Cisco NFVIS SD-Branch ソリューションの操作

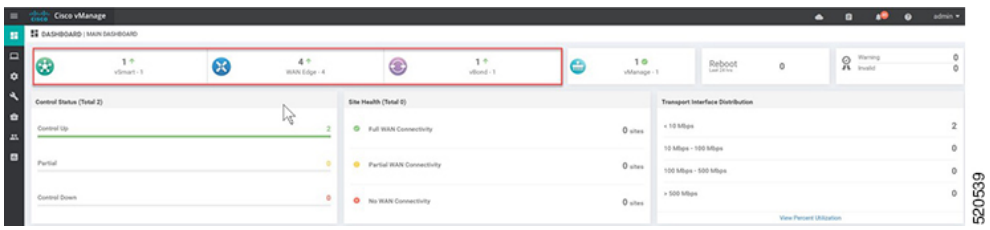
Cisco vManage を使用して、WAN エッジデバイスをモニタ、トラブルシューティング、および管理できます。ここでは、一般的なトラブルシューティングとモニタリングの手順について説明します。

Cisco vManage を使用した SD-WAN コンポーネントのステータスの監視と管理

Cisco vManage ダッシュボード画面を使用して、SD-WAN オーバーレイネットワークの全体的な状態をモニタします。

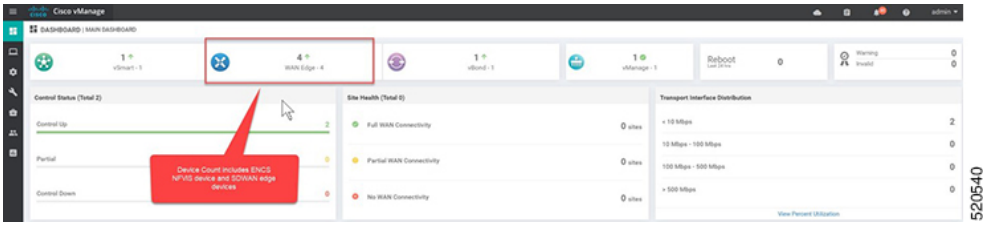
デバイスペインによる SD-WAN コンポーネントの監視

1. Cisco vManage メインダッシュボードで、ダッシュボード画面の上部にある [Device Pane] を表示します。このペインには、Cisco vManage からオーバーレイネットワークの vSmart コントローラ、vEdge ルータ、および vBond オーケストレータへのすべての制御接続が表示されます。ペインには、ネットワーク内の Cisco vManage のステータスも表示されます。すべての SD-WAN コンポーネントの接続が確立されていることを確認します。

