

Intersight 연결을 위한 독립형 Nexus 구성 및 클레임

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[연결 이점](#)

[빠른 시작 비디오](#)

[수동으로 NXOS 디바이스 클레임](#)

[연결 확인](#)

[OpenSSL 클라이언트를 사용한 TLS 확인](#)

[HTTPS 연결 가능성 확인](#)

[구성](#)

[디바이스 클레임 withinintersight.com](#)

[Nexus 디바이스에서](#)

[Intersight 포털에서](#)

[Ansible@을 사용하여 intersight.com에 있는 여러 독립형 Nexus 디바이스를 클레임합니다.](#)

[Nexus NXAPI 구성\(ansible.netcommon.httpapi를 사용하는 경우에만 사용\)](#)

[Intersight API 키 생성](#)

[예: Ansibleinventory.yaml](#)

[예:playbook.yamlExecution](#)

[다음을 확인합니다.](#)

[Nexus 스위치에서](#)

[10.3\(4a\)M 이전 릴리스](#)

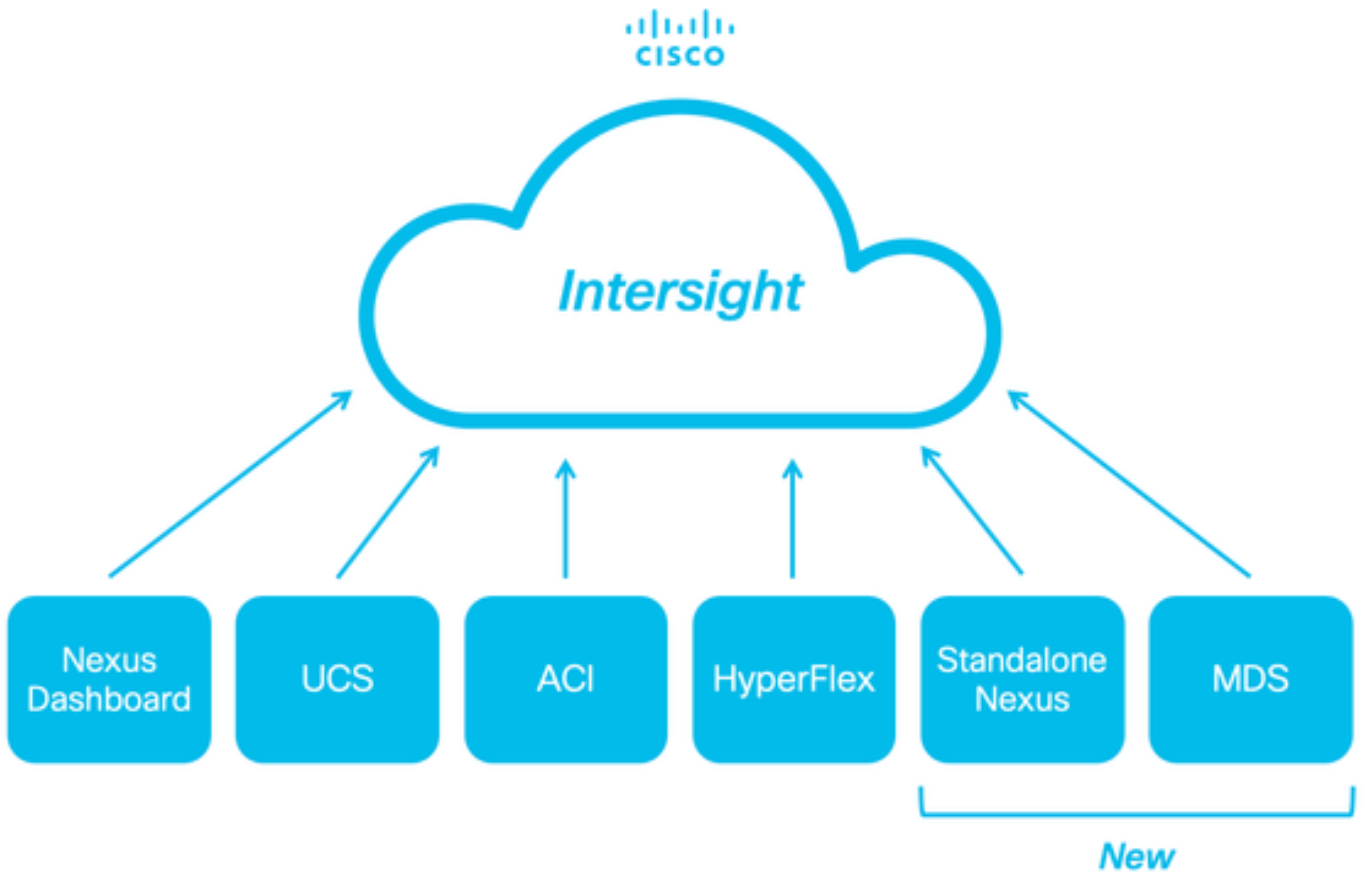
[10.3\(4a\)M으로 시작하는 릴리스](#)

[앤서블](#)

[장치 커넥터 사용 안 함](#)

소개

이 문서에서는 향상된 Cisco TAC 지원을 위해 Intersight에서 독립형 Nexus 스위치를 활성화하고 클레임하는 데 필요한 단계를 설명합니다.



사전 요구 사항

Intersight.com에 계정이 있어야 합니다. Cisco NX-OS® 청구에는 라이선스가 필요하지 않습니다. 새 Intersight 어카운트를 만들어야 하는 경우 어카운트 생성을 [참조하십시오](#).

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

독립형 Nexus 스위치에서 NXDC는 다음과 같은 지침과 제한 사항을 가지고 있습니다.

- Cisco NX-OS는 릴리스 10.2(3)F 이상을 실행해야 합니다.
- [DNS](#)는 적절한 VRF(Virtual Routing and Forwarding)에서 구성해야 합니다.
- svc.intersight.com 포트 443에서 아웃바운드에서 시작된 HTTPS 연결을 허용해야 합니다. 이 항목은 및 `openssl` 확인할 수 있습니다. ICMP(Internet Control Message Protocol) 요청은 무시됩니다.
- [에 대한 HTTPS 연결에 프록시가 필요한 경우 svc.intersight.com NXDC\(Nexus Switch Device Connector\) 컨피그레이션에서 프록시를 구성할 수 있습니다. 프록시 컨피그레이션에 대해서는 NXDC 구성을 \[참조하십시오\]\(#\).](#)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Intersight는 고급 인프라, 워크로드 최적화 및 Kubernetes 서비스의 선택적 모듈형 기능으로 구성된 클라우드 운영 플랫폼입니다. 자세한 내용은 [Intersight Overview](#)를 참조하십시오.

디바이스는 각 시스템의 Cisco NX-OS 이미지에 포함된 NXDC를 통해 Intersight 포털에 연결됩니다. Cisco NX-OS 릴리스 10.2(3)F부터는 보안 인터넷 연결을 사용하여 연결된 디바이스에서 Cisco Intersight 포털에서 정보를 전송하고 제어 명령을 수신할 수 있는 안전한 방법을 제공하는 디바이스 커넥터 기능이 지원됩니다.

