

Intersight接続用のスタンドアロンNexusの設定と要求

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[接続の利点](#)

[クイックスタートビデオ](#)

[NXOSデバイスの手動要求](#)

[接続の検証](#)

[OpenSSL Clientを使用したTLS検証](#)

[HTTPS到達可能性の検証](#)

[設定](#)

[デバイスの要求withinintersight.com](#)

[Nexusデバイス](#)

[Intersightポータル](#)

[Ansible®を使用して、intersight.com内で1対多のスタンドアロンNexusデバイスを主張する](#)

[Nexus NXAPIの設定 \(ansible.netcommon.httpapiを使用している場合のみ使用 \)](#)

[Intersight APIキーの生成](#)

例 : [Ansibleinventory.yaml](#)

例 : [playbook.yamlExecution](#)

[確認](#)

[Nexusスイッチ](#)

[10.3\(4a\)Mよりも前のリリース](#)

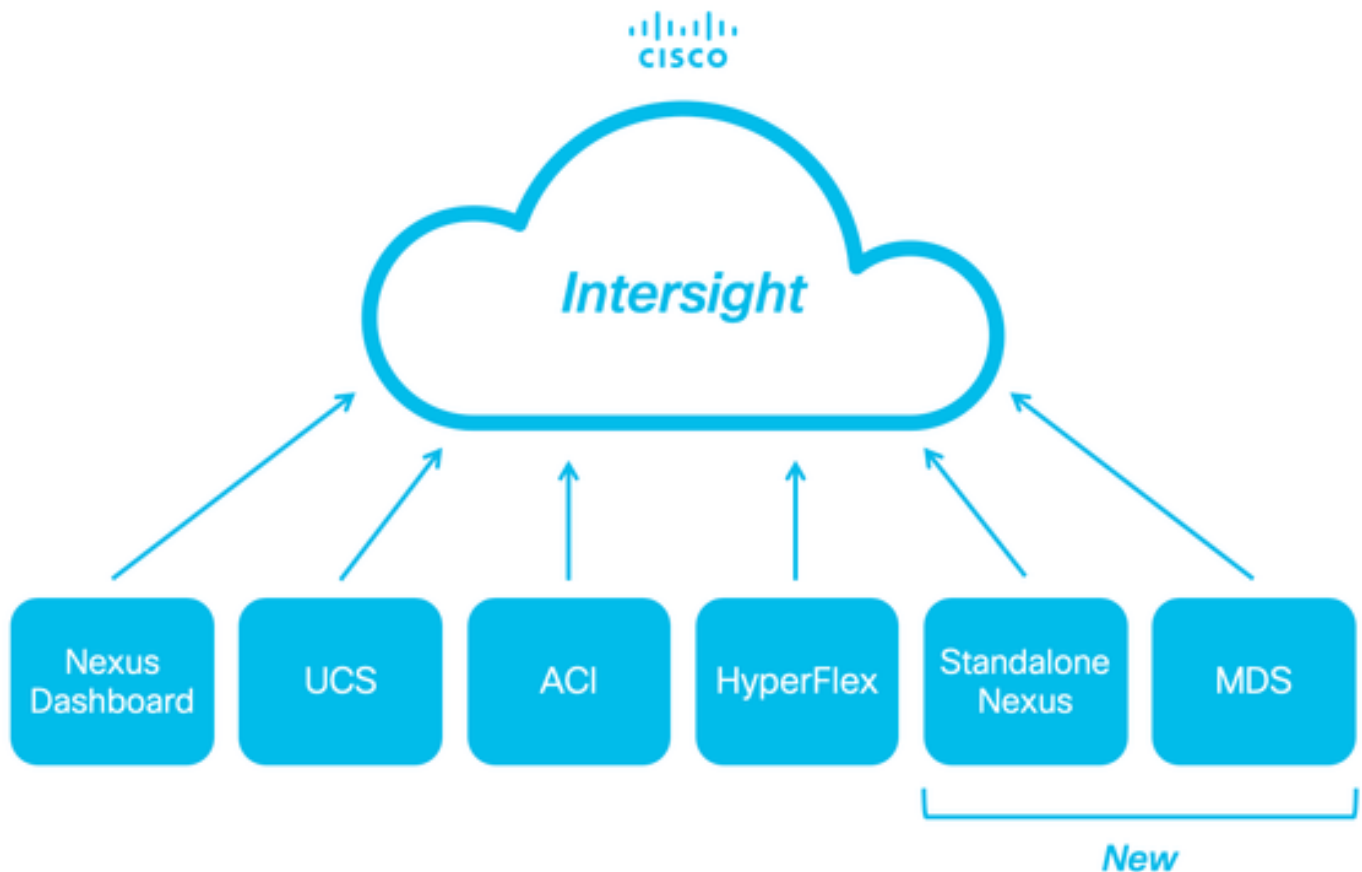
[10.3\(4a\)M以降のリリース](#)

[アンサブル](#)

[デバイスコネクタの無効化](#)

はじめに

このドキュメントでは、IntersightでスタンドアロンのNexusスイッチを有効にして要求し、Cisco TACサポートを強化するために必要な手順について説明します。



前提条件

[Intersight.com](https://intersight.com)のアカウントが必要です。Cisco NX-OS®のクレーム申請にはライセンスは必要ありません。新しいIntersightアカウントを作成する必要がある場合は、「[アカウントの作成](#)」を参照してください。

