



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.

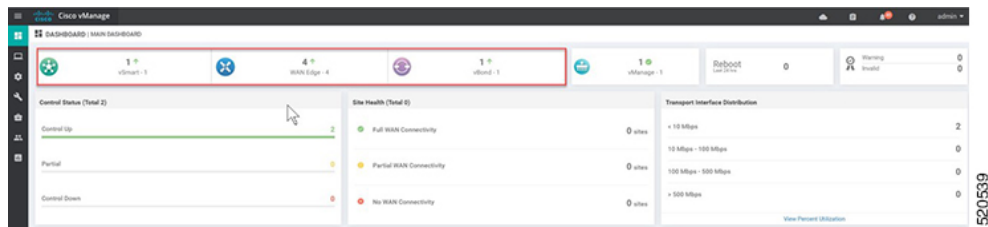
Monitor the Cisco Catalyst SD-WAN Control Components Through Device Pane

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

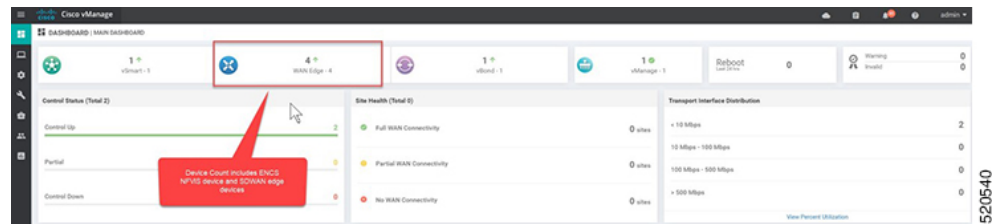


View WAN Edge Device Details and Statistics Through Device Pane

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**.

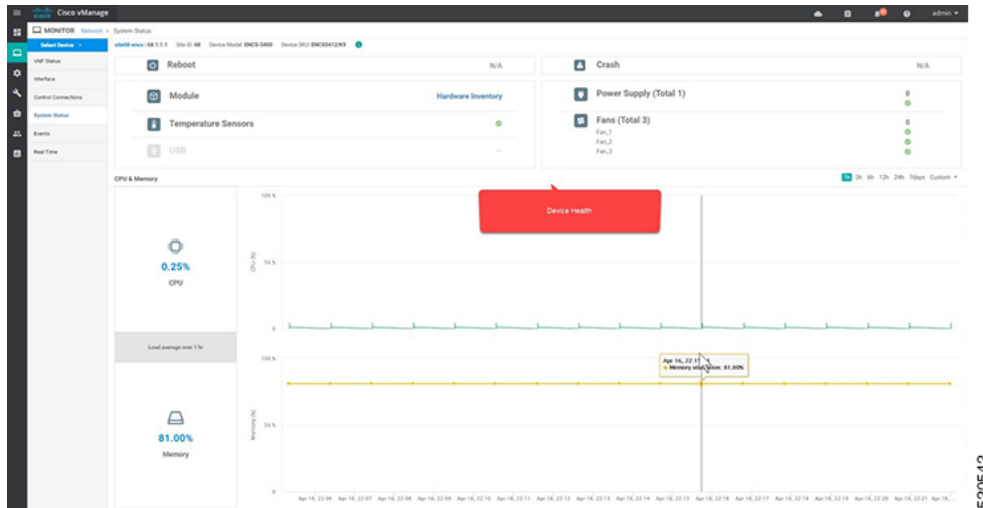
2. To view device statistics, click on the number, to display a table with detailed information for each connection.



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**.

