

Standalone Nexus configureren en claimen voor intersight-connectiviteit

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Connectiviteitsvoordelen](#)

[Quickstart-video](#)

[Handmatig een NXOS-apparaat claimen](#)

[Connectiviteitsverificatie](#)

[TLS-verificatie met OpenSSL-client](#)

[HTTPS-toegangsverificatie](#)

[Configureren](#)

[Het apparaat claimen withinintersight.com](#)

[Op het Nexus-apparaat](#)

[Op Intersight-portal](#)

[Claim One naar veel standalone Nexus-apparaten binnen intersight.com met behulp van Ansible@](#)

[Nexus NXAPI configureren \(alleen gebruikt als ansible.netcommon.httpapi wordt gebruikt\)](#)

[Intersight API-toetsen genereren](#)

[Voorbeeld: Ansibleinventaris.yaml](#)

[Voorbeeld:playbook.yamlExecution](#)

[Verifiëren](#)

[Op de Nexus Switch](#)

[releases voorafgaand aan 10.3\(4a\)M](#)

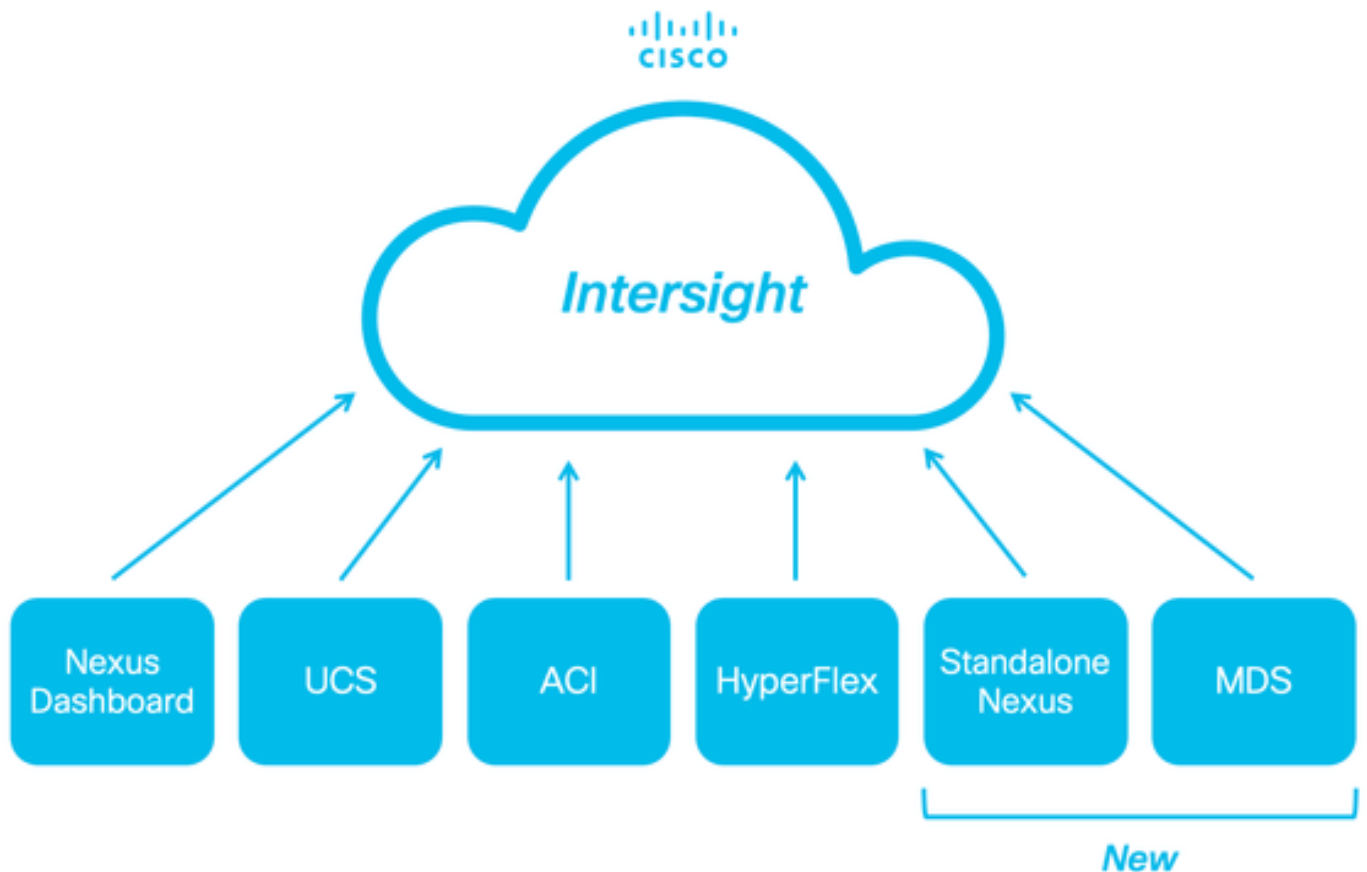
[releases die beginnen met 10.3\(4a\)M](#)

[anabel](#)

[Apparaatconnector uitschakelen](#)

Inleiding

Dit document beschrijft de stappen die nodig zijn om standalone Nexus switch(s) in Intersight in te schakelen en te claimen voor uitgebreide Cisco TAC-ondersteuning.



Voorwaarden

U moet een account hebben op intersight.com, er is geen licentie vereist voor een claim van Cisco NX-OS®. Als er een nieuwe Intersight-account moet worden aangemaakt, zie [Account aanmaken](#).

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Op de Standalone Nexus switch, NXDC heeft deze richtlijnen en beperkingen:

- Cisco NX-OS moet softwarerelease 10.2(3)F of hoger zijn
- [DNS](#) moet worden geconfigureerd onder de juiste virtuele routing en doorsturen (VRF)
- `svc.intersight.com` moet opgelost worden en uitgaande geïnitieerde HTTPS-verbindingen op poort 443 toestaan. Dit kan worden gecontroleerd met `openssl` en **krullen**. ICMP-verzoeken (Internet Control Message Protocol) worden genegeerd.
 - Als er een proxy vereist is voor een HTTPS-verbinding naar `svc.intersight.com`HST, kan de proxy worden geconfigureerd in de Nexus Switch Device Connector (NXDC)-configuratie. Raadpleeg voor proxyconfiguratie [NXDC configureren](#).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Intersight is een cloud-operationeel platform dat bestaat uit optionele, modulaire mogelijkheden van geavanceerde infrastructuur, werklastoptimalisatie en Kubernetes-services. Bezoek [Intersight Overzicht](#) voor meer informatie.

Apparaten worden aangesloten op het Intersight-portal via een NXDC die is ingesloten in de Cisco NX-OS-afbeelding van elk systeem. Beginnend met Cisco NX-OS release 10.2(3)F wordt de voorziening Device Connector ondersteund die een veilige manier biedt waarop de aangesloten apparaten informatie kunnen verzenden en controle-instructies kunnen ontvangen van het Cisco Intersight-portal, met behulp van een beveiligde internetverbinding.