要件

次の項目に関する知識があることが推奨されます。

スタンドアロンNexusスイッチでは、NXDCに次のガイドラインと制限事項があります。

- リリース10.2(3)F以降を実行しているCisco NX-OS
- [DNS](#)は、適切なVirtual Routing and Forwarding(VRF)で設定する必要があります
- `svc.intersight.com` 解決され、ポート443で発信が開始されたHTTPS接続を許可する必要があります。これは、`openssl`および`curl`で確認できます。インターネット制御メッセージプロトコル(ICMP)要求は無視されます。
- へのHTTPS接続にプロキシが必要な場合は、Nexusスイッチデバイスコネクタ(NXDC)設定でプロキシを設定できます。
。 `svc.intersight.com`プロキシ設定については、「[NXDCの設定](#)」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Intersightは、高度なインフラストラクチャ、ワークロード最適化、およびKubernetesサービスのオプションのモジュラ機能で構成されるクラウド運用プラットフォームです。詳細については、「[Intersightの概要](#)」を参照してください。

デバイスは、各システムのCisco NX-OSイメージに組み込まれたNXDCを介してIntersightポータルに接続されます。Cisco NX-OSリリース10.2(3)F以降、デバイスコネクタ機能がサポートされるようになりました。この機能を使用すると、接続されたデバイスは、セキュアなインターネット接続を使用して、Cisco Intersightポータルで情報を送信したり、制御命令を受信したりできます。

接続の利点

Intersight接続は、Cisco NX-OSベースのプラットフォームに次の機能と利点を提供します。

- [迅速な問題解決](#)によるshow tech-support detailsの自動収集 (TACサービスリクエストのオープンのためのRPR)
- リモートオンデマンド収集 : show tech-support details
- 将来の機能は次のとおりです。
 - テレメトリまたはハードウェア障害に基づく予防的なTAC SRのオープン
 - 個々のshowコマンドなどのリモートオンデマンド収集

クイックスタートビデオ

NXOSデバイスの手動要求

接続の検証



注: ping応答は抑制されます (ICMPパケットはドロップされます)。

Transport Layer Security(TLS)とHTTPSの接続を確認するには、bashを有効にして、必要なVRF(ip netns exec <VRF>)でopensslコマンドとcurlコマンドを実行することが推奨されます。

