

# Configuración y reclamación de Nexus independiente para la conectividad entre puntos de vista

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Ventajas de conectividad](#)

[Vídeo de inicio rápido](#)

[Solicitar manualmente un dispositivo NXOS](#)

[Verificación de conectividad](#)

[Verificación de TLS con OpenSSL Client](#)

[Verificación de disponibilidad de HTTPS](#)

[Configurar](#)

[Solicite el dispositivo withinintersight.com](#)

[En el dispositivo Nexus](#)

[En Intersight Portal](#)

[Reclamación de uno a varios dispositivos Nexus independientes en intersight.com mediante Ansible®](#)

[Configuración de Nexus NXAPI \(solo se utiliza si se usa ansible.netcommon.httapi\)](#)

[Generar claves de API de Intersight](#)

[Ejemplo: AnsibleInventory.yaml](#)

[Ejemplo:cuaderno.yamlExecution](#)

[Verificación](#)

[En el switch Nexus](#)

[Versiones anteriores a 10.3\(4a\)M](#)

[Versiones que comienzan con 10.3\(4a\)M](#)

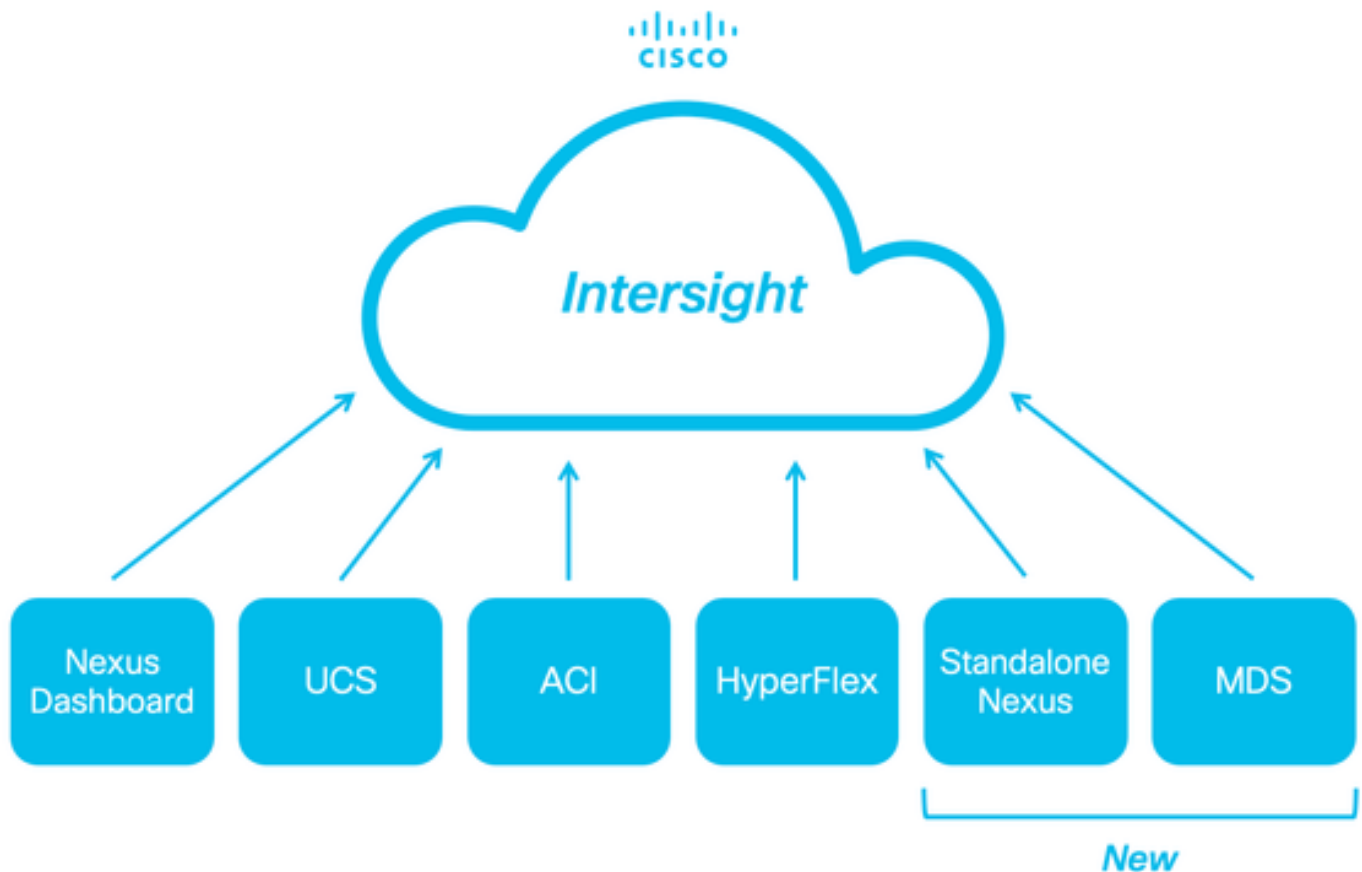
[Ansible](#)

[Desactivar el conector de dispositivo](#)

---

## Introducción

En este documento se describen los pasos necesarios para habilitar y solicitar switches Nexus independientes en Intersight para mejorar la compatibilidad con Cisco TAC.



## Prerequisites

Debe tener una cuenta en [Intersight.com](https://intersight.com), no se necesita licencia para realizar solicitudes de Cisco NX-OS®. Si necesita crear una nueva cuenta de Intersight, consulte [Creación de cuenta](#).