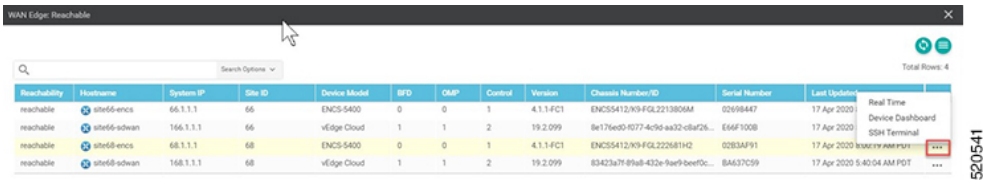


デバイスペインによる WAN エッジデバイスの詳細と統計情報の表示

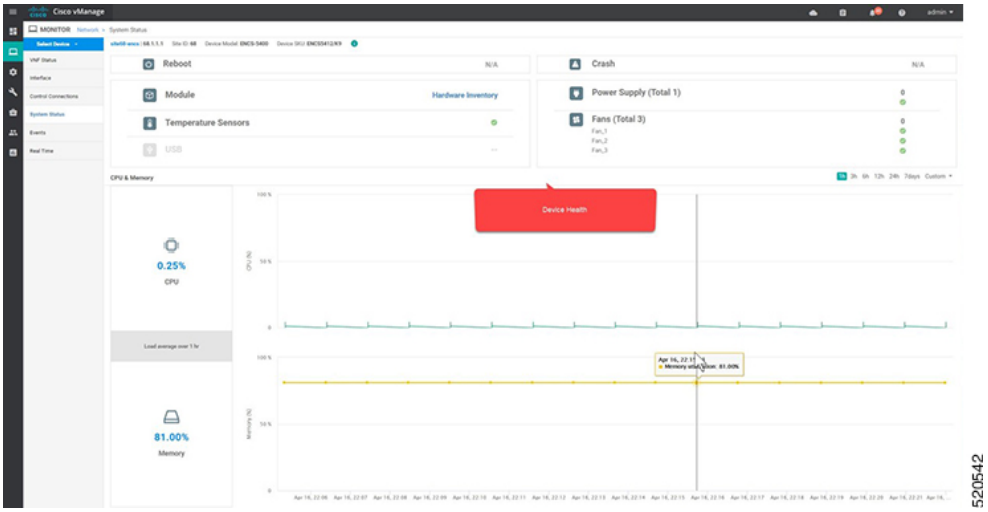
1. Cisco vManage メインダッシュボードで、デバイス統計情報を表示するには、番号または WAN エッジの上にある上下の矢印（4）をクリックして、各接続の詳細情報を含むテーブルを表示します。



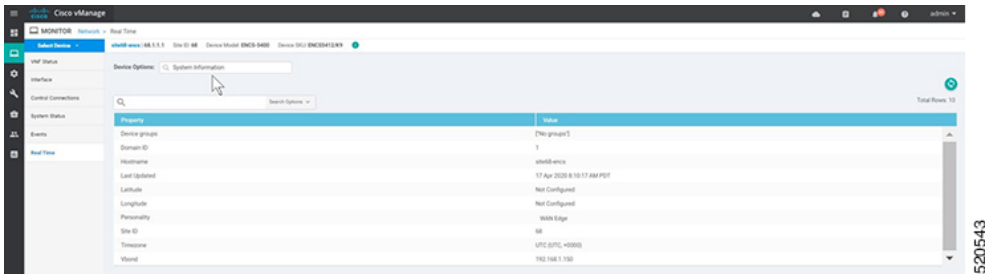
2. テーブルには、[System IP]、[Site ID]、[Device Model]、[Software Version] などが表示されます。デバイス固有の詳細については、各行の末尾にある [...] をクリックしてください。ここから、[Device Dashboard]、[Real Time data]、または [SSH Terminal] にアクセスできます。



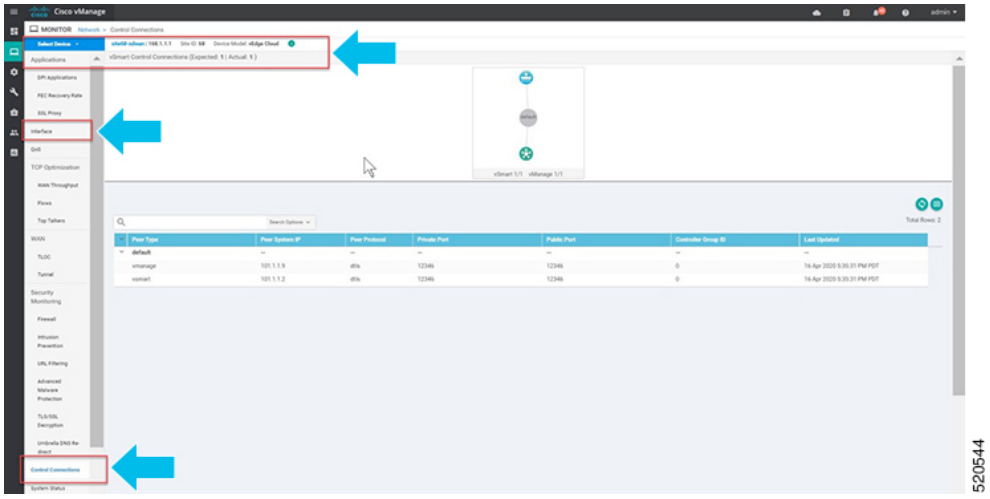
[Device Dashboard] には、デバイスの [System Status]、デバイスの [Module Hardware Inventory] 情報、[CPU & Memory] のリアルタイム統計情報が表示されます。