! Enable bash

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

! Verify TLS

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

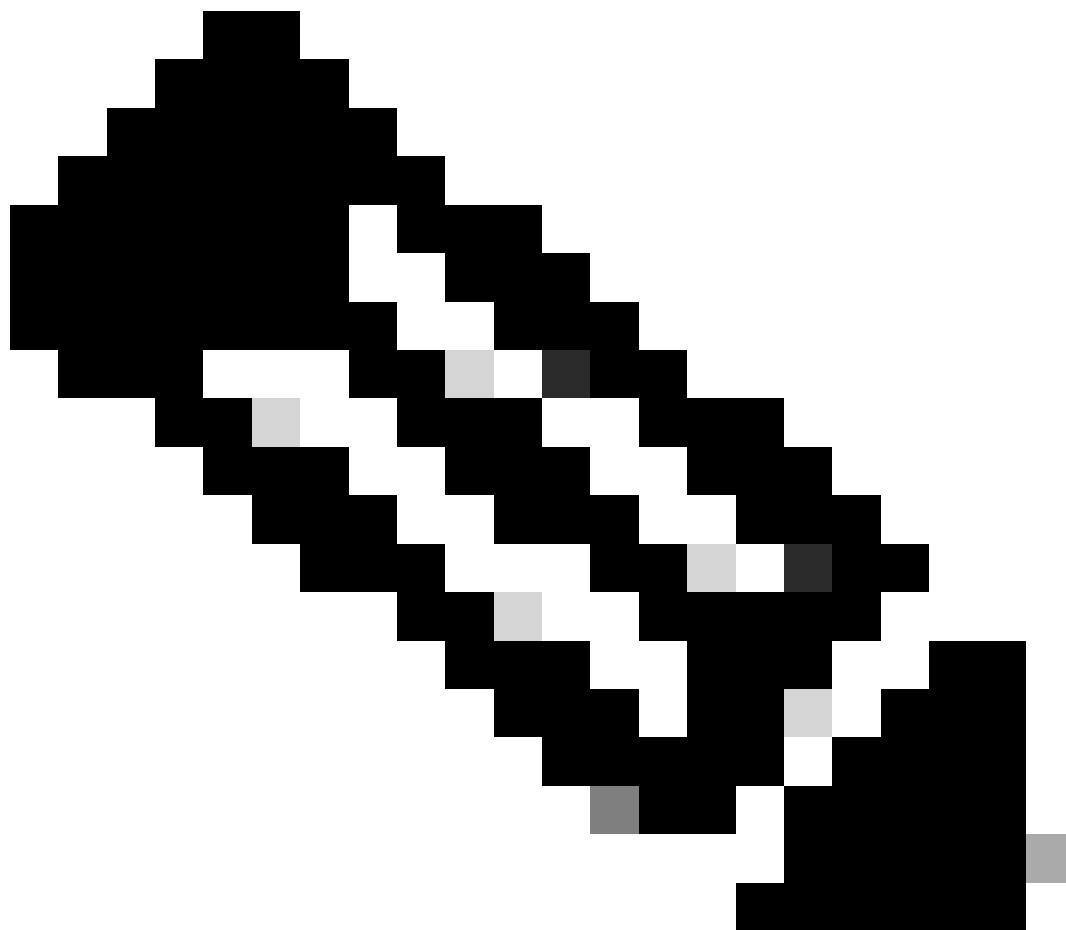
! Verify https

```
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 Clientを使用したTLS検証

OpenSSLを使用して、svc.intersight.com:443へのTLS接続を確認できます。正常に実行されると、サーバによって公開署名証明書が取得され、認証局チェーンが表示されます。

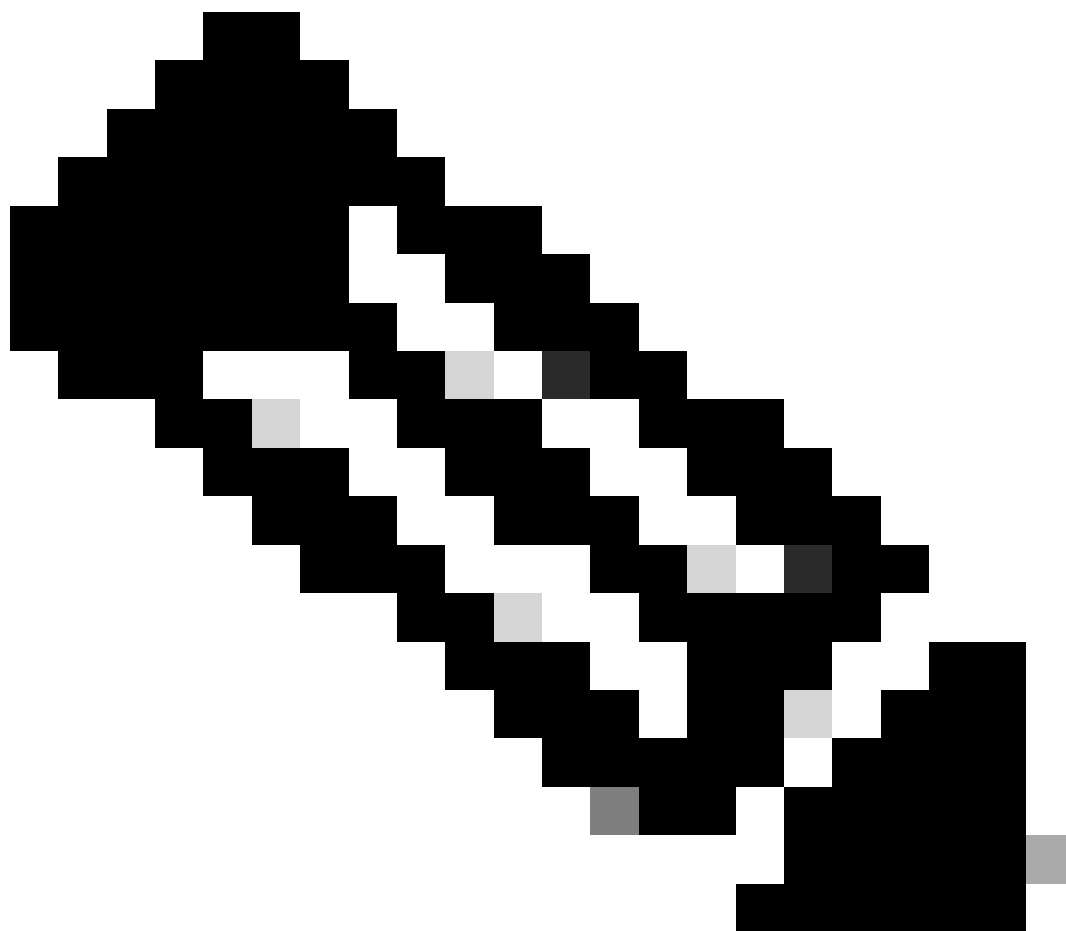


注：次の例は、VRF管理のopenssl s_clientコマンドを実行します。 ip netns exec <VRF>の構成で必要なものを置き換えます。

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

HTTPS到達可能性の検証

HTTPS接続を確認するには、`curl`コマンドと`-v` verbose flag (プロキシが使用されているかどうかを表示)を使用します。