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

En el switch Nexus independiente, NXDC tiene estas directrices y limitaciones:

- Cisco NX-OS debe ejecutar la versión 10.2(3)F o posterior
- [DNS](#) se debe configurar en el reenvío y routing virtual (VRF) adecuado
- `svc.intersight.com` debe resolverse y permitir las conexiones HTTPS salientes iniciadas en el puerto 443. Esto se puede comprobar con `openssl` y `rizar`. Las solicitudes de Protocolo de mensajes de control de Internet (ICMP) se omiten.
- Si se requiere un proxy para una conexión HTTPS con `svc.intersight.com`, el proxy se puede configurar en la configuración del conector del dispositivo del switch Nexus (NXDC). Para la configuración de proxy, consulte [Configuración de NXDC](#).

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

Cisco Intersight es una plataforma de operaciones en la nube que consta de capacidades modulares opcionales de infraestructura avanzada, optimización de cargas de trabajo y servicios de Kubernetes. Visite [Intersight Overview](#) para obtener más información.

Los dispositivos se conectan al portal Intersight a través de un NXDC que está integrado en la imagen de Cisco NX-OS de cada sistema. A partir de Cisco NX-OS versión 10.2(3)F, se admite la función Device Connector, que proporciona una forma segura para que los dispositivos conectados envíen información y reciban instrucciones de control desde el portal Cisco Intersight mediante una conexión a Internet segura.

#### Ventajas de conectividad

La conectividad Intersight proporciona estas funciones y ventajas para las plataformas basadas en Cisco NX-OS:

- Recopilación automatizada de show tech-support details mediante la [resolución rápida de problemas](#) (RPR para las solicitudes de servicio TAC abiertas)
- Recopilación remota a demanda de show tech-support details
- Las funciones futuras incluyen:
  - Apertura de TAC SR proactivos en función de fallos de telemetría o hardware
  - Recopilación remota a petición de comandos show individuales y más

#### Vídeo de inicio rápido

Solicitar manualmente un dispositivo NXOS

#### Verificación de conectividad



**Nota:** se suprimen las respuestas de ping (se descartan los paquetes ICMP).

---

Para verificar la seguridad de la capa de transporte (TLS) y la conectividad HTTPS, se recomienda habilitar bash y ejecutar openssl y curl comandos en el VRF (ip netns exec <VRF>) deseado.

