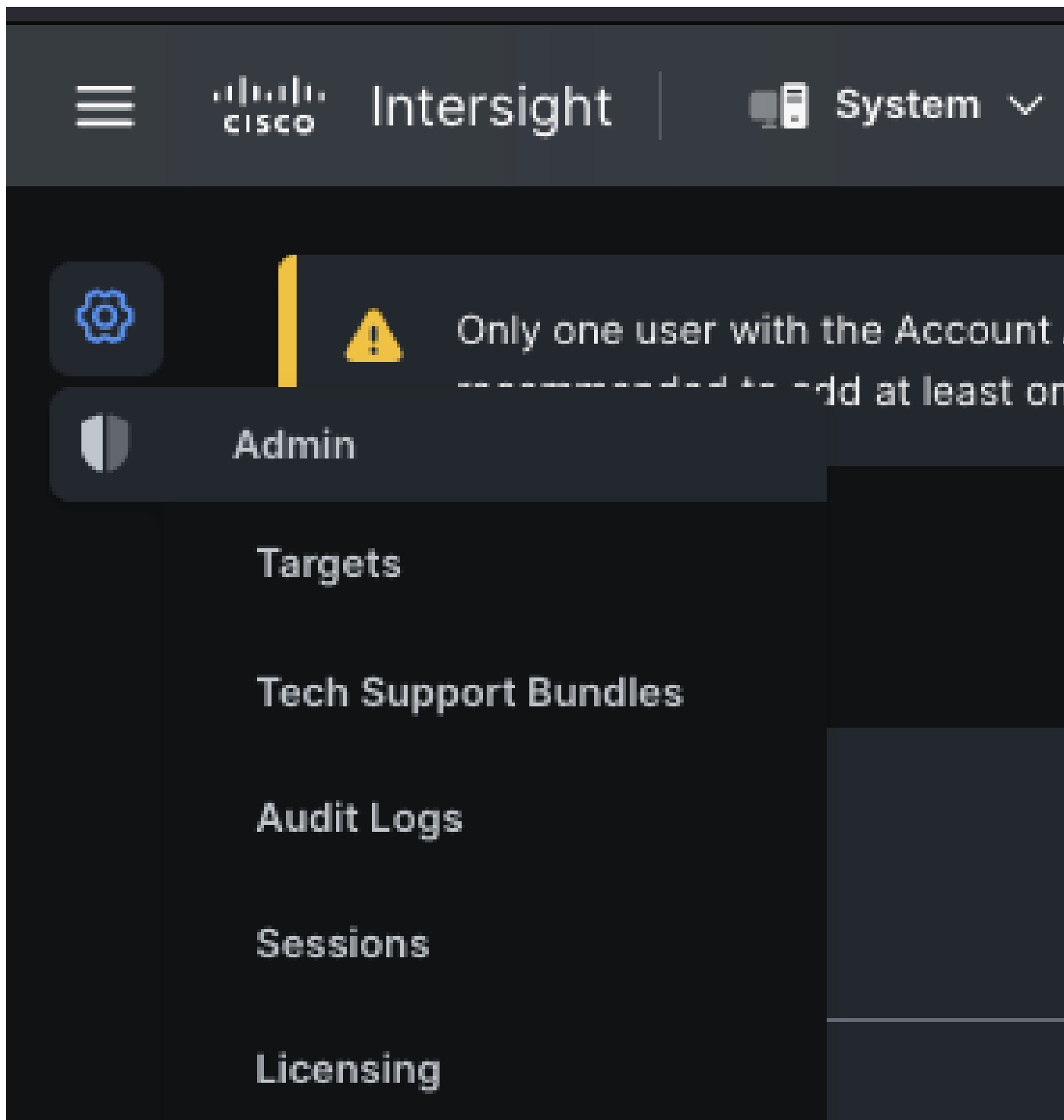


Remarque : la fonctionnalité de demande de remboursement de périphérique Cisco Intersight n'est pas disponible pour la région EMEA. Ces étapes ne s'appliquent qu'à la région Amérique du Nord.