注：プロキシを有効または無効にした結果を確認するには、`--proxy [protocol://]host[:port]`または`--noproxy [protocol://]host[:port]`のオプションを追加できます。

コンストラクトip netns exec <VRF>は、VRF管理などのために、目的のVRFでcurlを実行するために使用されます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.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 >

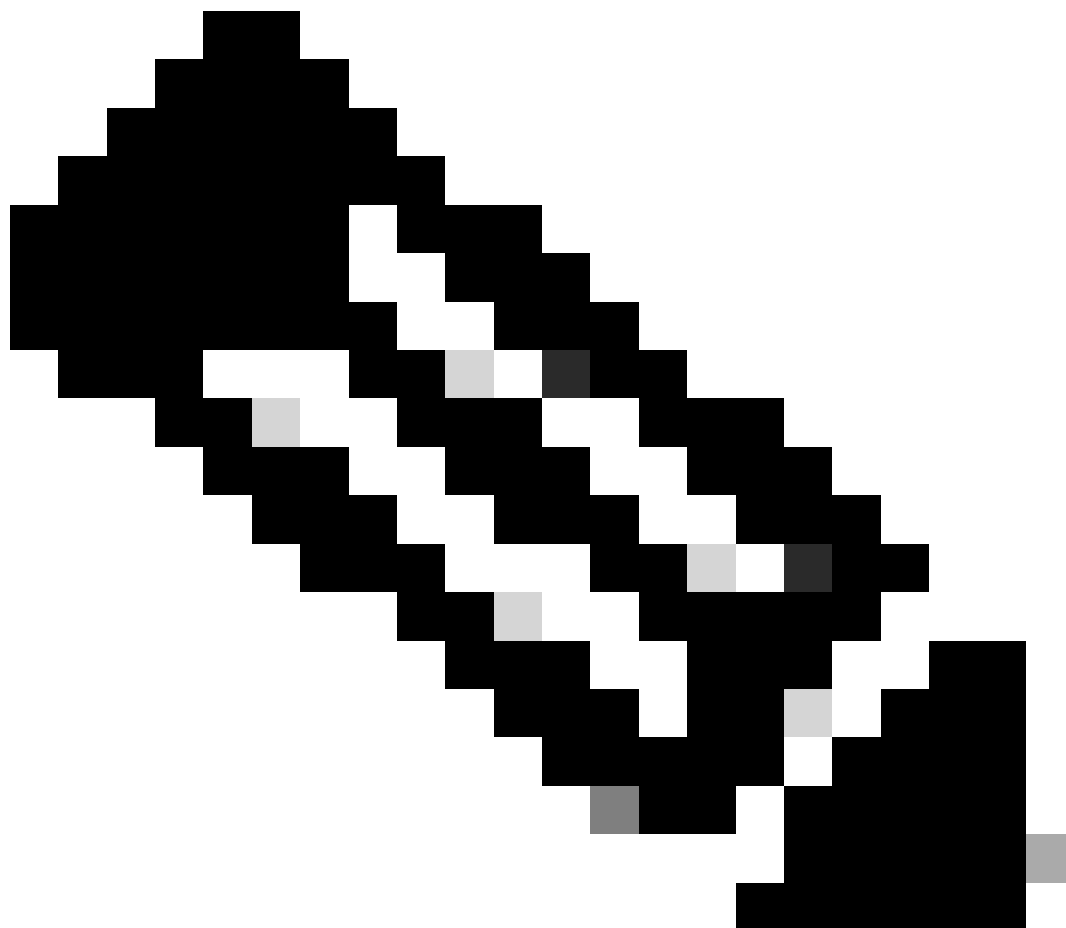
設定

内でデバイスを要求する intersight.com

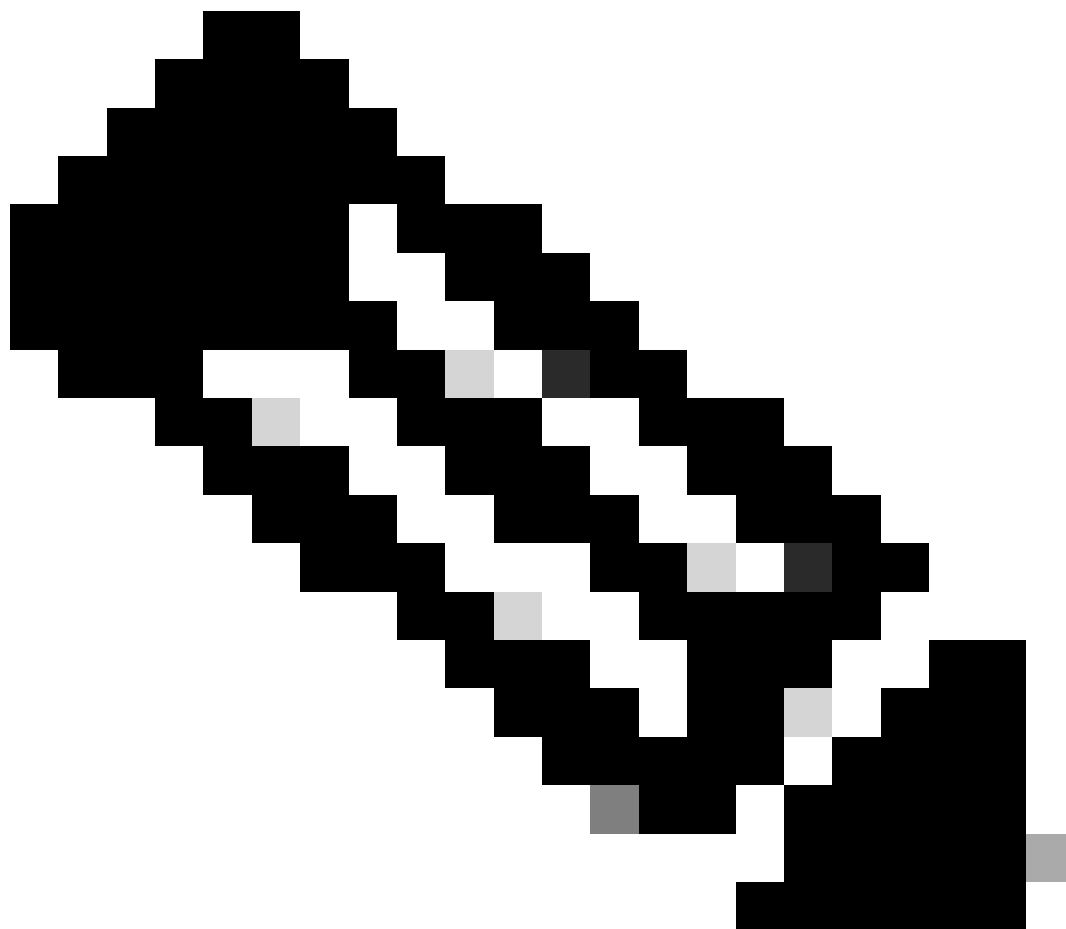
Intersightで新しいターゲットを要求するには、前述の手順を実行します。

Nexusデバイス

Cisco NX-OSコマンドshow system device-connector claim-infoを発行します。



注:NX-OS 10.3(4a)よりも前のリリースでは、「show intersight claim-info」コマンドを使用します。



注:Nexusが生成した請求情報は、次のIntersight要求フィールドにマッピングされます。

シリアル番号= Intersight **Claim ID**