! 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

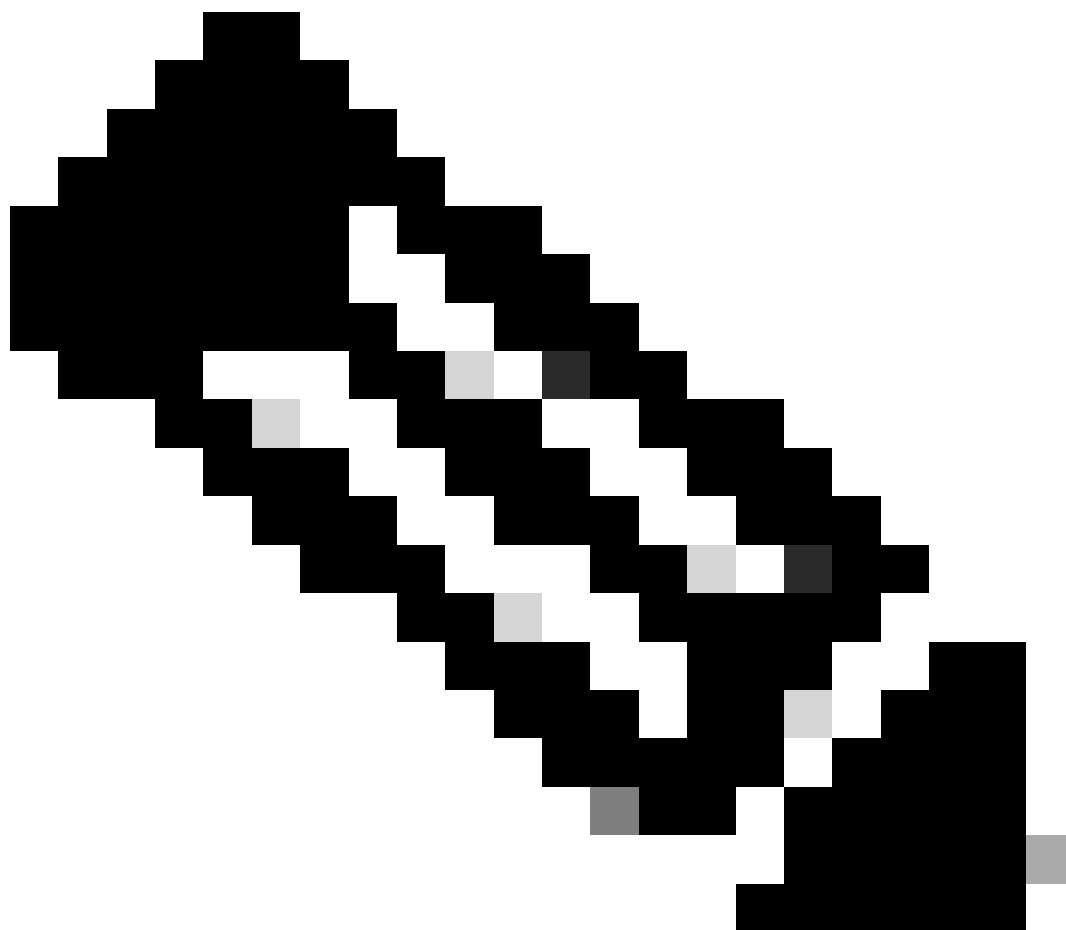
```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

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

#### Verificación de TLS con OpenSSL Client

Con OpenSSL, puede comprobar la conectividad TLS con svc.intersight.com:443. Cuando se realice correctamente, recupere el certificado público firmado por el servidor y muestre la cadena de la autoridad certificadora.

---



**Nota:** El siguiente ejemplo ejecuta el openssl s\_client comando en la administración VRF. Reemplace el valor deseado en la ip netns exec <VRF> construcción.

---

---

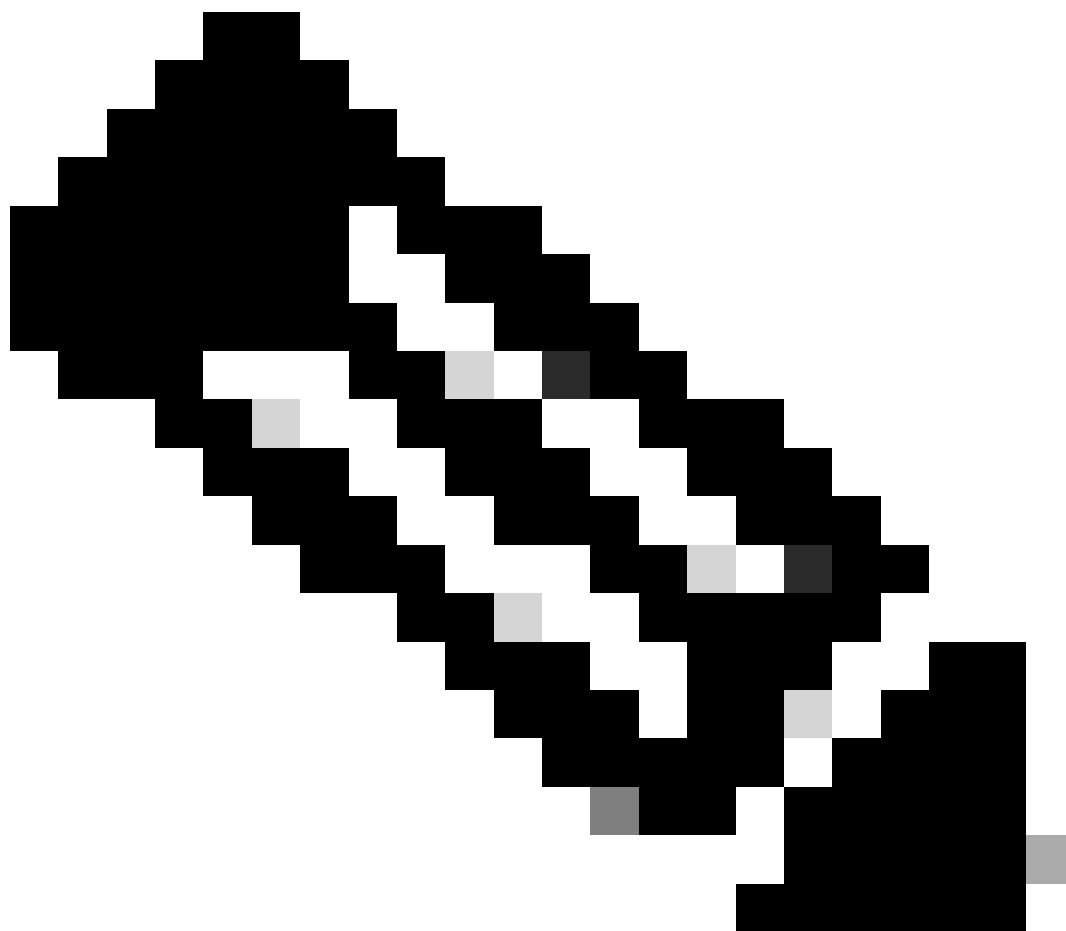
---

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

Verificación de disponibilidad de HTTPS

Para verificar la conectividad HTTPS, utilice el comando **curl** con el comando **-v** verbose flag (muestra si se utiliza o no un proxy).

---



**Nota:** Para comprobar el impacto de activar o desactivar un proxy, puede agregar las opciones `--proxy [protocol://]host[:port]` o `--noproxy [protocol://]host[:port]`.

---

---

La construcción ip netns exec <VRF> se utiliza para ejecutar curl en el VRF deseado; por ejemplo, ip netns exec management para la gestión de VRF.

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

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

```
<#root>
```

```
#
```

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

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

```
*
```

```
Connected to proxy.es1.cisco.com (10.201.255.40) port 80
```

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