Connectiviteitsvoordelen

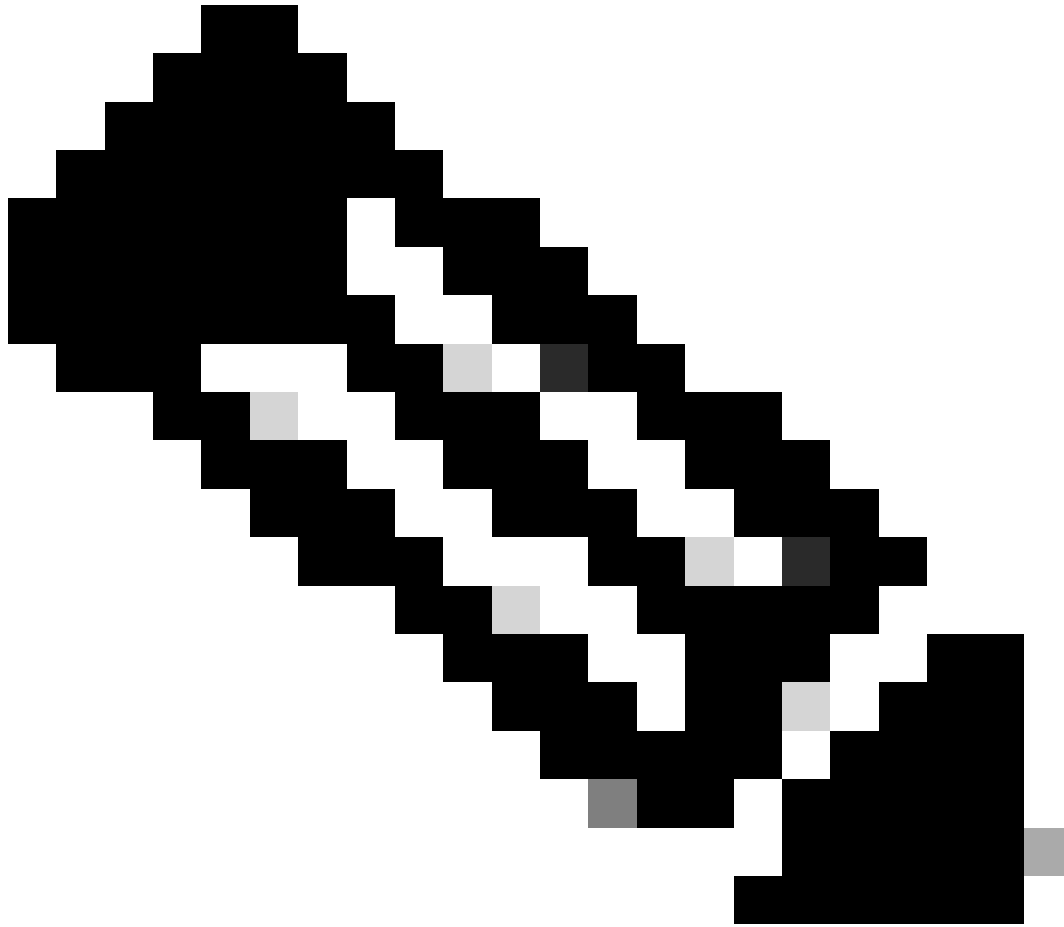
Intersight-connectiviteit biedt deze functies en voordelen voor de op Cisco NX-OS gebaseerde platforms:

- Geautomatiseerde verzameling van gegevens show tech-support details via [snelle probleemoplossing](#) (RPR voor de geopende TAC-serviceaanvragen)
- Remote-on-demand verzameling van show tech-support details
- Toekomstige functies zijn onder meer:
 - Proactieve TAC SR's openen op basis van telemetrie of hardwarestoring
 - Remote on-demand verzameling van individuele showopdrachten en meer

Quickstart-video

Handmatig een NXOS-apparaat claimen

Connectiviteitsverificatie



Opmerking: ping-reacties worden onderdrukt (ICMP-pakketten worden verbroken).

Om de connectiviteit van Transport Layer Security (TLS) en HTTPS te controleren, wordt het inschakelen van bash en het uitvoeren openssl en het uitvoeren van curl opdrachten in de gewenste VRF (ip netns exec <VRF>) aanbevolen.

! Enable bash

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

! Verify TLS

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

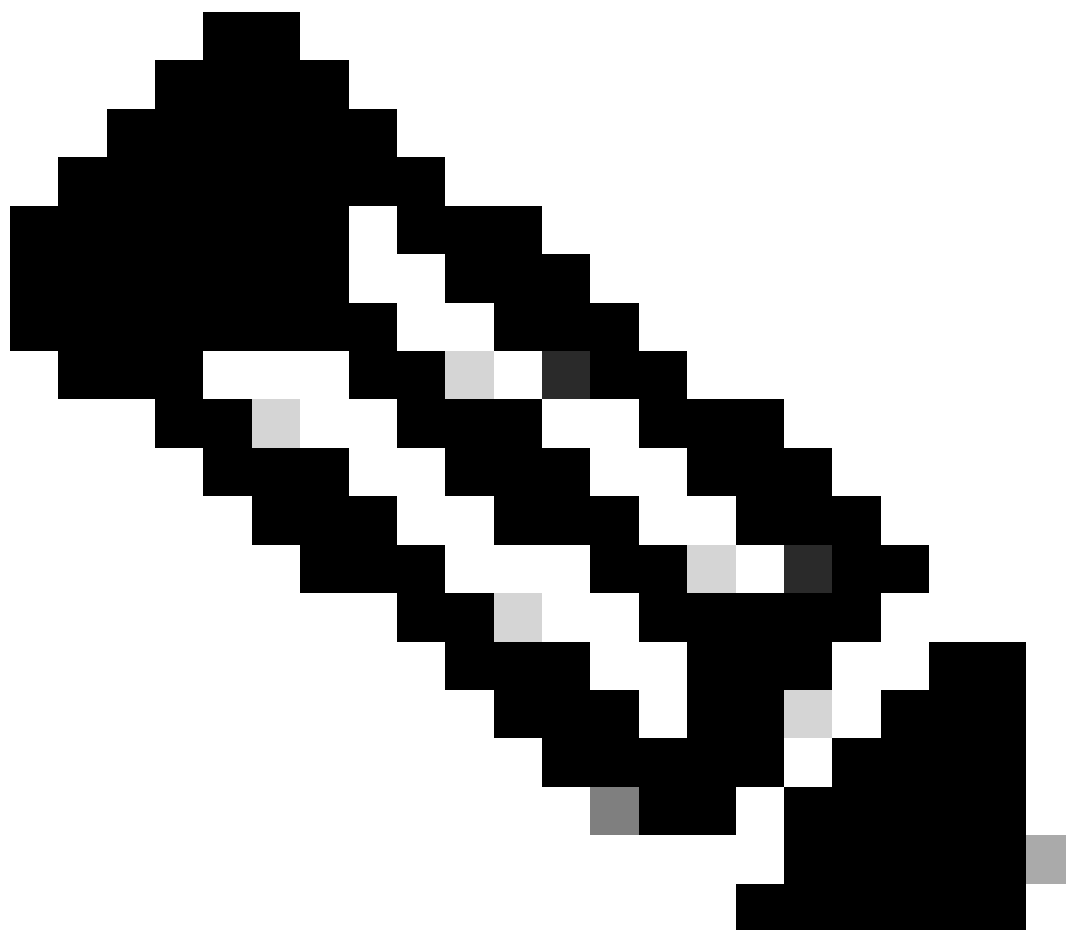
! Verify https

```
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]
```

TLS-verificatie met OpenSSL-client

Met OpenSSL kunt u de TLS-verbinding controleren op svc.intersight.com:443. Indien geslaagd, haal het openbare ondertekende certificaat door de server terug en toon de ketting van de Certificaatautoriteit.