[Real Time] には、[Site ID]、[Vbond]、[Hostname]、[Latitude]、[Longitude] など、デバイスの基本的なシステム情報が表示されます。

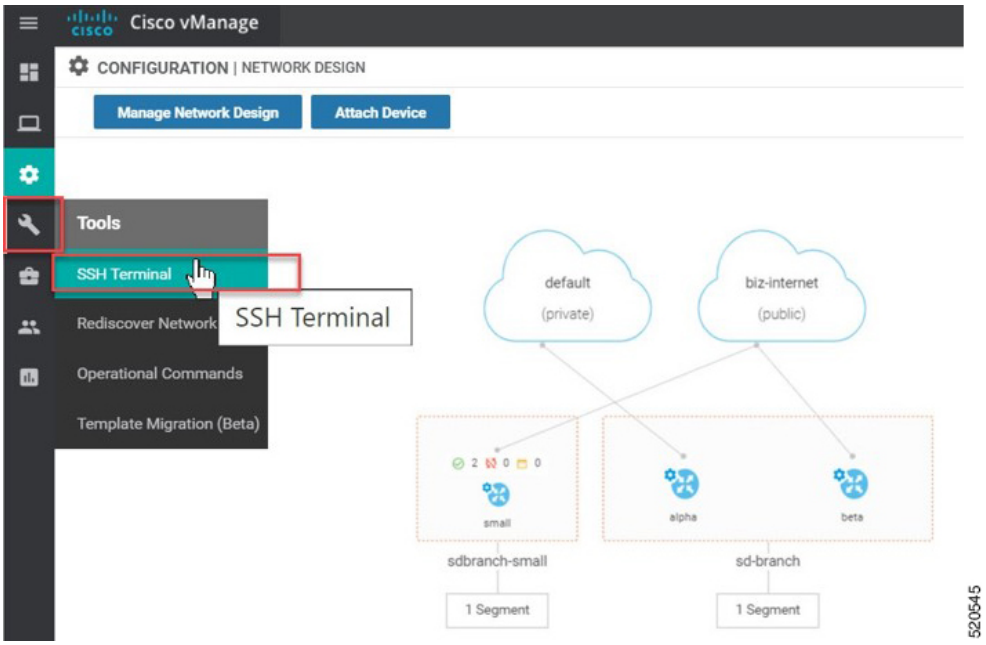


3. WAN エッジデバイスのインターフェイスを介した [Control Connections] などの追加情報は、Cisco vManage から表示できます。[Cisco vManage] メニューから**[Monitor]** > **[Network]** を選択し、リストからデバイスを選択して、左側のパネルからデバイス情報を探します。



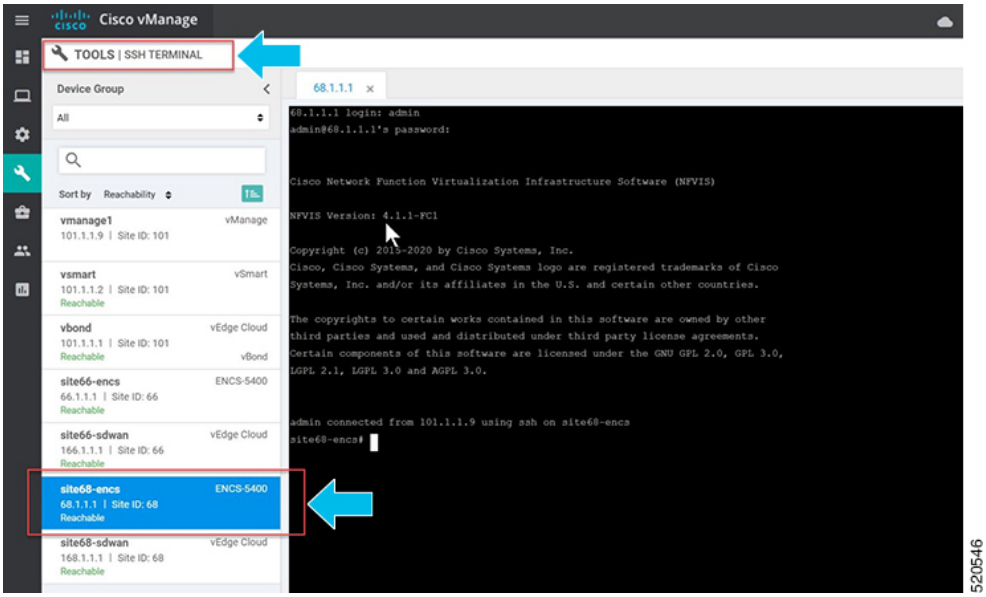
CLI コマンドを使用した Cisco vManage SSH サーバーダッシュボードによる WAN エッジデバイスの監視