연결 이점

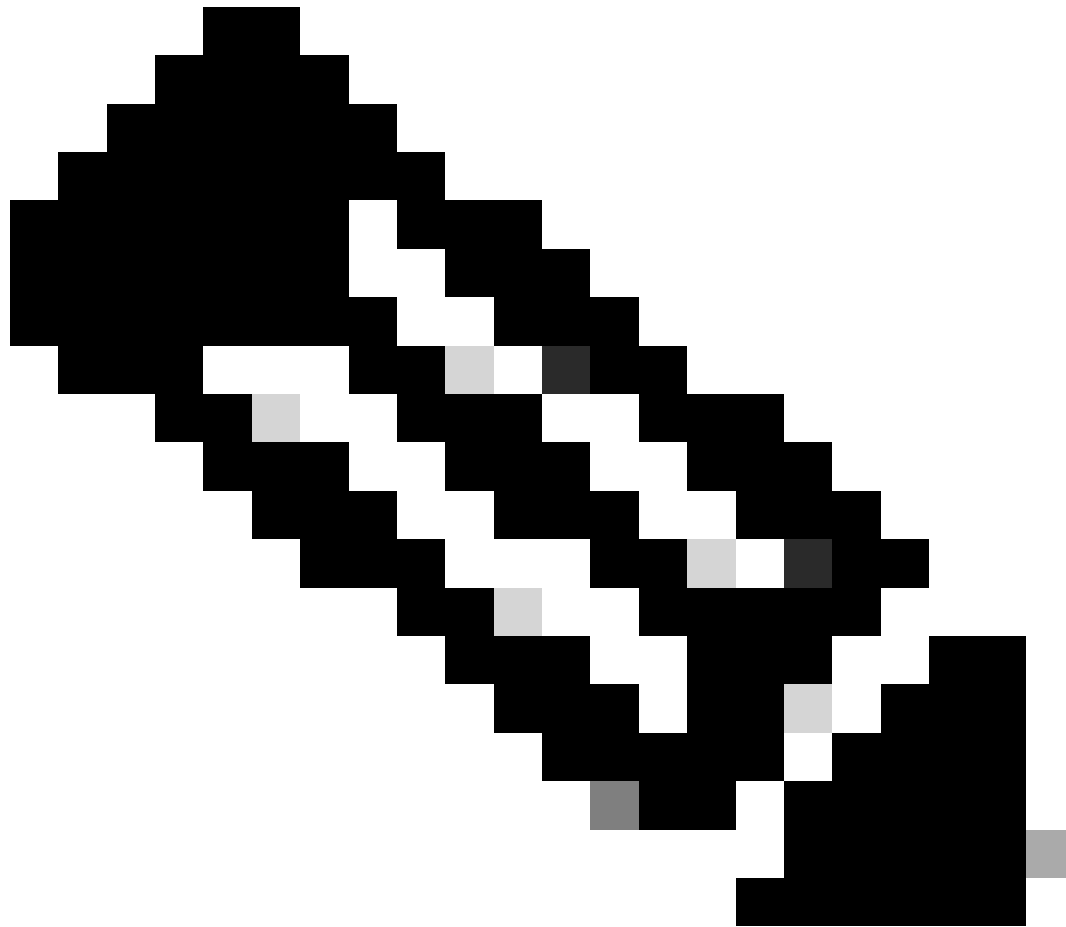
Intersight 연결은 Cisco NX-OS 기반 플랫폼에 다음과 같은 기능과 이점을 제공합니다.

- 신속한 문제 해결(show tech-support details열린 TAC 서비스 [요청](#)에 대한 RPR)을 통한 자동 수집
- 원격 온디맨드 수집 show tech-support details
- 향후 제공될 기능은 다음과 같습니다.
 - 텔레메트리 또는 하드웨어 장애를 기반으로 사전 대응적 TAC SR 열기
 - 개별 show 명령 등의 원격 온디맨드 모음

빠른 시작 비디오

수동으로 NXOS 디바이스 클레임

연결 확인



참고: Ping 응답은 억제됩니다(ICMP 패킷은 삭제됨).

openssl

curl TLS(Transport Layer Security) 및 HTTPS 연결을 확인하려면 bash를 활성화하고 원하는 VRF(ip netns exec <VRF>)에서 및 명령을 실행하는 것이 좋습니다.

! Enable bash

config terminal ; feature bash ; end

! Verify TLS

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

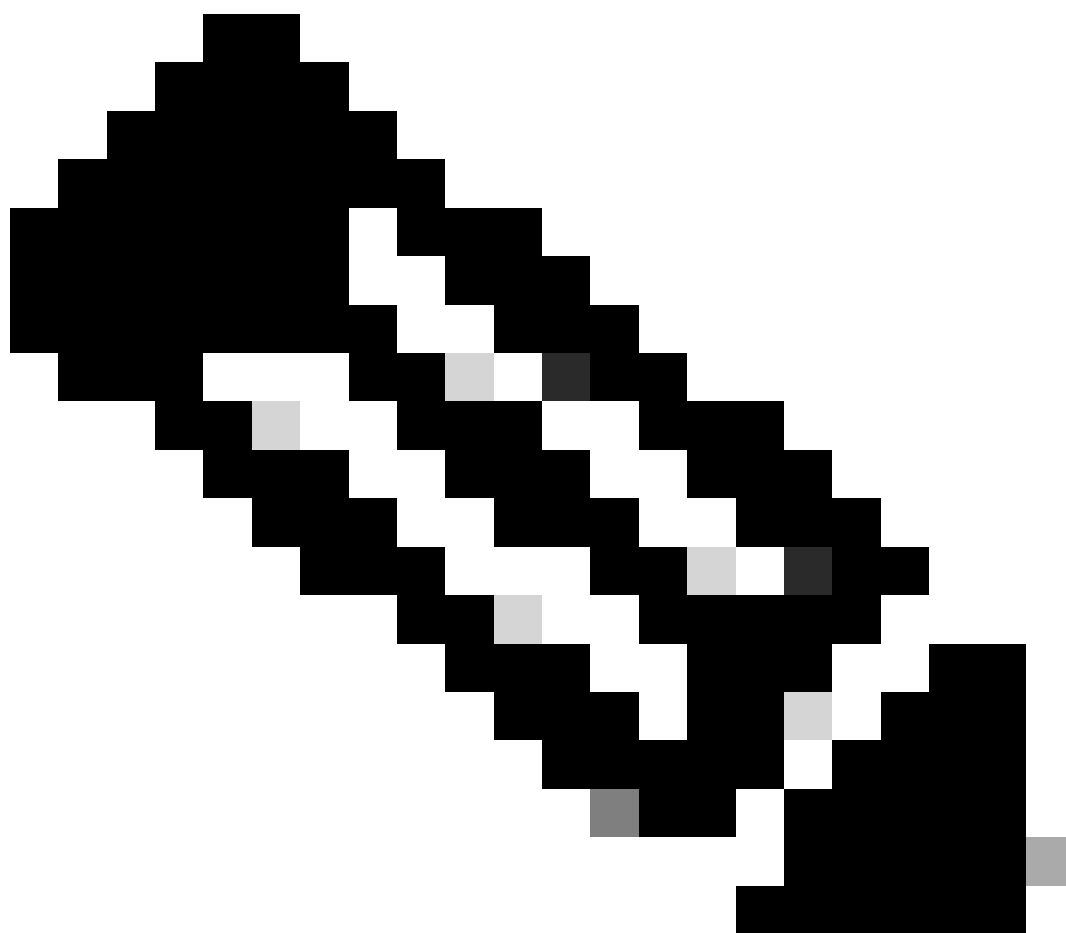
! Verify https

```
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]
```

OpenSSL 클라이언트를 사용한 TLS 확인

OpenSSL을 사용하여 의 TLS 연결을 확인할 수 svc.intersight.com:443 있습니다. 성공하면 서버에서 공용 서명 인증서를 검색하고 인증 기관 체인을 표시합니다.



