



Troubleshooting Cisco SD-WAN Issues

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

- [Troubleshooting Cisco SD-WAN Reachability Issues, on page 1](#)
- [Troubleshooting ENCS Reachability Issues, on page 5](#)
- [Changing MSX Trace Logging Level During Runtime, on page 5](#)
- [Troubleshooting Control Plane, on page 7](#)
- [Data Plane Troubleshooting, on page 12](#)
- [PnP Server Troubleshooting Commands, on page 14](#)
- [IPsec Tunnel Cannot be Established , on page 16](#)

Troubleshooting Cisco SD-WAN Reachability Issues

Table 1: SD-WAN Reachability Issues

Color	Green	Red	Comment
Deployment Status	Provisioned	Provisioned-Failed: See Troubleshooting notes Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Errors .	Checks that VNF(s) is fully deployed and in active state.
Reachability Status	Reachable	Not Reachable: See Troubleshooting notes Troubleshooting Cisco SD-WAN vEdge Reachability Errors .	Checks the connectivity between the deployed vEdge and Cisco SD-WAN Control Plane.

Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Deployment Errors

After the service packs are deployed on MSX, the customer configuration templates are imported into the Cisco Network Services Orchestrator (NSO) platform for automating network orchestration. These configurations are then pushed from MSX to customer devices as part of the orchestration of device configuration. If the SD-WAN provisioning is not successful, most times, it is due to wrong parameters in the deployment data on NSO. There are multiple NSO instances if you are deploying more than one service pack. Therefore, these steps must be performed on the service pack-specific NSO node. SD-WAN uses SD-Branch's NSO, so in this case, the nso node will be nso-vbranch.

Step 1 Log in to one of the kubernetes master nodes.

```
# grep master inventory/inventory
[kube-master]
kubernetes-master-ctsai-east-2-1 ansible_host=<master_1_ip_address> ansible_user=centos
ansible_become=true
kubernetes-master-ctsai-east-2-2 ansible_host=<master_2_ip_address> ansible_user=centos
ansible_become=true
kubernetes-master-ctsai-east-2-3 ansible_host=<master_3_ip_address> ansible_user=centos
ansible_become=true
# ssh -F ssh.cfg centos@<master_1_ip_address>
```

Step 2 Access the NSO node using this command:

```
kubectl -n vms exec -it nso-vbranch-0 -c nso-vbranch /bin/sh
```

Step 3 Change to vms user.

```
su vmsnso
```

Step 4 Run NSO CLI

```
ncs_cli -u admin
```

Step 5 Get the branch-cpe name, using the following command:

```
vmsnso@ncs> show branch-infra:branch-infra
```

Example:

```
branch-cpe axj9AUv5A06MXXSSWWSAAA {
  provider admin;
  type ENCS;
  serial <Device serial number>;
  var SD-Branch_DEVICE_TYPE {
    val ENCS;
  }
  var contact {
    val "Samuel";
  }
  var email {
    val noreply@cisco.com;
  }
  var phone {
    val 1112221234;
  }
  vnf SD-Branch-vEdge-18.3.0 {
    vdu vEdge;
  }
}
```

Step 6 Check the deployment summary, using the following command. Replace the branch-cpe name with the name that was identified in step 2.

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe <name_from_above_command> plan component
state | tab
```

For example:

Example:

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe axj9AUv5A06MXXSSWWSAAA plan component
state | tab
```

```
NAME STATE STATUS WHEN ref MESSAGE
```

```
self init reached 2018-09-06T19:30:32 -
ready failed 2018-09-06T20:33:11 -
axj9AUv5A06MdGMqHpmQ5ffN init reached 2018-09-06T19:30:32 -
pnp-callhome reached 2018-09-06T19:30:32 -
ready reached 2018-09-06T19:31:28 - Ready
vEdge_SD-Branch-vEdge-18.3.0 init reached 2018-09-06T19:31:36 -
ready reached 2018-09-06T19:32:30 - Ready
vEdge_axj9AUv5A06MdGMqHpmQ5ffN init reached 2018-09-06T19:32:31 -
vm-deployed reached 2018-09-06T19:32:58 -
vm-alive reached 2018-09-06T19:42:58 -
ready failed 2018-09-06T20:33:11 - NFVIS Error - Recovery: Recovery completed with errors for VM:
[axj9AUv5A06MdGMq_vEdge-_0_828e4709-1644-4706-946a-12d7fa71c8e3]
vm-recovered failed 2018-09-06T20:33:11 -
```

The summary displays the problem, if any. In the above example, SYSTEM_IP variable is wrong, because of which ENCS was unable to configure the VNF and was unable to attach the deployed Control plane on MSX.

