

Operate Cisco NFVIS SD-Branch Solution

You can monitor, troubleshoot and manage the WAN Edge devices using Cisco SD-WAN Manager. Some of the common troubleshooting and monitoring steps are covered in this section.

- Monitor and Manage the Status of Cisco Catalyst SD-WAN Control Components using Cisco SD-WAN Manager, on page 1
- Troubleshooting Device Onboarding , on page 7

Monitor and Manage the Status of Cisco Catalyst SD-WAN Control Components using Cisco SD-WAN Manager

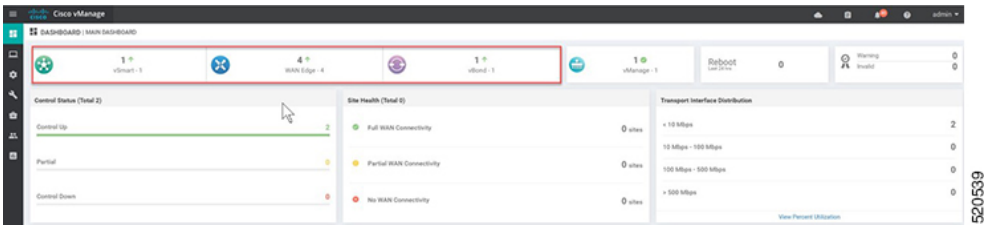
From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, to monitor the overall health of the Cisco Catalyst SD-WAN overlay network.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** to monitor the overall health of the Cisco Catalyst SD-WAN overlay network.

Monitor the Cisco Catalyst SD-WAN Control Components Through Device Pane

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, to view the **Hero Bar** with five panes, which runs across the top of the dashboard screen that displays all the control connections from Cisco SD-WAN Manager to the Cisco SD-WAN Controller, vEdge routers, and Cisco SD-WAN Validator in the overlay network. The pane also displays the status of the Cisco SD-WAN Manager in the network. Ensure that the connections for all the Cisco SD-WAN Control Components are up.

Note In Cisco vManage Release 20.6.x and earlier releases, the **Device Pane** is part of the **Dashboard** > **Main Dashboard** page.

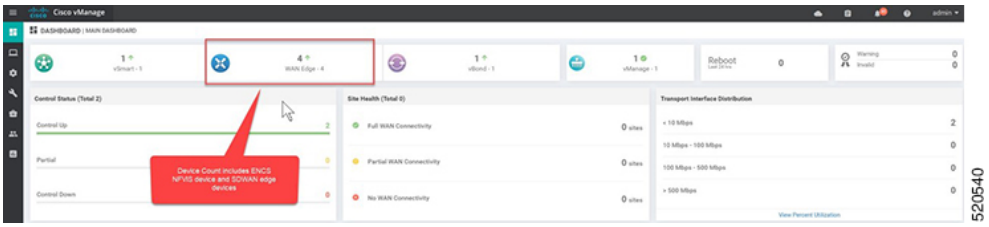


View WAN Edge Device Details and Statistics Through Device Pane

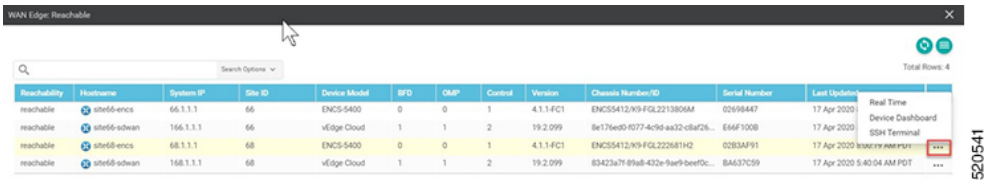
1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