1. [Cisco vManage] メニューから、**[Tools]** > **[SSH Terminal]**を選択します。



2. [Device Group] から WAN エッジを選択します。

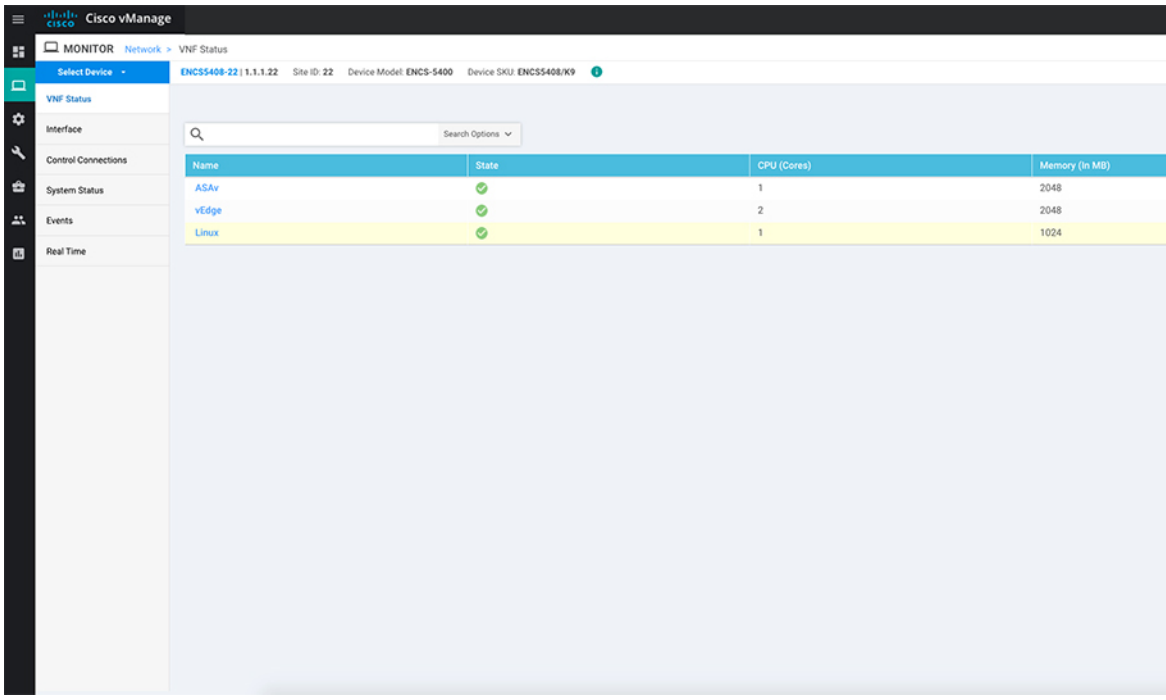
   WAN エッジデバイスが SD-WAN コントローラとのセキュアな制御接続を確立したかどうかを確認するには、**show control connections** コマンドを入力します。