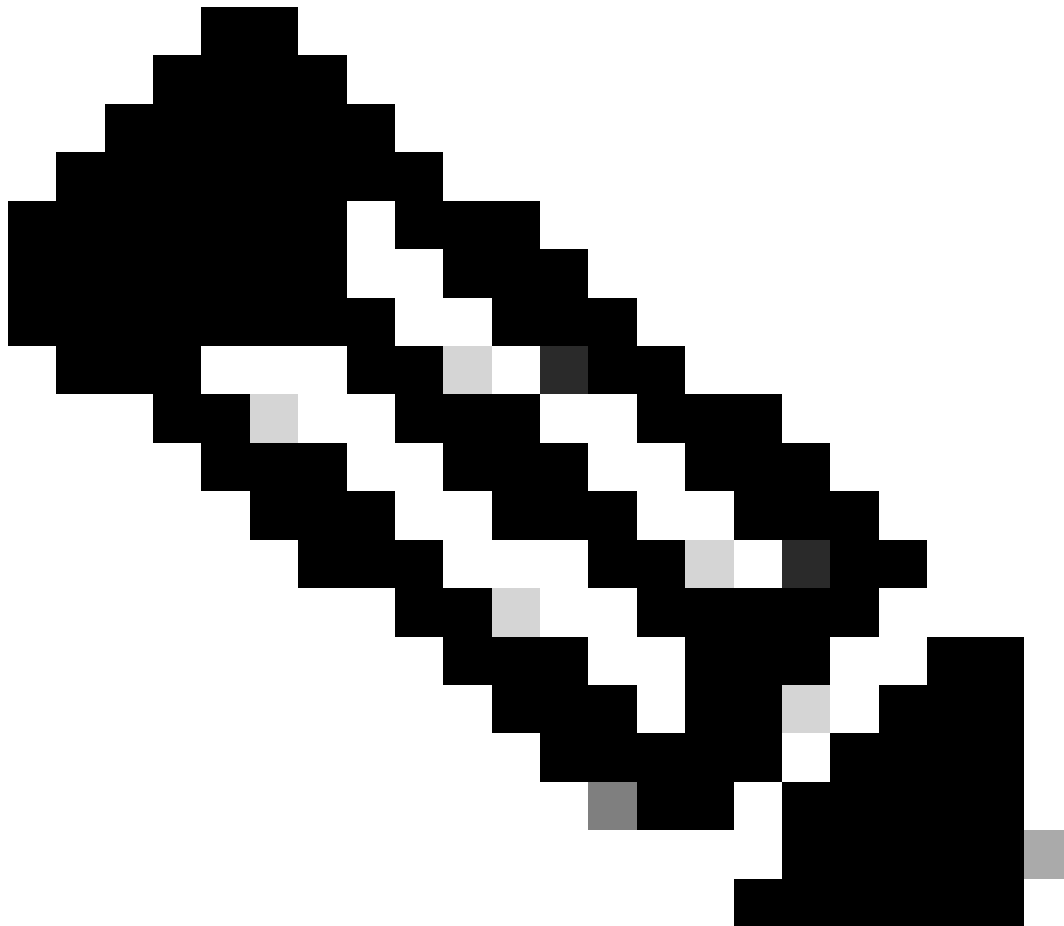


Opmerking: het volgende voorbeeld voert de opdracht uit in hetopenssl s_client VRF-beheer. Vervang de gewenste instellingen in het ip netns exec <VRF> concept.

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

HTTPS-toegangsverificatie

Om de connectiviteit te controleren HTTPS, gebruik het **curl** bevel met **-v** verbose flag (toont of een volmacht of niet wordt gebruikt).



Opmerking: om het effect van het in- of uitschakelen van een proxy te controleren, kunt u de opties `--proxy [protocol://]host[:port]` of `--noproxy [protocol://]host[:port]` toevoegen.