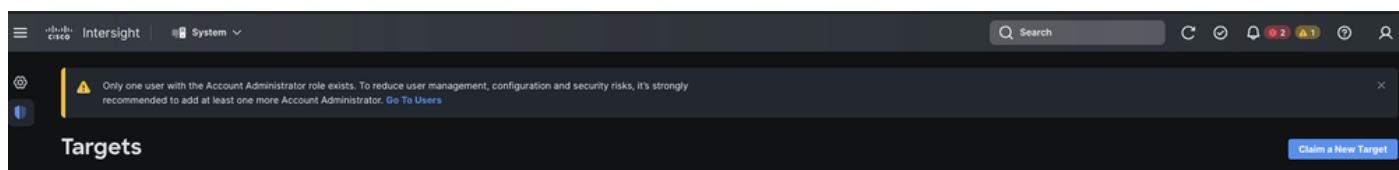
1. Dans les 10 minutes, connectez-vous à Intersight avec les privilèges d'administrateur de compte, d'administrateur de périphérique ou de technicien de périphérique.
2. Dans la liste déroulante Sélectionneur de service, sélectionnez Système.



3. Accédez à ADMIN > Targets > Claim a New Target.



3.1. Cliquez sur Demander une nouvelle cible comme illustré dans l'image.



4. Choisissez Disponible pour la demande et choisissez le type de cible (par exemple, Réseau) que vous souhaitez demander. Cliquez sur Démarrer.

⚙️

⚠️ 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

Cisco Nexus Switch

Cisco APIC

Cisco Cloud APIC

Cisco DCNM

Cisco Nexus Dashboard

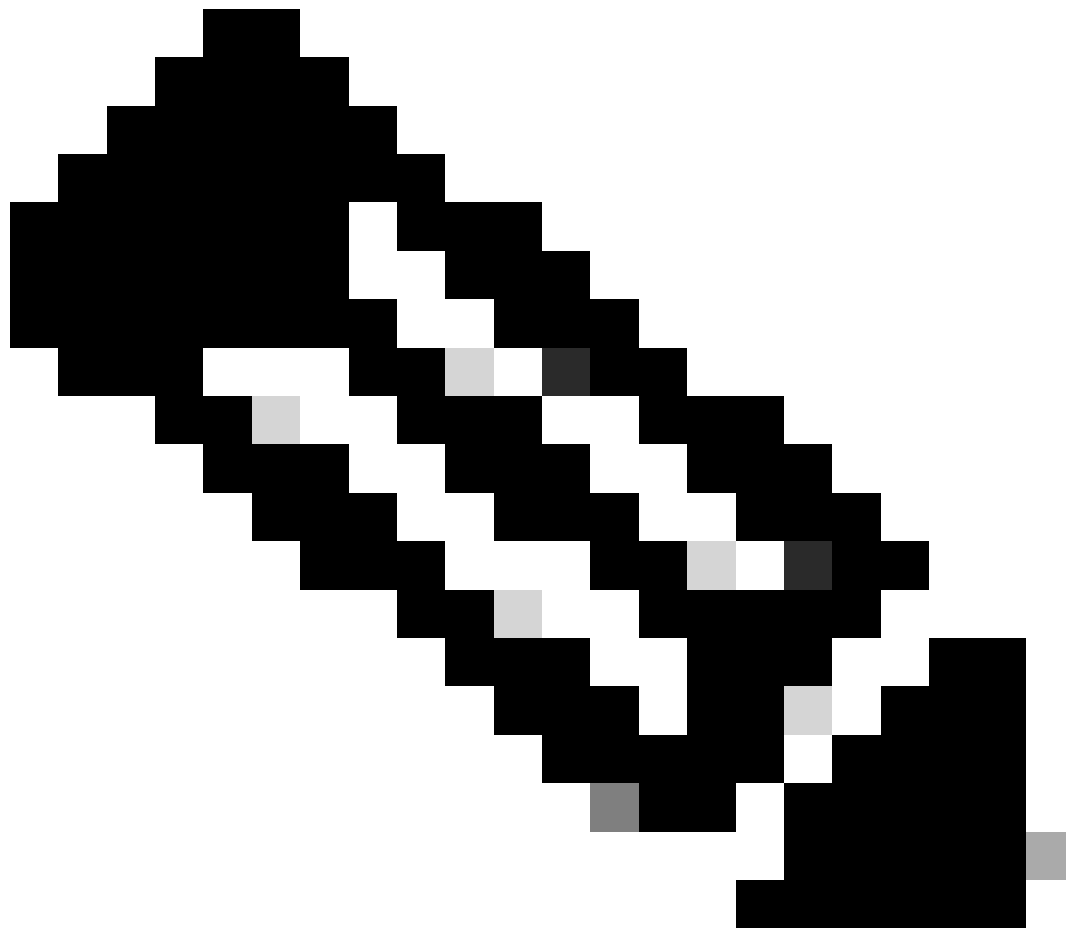
[Cancel](#) [Start](#)