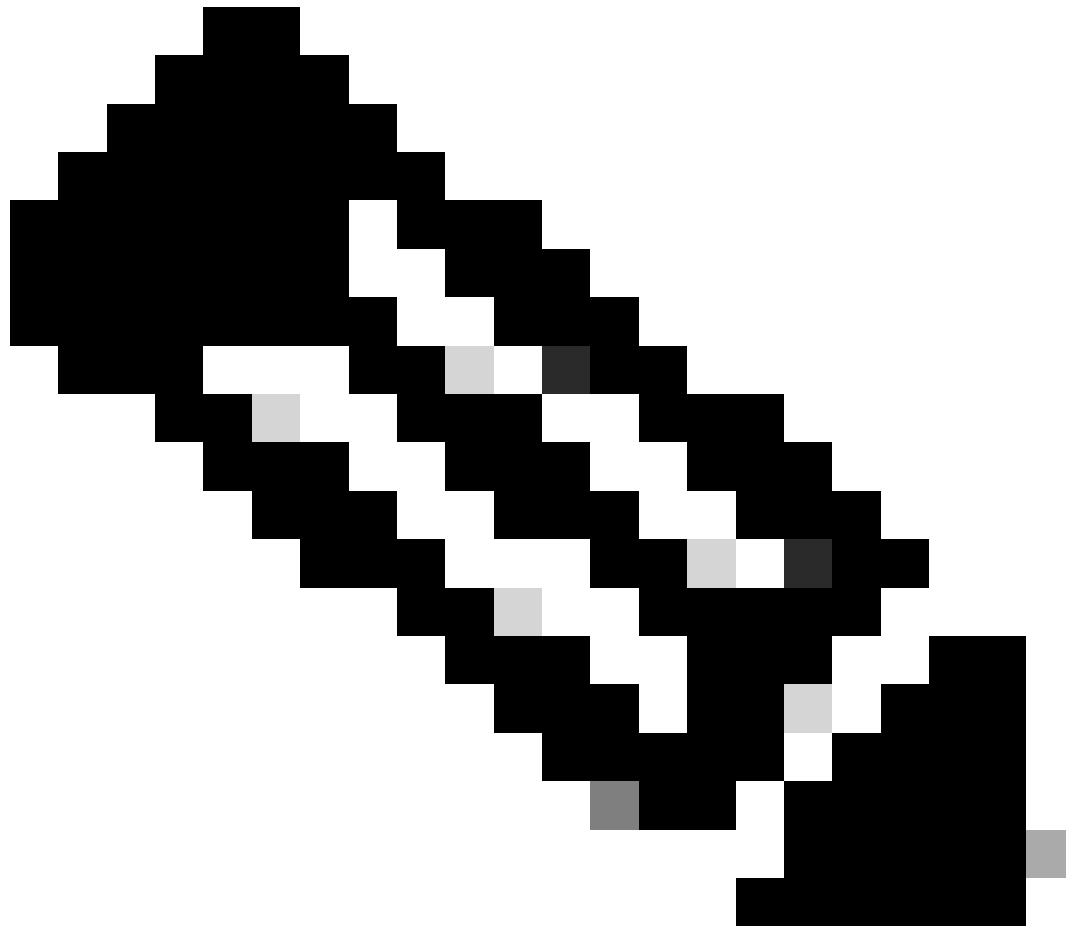
참고: 다음 예에서는 VRF 관리에서 openssl s_client 명령을 실행합니다. 구성에서 원하는 를 ip netns exec <VRF> 교체합니

다.

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

HTTPS 연결 가능성 확인

HTTPS 연결을 확인하려면 와 함께 **curl** 명령을 사용합니다(-v verbose flag프록시 사용 여부 표시).



참고: 프록시 활성화 또는 비활성화의 영향을 확인하려면 또는 옵션을 추가할 수 --proxy [protocol://]host[:port] 있습니다--
noproxy [protocol://]host[:port].

이 구성 ip netns exec <VRF>은 원하는 VRF에서 컬(curl)을 실행하는 데 사용됩니다(예: VRF 관리를 위해 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://]host[:port]
```

```
<#root>
```

```
#
```

```
run bash ip netns exec management curl -v -I -L -X POST https://svc.intersight.com:443 --proxy http://pr
```