Het concept ip netns exec <VRF> wordt gebruikt om krul in de gewenste VRF uit te voeren; bijvoorbeeld ip netns exec management voor VRF-beheer.

```
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 >

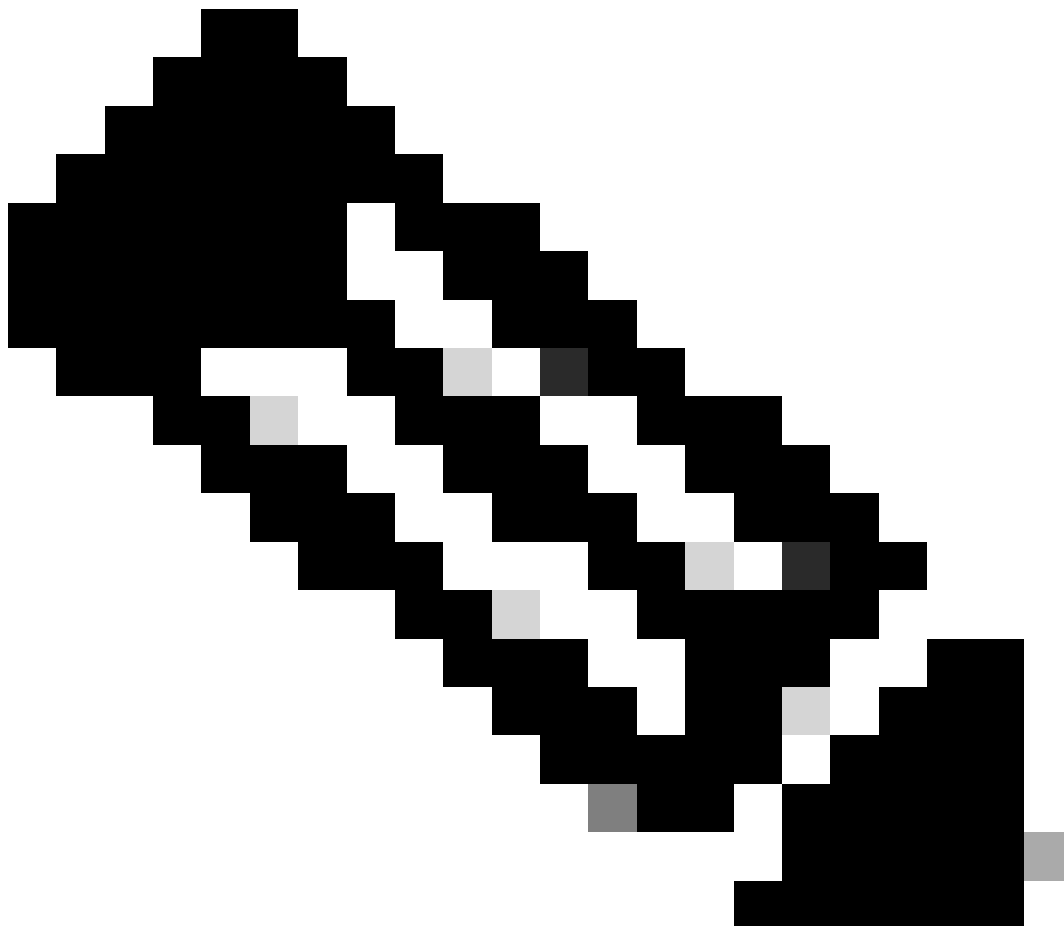
Configureren

Het apparaat claimen binnen intersight.com

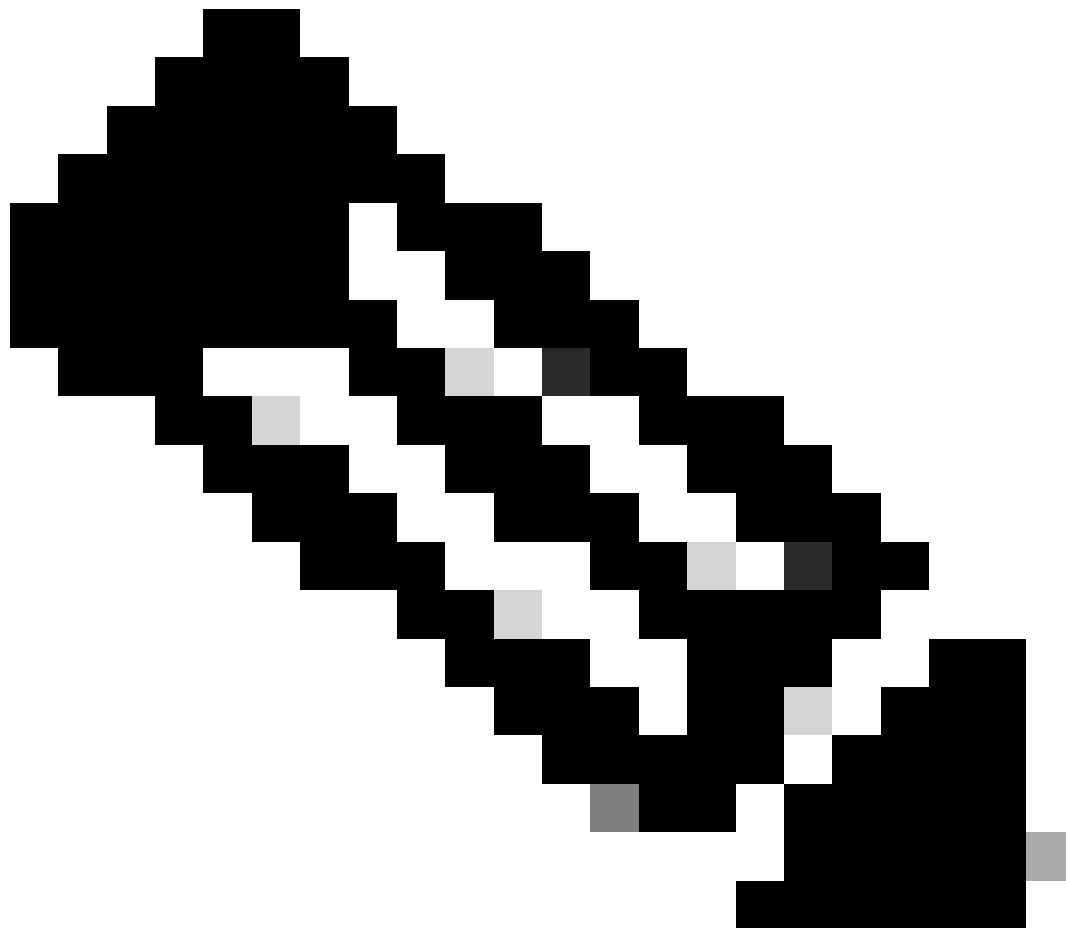
Om een nieuw doel in Intersight te claimen, voer de genoemde stappen uit.

Op het Nexus-apparaat

Geef de opdracht Cisco NX-OS uit show system device-connector claim-info.



Opmerking: voor releases voorafgaand aan NX-OS 10.3(4a) gebruik de opdracht "show intersight claim-info"



Opmerking: Nexus genereerde claiminfo-kaarten voor deze intersight claimvelden:

Serienummer = Intersight **Claim ID**

Device-ID security token = **code** voor **aanvraag** van **Intersight**

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

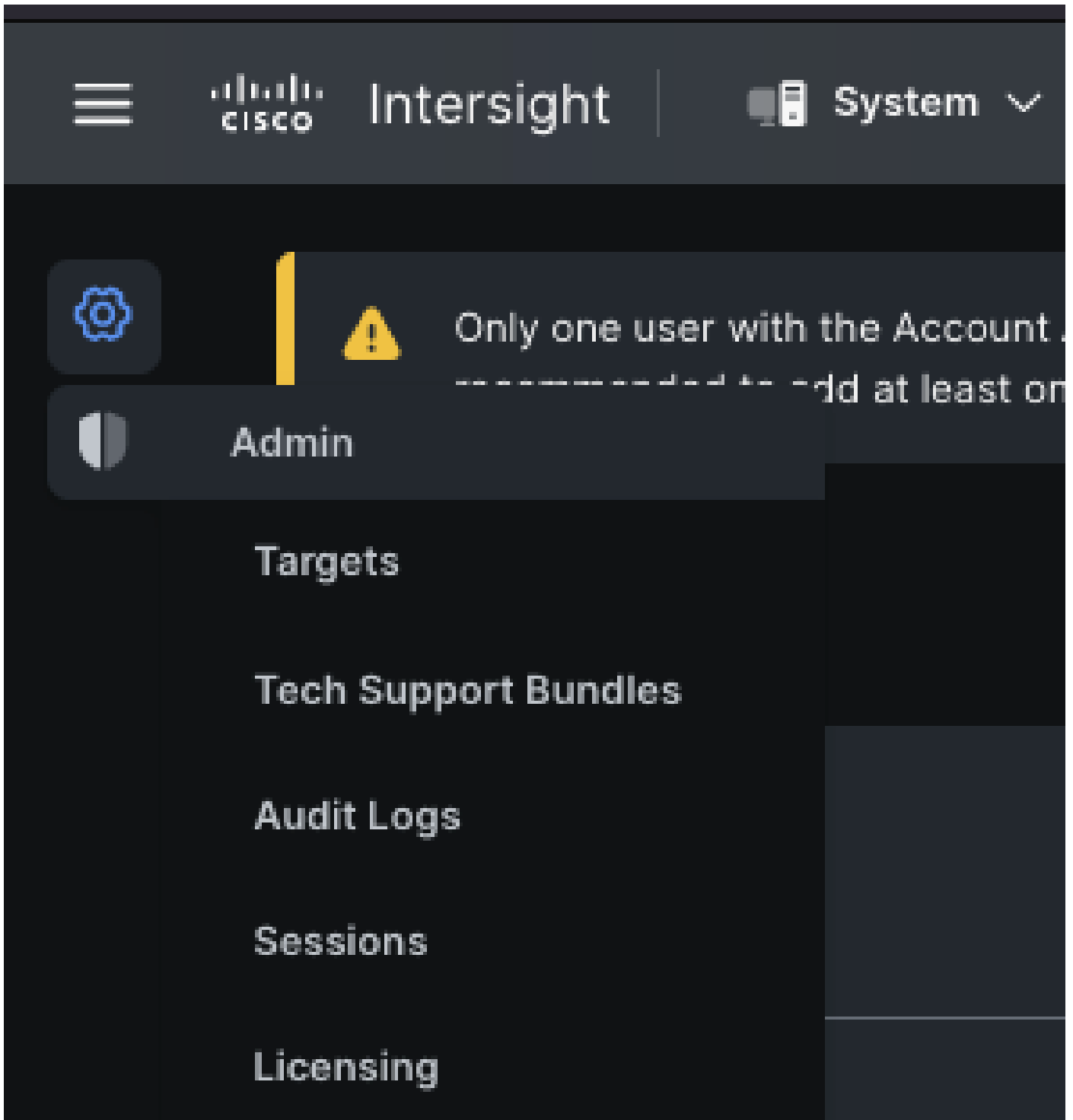
De hier gerapporteerde **duur** is in seconden.

On Intersight-portal

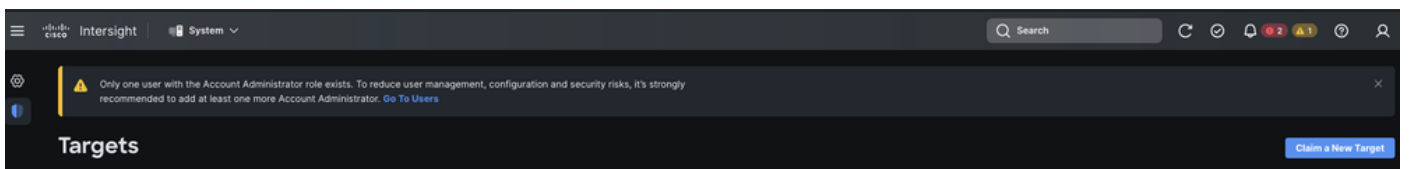
1. Meld u binnen 10 minuten aan bij **Interview** met de accountbeheerder, de apparaatbeheerder of de rechten van de apparaattechnicus.
2. Kies **System in** de vervolgkeuzelijst **Service Selector**.



3. Navigeer naar ADMIN > Targets > Claim a New Target.



3.1. Klik op **Claim a New Target** zoals in de afbeelding.



4. Kies **Beschikbaar voor opeisen** en kies het **doeltype** (bijvoorbeeld Network) dat u wilt opeisen. Klik op **Start**.