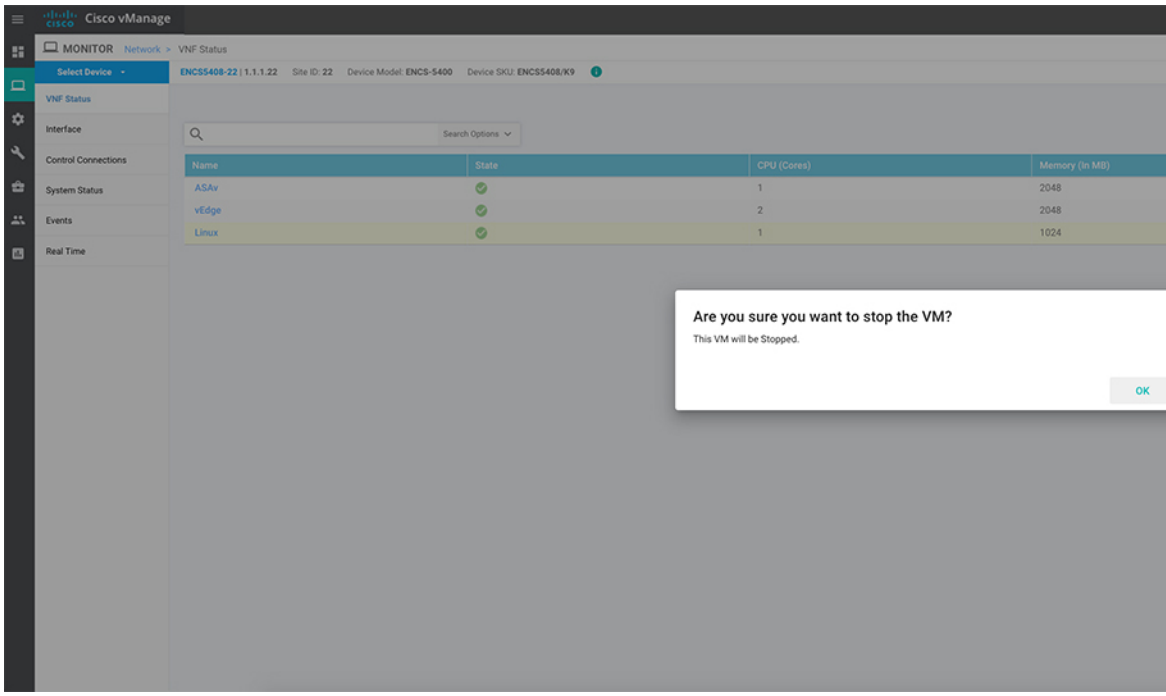
WAN エッジデバイスの開始、停止、および再起動

1. [Cisco vManage] メニューから、[Monitor]、[Network] の順に選択します。
2. WAN エッジデバイスを選択します。

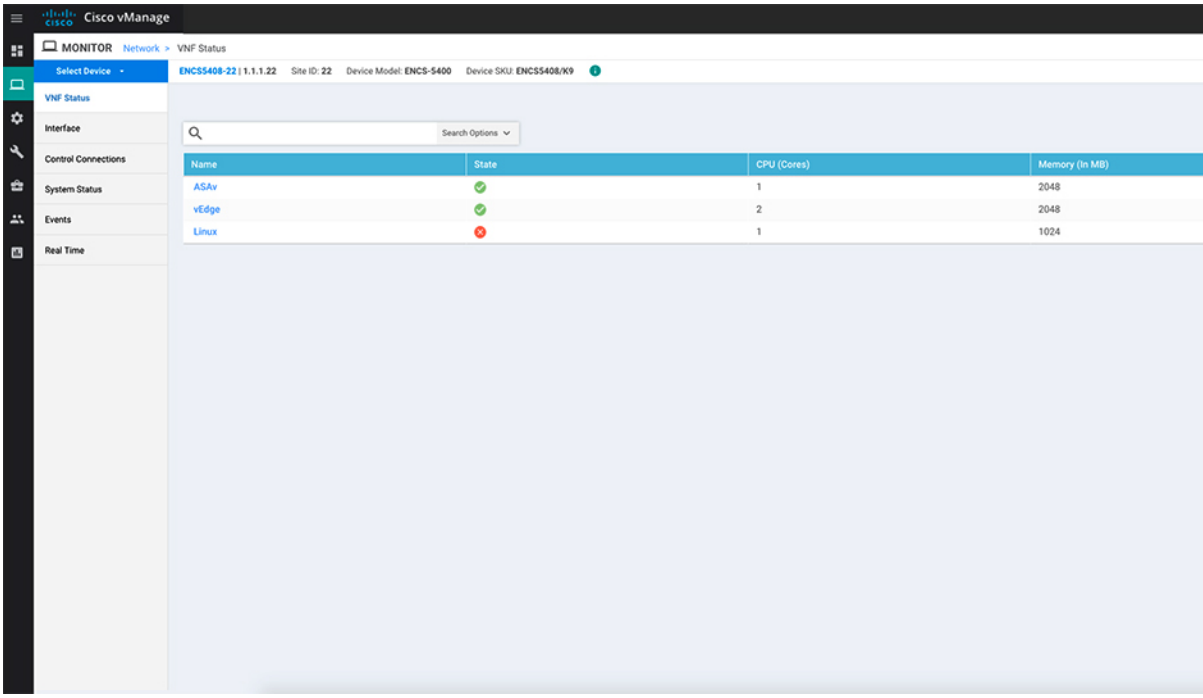
3. デバイスに展開された VM のリストが画面に表示されます。VM の横にある [...] をクリックして、デバイスを起動、停止、または再起動します。