```
Trying 10.201.255.40:80...
```

```
*
```

```
Connected to proxy.esl.cisco.com (10.201.255.40) port 80
```

```
* CONNECT tunnel: HTTP/1.1 negotiated
* allocate connect buffer
* Establish HTTP proxy tunnel to svc.intersight.com:443
> CONNECT svc.intersight.com:443 HTTP/1.1
> Host: svc.intersight.com:443
> User-Agent: curl/8.4.0
> Proxy-Connection: Keep-Alive
>
```

< HTTP/1.1 200 Connection established

HTTP/1.1 200 Connection established
< snip >

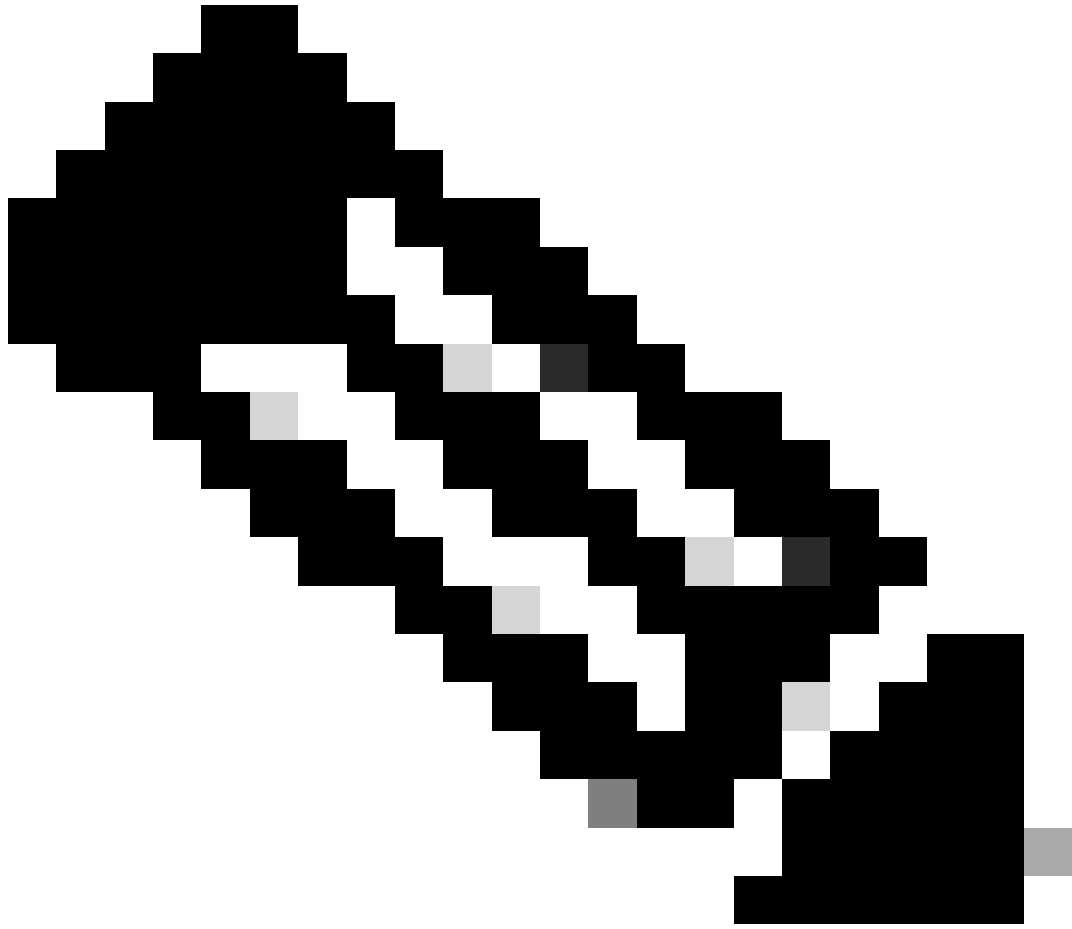
구성

내 장치 클레임 intersight.com

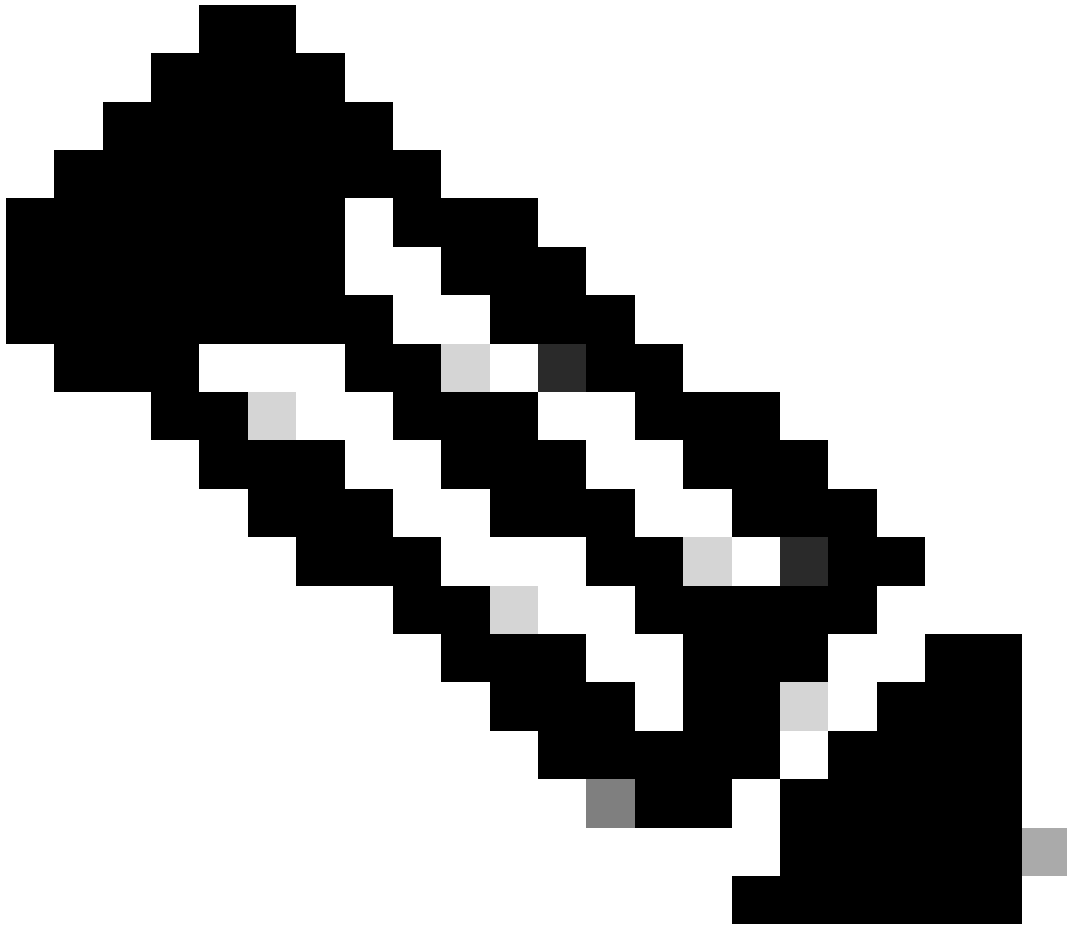
Intersight에서 새 대상을 요청하려면 다음 단계를 수행합니다.

Nexus 디바이스에서

Cisco NX-OS 명령을 실행합니다 `show system device-connector claim-info`.



참고: NX-OS 10.3(4a) 이전 릴리스의 경우 "show intersight claim-info" 명령을 사용합니다.



참고: Nexus에서 생성한 클레임 정보는 다음 Intersight 클레임 필드에 매핑됩니다.

일련 번호 = Intersight **Claim ID**

Device-ID Security Token = Intersight **클레임 코드**