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

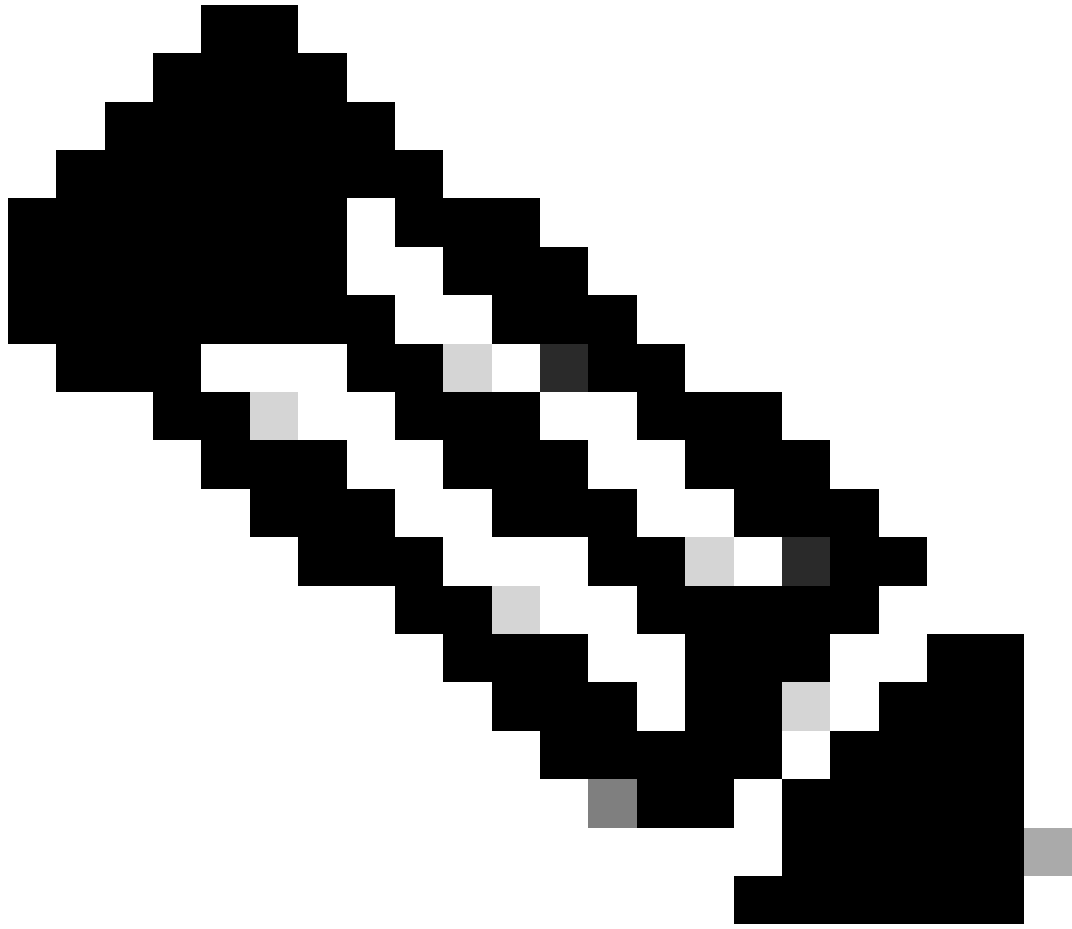
🔍 Search

Network

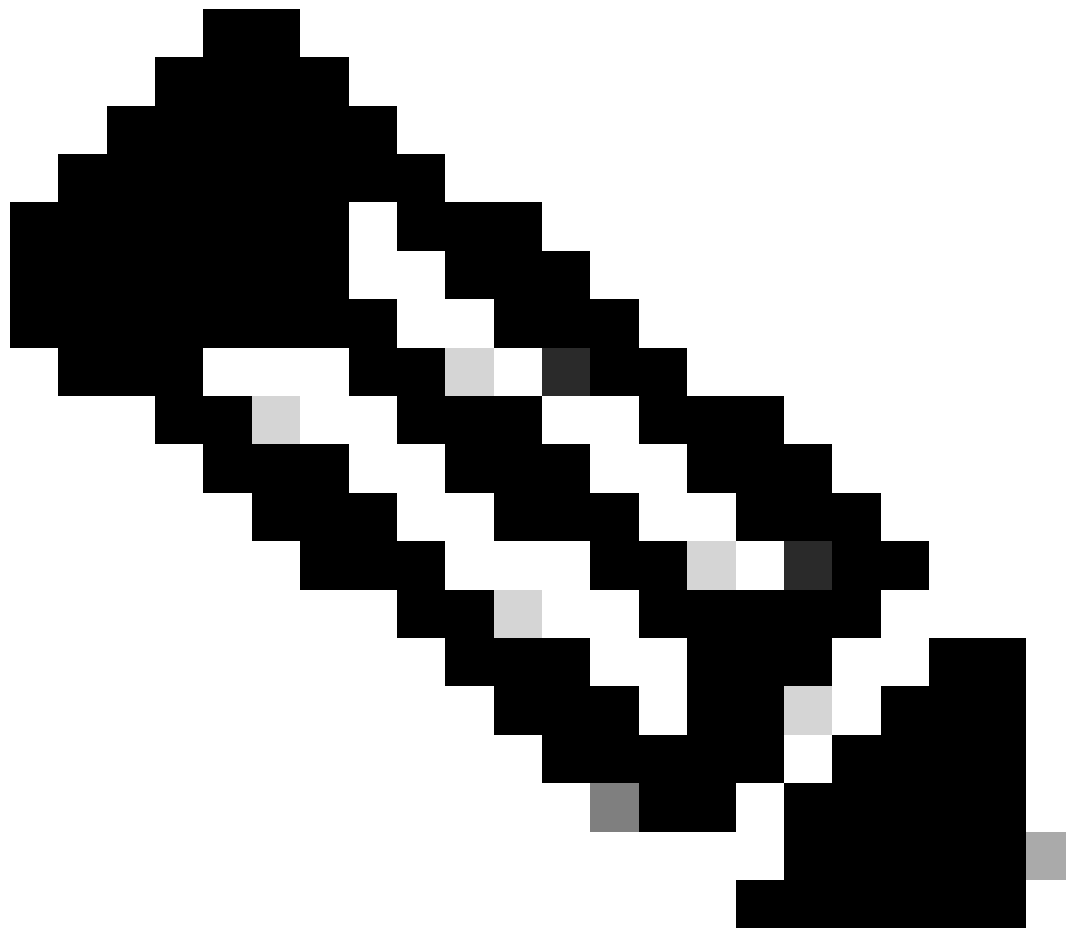
| | | |
|----------------------|---|---------------------------|
| Cisco MDS Switch | <input checked="" type="checkbox"/> Cisco Nexus Switch | Cisco APIC |
| Cisco Cloud APIC | Cisco DCNM | Cisco Nexus Dashboard |

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

5. Voer de vereiste gegevens in en klik op **Claim** om de claimprocedure te voltooien.



Opmerking: het **beveiligingstoken** op de switch wordt gebruikt als de claimcode en het **serienummer** van de switch is de apparaat-ID.



Opmerking: het beveiligingstoken verloopt. U moet de claim voltooien voordat of het systeem u vraagt om er een te regenereren.



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

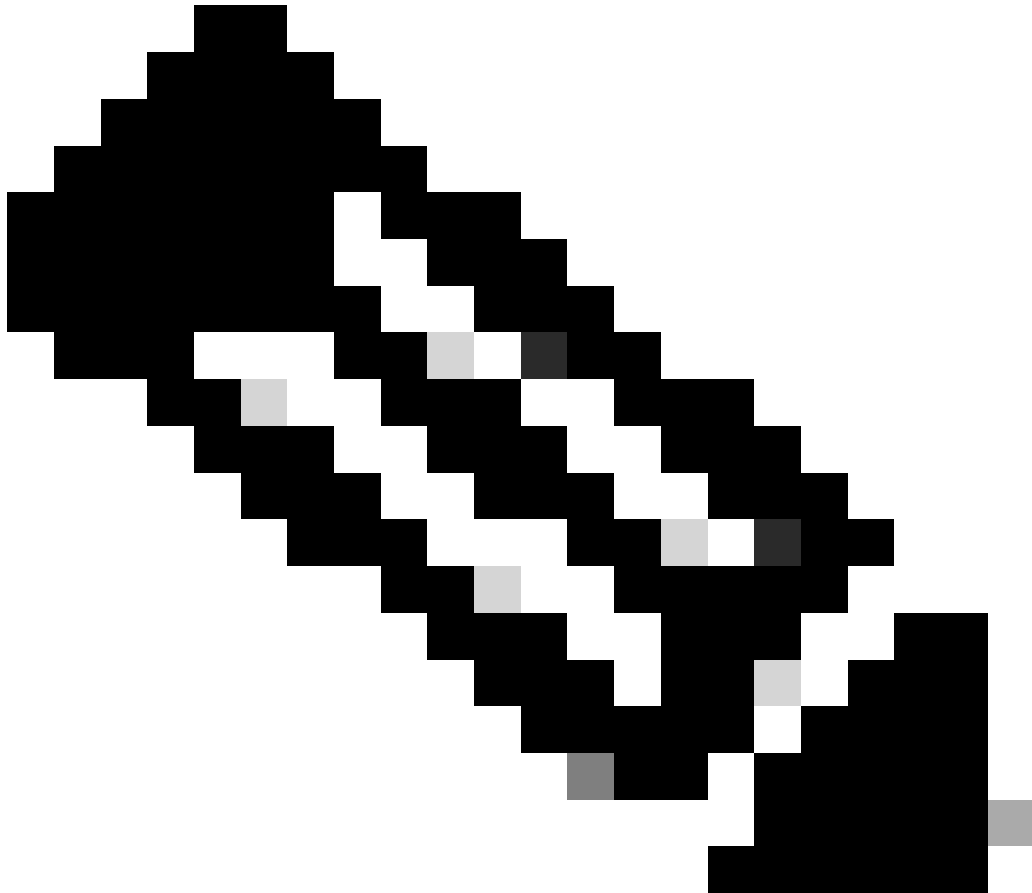


[Details](#)

Om te kunnen claimen dat er één of meerdere Nexus apparaten zijn, kan er een Ansible playbook worden uitgevoerd.

- De ansible inventaris en de playbook kunnen worden gekloond vanaf <https://github.com/datacenter/ansible-intersight-nxos>.
- In de Ansible inventory.yaml is hetansible_connection type ingesteld op ansible.netcommon.network_cli om opdrachten naar de Nexus switch te sturen. Dit kan worden gewijzigd ansible.netcommon.httpapi om connectiviteit via NXAPI mogelijk te maken.
- Een zichtbare verbinding met het Intersight-eindpunt vereist een API-sleutel, die kan worden gegenereerd vanuit uw **intersight.com**-account.