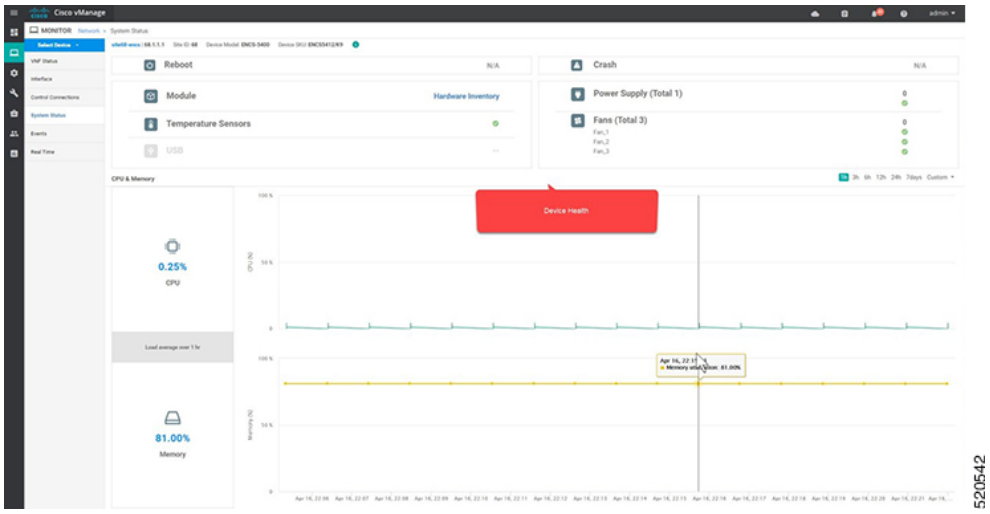
2. To view device statistics, click on the number, to display a table with detailed information for each connection.



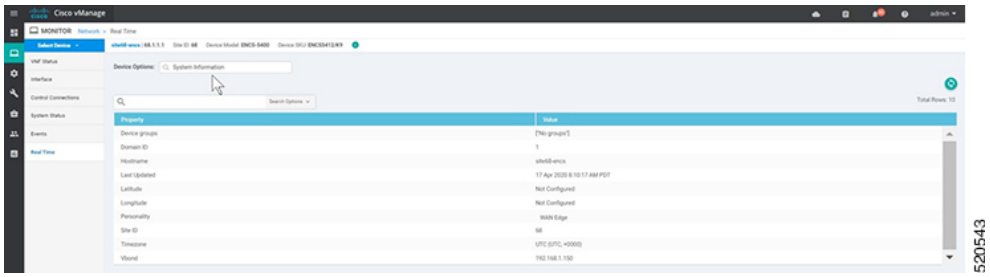
3. The table lists **System IP**, **Site ID**, **Device Model**, **Software Version** and more. For more device-specific information, click **…** at the end of each row. From here you can access **Device Dashboard**, **Real Time data**, or the **SSH Terminal**.



The **Device Dashboard** displays the **System Status** of the device, the device **Module Hardware Inventory** information, **CPU & Memory** real time statistics.

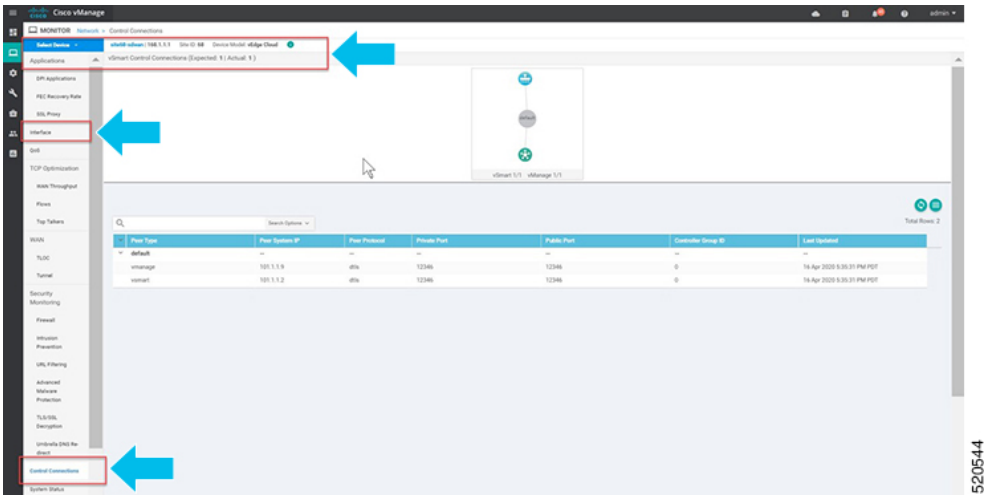


Real Time displays the basic system information of the device such as **Site ID**, **Vbond**, **Hostname**, **Latitude**, **Longitude** and more.