Troubleshooting Cisco SD-WAN vEdge Reachability Errors

If there is no connectivity between the deployed vEdge and Cisco SD-WAN Control Plane:

Step 1 Login to the deployed vEdge and check the status of deployed vEdges.

- For a physical vEdge, directly login to the vEdge device.
- For an IOS XE device, login to IOS device then login to SD-WAN instance installed on the device.

```
ssh admin@<vEdge IP address>
a5fG2U3kulIE8EqDfHzPHKYZ# show system deployments
NAME ID STATE
-----
a5fG2U3kulIE8EqDfHzPHKYZ vEdge.vEdge-vEdge 6 running
a5fG2U3kulIE8EqDfHzPHKYZ# vmConsole a5fG2U3kulIE8EqDfHzPHKYZ_vEdge.vEdge-vEdge
Connected to domain a5fG2U3kulIE8EqDfHzPHKYZ_vEdge.vEdge-vEdge
Escape character is ^]
viptela 18.3.0
Site001 login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on Canada_Site001
Site001#
```

Step 2 Check the status of control connection, using the following command:

```
show control connections

Site001# show control connections
PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
```

```

TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR PROXY STATE UPTIME ID
-----
vbond dtls 0.0.0.0 0 0 <vbond IP> 12346 5<vbond ip> 12346 default - connect 0
Site001#
Site001# show control connections
Site001#

```

If nothing shows up in the output, it shows that the vEdge is unable to establish dtls connection to vBond.

Step 3 To check why the connection has not been established, use the following command.

```

show control connections-history

Site001# show control connections-history
Legend for Errors
ACSRREJ - Challenge rejected by peer. NOVCMCFG - No cfg in vmanage for device.
BDSGVERFL - Board ID Signature Verify Failure. NOZTPEN - No/Bad chassis-number entry in ZTP.
BIDNTPR - Board ID not Initialized. OPERDOWN - Interface went oper down.
BIDNTVRFD - Peer Board ID Cert not verified. ORPTMO - Server's peer timed out.
BIDSIG - Board ID signing failure. RMGSPR - Remove Global saved peer.
CERTEXPRD - Certificate Expired RXTRDWN - Received Teardown.
CRTREJSER - Challenge response rejected by peer. RDSIGFBD - Read Signature from Board ID failed.
CRTVERFL - Fail to verify Peer Certificate. SERNTPRES - Serial Number not present.
CTORGNMIS - Certificate Org name mismatch. SSLNFAIL - Failure to create new SSL context.
DCONFAIL - DTLS connection failure. STNMODETD - Teardown extra vBond in STUN server mode.
DEVALC - Device memory Alloc failures. SYSIPCHNG - System-IP changed.
DHSTMO - DTLS HandShake Timeout. SYSPRCH - System property changed
DISCVBD - Disconnect vBond after register reply. TMRALC - Timer Object Memory Failure.
DISTLOC - TLOC Disabled. TUNALC - Tunnel Object Memory Failure.
DUPCLHELO - Recd a Dup Client Hello, Reset Gl Peer. TXCHTOBD - Failed to send challenge to BoardID.
DUPSER - Duplicate Serial Number. UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSYSIPDEL- Duplicate System IP. UNAUTHHEL - Recd Hello from Unauthenticated peer.
HAFAIL - SSL Handshake failure. VBDEST - vDaemon process terminated.
IP_TOS - Socket Options failure. VECRTREV - vEdge Certification revoked.
LISFD - Listener Socket FD Error. VSCRTREV - vSmart Certificate revoked.
MGRTBLCKD - Migration blocked. Wait for local TMO. VB_TMO - Peer vBond Timed out.
MEMALCFL - Memory Allocation Failure. VM_TMO - Peer vManage Timed out.
NOACTVB - No Active vBond found to connect. VP_TMO - Peer vEdge Timed out.
NOERR - No Error. VS_TMO - Peer vSmart Timed out.
NOSLPRCRT - Unable to get peer's certificate. XTVMTRDN - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections. XTVSTRDN - Teardown extra vSmart.
NTPRVMINT - Not preferred interface to vManage. STENTRY - Delete same tloc stale entry.
EMBARGOFAIL - Embargo check failed

PEER PEER
PEER PEER PEER SITE DOMAIN PEER PRIVATE PEER PUBLIC LOCAL REMOTE REPEAT
TYPE PROTOCOL SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR STATE ERROR ERROR COUNT
DOWNTIME
-----
vbond dtls 0.0.0.0 0 0 <vbond IP> 12346 52.206.47.80 12346 default connect DCONFAIL NOERR 14
2018-09-06T16:44:56+0000
Site001#

```

As seen above, the LOCAL ERROR is mostly "DCONFAIL" which means DTLS connection failure. This happens when the vEdge is unable to reach the vBond either due to network connectivity issues or firewall is blocking the DTLS connection. For an understanding of other reachability errors, see the [Cisco SD-WAN knowledge base](#).