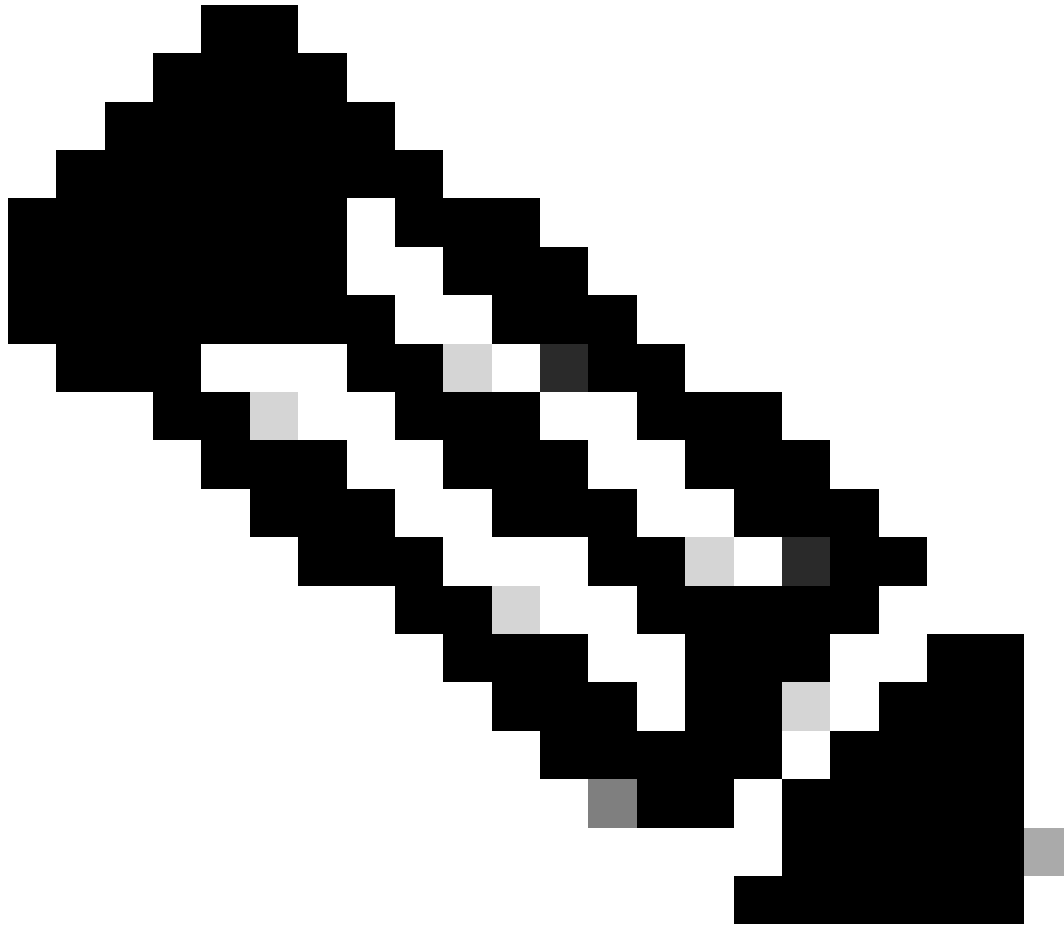
Nexus NXAPI configureren (alleen gebruikt als ansible.netcommon.httpapi gebruiken)



Opmerking: als een proxy op systeemniveau is geconfigureerd (**HTTP(S)_PROXY**) en Ansible geen proxy moet gebruiken om verbinding te maken met het Nexus NXAPI-eindpunt, is het wenselijk om `ansible_httppapi_use_proxy: False` een proxy in te stellen (Default is True).

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

Om de HTTP-connectiviteit met het NXAPI-eindpunt onafhankelijk te verifiëren, kunt u proberen een show clock bestand te verzenden. Switch
In het volgende voorbeeld wordt de client geverifieerd met behulp van basisverificatie. Het is ook mogelijk om de NXAPI-server te configureren om clients te verifiëren op basis van X.509-gebruikerscertificaat.



Opmerking: Basis Verificatie hash is verkregen uit base64 encoding van **gebruikersnaam:password**. In dit voorbeeld is **admin:cisco!123** base64 encoding YWRtaW46Y2lzY28hMTIz.

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

Curl-respons:

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

Intersight API-toetsen genereren

Raadpleeg het gedeelte [README.md](#) over het verkrijgen van de API-sleutel uit het Intersight System > Settings > API keys > Generate API Key.