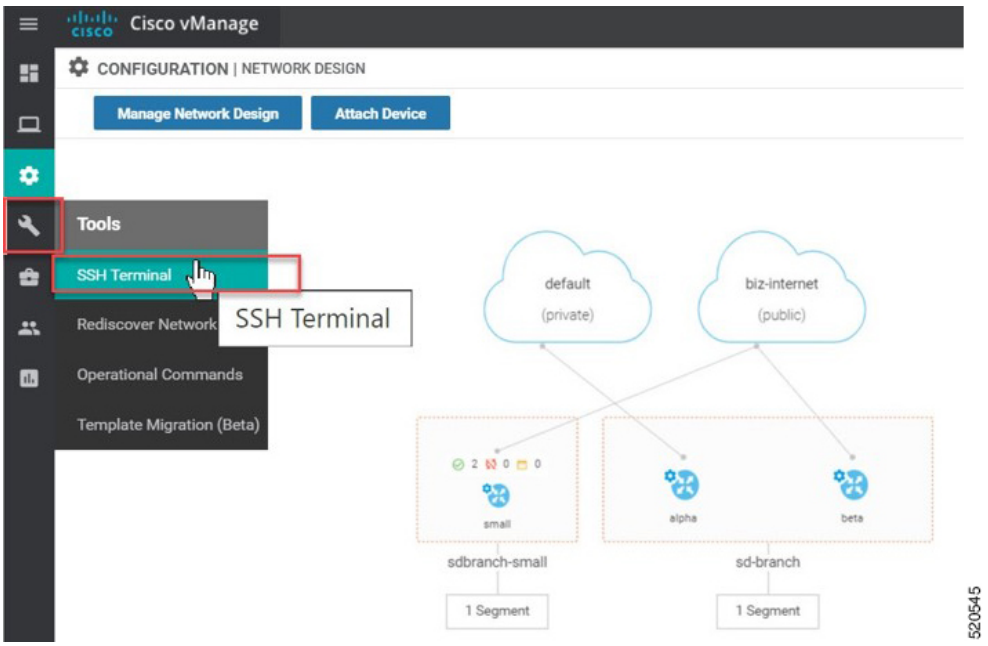
4. Additional information such as **Control Connections** over the interfaces of the WAN Edge device can be viewed from Cisco SD-WAN Manager. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.Choose the device from the list and look for device information from the left-side panel.

Note In Cisco vManage Release 20.6.x and earlier releases, device information is available in the **Monitor** > **Network** page.



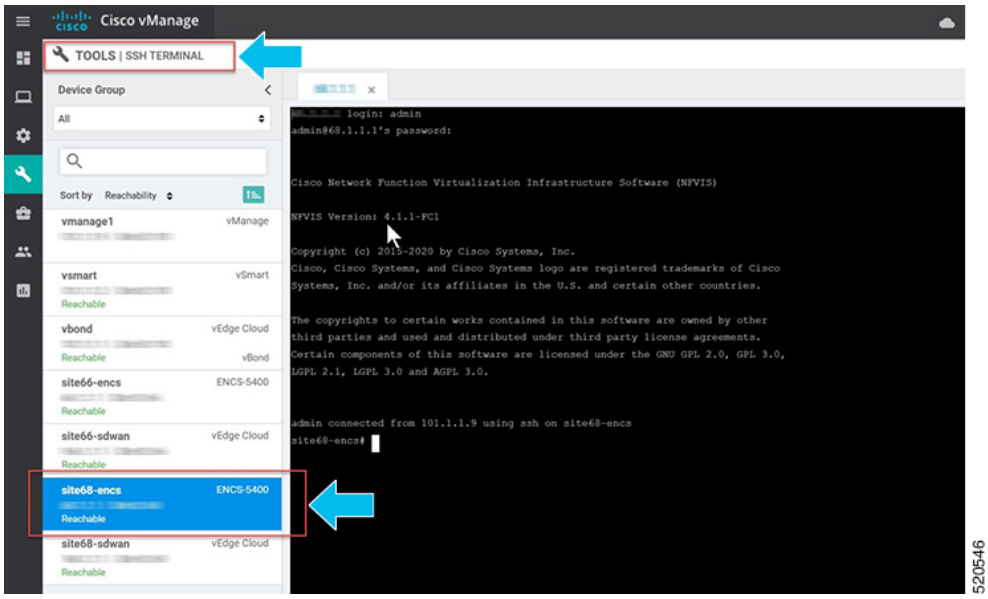
Monitor WAN Edge Device Through Cisco SD-WAN Manager SSH Server Dashboard using CLI Commands

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.