```
# show system device-connector claim-info
SerialNumber: FDO23021ZUJ
SecurityToken: 9FFD4FA94DCD
```

Duration: 599

Message:

Claim state: Not Claimed

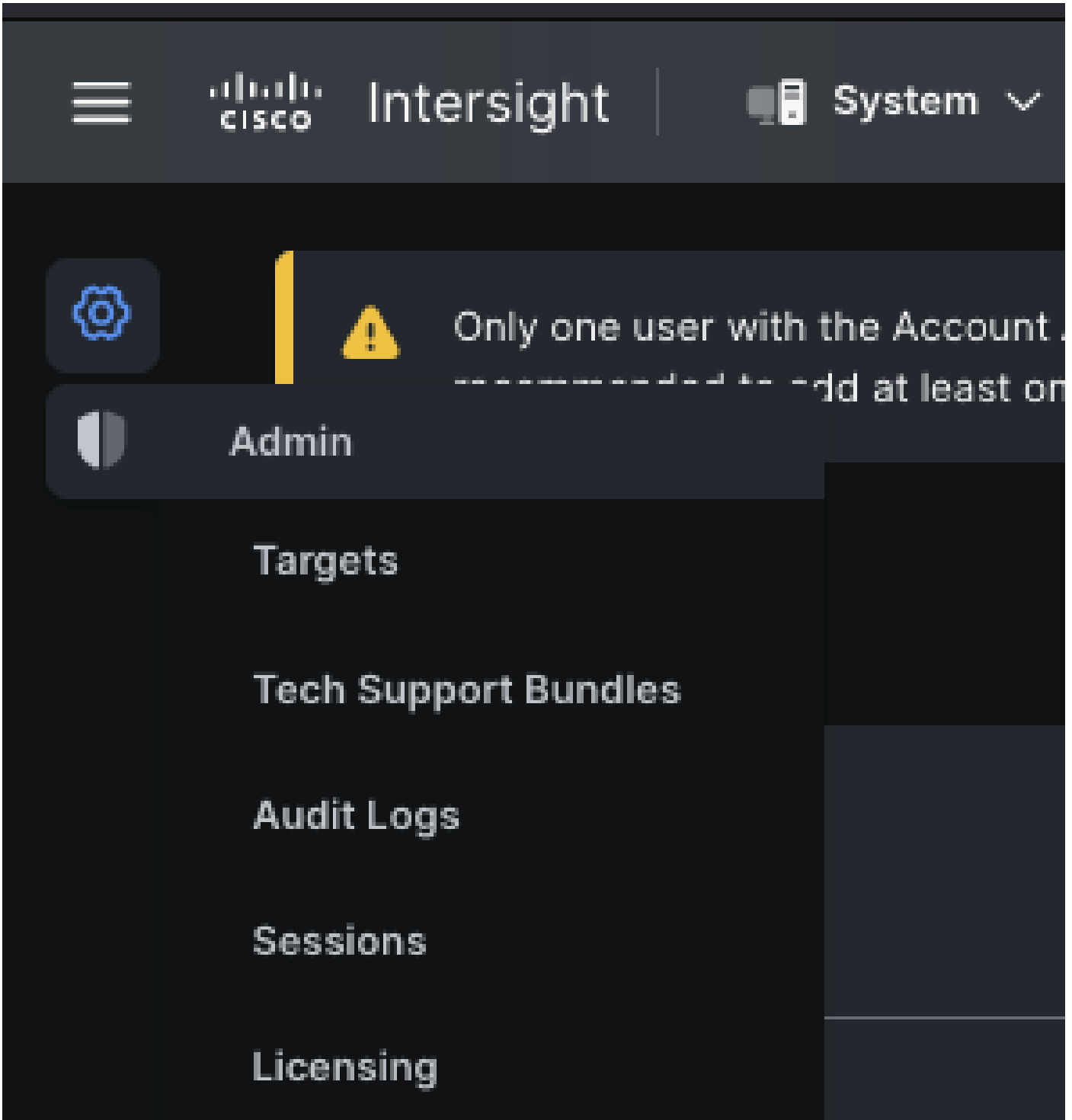
여기에 보고된 기간은 초 단위입니다.

Intersight 포털에서

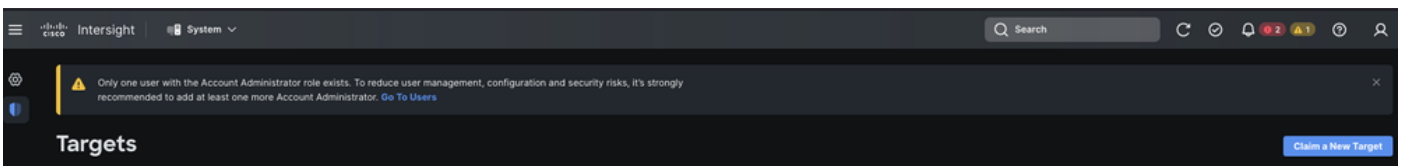
1. 10분 이내에 **Intersight**에 계정 관리자, 장치 관리자 또는 장치 기술자 권한으로 로그인합니다.
2. 서비스 선택기 드롭다운 목록에서 시스템을 선택합니다.



3. 로 ADMIN > Targets > Claim a New Target 이동합니다.



3.1. 이미지에 표시된 대로 **Claim a New Target**(새 대상 요청)을 클릭합니다.



4. 청구 기능을 선택하고 청구할 대상 유형(예: 네트워크)을 선택합니다. 시작을 클릭합니다.



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

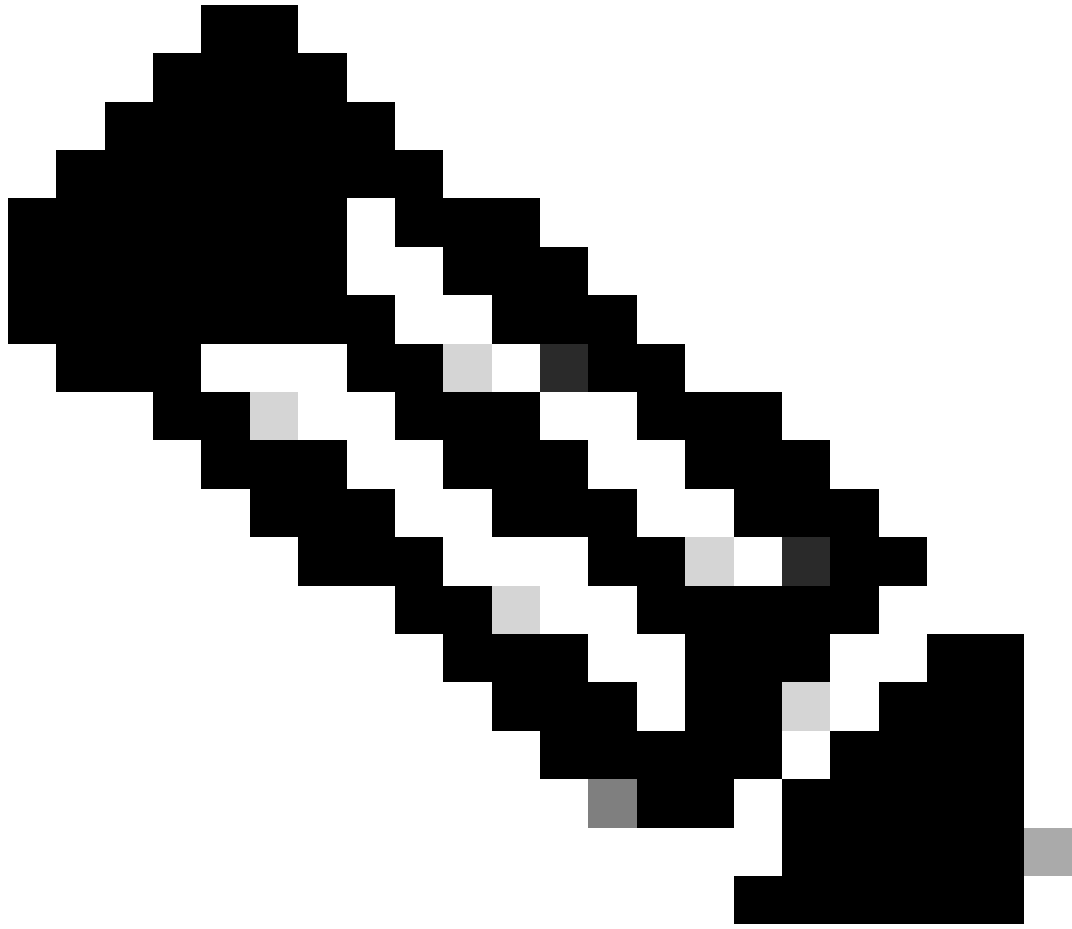
🔍 Search

Network

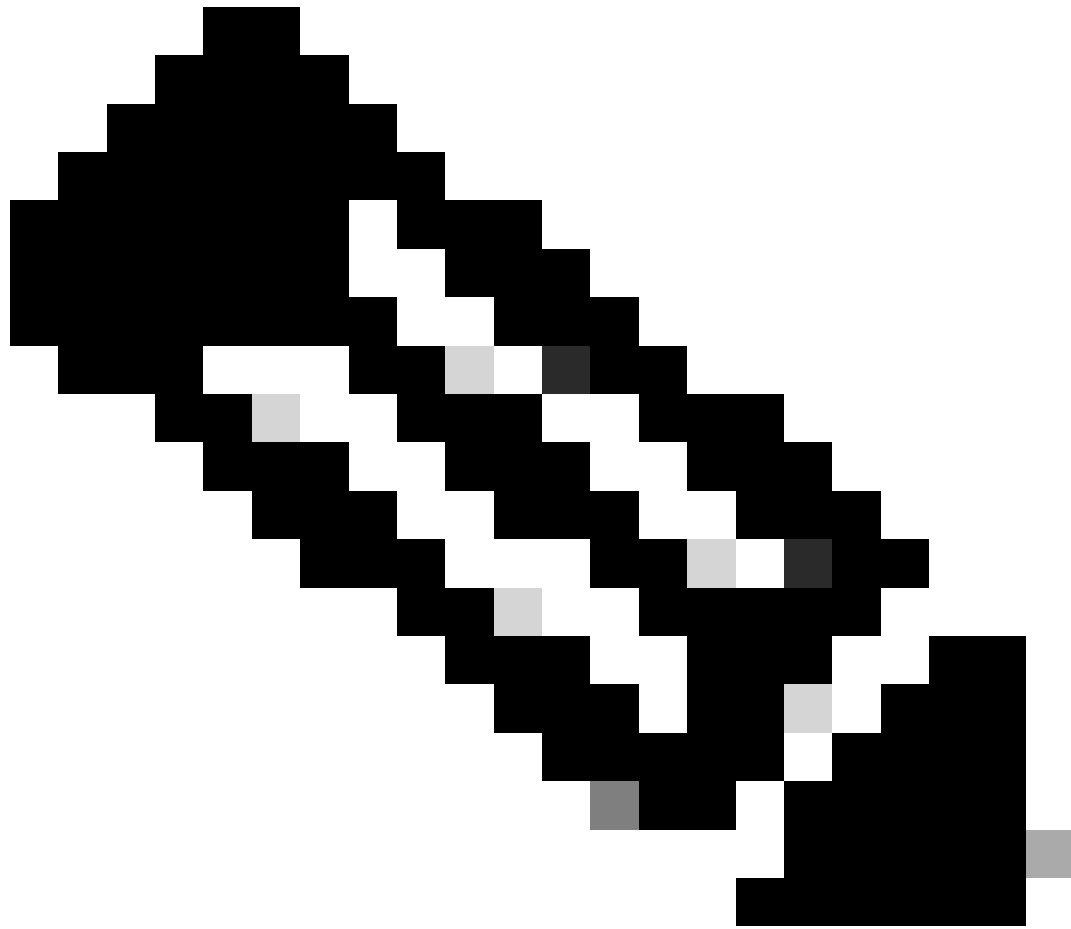
 Cisco MDS Switch	<input checked="" type="checkbox"/> Cisco Nexus Switch	<input type="checkbox"/> Cisco APIC