5. Entrez les détails requis et cliquez sur Demande afin de terminer le traitement de demande.




Remarque : le jeton de sécurité sur le commutateur est utilisé comme code de revendication et le numéro de série du commutateur est l'ID de périphérique.


---



Remarque : le jeton de sécurité expire. Vous devez terminer la demande avant ou le système vous invite à en régénérer une.

---



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

[Details](#)

Revendication d'un à plusieurs périphériques Nexus autonomes dans [intersight.com](https://intersight.com) en utilisant Ansible®

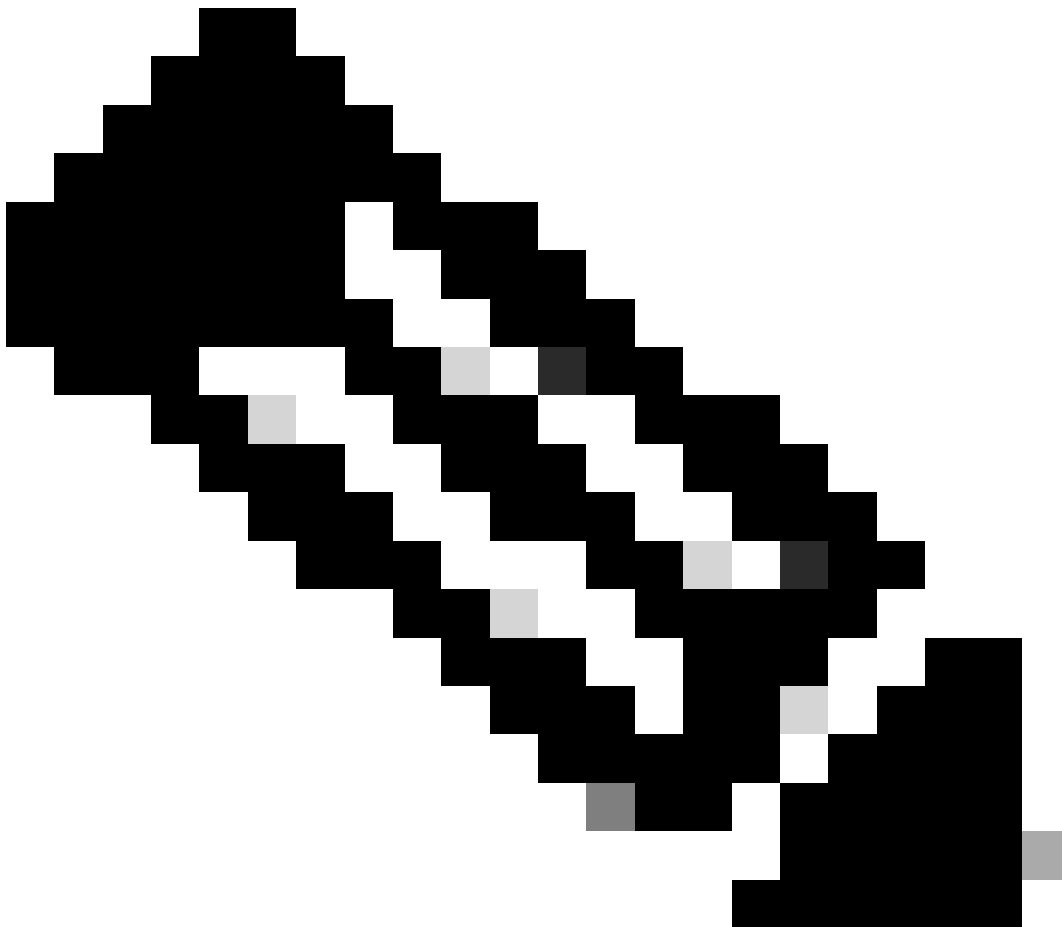
Afin de revendiquer un ou plusieurs périphériques Nexus, un guide Ansible peut être exécuté.