2. Choose the WAN Edge from the **Device Group**.

   To verify if the WAN Edge device has established secure control connections with the Cisco SD-WAN Control Components, enter the **show control connections** command.



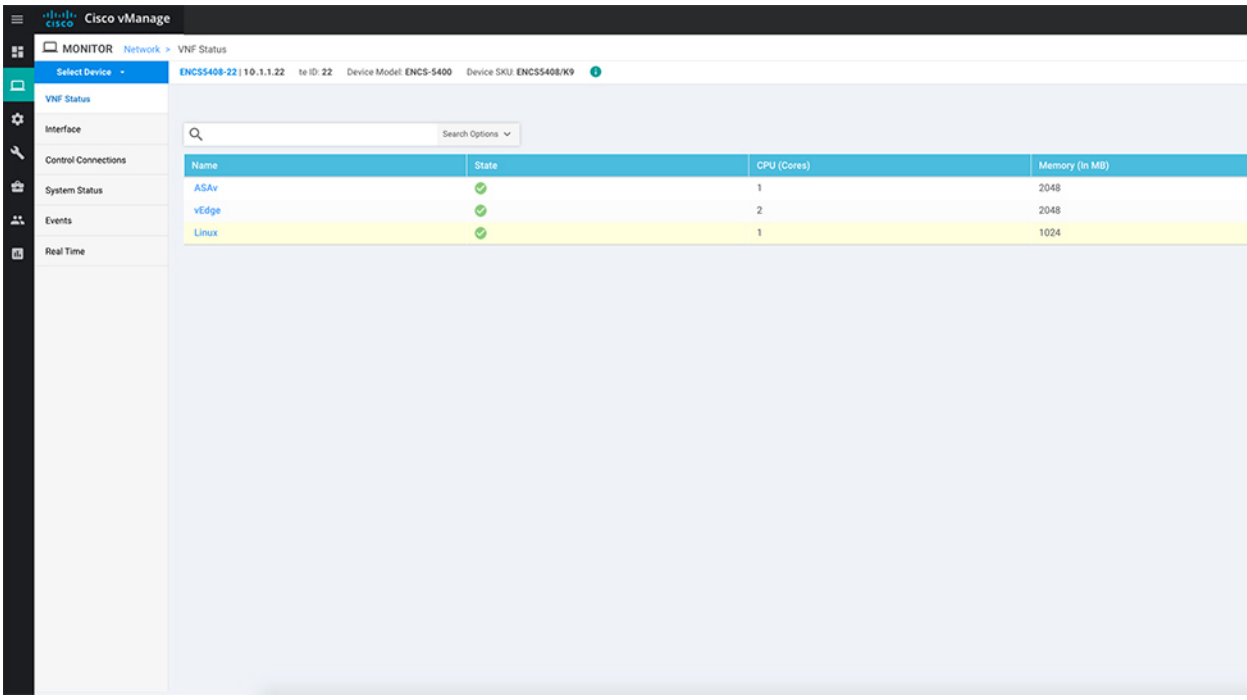
Start, Stop, and Restart WAN Edge Devices