Troubleshooting ENCS Reachability Issues

If the ENCS device is unreachable or unavailable, then do the following:

Step 1 Log into the **ENCS** box. Use SSH to connect to the ENCS box.

```
ssh <username>@<management IP address>
```

Step 2 Do the following on the ENCS box:

a. Enter the configuration mode.

```
config
```

b. Revert the IP to the WAN interface of the ENCS, if the ENCS was set in the single IP mode.

```
no single-ip-mode
```

c. Remove the VPN configurations.

```
no secure-overlay
```

d. Remove all deployments.

```
no vm_lifecycle tenants tenant admin deployments deployment
```

Note If a specific VNF needs to be deleted, enter the deployment name in the above command.

e. Removes all images.

```
no vm_lifecycle images image
```

Note If a specific image needs to be deleted, enter the image name in the above command.

f. Save the changes and exit the configuration mode.

```
commit and-quit
```

g. Restarts PNP process.

```
pnp action command restart
```

Changing MSX Trace Logging Level During Runtime

Using the procedure in this section you can change any MSX trace logging level during the runtime. The following shows SD-WAN log definition in logback.xml.

```
<property name="LOG_FILE" value="logs/sdwanservice.log"/>
```

```

<!-- the rollover settings with mean a max size per log of 100Mb and 7 days -->
<property name="MAX_HISTORY" value="7"/>
<property name="MAX_FILE_SIZE" value="100MB"/>

<include resource="com/cisco/nfv/logging/nfv_base_logback.xml"/>

<!-- the specific loggers -->
<logger name="com.cisco.phiservice" level="DEBUG"/>
<logger name="com.cisco.vms.sdwanservice" level="DEBUG"/>
<logger name="com.cisco.vms.sdwanservice.integration.viptela" level="DEBUG"/>
<logger name="com.cisco.vms.svcpack.logging" level="DEBUG"/>

<logger name="org.springframework" level="INFO"/>
<logger name="org.springframework.security.oauth2" level="INFO"/>
<logger name="org.springframework.integration" level="OFF"/>
<logger name="org.springframework.oauth" level="OFF"/>
<logger name="org.springframework.http" level="ERROR"/>

```

To change the logging level during runtime:

Step 1 Obtain the MSX client credentials.

Use the credential you use for logging in to the MSX Portal. If you do not have these credentials, contact your Service Provider Administrator.

Step 2 Obtain an access token from the MSX authorization Server. Use the following curl command to get the access token. Use the following curl command to get the access token.

```

curl -X POST 'https://<MSX_URL>/idm/v2/token?grant_type=password' -H 'Authorization: Basic
<MSX_BASIC_AUTH>' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'cache-control: no-cache' \
-d 'username=<MSXportal_username>&password=<MSXportal_password>'

```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <MSX_BASIC_AUTH> with real value of the Authorization of clientID and clientSecret, which is base64 of “clientID:clientSecret”. User defined their OAuth2 Authentication clientID and clientSecret in **Settings > BSS Integration > REST Configuration**
- Replace <MSXportal_username> by Portal username
- Replace <MSXportal_password> by Portal password

Step 3 Check the current package logging level. Use the following curl command to check the current package log level:

```

curl -X GET https://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer
<access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache'

```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (For example: sdwanservice)

- Replace <package> by real package name (For example: com.cisco.vms.sdwan.service.integration.viptela)
- Replace <access_token> from Step 2.

Step 4 Change the package logging level. Use the following curl command to update the package log level:

```
curl -X POST https://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer <access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d '{
  "configuredLevel": "<LOG_LEVEL>"
}'
```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (for example: sdwan.service)
- Replace <package> by real package name (for example: com.cisco.vms.sdwan.service)

Note This package name does not necessarily be defined in logback.xml, as long as this package exists in the source code.