<input type="checkbox"/> Cisco Cloud APIC	<input type="checkbox"/> Cisco DCNM	<input type="checkbox"/> Cisco Nexus Dashboard

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

5. 청구 프로세스를 완료하려면 필요한 상세내역을 입력하고 청구를 누릅니다.



참고: 스위치의 보안 토큰은 청구 코드로 사용되며 스위치의 일련 번호는 장치 ID입니다.



참고: 보안 토큰이 만료됩니다. 청구를 재생성하기 전에 완료해야 합니다. 그렇지 않으면 시스템에서 청구를 재생성하라는 메시지를 표시합니다.



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



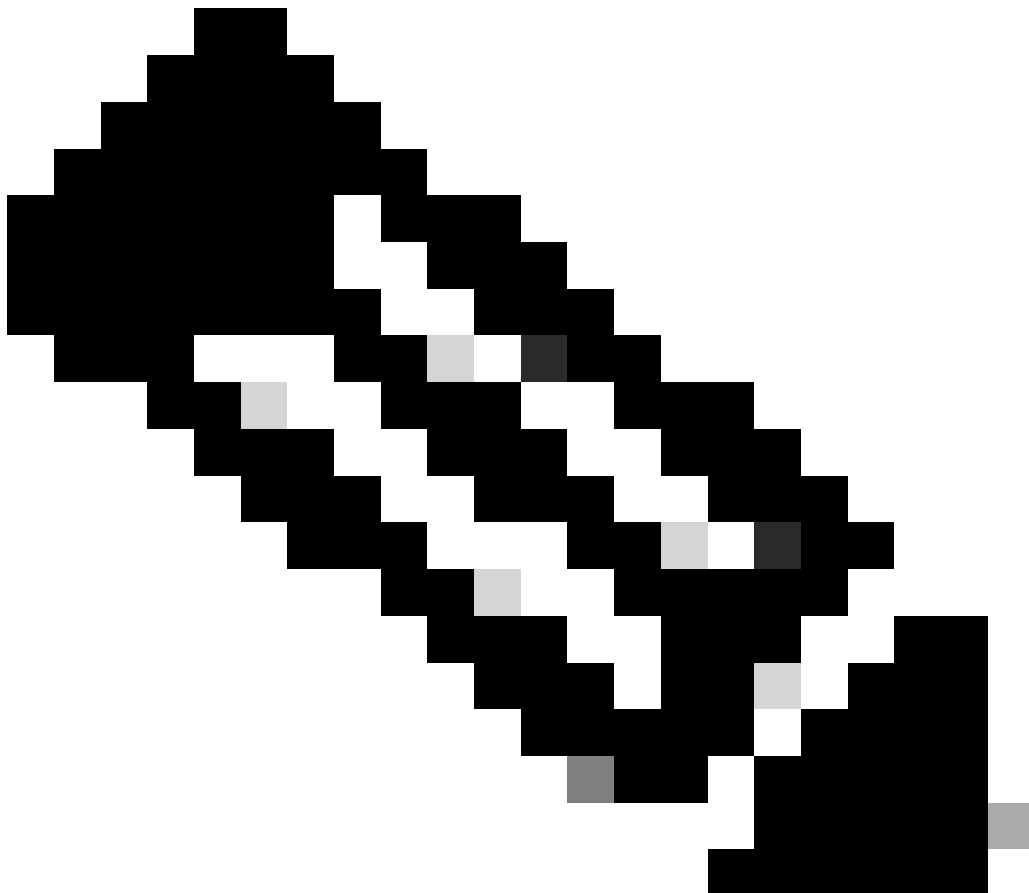
[Details](#)

Ansible을 사용하여 intersight.com에서 1대 다수의 독립형 Nexus 디바이스를 클레임합니다®

하나 이상의 Nexus 디바이스를 클레임하기 위해 Ansible 플레이북을 실행할 수 있습니다.

- Ansible 인벤토리 및 플레이북은 <https://github.com/datacenter/ansible-intersight-nxos>에서 Git 복제할 수 [있습니다](#).
- Ansible에서 `inventory.yaml` Nexus `ansible_connection` 스위치로 명령을 전송하기 위해 `ansible.netcommon.network_cli` 유형이 로 설정됩니다. NXAPI를 통한 연결을 허용하기 위해 이를 `ansible.netcommon.httpapi` 로 변경할 수 있습니다.