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

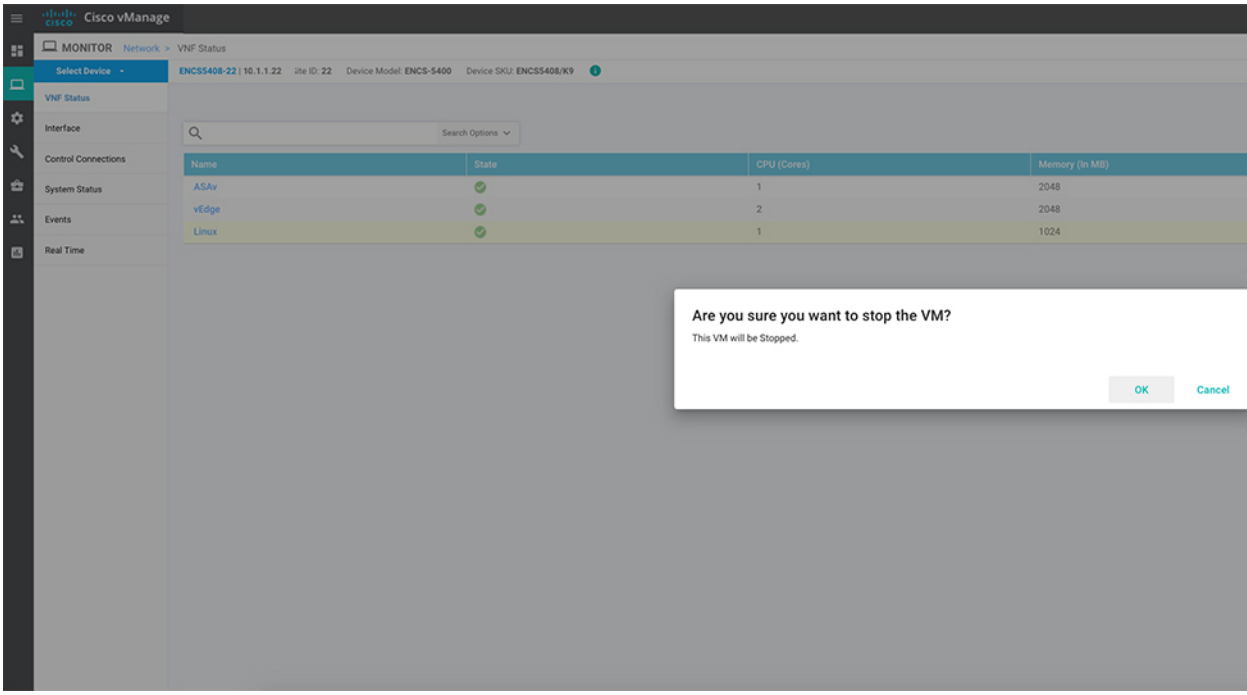
   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose the WAN Edge device.

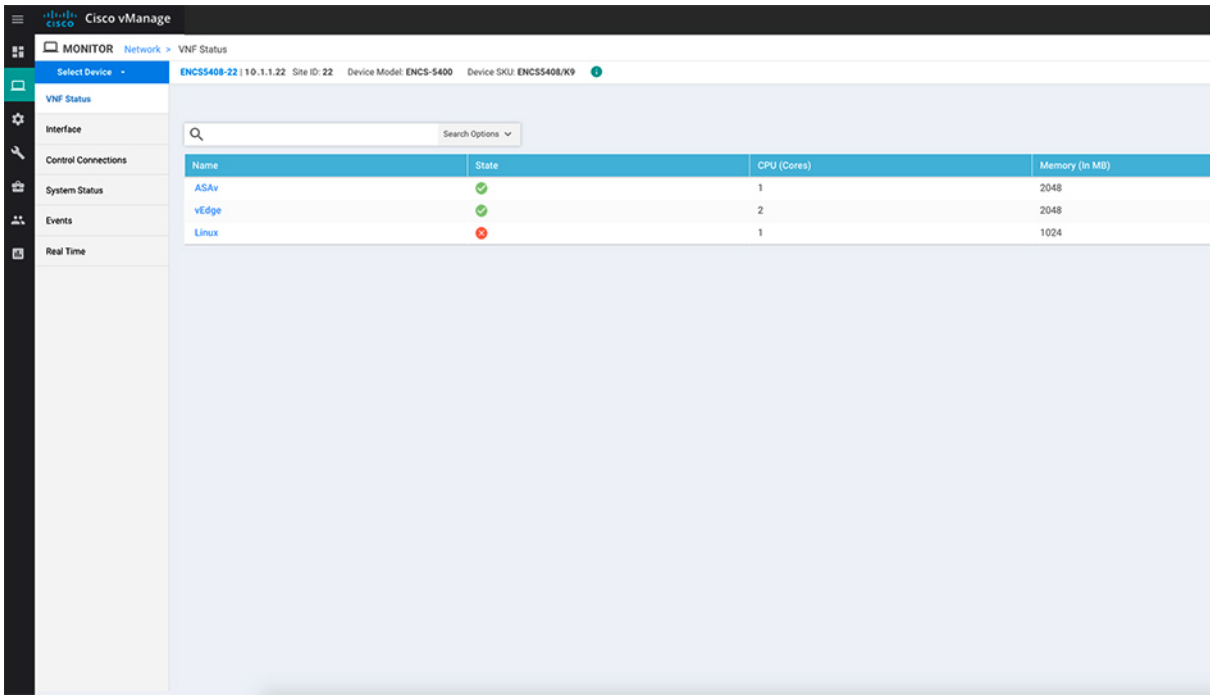
3. A list of deployed VMs for the device appears on screen. Click **…** next to the VM to start, stop or restart the device.