The screenshot shows the Intersight Settings interface. At the top, there's a navigation bar with the Cisco logo, 'Intersight', and 'System' dropdown. A search bar and several utility icons are on the right. A warning banner at the top states: '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 heading is 'Settings'. On the left, a sidebar lists various settings categories: Single Sign-On, Domain Names, Cisco ID, Trusted Certificates, ACCESS & PERMISSIONS, IP Access Management, Security & Privacy, Users, Groups, Roles, Organizations, Resource Groups, API, API Keys (highlighted), OAuth2 Tokens, and Webhooks. The main content area is titled 'API Keys' and includes a 'Generate API Key' button. Below this, there's a filter section with 'All API Keys' and an 'Add Filter' button. A table header is visible with columns: Description, API Key ID, Purpose, Cre..., Email, Role, and Identity Provider. The table body is empty, displaying 'NO ITEMS AVAILABLE'. At the bottom right of the table area, it shows '0 of 0' items.

Generate API Key





Description

Nexus Intersight key



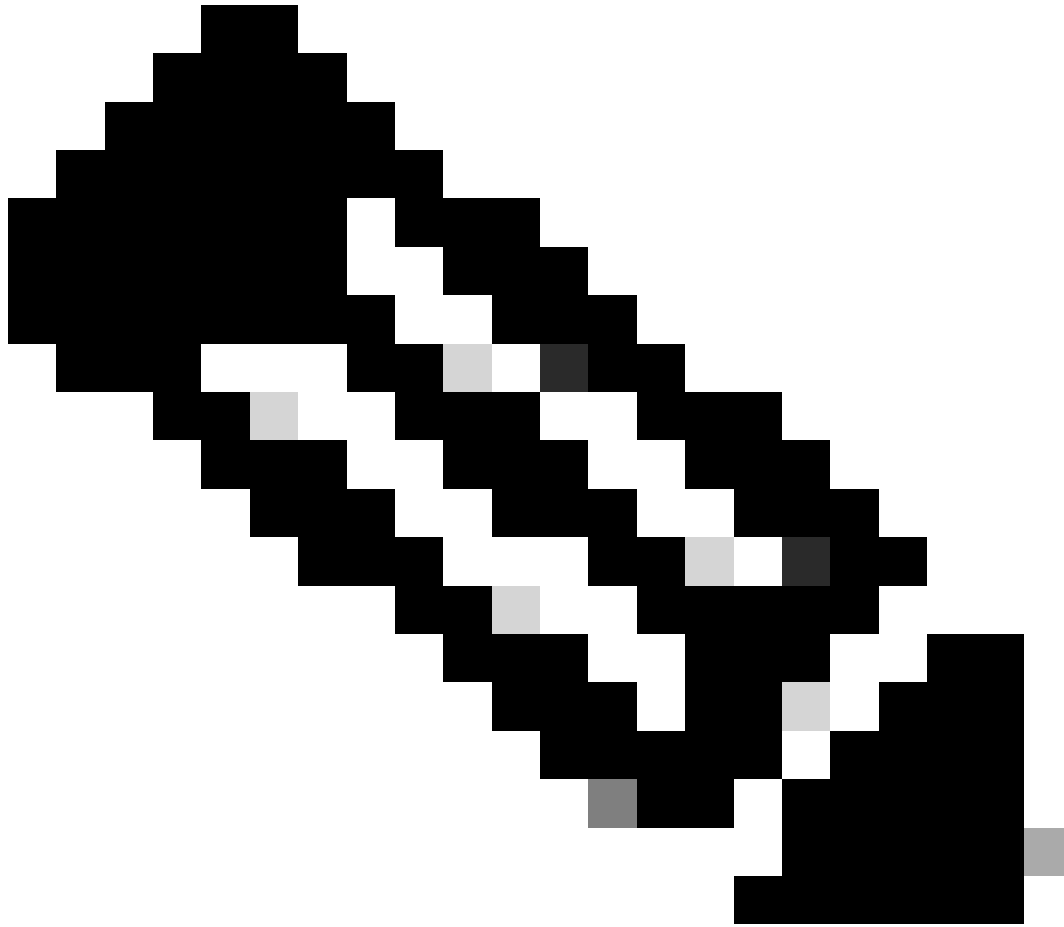
API Key Purpose

- 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) 

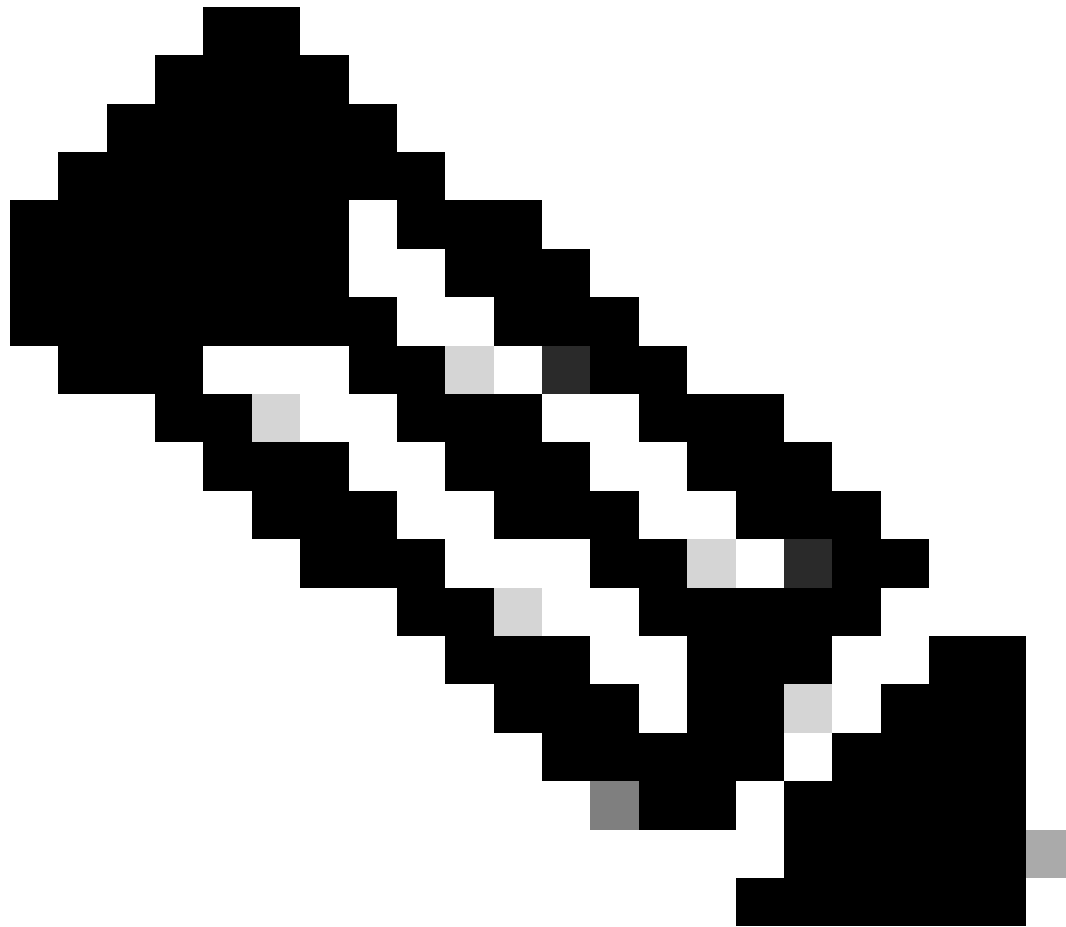
Close

Generate

Voorbeeld: Ansible inventory.yaml



Opmerking: in het volgende voorbeeld is Ansible geconfigureerd om de proxyinstellingen van het besturingssysteem te negeren met `ansible_httppapi_use_proxy: False`. Als u uw Ansible-server nodig hebt om een proxy te gebruiken om de switch te bereiken, kunt u die configuratie verwijderen of op `True` instellen (standaard).