次の例は、VM の停止方法と VM のステータスの変化を示しています。



注 VM のステータスを表示するには、Cisco vManage メニューから**[Tools]** > **[Discover Network]**を選択します。[Device] を選択し、[Rediscover] をクリックして最新のステータスを同期します。



vmAction vmName Linux actionType STOP/START/REBOOTコマンドを使用して VM を起動、停止、または再起動することもできます。VM のステータスを表示するには、**show system:system deployments**または**show vm_lifecycle deployments all**コマンドを使用します。

```
Device# vmAction vmName Linux actionType STOP

Device# show system:system deployments
NAME   ID  STATE
--------------------
ASAv   1   running
vEdge  2   running
Linux  -   shut
```

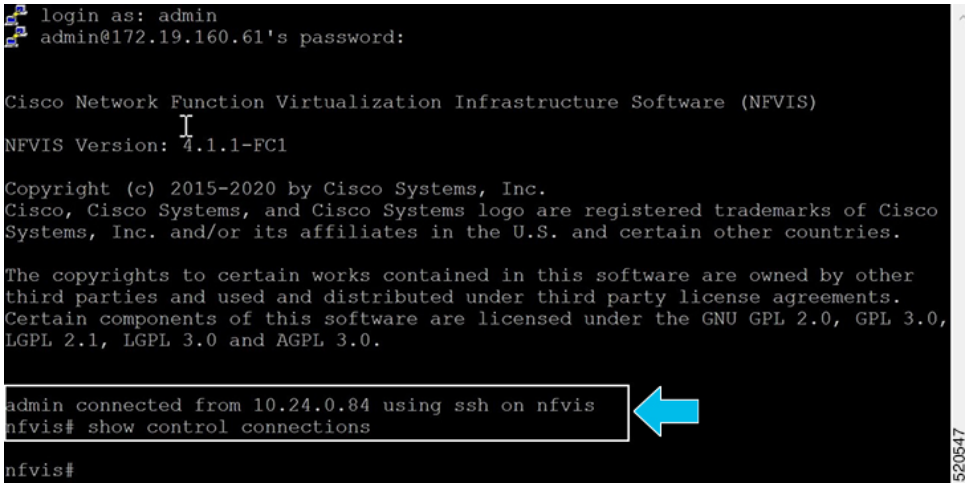
デバイスオンボーディングのトラブルシューティング

ここでは、一般的なトラブルシューティング手順について説明します。

オンボーディングの問題の診断