- L'inventaire et le guide de vente ansible peuvent être clonés à partir de <https://github.com/datacenter/ansible-intersight-nxos>.
- Dans l'Ansible `inventory.yaml`, le type `ansible_connection` est défini sur `ansible.netcommon.network_cli` afin d'envoyer des commandes au commutateur Nexus. Il peut être remplacé par `ansible.netcommon.httpapi` afin de permettre la connectivité via NXAPI.
- Une connexion fiable au point de terminaison Intersight nécessite une clé API, qui peut être générée à partir de votre compte `intersight.com`.

Configurer Nexus NXAPI (utilisé uniquement en cas d'utilisation de `ansible.netcommon.httpapi`)

---



Remarque : dans le cas où un proxy de niveau système est configuré (`HTTP(S)_PROXY`) et qu'Ansible ne doit pas utiliser de proxy pour se connecter au point d'extrémité NXAPI de Nexus, il est souhaitable de définir `ansible_httpapi_use_proxy: False` (la valeur par défaut est `True`).

---

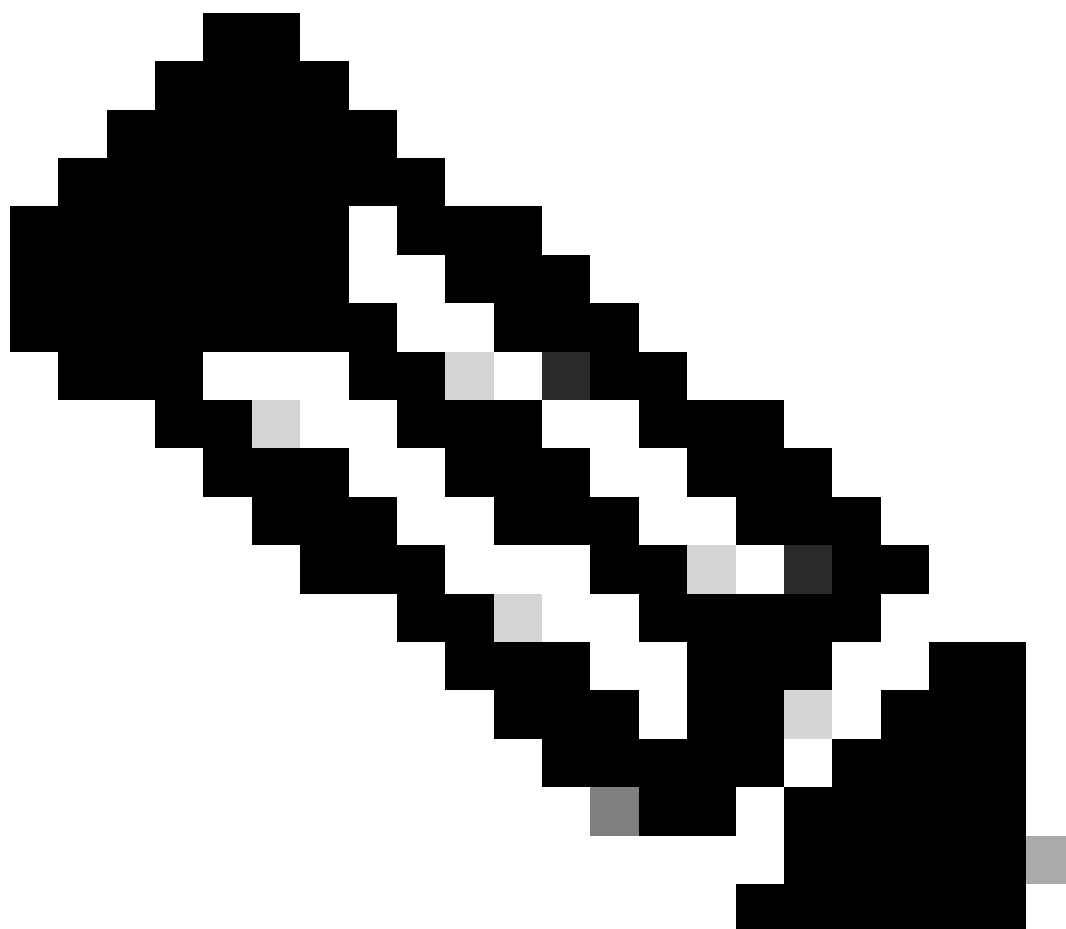
```
# configure terminal
# cfeature nxapi
```

```
# 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
```