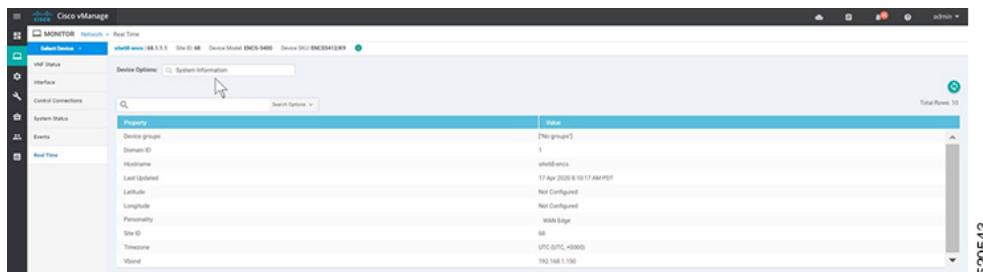
Reachability	Hostname	System IP	Site ID	Device Model	BFD	OMP	Control	Version	Chassis Number/ID	Serial Number	Last Update	
reachable	site6-encs	66.1.1.1	66	ENC5-S400	0	0	1	4.1.1-FC1	ENC5412/K9-FGL221806M	02698447	17 Apr 2020	Real Time
reachable	site6-sdwan	166.1.1.1	66	vEdge Cloud	1	1	2	19.2.099	Be176e80-f077-4c9d-a432-c8af26...	E64F100B	17 Apr 2020	Device Dashboard
reachable	site6-encs	66.1.1.1	66	ENC5-S400	0	0	1	4.1.1-FC1	ENC5412/K9-FGL222681H2	0283AF91	17 Apr 2020	SSH Terminal
reachable	site6-sdwan	166.1.1.1	66	vEdge Cloud	1	1	2	19.2.099	83423a7f-89a8-432e-9ae9-beef0c...	8A637C59	17 Apr 2020 5:40:04 AM PDT	...

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



520542

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

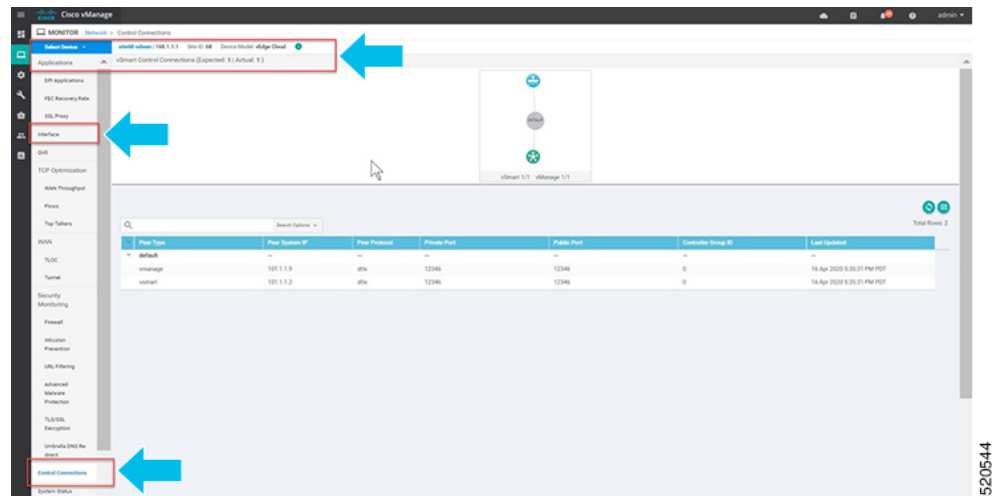


520543

- 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.