```
< HTTP/1.1 200 Connection established
```

HTTP/1.1 200 Connection established  
< snip >

Configurar

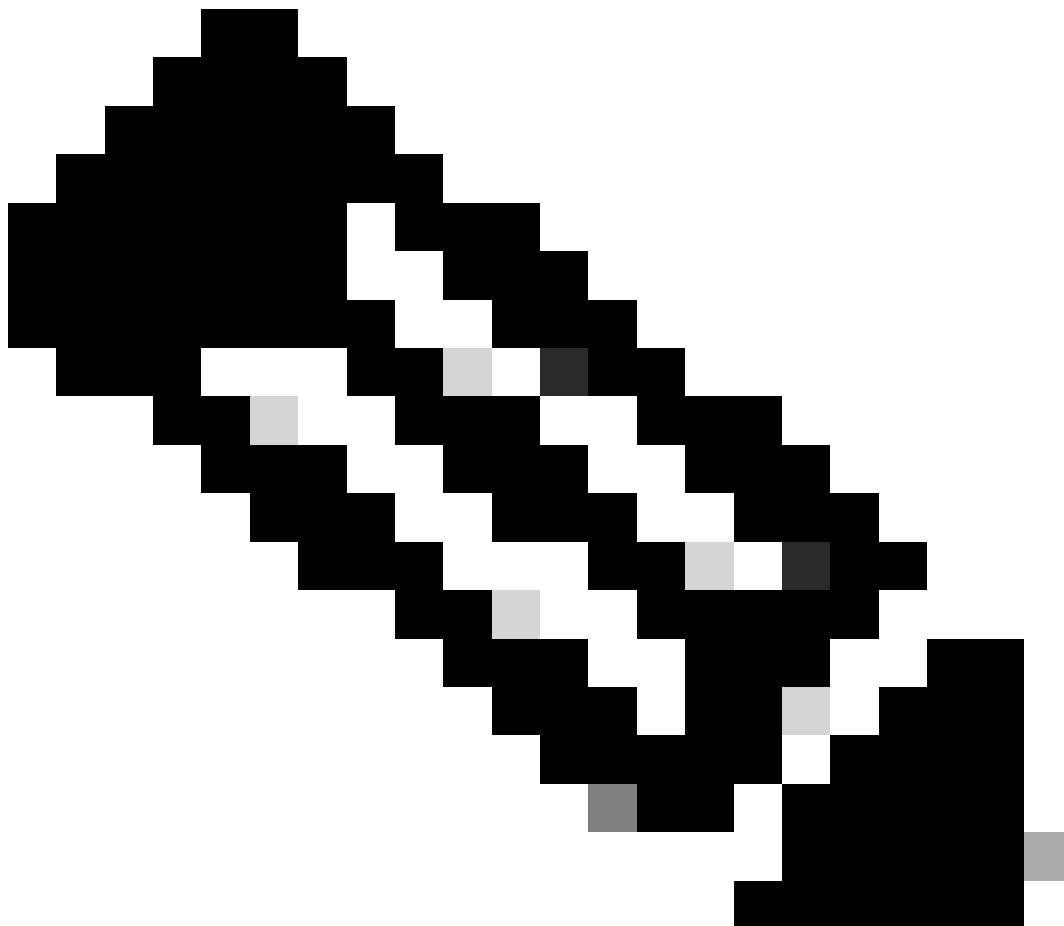
Reclamar el dispositivo en intersight.com

Para reclamar un nuevo objetivo en Intersight, realice los pasos mencionados.

En el dispositivo Nexus

Ejecute el comando Cisco NX-OS show system device-connector claim-info.

---



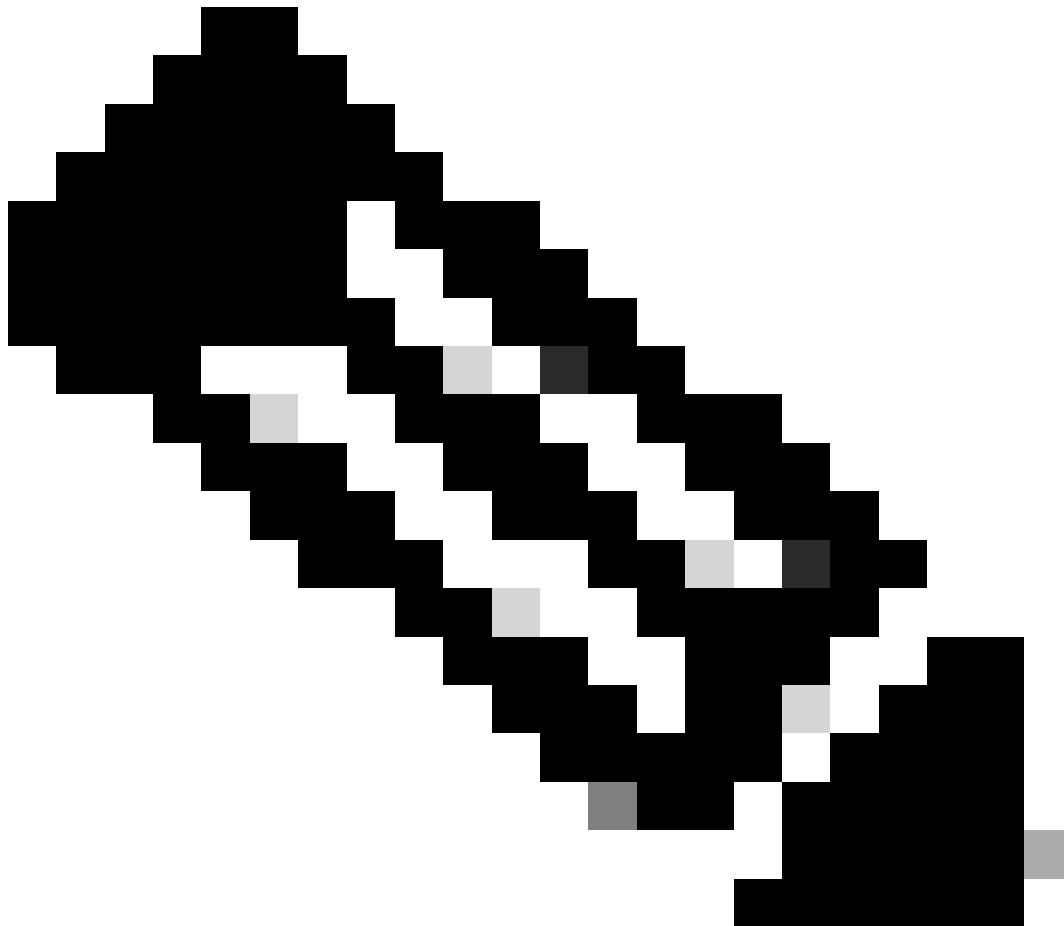


---

**Nota:** para las versiones anteriores a NX-OS 10.3(4a), utilice el comando "show intersight Claims-info"

---

---



**Nota:** Nexus genera mapas de información de justificantes de venta en los siguientes campos de justificantes de venta de Intersight:

Número de serie = **ID de reclamación de** intercepción

Device-ID Security Token = **Código de reclamación de** intercepción

---

---

---

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

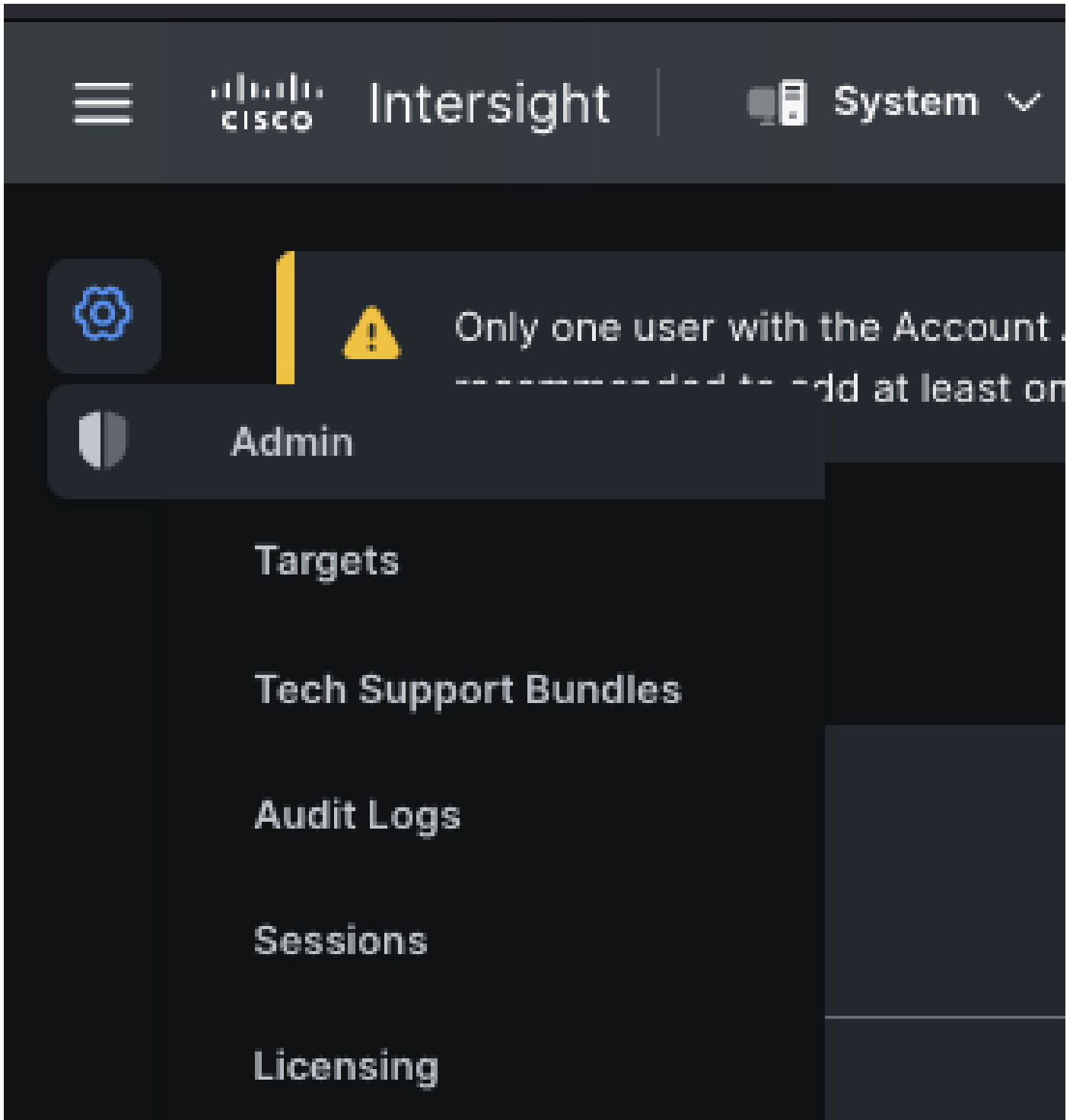
La **duración** indicada aquí se expresa en segundos.

En Intersight Portal

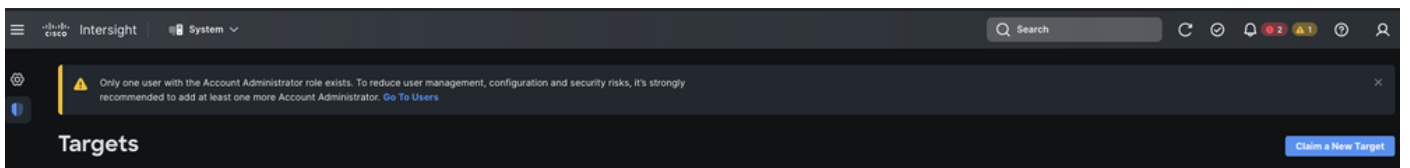
1. En el plazo de 10 minutos inicie sesión en **Intersight** con los privilegios de administrador de cuenta, administrador de dispositivo o técnico de dispositivo.
2. En la lista desplegable **Selector de Servicios**, seleccione **Sistema**.



3. Acceda a ADMIN > Targets > Claim a New Target.



3.1. Haga clic en **Reclamar un nuevo destino** como se muestra en la imagen.