Afin de vérifier indépendamment la connectivité HTTP au point d'extrémité NXAPI, vous pouvez tenter d'envoyer un `show clock`. Dans l'exemple suivant, le commutateur authentifie le client à l'aide de l'authentification de base. Il est également possible de configurer le serveur NXAPI afin d'authentifier les clients sur la base du certificat utilisateur X.509.

---



---

Remarque : le hachage d'authentification de base est obtenu à partir du codage base64 de username:password. Dans cet exemple, le codage admin:cisco!123 base64 est YWRtaW46Y2lzY28hMTIz.

---

```
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"  
    }  
  }'  
'
```

Réponse à la boucle :

```
* 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:xRYwR011Tra64Vf0MVuD4oI4=; Secure; HttpOnly;  
< anticrsrf: /i3vzCvxh0r4w2IrKP+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
}%
```

## Générer des clés API Intersight

Reportez-vous à la section [README.md](#) sur la façon d'obtenir la clé API à partir de la Intersight System

> Settings > API keys > Generate API Key.

The screenshot shows the Cisco Intersight Settings page. The top navigation bar includes the Cisco logo, 'Intersight', and 'System'. A search bar and several utility icons are also present. A warning message is displayed at the top: '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'. The main content area is titled 'Settings' and features a sidebar with various configuration options. The 'API Keys' section is active, showing a 'Generate API Key' button and a table with the following columns: Description, API Key ID, Purpose, Cre..., Email, Role, and Identity Provider. The table is currently empty, displaying 'NO ITEMS AVAILABLE'.

# 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

Exemple : Ansible `inventory.yaml`



Remarque : dans l'exemple suivant, Ansible a été configuré afin d'ignorer les paramètres proxy du système d'exploitation avec `ansible_httpapi_use_proxy: False`. Si vous avez besoin que votre serveur Ansible utilise un proxy pour atteindre le commutateur, vous pouvez supprimer cette configuration ou la définir sur `True` (par défaut).

---

---

Remarque : l'ID de clé API est une chaîne. La clé privée de l'API inclut le chemin d'accès complet à un fichier qui contient la clé privée. Pour l'environnement de production, il est recommandé d'utiliser le coffre-fort Ansible.

---

```
---
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"
...
```

## Exemple :playbook.yml exécution

Pour plus d'informations sur la programmation de périphériques Nexus autonomes avec Ansible, reportez-vous à la section Applications/Using Ansible avec Cisco NX-OS du [Guide de programmabilité NX-OS de la gamme Cisco Nexus 9000](#) pour votre version actuelle.

```
> 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 running configuration
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

## Vérifier

Afin de vérifier la revendication d'une nouvelle cible, procédez comme suit :

### Sur le commutateur Nexus

Versions antérieures à 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": "6620503275646133014ec978",  
  "AccountMoid": "6620503275646133014ec977",  
  "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\nD18Ta5YvuIYFLZrY1HLyCDOhS5035AUEGNTeCeIphQjOCvRumyJD\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"
```

## Versions commençant par 10.3(4a)M

```
# show system device-connector claim-info
```

```
N9k-Leaf-2# show system device-connector claim-info
SerialNumber: FD023021ZUJ
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
  Preference             :0
  ProxyType              :Manual
  Target[1]:
    ProxyHost            :proxy.cisco.com
    ProxyPort            :8080
    Preference           :0
LogLevel                :info
DbVersion               :1
AutoUpgradeAdminState  :Automatic

```

## Ansible

Il est possible d'ajouter une tâche à la fin de la `playbook.yaml` commande afin d'obtenir les informations d'aperçu du commutateur.

```

- 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') }}"

```

Voici le résultat correspondant :

```

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"
]
}

```

## Désactiver le connecteur du périphérique

	Commande ou action	Objectif
Étape 1	aucune visibilité de fonctionnalité  Exemple :  switch(config)# no feature intersight	Désactive le processus d'analyse et supprime toute la configuration NXDC et le magasin de journaux.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.