デバイスIDセキュリティトークン= Intersight**要求コード**

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

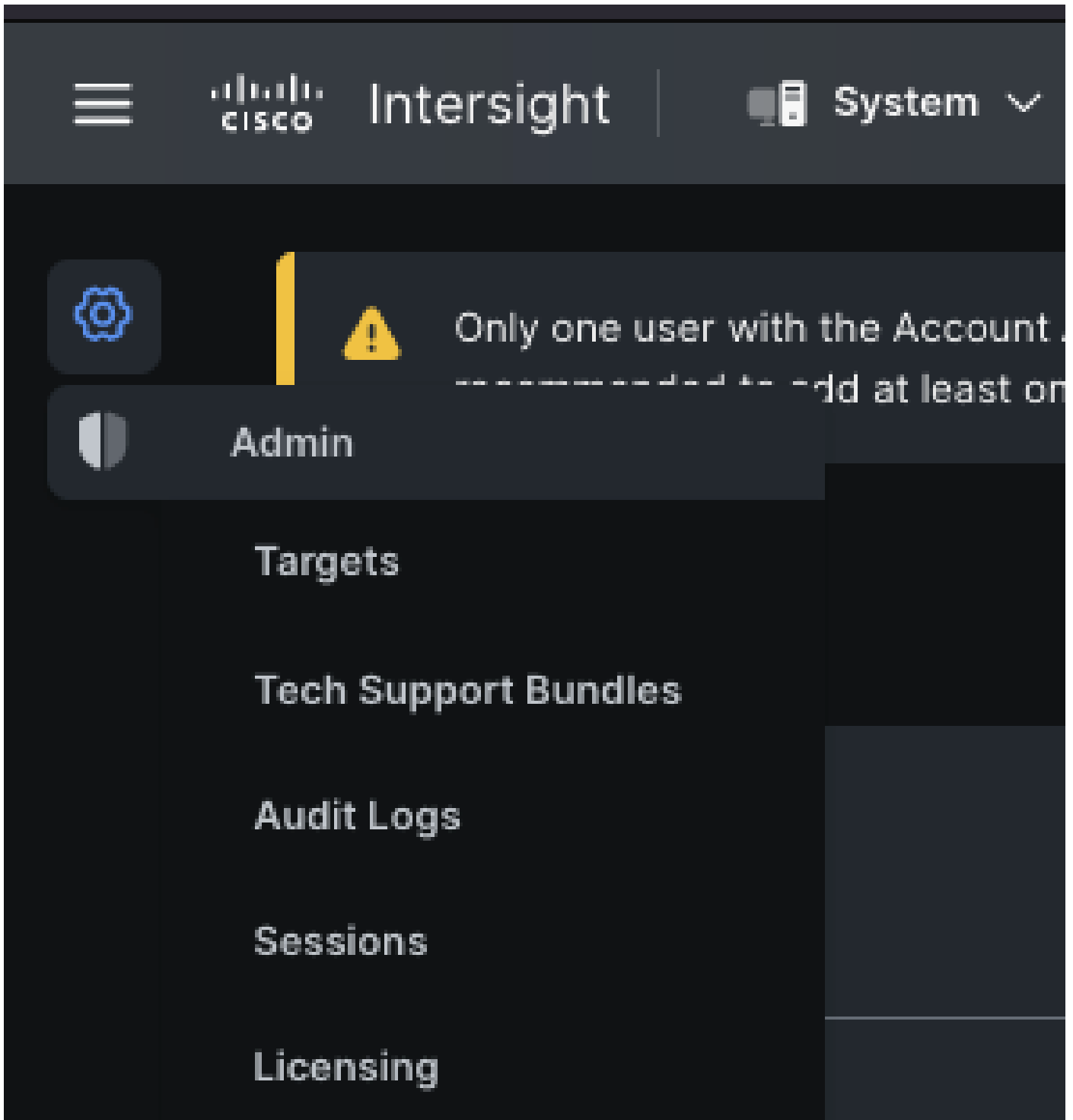
ここで報告される期間は秒単位です。

Intersight ポータル

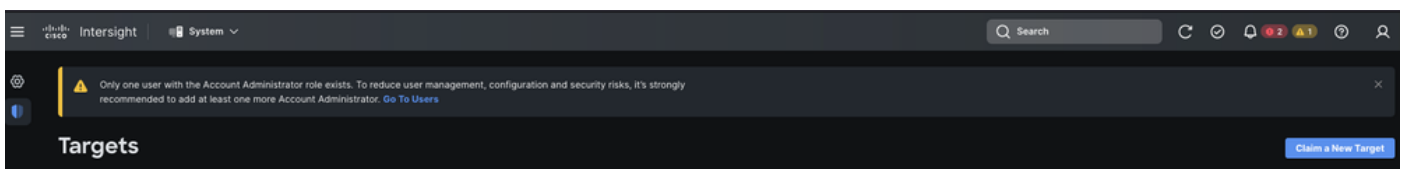
1. アカウント管理者、デバイス管理者、またはデバイス技術者の権限でIntersightに10分以内にログインします。
2. Service Selector ドロップダウンリストから、Systemを選択します。



3. ADMIN > Targets > Claim a New Targetに移動します。



3.1.図に示すように、**Claim a New Target**をクリックします。



4. 「要求に使用可能」を選択し、要求するターゲット・タイプ（ネットワークなど）を選択します。[Start（スタート）]をクリックします。



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

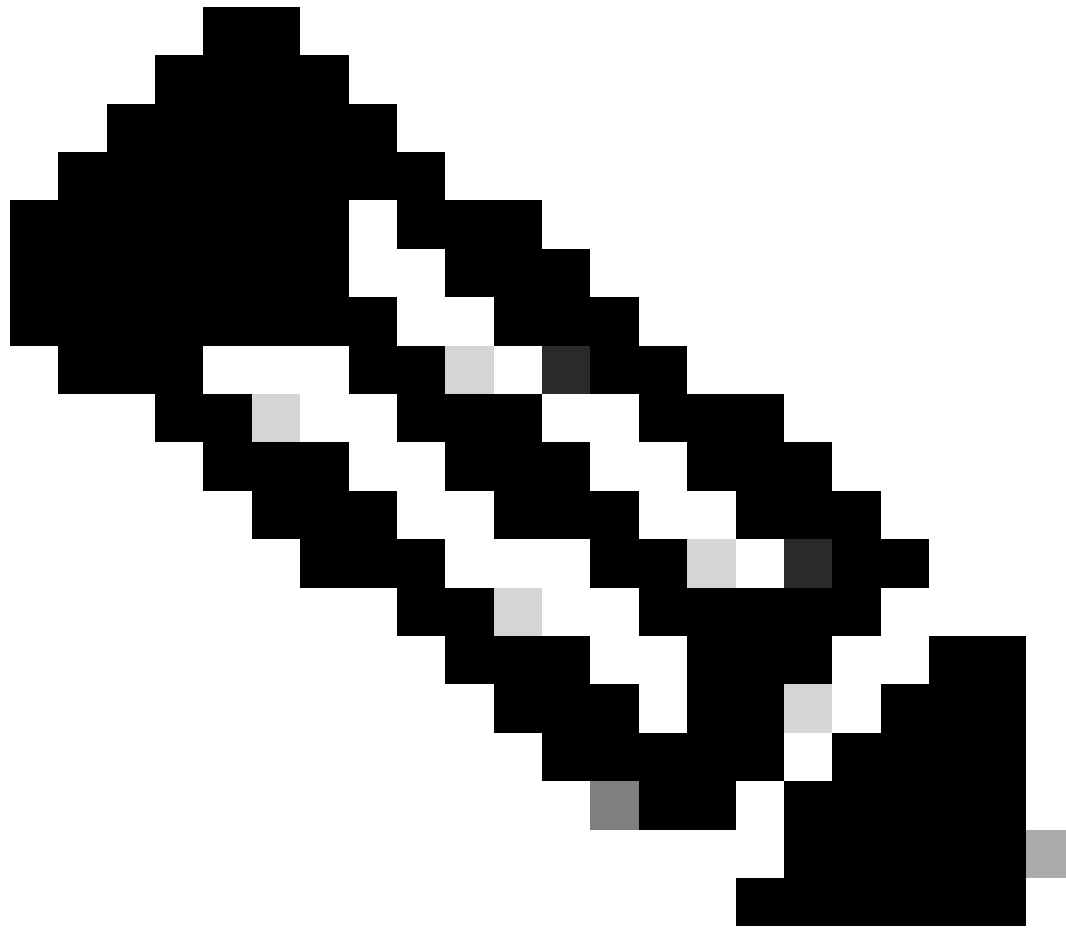
[Cancel](#)

[Start](#)

5. 必要な情報を入力し、請求をクリックして請求プロセスを完了します。