4. Seleccione **Disponible para Reclamación** y elija el **tipo de destino** (por ejemplo, Red) que desea reclamar. Haga clic en Start (Inicio).

⚙️

⚠️ 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

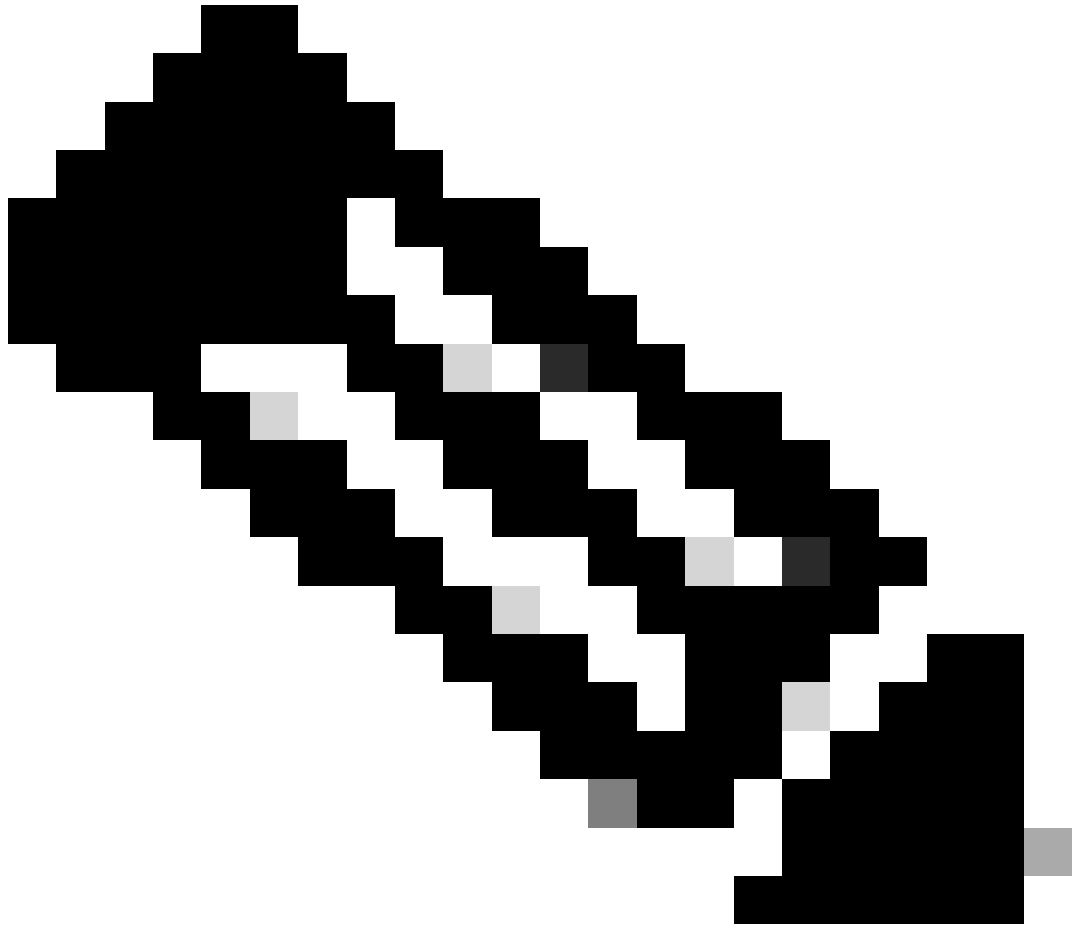
Orchestrator

🔍 Search

**Network**

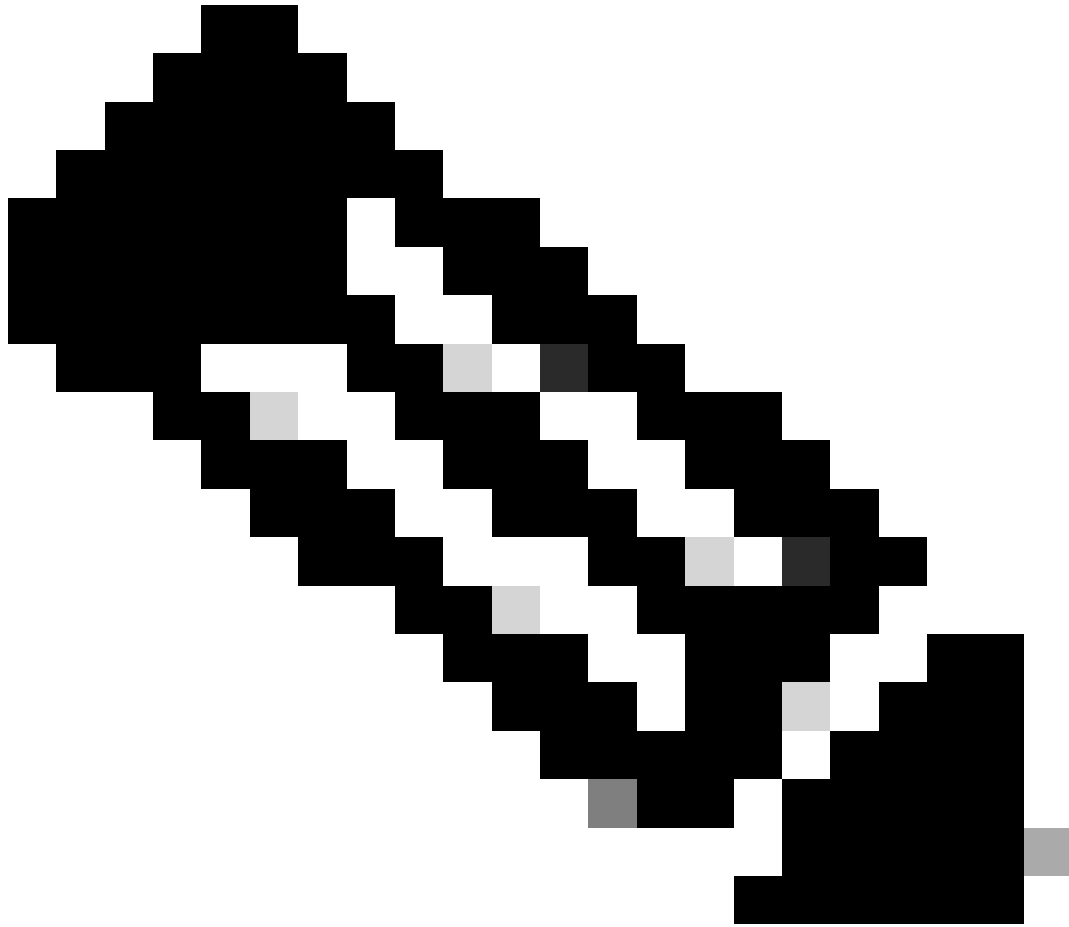
 Cisco MDS Switch	<input checked="" type="checkbox"/>  Cisco Nexus Switch	 Cisco APIC
 Cisco Cloud APIC	 Cisco DCNM	 Cisco Nexus Dashboard

5. Introduzca los detalles necesarios y haga clic en **Reclamar** para completar el proceso de reclamación.



**Nota:** el **token de seguridad** del switch se utiliza como código de reclamación y el **número de serie del switch** es el **ID de dispositivo**.

---



**Nota:** El token de seguridad caduca. Debe completar la reclamación antes o el sistema le solicitará que vuelva a generar una.



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



[Details](#)

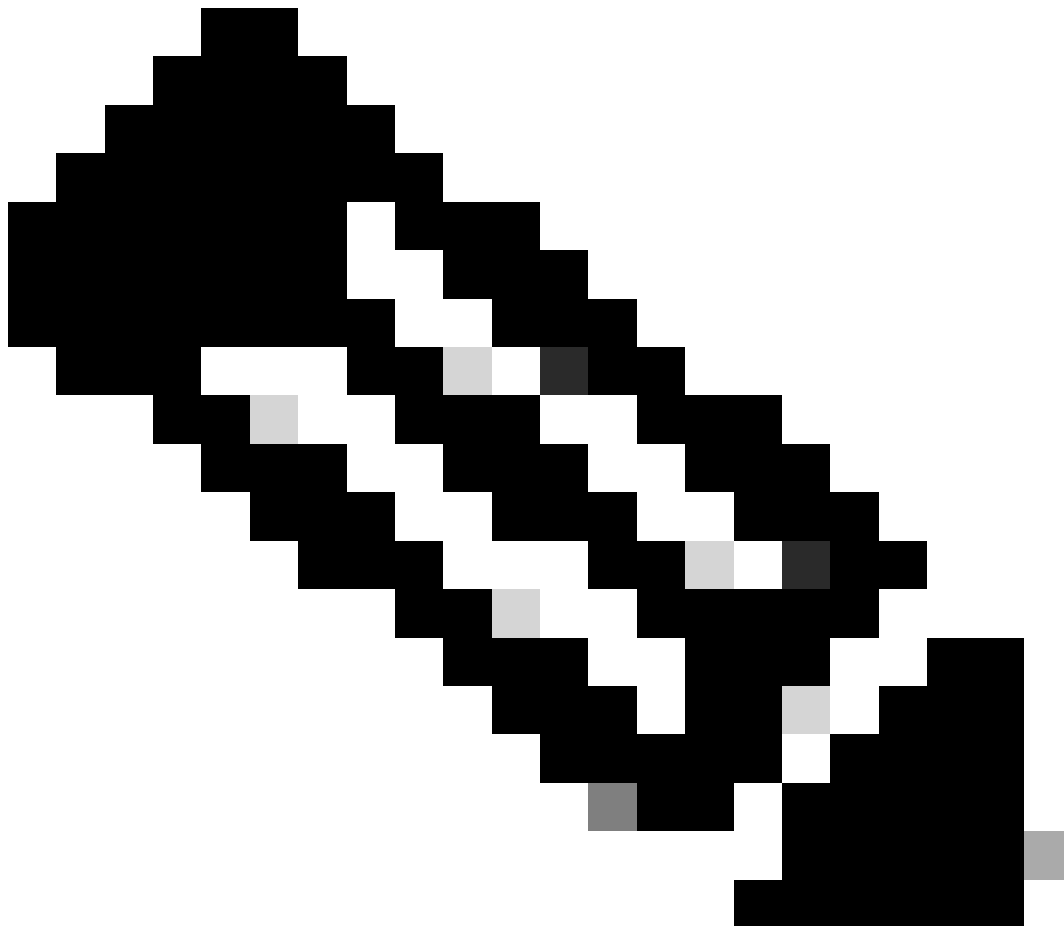
Reclamación de uno a varios dispositivos Nexus independientes en [intersight.com](https://intersight.com) mediante Ansible®

Para reclamar uno o varios dispositivos Nexus, se puede ejecutar un cuaderno Ansible.

- El inventario y el cuaderno de campaña se pueden clonar desde <https://github.com/datacenter/ansible-intersight-nxos>.
- En el Ansible `inventory.yaml`, el `ansible_connection` tipo se establece `ansible.netcommon.network_cli` en para enviar comandos al switch Nexus. Esto se puede cambiar a `ansible.netcommon.httpapi` para permitir la conectividad a través de NXAPI.