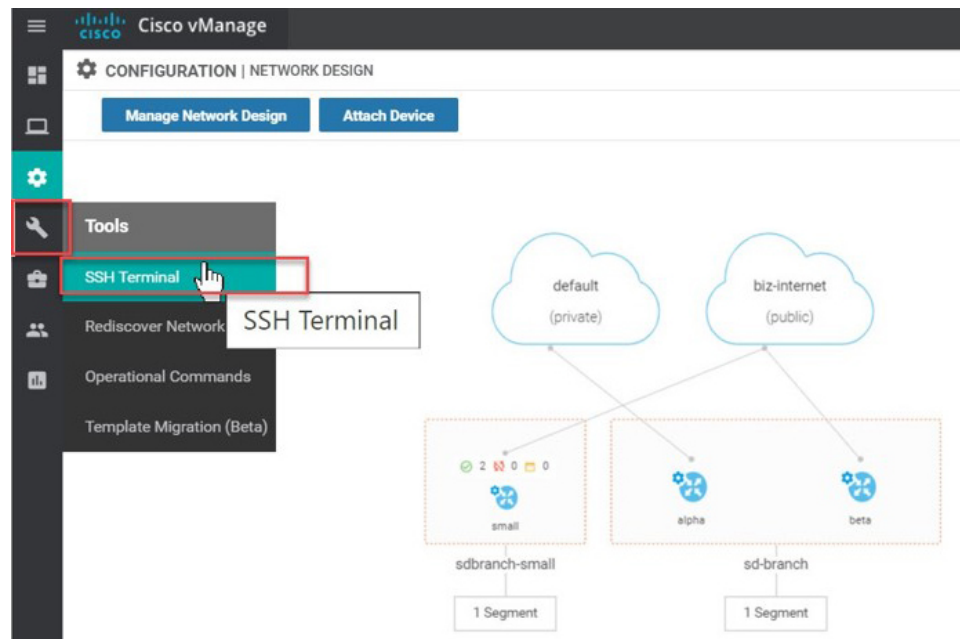
Note In Cisco vManage Release 20.6.x and earlier releases, device information is available in the **Monitor > Network** page.



520544

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

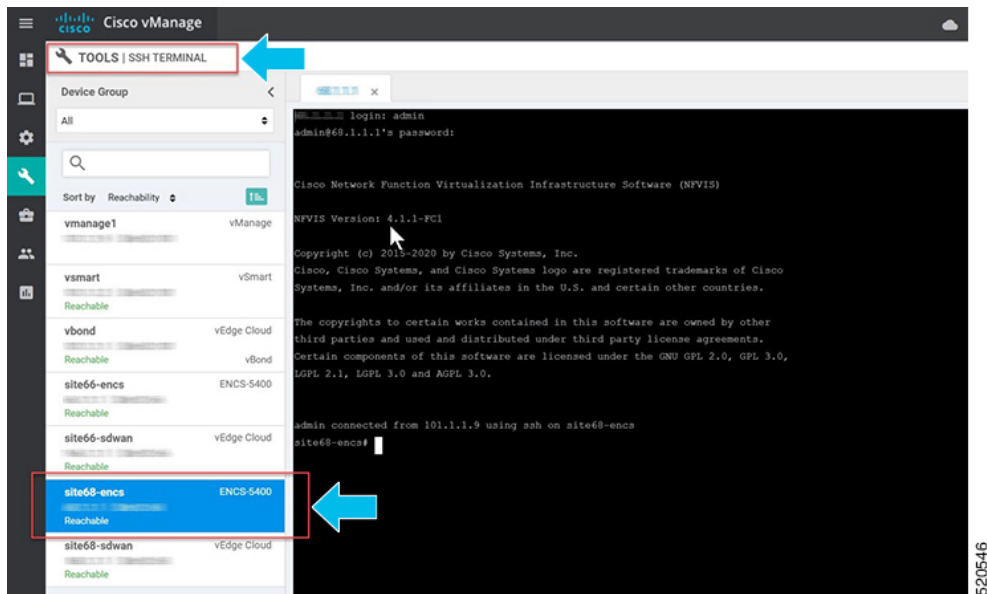
1. From the Cisco SD-WAN Manager menu, choose **Tools > SSH Terminal**.