注：スイッチ上のセキュリティトークンはクレームコードとして使用され、スイッチのシリアル番号はデバイスIDです。
。



注：セキュリティトークンの有効期限が切れます。要求は前に完了する必要があります。完了しない場合、要求の再生成を求めるメッセージが表示されます。



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



[Details](#)

intersight.com内でAnsible®を使用して1対多のスタンドアロンNexusデバイスを主張する

1対多のNexusデバイスを要求するために、Ansibleプレイブックを実行できます。

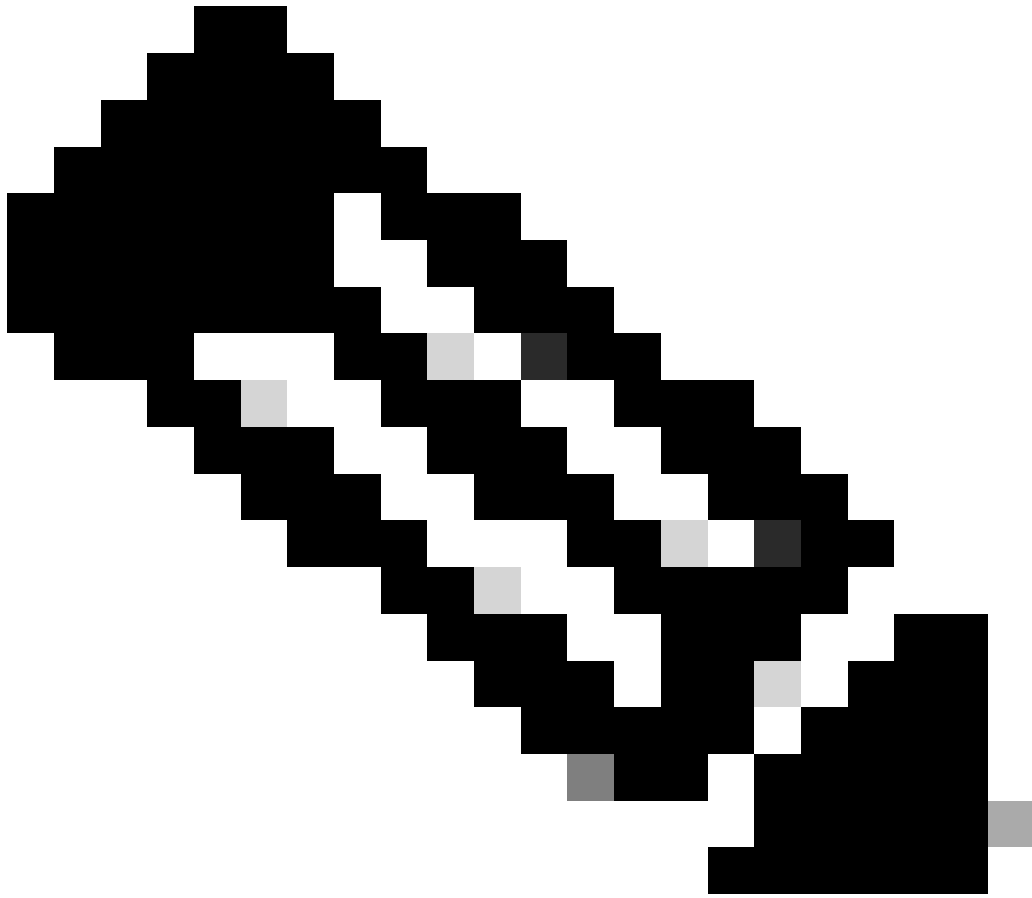
- ansibleのインベントリとプレイブックは、<https://github.com/datacenter/ansible-intersight-nxos>からgitクローンできます。
- Ansibleinventory.yamlでは、Nexusスイッチにコマンドを送信するために、ansible_connectionタイプがansible.netcommon.network_cliに設定されます。NXAPI経由の接続を許可するには、これをansible.netcommon.httpapiに変更できます。
- Intersightエンドポイントへの応答可能な接続には、intersight.comアカウントから生成できるAPIキーが必要です。