- La conexión de Ansible al extremo de Intersight requiere una clave de API, que se puede generar desde su cuenta de **intersight.com**.

Configuración de Nexus NXAPI (solo se utiliza si se utiliza `ansible.netcommon.httpapi`)

---



---

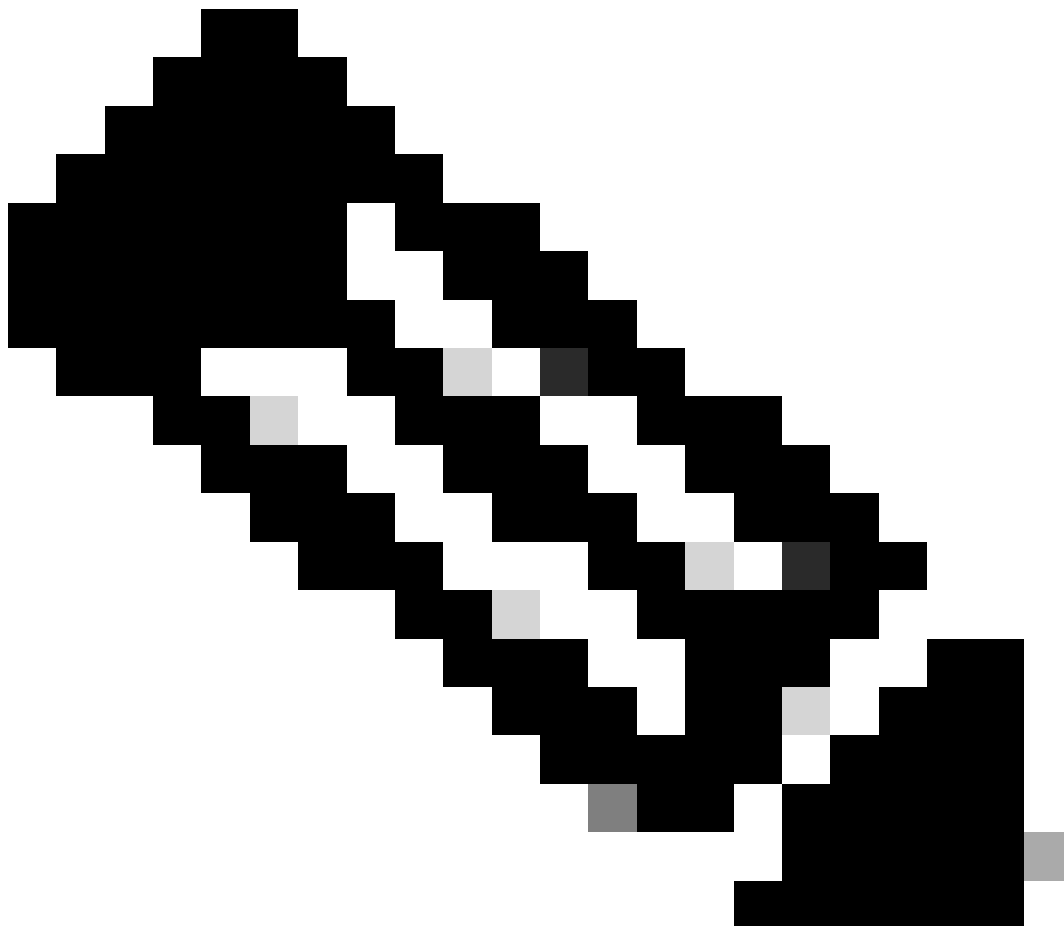
**Nota:** En el caso de que se configure un proxy de nivel de sistema (**HTTP(S)\_PROXY**) y Ansible no debe utilizar un proxy para conectarse con el extremo Nexus NXAPI, es deseable establecer `ansible_httpapi_use_proxy: False` (el valor predeterminado es `True`).

---

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

Para verificar independientemente la conectividad HTTP con el punto final de NXAPI, puede intentar enviar un mensaje `show clock`. En el siguiente ejemplo, el switch autentica al cliente mediante la autenticación básica. También es posible configurar el servidor NXAPI para autenticar clientes basados en el certificado de usuario X.509.

---





**Nota:** El hash de autenticación básica se obtiene de la codificación base64 de **username:password**. En este ejemplo, la codificación **admin:cisco!123** base64 es YWRtaW46Y2lzY28hMTIz.

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

Respuesta de rizo:

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

Generar claves de API de Intersight