The following examples show how to stop a VM and the change in status of the VM.



Note You can view the VM status by choosing **Tools** > **Discover Network** from the Cisco SD-WAN Manager menu. Choose the **Device** and click **Rediscover** to sync the latest status.



You can also start, stop or restart the VM using the **vmAction vmName Linux actionType STOP/START/REBOOT** command. To view the status of the VMs, use the **show system:system deployments** or **show vm_lifecycle deployments all** command.

```
Device# vmAction vmName Linux actionType STOP

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

Troubleshooting Device Onboarding

This section explains some of the common troubleshooting procedures.

Diagnosing Onboarding Issues

This section covers the most common issues that could be encountered during the WAN Edge device onboarding process and recommended resolution to resolve the issues.

1. To verify the WAN Edge device has established a secure control connection with the Cisco SD-WAN Control Components, enter the **show control connections** command.

```
login as: admin
admin@172.19.160.61's password:


Cisco Network Function Virtualization Infrastructure Software (NFVIS)

NFVIS Version: 4.1.1-FC1

Copyright (c) 2015-2020 by Cisco Systems, Inc.
Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco
Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

The copyrights to certain works contained in this software are owned by other
third parties and used and distributed under third party license agreements.
Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0,
LGPL 2.1, LGPL 3.0 and AGPL 3.0.

admin connected from 10.24.0.84 using ssh on nfvis
nfvis# show control connections

nfvis#
```

520547

2. To verify the device properties used to authenticate WAN Edge devices, enter the **show control local-properties** command.

```
INDEX   IP                                      PORT
-------------------------------------------------------
0       192.168.1.150                           12346

number-active-wan-interfaces      2

 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                  RESTRICT/          LAST                        VM
                    PUBLIC             PUBLIC PRIVATE          PRIVATE                          PRIVATE
          MAX     CONTROL/           LAST          SPI TIME    NAT  CON
INTERFACE                  IPv4                  PORT   IPv4          IPv6                       PORT     VS/VM COLOR
    STATE CNTRL   STUN        LR/LB  CONNECTION   REMAINING   TYPE PRF
-------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
wan-br                192.168.1.61    12426  192.168.1.61     ::                                12426    0/0  gold
    up     2      no/yes/no   No/No  0:00:00:04   0:00:00:00  N    5
wan2-br               0.0.0.0         0      0.0.0.0          ::                                0        0/0  silver
    down   2      no/yes/no   No/No  10:14:50:04  0:00:00:00  N    5

nfvis#
```

520548

In the output, ensure that:

```
nfvis# show control local-properties
personality                     vedge
sp-organization-name            enfv-sdwan-CL
organization-name               enfv-sdwan-CL
root-ca-chain-status            Installed

certificate-status              Installed
certificate-validity            Valid
certificate-not-valid-before    Jul 07 10:34:38 2016 GMT
certificate-not-valid-after     Jul 07 10:34:38 2026 GMT

enterprise-cert-status          Not-Applicable
enterprise-cert-validity        Not Applicable
enterprise-cert-not-valid-before Not Applicable
enterprise-cert-not-valid-after Not Applicable