- Intersight 엔드포인트에 연결할 수 있으려면 intersight.com 계정에서 생성할 수 있는 API 키가 필요합니다.

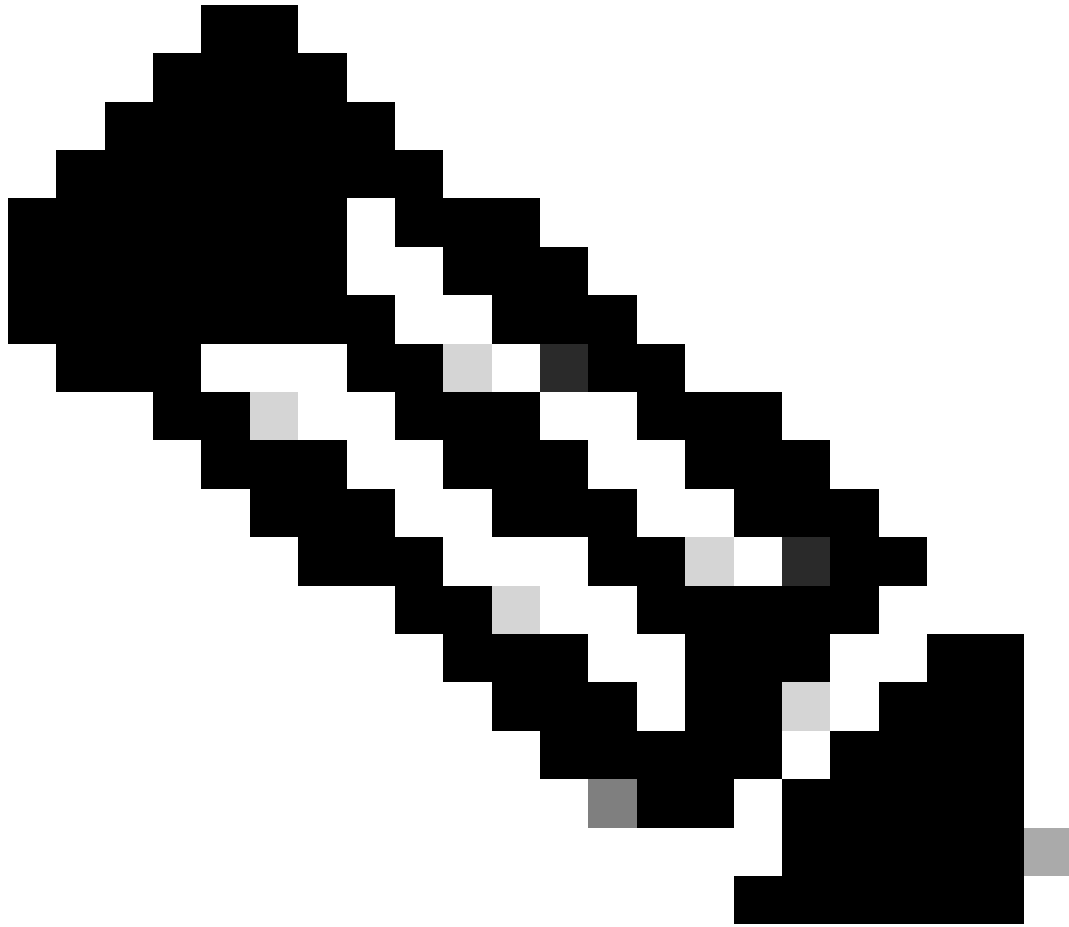
Nexus NXAPI 구성(사용 중인 경우에만 사용 `ansible.netcommon.httpapi`)



참고: 시스템 레벨 프록시가 구성되어 있고(**HTTP(S)_PROXY**) Ansible이 Nexus NXAPI 엔드포인트와 연결하기 위해 프록시를 사용하지 않아야 하는 경우 (기본값은 Trueansible_httpapi_use_proxy: False임) 설정하는 것이 좋습니다.

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

NXAPI 엔드포인트에 대한 HTTP 연결을 독립적으로 확인하려면 를 전송하려고 시도할 수 show clock 있습니다. 다음 예에서는 스위치에서 기본 인증을 사용하여 클라이언트를 인증합니다. X.509 사용자 인증서를 기반으로 클라이언트를 인증하도록 NXAPI 서버를 구성할 수도 있습니다.



참고: 기본 인증 해시는 base64 인코딩 **username:password**에서 가져옵니다. 이 예에서는 **admin:cisco!123** base64 인코딩이 **YWRtaW46Y2lzY28hMTIz**됩니다.

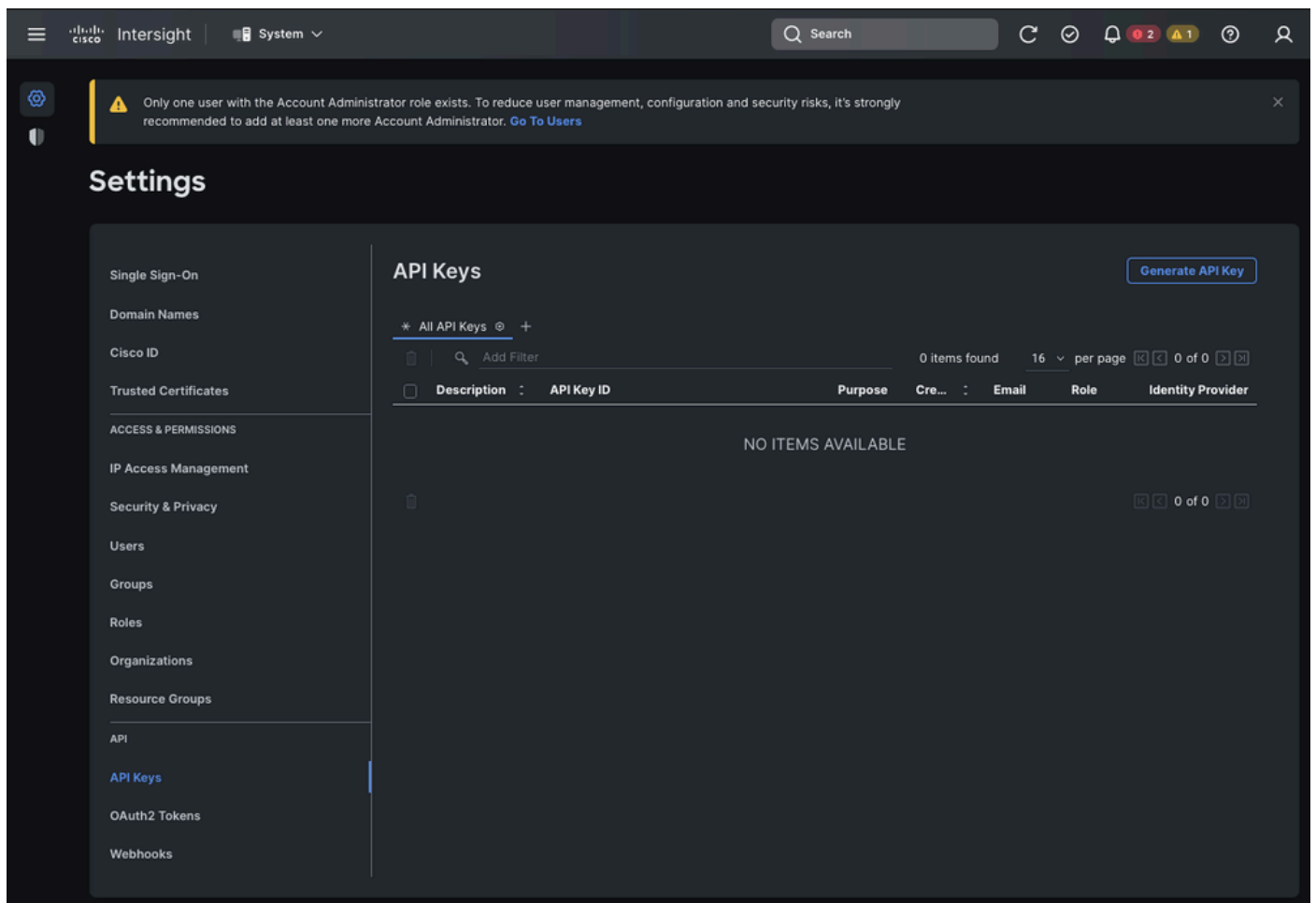
```
curl -v --no-proxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