Nexus NXAPIの設定(ansible.netcommon.httpapiを使用する場合のみ使用)

注：システムレベルのプロキシが設定されていて(HTTP(S)_PROXY)、AnsibleがNexus NXAPIエンドポイントに接続するためにプロキシを使用してはいけない場合、ansible_httppapi_use_proxy: False (デフォルトはTrue) を設定することが望ましい。

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

NXAPIエンドポイントへのHTTP接続を単独で確認するには、show clockを送信できます。次の例では、スイッチは基本認証を使用してクライアントを認証します。X.509ユーザ証明書に基づいてクライアントを認証するようにNXAPIサーバを設定することもできます。



注：基本認証ハッシュは、**username:password**のbase64エンコーディングから取得されます。この例では、**admin:cisco!123** base64エンコーディングはYWRtaW46Y2lzY28hMTIzです。

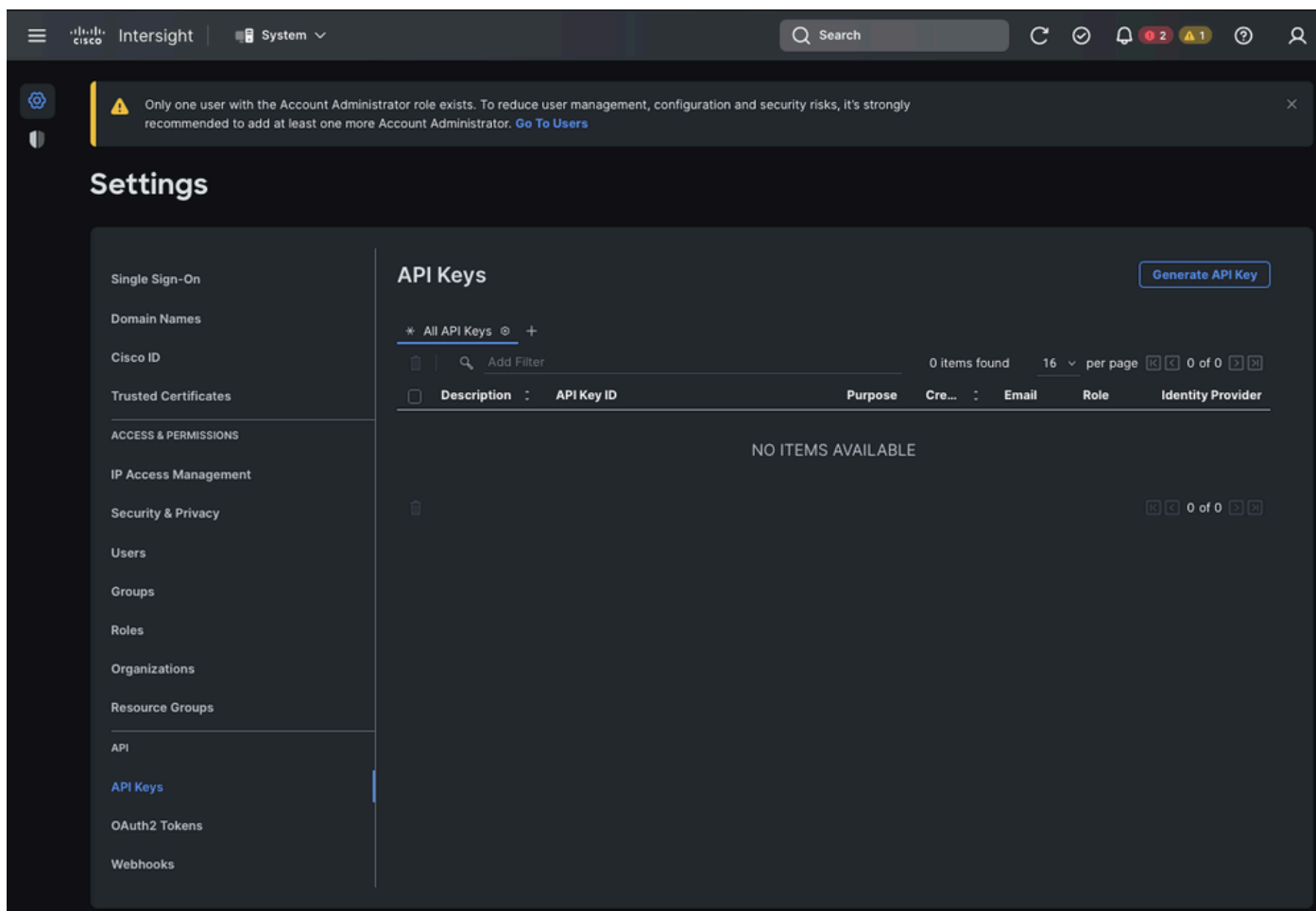
```
curl -v --no-proxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