dns-name                        192.168.1.150
site-id                         0
domain-id                       1
protocol                        dtls
tls-port                        0
system-ip                       0.0.0.0
chassis-num/unique-id           ENCS5406/K9-FGL202811JH
serial-num                      EA60C0
enterprise-serial-num           No certificate installed
token                           Invalid
keygen-interval                 1:00:00:00
retry-interval                  0:00:00:15
no-activity-exp-interval        0:00:00:20
dns-cache-ttl                   0:00:02:00
port-hopped                     TRUE
time-since-last-port-hop        2:17:25:44
pairwise-keying                 Disabled
embargo-check                   success
edb-locked                      false
number-vbond-peers              1
```

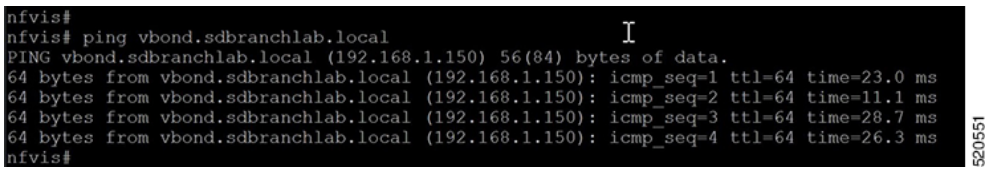
520549



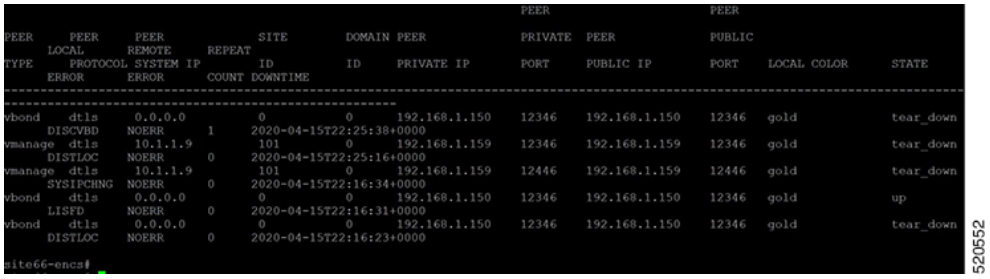
- system parameters are configured to include organization-name and site-id
- certificate-status and root-ca-chain-status are installed
- certificate-validity is Valid
- dns-name is pointing to Cisco SD-WAN Validator IP address/DNS
- system-ip is configured and chassis-num/unique-id and serial-num/token is available on the device

The above parameters must be available on the WAN Edge device to mutually authenticate with the Cisco SD-WAN Control Componentsbefore establishing the connections.

3. To verify the reachability of the Cisco SD-WAN Validator from the WAN Edge device:



4. If a WAN Edge device fails to establish connection with the Cisco SD-WAN Control Components, enter the **show control connections-history** command to view the reason for failure. View the LOCAL ERROR and REMOTE ERROR column to gather error details.



Some of the reasons for the WAN Edge device failure to establish control connections with the Cisco SD-WAN Control Components are listed below:

CRTVERFL – the error state indicates the WAN Edge device authentication is failing because of a root-ca certificate mismatch between the WAN device and the Cisco SD-WAN Control Components. Use the show certificate root-ca-cert on vEdge devices or show sdwan certificate root-ca-cert on IOS-XE Catalyst SD-WAN devices to confirm the same certificates are installed on the WAN Edge device and the Cisco SD-WAN Control Components.

CTORGNMMIS - the error state indicates the WAN Edge device authentication is failing because of a mismatch organization-name, compared with the organization-name configured on the Cisco SD-WAN Control Components. Use show sdwan control local-properties on vEdge devices and show sdwan control local-properties on IOS-XE Catalyst SD-WAN devices to confirm all the Cisco SD-WAN Control Components are configured with same organization-name across the Cisco Catalyst SD-WAN environment.

NOZTPEN – the error state indicates the onboarding vEdge device is not part of the authorized whitelist device on the ZTP server. Use show ztp entry on the on-prem ZTP server to verify the device whitelist.

NOVMCFG – the error status indicates the WAN Edge device has not been attached with a device template in Cisco SD-WAN Manager. This status is seen when onboarding the device using automated deployment options, which is the PnP or ZTP process.

VB_TMO, VM_TMO, VP_TMO, VS_TMO – the error indicates the WAN Edge device has lost reachability to the Cisco SD-WAN Control Components.

5. Use the following show commands to verify control connections on the WAN Edge device:
   - **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**

Missing root ca certificate on the WAN Edge device

If the root-ca-chain certificates for the onboarding platform is missing, device authentication will fail. A failure in device authentication cannot establish control connection to the Cisco SD-WAN Control Components. The following steps shows how to install root-ca certificate on the device components:

Login into the device and view the root-ca-chain status from the **show control local-properties** command. The following example is a sample output that shows the root-ca-chain-status is in **Not-Installed** state.

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

The following is an example of how to upload the root certificate in NFVIS:

```
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#
```