Opmerking: de API key ID is een string. De privé-API-sleutel bevat het volledige pad naar een bestand dat de privé-sleutel bevat. Voor de productieomgeving wordt het gebruik van de ansible kluis aanbevolen.

```
---
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"
...

```

Voorbeeld: playbook.yaml uitvoering

Applications/Using Ansible Raadpleeg de handleiding met de sectie Cisco NX-OS van de [Cisco Nexus 9000 Series NX-OS Programmability Guide](#) voor uw huidige release voor meer informatie over het programmeren van standalone Nexus-apparaten met Ansible.

```

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

```

Verifiëren

Om de claim van een nieuw doel te verifiëren, moet u dit realiseren:

Op de Nexus Switch

releases voorafgaand aan 10.3(4a)M

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

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

releases die beginnen met 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
```

anabel

Aan het einde van de rit kan een opdracht worden toegevoegd om de informatie over hetplaybook.yaml intersight van de switch te verkrijgen.

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

Hier is de corresponderende uitvoer:

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

Apparaatconnector uitschakelen

| | Opdracht of handeling | Doel |
|---------------|---|---|
| Stap 1 | geen functieonderschepping Voorbeeld: switch(config)# no feature intersight | Schakelt het intersight-proces uit en verwijdert alle NXDC-configuratie en logboekopslag. |

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.