520545

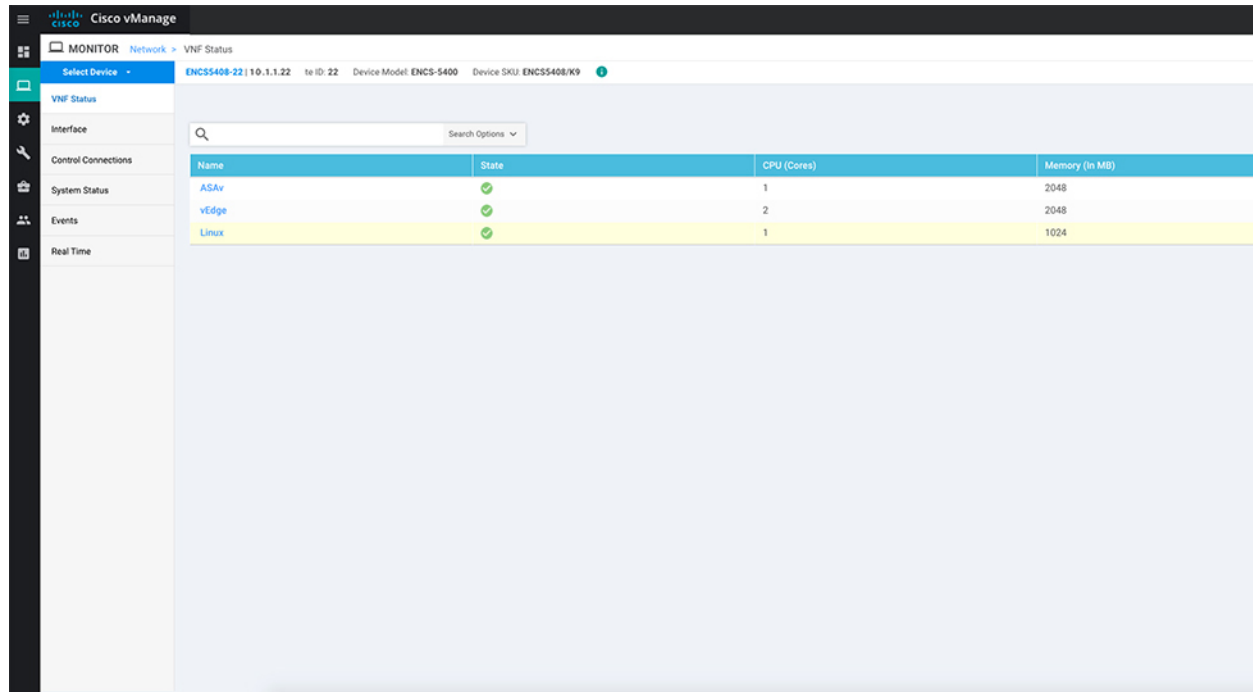
2. Choose the WAN Edge from the **Device Group**.

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

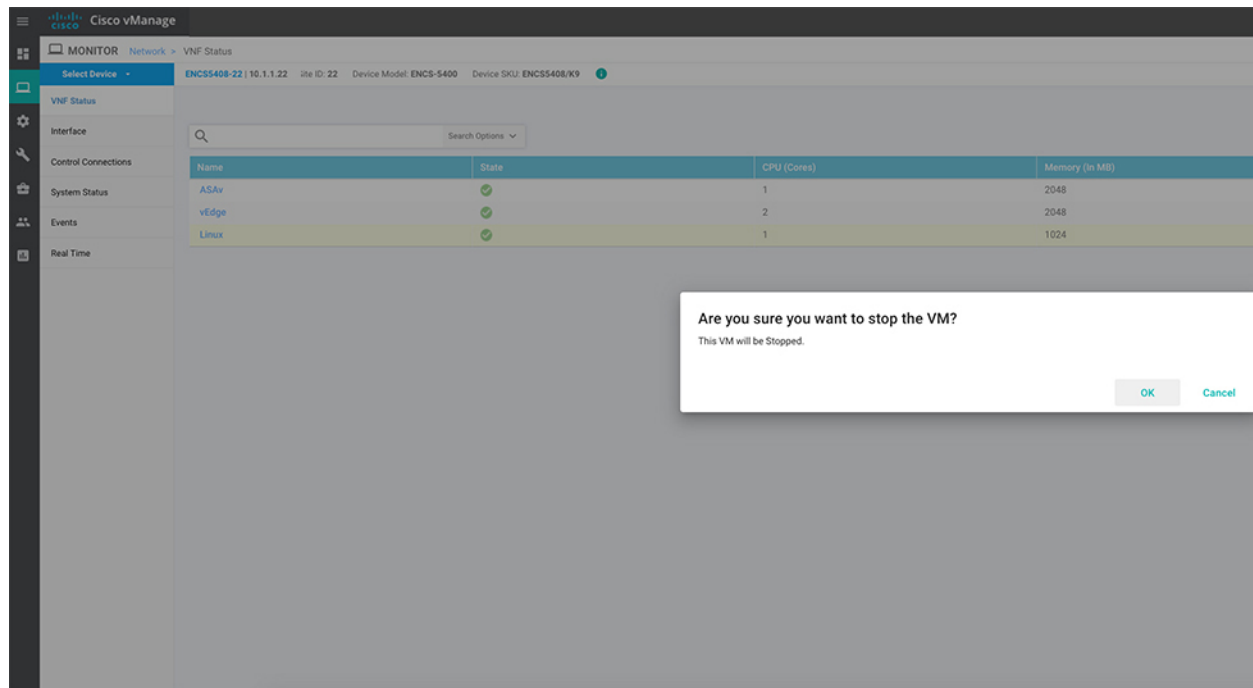
1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose the WAN Edge device.
3. A list of deployed VMs for the device appears on screen. Click ... next to the VM to start, stop or restart the device.