Curl応答：

```
* 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キーの生成

Intersight System > Settings > API keys > Generate API KeyからAPIキーを取得する方法については、「[README.md](#)」のセクションを参照してください。



The screenshot shows the Intersight Settings page. At the top, there is a navigation bar with the Cisco Intersight logo, a search bar, and system status indicators. A warning message is displayed: "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 contains a sidebar with various configuration options. The "API Keys" section is selected, showing a "Generate API Key" button. Below this, there is a table header for "API Keys" with columns: Description, API Key ID, Purpose, Cre..., Email, Role, and Identity Provider. The table currently displays "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

例：Ansible inventory.yaml



注：次の例では、ansibleは、`ansible_httppapi_use_proxy: False`によるオペレーティングシステムのプロキシ設定を無視するように設定されています。スイッチに到達するためにAnsibleサーバでプロキシを使用する必要がある場合は、その設定を削除するか、`True`（デフォルト）に設定します。

注:APIキーIDは文字列です。API秘密キーには、秘密キーを含むファイルへの完全パスが含まれます。実稼働環境では、Ansibleポールの使用することをお勧めします。

```
---
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"
...

```

例 : playbook.yaml Execution

Ansibleを使用したスタンドアロンNexusデバイスのプログラミングの詳細については、現在のリリースの『[Cisco Nexus 9000 Series NX-OS Programmability Guide](#)』の「Applications/Using Ansible with the Cisco NX-OS」の項を参照してください。

```

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

```

確認

新しいターゲットの要求を確認するには、次の手順を実行します。

Nexusスイッチ

10.3(4a)Mよりも前のリリース

```
# bash sudo cat /mnt/pss/connector.dbを実行します
```

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

10.3(4a)M以降のリリース

```
# 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
```

アンサブル

スイッチのインターサイト情報を取得するために、playbook.yamlの最後にタスクを追加できます。

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

対応する出力を次に示します。

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

デバイスコネクタの無効化

	コマンドまたはアクション	目的
ステップ 1	<p data-bbox="180 504 347 533">機能の介入なし</p> <p data-bbox="180 779 408 808">以下に例を挙げます。</p> <pre data-bbox="180 987 719 1016">switch(config)# no feature intersight</pre>	<p data-bbox="860 600 1477 663">Intersightプロセスを無効にし、すべてのNXDC設定とログストアを削除します。</p>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。