Consulte la sección [README.md](#) para obtener información sobre cómo obtener la clave de API de la Intersight System > Settings > API keys > Generate API Key.

The screenshot shows the Cisco Intersight web interface. At the top, there's a navigation bar with the Cisco logo, 'Intersight', and 'System' dropdown. A search bar and several notification icons are on the right. Below the navigation bar, a warning message 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 content area is titled 'Settings' and has a sidebar on the left with various configuration categories. The 'API Keys' section is selected, showing a 'Generate API Key' button and a table with 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

Ejemplo: Ansible inventory.yaml



**Nota:** En el siguiente ejemplo, ansible se configuró para ignorar la configuración de proxy del sistema operativo con `ansible_httpapi_use_proxy: False`. Si necesita que el servidor Ansible utilice un proxy para alcanzar el switch, puede quitar esa configuración o establecerla en `True` (valor predeterminado).

---

---

**Nota:** El ID de clave de la API es una cadena. La clave privada de la API incluye la ruta de acceso completa a un archivo que contiene la clave privada. Para el entorno de producción, se recomienda utilizar la bóveda 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"
...

```

Ejemplo: playbook.yaml Ejecución

Para obtener más información sobre la programación de dispositivos Nexus independientes con Ansible, consulte la Applications/Using Ansible sección sobre Cisco NX-OS de la [Guía de programación de Cisco Nexus serie 9000 en NX-OS](#) para su versión actual.

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

### Verificación

Para verificar la reclamación de un nuevo destino, realice lo siguiente:

En el switch Nexus

Versiones anteriores a 10.3(4a)M

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

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

Versiones que comienzan con 10.3(4a)M

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

```
N9k-Leaf-2# show system device-connector claim-info SerialNumber: FD023021ZUJ SecurityToken: Duration: 0
```

```
# show system internal intersight info
```

```
# show system internal intersight info Intersight connector.db Info: ConnectionState :Connected Connect
```

Ansible

Es posible agregar una tarea al final del playbook,yamlpara obtener la información de la intercepción del switch.

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

Este es el resultado correspondiente:

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

Desactivar el conector de dispositivo

	Comando o acción	Propósito
Paso 1	<pre>no feature intersight</pre> <p>Ejemplo:</p> <pre>switch(config)# no feature intersight</pre>	Inhabilita el proceso de intersight y elimina toda la configuración de NXDC y el almacén de registros.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).