The screenshot shows the Cisco vManage interface for monitoring VNF status. The selected device is ENC55408-22 with IP 10.1.1.22. The table below lists the VMs and their resource usage:

Name	State	CPU (Cores)	Memory (in MB)
ASAv	✓	1	2048
vEdge	✓	2	2048
Linux	✓	1	1024

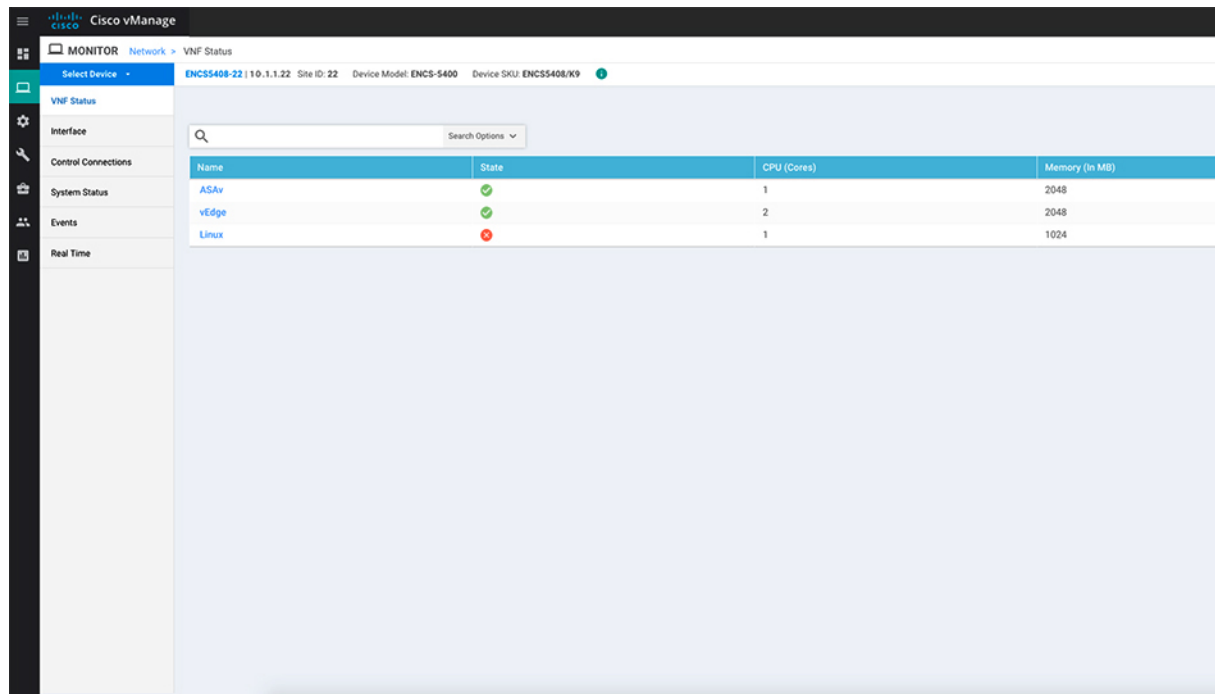
The following examples show how to stop a VM and the change in status of the VM.