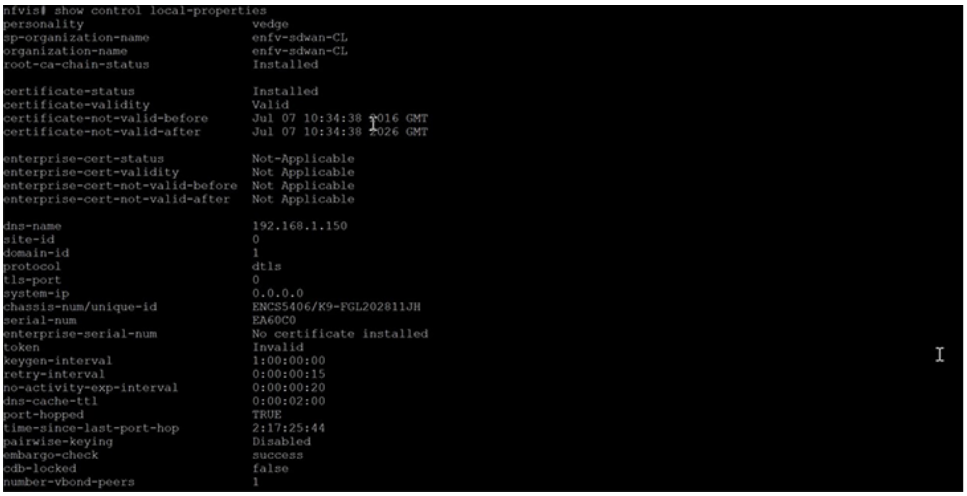
ここでは、WAN エッジデバイスのオンボーディングプロセス中に発生する可能性のある最も一般的な問題と、問題を解決するための推奨される解決方法について説明します。

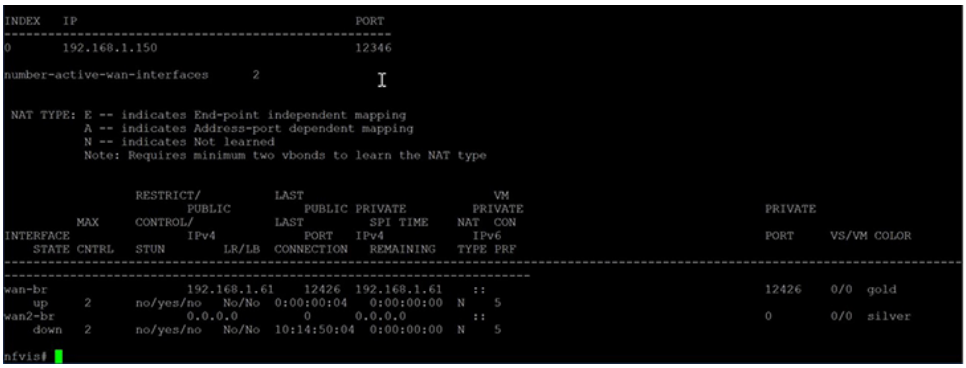
1. WAN エッジデバイスが SD-WAN コントローラとのセキュアな制御接続を確立したことを確認するには、**show control connections**コマンドを入力します。



2. WANエッジデバイスの認証に使用されるデバイスプロパティを確認するには、**show control local-properties**コマンドを入力します。

出力で、次のことを確認します。

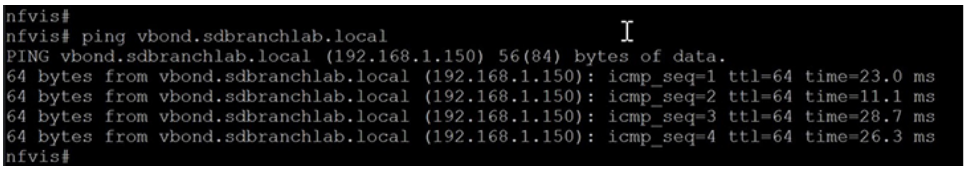




- システムパラメータは、organization-name と site-id を含むように設定されている
- certificate-status および root-ca-chain-status がインストールされている
- certificate-validity が有効になっている
- dns-name が vBond IP アドレス/DNS を指している
- system-ip が設定されており、chassis-num/unique-id および serial-num/token がデバイスで使用可能