통화 응답:

```
* 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 키 생성

에서 API 키를 가져오는 방법에 대해서는 README.md 섹션을 Intersight System > Settings > API keys > Generate API Key 참조하십시오.



Generate API Key





Description

Nexus Intersight key



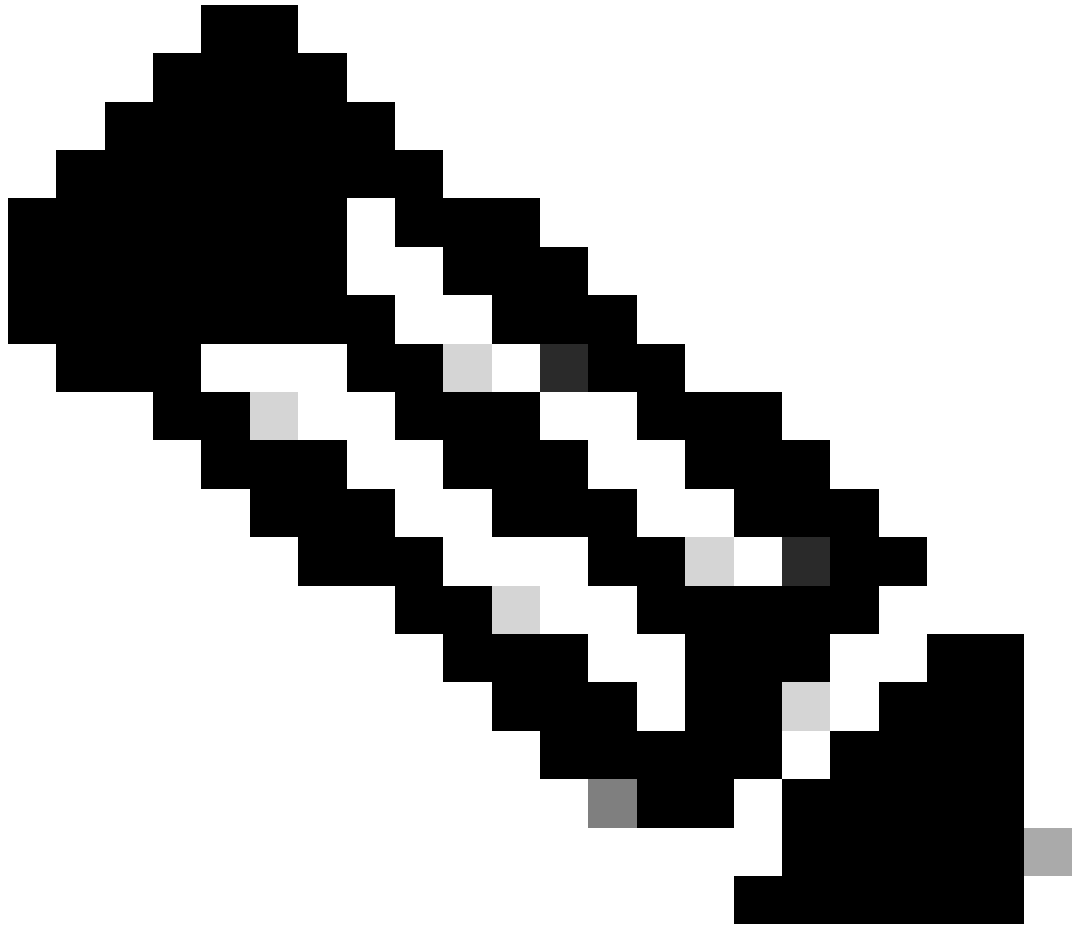
API Key Purpose

- 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

예: Ansible inventory.yaml



참고: 다음 예에서는 운영 체제 프록시 설정을 무시하도록 ansible을 `ansible_httppapi_use_proxy: False` 구성했습니다. Ansible 서버에서 스위치에 연결하기 위해 프록시를 사용해야 하는 경우 해당 컨피그레이션을 제거하거나 `True`(기본값)로 설정할 수 있습니다.

참고: API 키 ID는 문자열입니다. API 개인 키에는 개인 키가 포함된 파일의 전체 경로가 포함됩니다. 프로덕션 환경에서는 Ansible Vault를 사용하는 것이 좋습니다.

```
---
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"
...

```

예: playbook.yaml Execution

Ansible을 사용하여 독립형 Nexus 디바이스를 프로그래밍하는 방법에 대한 자세한 내용은 현재 릴리스의 [Applications/Using Ansible Cisco Nexus 9000 Series NX-OS Programmability Guide](#)에서 Cisco NX-OS를 사용하여 섹션을 참조하십시오.

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

다음을 확인합니다.

새 대상의 주장을 확인하려면 다음을 수행합니다.

Nexus 스위치에서

10.3(4a)M 이전 릴리스

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

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

10.3(4a)M으로 시작하는 릴리스

```
# 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
```

앤서블

스위치 인터사이트 정보를 획득하기 위해, 의playbook.yaml 끝에 태스크를 추가하는 것이 가능하다.

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

다음은 해당 출력입니다.

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

장치 커넥터 사용 안 함

	명령 또는 작업	목적
1단계	<p>기능 가시성 없음</p> <p>예:</p> <p>switch(config)# no feature intersight</p>	<p>intersight 프로세스를 비활성화하고 모든 NXDC 컨피그레이션 및 로그 저장소를 제거합니다.</p>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.