The screenshot shows the same VNF Status page as above, but with a confirmation dialog box overlaid. The dialog asks: "Are you sure you want to stop the VM?" and notes "This VM will be Stopped." There are "OK" and "Cancel" buttons.



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#

```

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/ PUBLIC LAST PUBLIC PRIVATE VM
INTERFACE MAX CONTROL/ IP4 LAST PORT SPI TIME NAT CON PRIVATE
STATE CNTRL STUN LR/LB CONNECTION REMAINING TYPE PRF
-----
wan-br      192.168.1.61 12426 192.168.1.61  ::
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  ::
down       2 no/yes/no No/No 10:14:50:04 0:00:00:00 N 5

nfvis#

```

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
odh-locked                 false
number-vbond-peers        1

```



```

INDEX IP PORT
-----
0 192.168.1.150 12346
number-active-wan-interfaces 2 I
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
RESTRIC/ PUBLIC LAST PUBLIC PRIVATE VM PRIVATE
CONTROL/ IPv4 LAST PORT IPV4 NAT CON PORT VS/VM COLOR
INTERFACE STATE CNTRL STUN LR/LB CONNECTION REMAINING TYPE PRF
-----
wan-br up 2 no/yes/no No/No 0:00:00:04 0:00:00:00 N :: 5 12426 0/0 gold
wan2-br down 2 no/yes/no No/No 10:14:50:04 0:00:00:00 N :: 5 0 0/0 silver
nfvinf

```

- 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 Components before establishing the connections.

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

```

nfvif# ping vbond.sbranchlab.local I
PING vbond.sbranchlab.local (192.168.1.150) 56(84) bytes of data.
64 bytes from vbond.sbranchlab.local (192.168.1.150): icmp_seq=1 ttl=64 time=23.0 ms
64 bytes from vbond.sbranchlab.local (192.168.1.150): icmp_seq=2 ttl=64 time=11.1 ms
64 bytes from vbond.sbranchlab.local (192.168.1.150): icmp_seq=3 ttl=64 time=28.7 ms
64 bytes from vbond.sbranchlab.local (192.168.1.150): icmp_seq=4 ttl=64 time=26.3 ms
nfvif#

```

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.

```

PEER LOCAL PEER PEER SITE DOMAIN PEER PEER PEER
TYPE LOCAL REMOTE REPEAT SITE DOMAIN PEER PRIVATE PEER PUBLIC
ERROR PROTOCOL SYSTEM IP COUNT DOWNTIME ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR STATE
-----
vbond dtls 0.0.0.0 0 0 2020-04-15T22:25:38+0000 192.168.1.150 12346 192.168.1.150 12346 gold tear_down
smanage dtls 10.1.1.9 101 0 2020-04-15T22:25:16+0000 192.168.1.159 12346 192.168.1.159 12346 gold tear_down
smanage dtls 10.1.1.9 101 0 2020-04-15T22:16:34+0000 192.168.1.159 12446 192.168.1.159 12446 gold tear_down
vbond dtls 0.0.0.0 0 0 2020-04-15T22:16:31+0000 192.168.1.150 12346 192.168.1.150 12346 gold up
vbond dtls 0.0.0.0 0 0 2020-04-15T22:16:23+0000 192.168.1.150 12346 192.168.1.150 12346 gold tear_down
site66-encs#

```

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://www.in.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#