上記のパラメータは、接続を確立する前に SD-WAN コントローラと相互認証するために WAN エッジデバイスで使用できる必要があります。

3. WAN エッジデバイスから vBond コントローラの到達可能性を確認するには、次の手順を実行します。



4. WAN エッジデバイスが SD-WAN コントローラとの接続を確立できない場合は、**show control connections-history** コマンドを入力して失敗の理由を表示します。[LOCAL ERROR] および [REMOTE ERROR] 列を表示して、エラーの詳細を収集します。

以下に、WAN Edge デバイスが SD-WAN コントローラとの制御接続を確立できない理由の一部を示します。

CRTVERFL：エラー状態は、WAN デバイスと SD-WAN コントローラ間のルート CA 証明書の不一致が原因で、WAN エッジデバイスの認証が失敗したことを示します。vEdge デバイスでは show certificate root-ca-cert を使用し、IOS-XE SD-WAN デバイスでは show sdwan certificate root-ca-cert を使用して、同じ証明書が WAN Edge デバイスと SD-WAN コントローラにインストールされていることを確認します。

CTorgNMMIS：エラー状態は、SD-WAN コントローラで設定された組織名と比較して、組織名が一致しないために WAN エッジデバイスの認証が失敗したことを示します。vEdge デバイスで show sdwan control local-properties を使用し、IOS-XE SD-WAN デバイスで show sdwan control local-properties を使用して、すべての SD-WAN コンポーネントが SD-WAN 環境全体で同じ組織名で設定されていることを確認します。

NOZTPEN：エラー状態は、オンボーディング vEdge デバイスが ZTP サーバー上の承認済みホワイトリストデバイスの一部ではないことを示します。オンプレミス ZTP サーバーで show ztp entry を使用して、デバイスのホワイトリストを確認します。

NOVMCFG：エラーステータスは、WAN エッジデバイスが Cisco vManage のデバイステンプレートにアタッチされていないことを示します。このステータスは、自動展開オプション（PnP または ZTP プロセス）を使用してデバイスをオンボーディングするときに表示されます。

VB_TMO、VM_TMO、VP_TMO、VS_TMO：このエラーは、WAN エッジデバイスが SD-WAN コントローラに到達できないことを示します。

5. WAN エッジデバイスの制御接続を確認するには、次の show コマンドを使用します。

   - **show control connections**
   - **show control connections-history**
   - **show control connections-info**
   - **show control local-properties**
   - **show control statistics**
   - **show control summary**

- **show control valid-vmanage-id**

ルート CA 証明書が WAN エッジデバイスで不明になっている

オンボーディングプラットフォームのルートCAチェーン証明書がない場合、デバイス認証は失敗します。デバイス認証の失敗では、SD-WAN コントローラへの制御接続を確立できません。次の手順は、デバイスコンポーネントにルートCA証明書をインストールする方法を示しています。

デバイスにログインし、**show control local-properties**コマンドから root-ca-chain ステータスを表示します。次の例は、root-ca-chain-status が **Not-Installed** 状態であることを示す出力例です。

```
show control local-properties
personality                     vedge
sp-organization-name            ENB-Solutions -21615
organization-name               ENB-Solutions -21615
root-ca-chain-status            Not-Installed
```

次に、NFVIS にルート証明書をアップロードする方法の例を示します。

```
nfvis# request root-cert-chain install scp://admin@10.28.13.168
Uploading root-ca-cert-chain via VPN 0
Enter directory of root CA certificate file : /ws/admin-sjc/
Enter root CA certificate file name (default: root-ca.crt) : TPMRootChain.pem
Copying ... admin@10.28.13.168:/ws/admin-sjc//TPMRootChain.pem via VPN 0
Warning: Permanently added '10.28.13.168' (ECDSA) to the list of known hosts.

WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON

This System is for the use of authorized users only. Individuals
using this computer without authority, or in excess of their
authority, are subject to having all of their activities on this
system monitored and recorded by system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement
officials.

Cisco Acceptable Use Policy:
http://wwwin.cisco.com/c/cec/organizations/security-trust/infosec/policies.html

admin@10.28.13.168's password:
TPMRootChain.pem 100% 7651 1.8MB/s 00:00
Updating the root certificate chain..
Successfully installed the root certificate chain
nfvis#
```