- Replace <access_token> from Step 2.
- Replace <LOG_LEVEL> by log level you want to set.

Step 5 Verify the changes in package logger logging level. Repeat Step 3. Use the following curl command to verify the log level after the changes:

```
curl -X GET http://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer <access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache'
# with output for logging level
{"configuredLevel":"TRACE","effectiveLevel":"TRACE"}
```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (for example: sdwan.service)
- Replace <package> by real package name

Troubleshooting Control Plane

Troubleshooting Control Plane on OpenStack

If MSX is unable to reach the OpenStack control plane, then it should be due to some issues pertaining to proxy settings.



Note When both MSX and OpenStack cloud are on the corp network, proxy is not required. Ensure that the vManage IP address is added to the "no proxy" list in the "sdwanservice-rc.yml" and then restart the SD-WAN pod.

This figure shows the list of Get APIs that can be used to query the database.

Figure 1: List of Get APIs for Querying the Database

osorch		Show/Hide List Operations Expand Operations
GET	/osorch/alive	Check if system is alive
GET	/osorch/v1/vims	Get all VIMs
GET	/osorch/v1/vims/{vimID}	Get a VIM
GET	/osorch/v1/vims/{vimID}/validate	Check a VIM config
GET	/osorch/v1/vims/{vimID}/flavors	Get a list of flavors on a VIM
GET	/osorch/v1/vims/{vimID}/flavors/{flavorName}	Get a Flavor
GET	/osorch/v1/vims/{vimID}/images	Get a list of images on a VIM
GET	/osorch/v1/vims/{vimID}/images/{imageName}	Get an image
GET	/osorch/v1/vims/{vimID}/volumes	Get a list of volumes on a VIM
GET	/osorch/v1/vims/{vimID}/volumes/{volumeName}	Get an volume
GET	/osorch/v1/cps	Get all Control Planes
GET	/osorch/v1/cps/{cpID}	Get a Control Plane
GET	/osorch/v1/jobs	Get all Jobs
GET	/osorch/v1/jobs/{jobID}	Get a Job by ID
GET	/osorch/v1/templates	List all the Ansible templates
GET	/osorch/v1/templates/{templateName}	Get a Template by Name

This figure shows a sample query to access the list of templates from the OS orchestrator using the curl command in this GET API page

Figure 2: Accessing the List Templates from OS Orchestrator

The screenshot shows a REST API interface for the endpoint `/osorch/v1/templates`. It includes a table for parameters, a table for response messages, a curl command, a request URL, and a JSON response body.

Parameter	Value	Description	Parameter Type	Data Type
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOi...	JWT token in the form 'Bearer {token}'. Tokens are retrieved by making a login call to the platform.	header	string

HTTP Status Code	Reason	Response Model	Headers
200	OK		
500	Internal Error		

curl
`curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOi...`

Request URL
`https://ssi-sdwan.lab.ciscomsx.com:443/osorch/v1/templates`

Response Body

```
[
  "ca-csr.json",
  "ca.j2",
  "clouds.j2",
  "controllers.yml.tpl",
  "hosts.j2",
  "ntp.j2",
  "openstack.yml.tpl",
  "ports.j2",
  "ports.yml.tpl",
  "vbond-fip-3-noCA.j2",
  "vbond-fip-3.j2",
  "vmanage-fip-noCA.j2",
  "vmanage-fip.j2",
  "vmanage-new-2.j2",
  "vsmart-fip-noCA.j2",
  "vsmart-fip.j2",
  "vsmart.j2"
]
```

Troubleshooting the OS orchestrator Logs

To access the OS orchestrator logs:

- Step 1** Log in to the Kubernetes-master mode.
- Step 2** Execute the given command to get the OS orchestrator pod name:


```
kubectl -n vms get po
```
- Step 3** To log in to the container, execute the given command:


```
kubectl -n vms exec -it <osorch_log_name> bash
```
- Step 4** To check the logs, execute the given command:


```
cd logs >
<jobID>_ansible.log
```

jobID: Specifies the job ID to access the specific job.

If there are errors during the creation of a control plane these logs can offer some guidance, it verifies the incorrect parameters and ways to resolve issues.

Change Control Plane Password or Vault Failures

Error Message

Failed to authenticate control plane user.

Solution

Use the Swagger interface to update the credentials for the control plane manager. The password input in base64.

Figure 3: Changing the Control Plane Password

PUT /v1/controlplanemanager/{id}/credentials

Implementation Notes
Update tenant control plane credentials in VMS system

Parameters

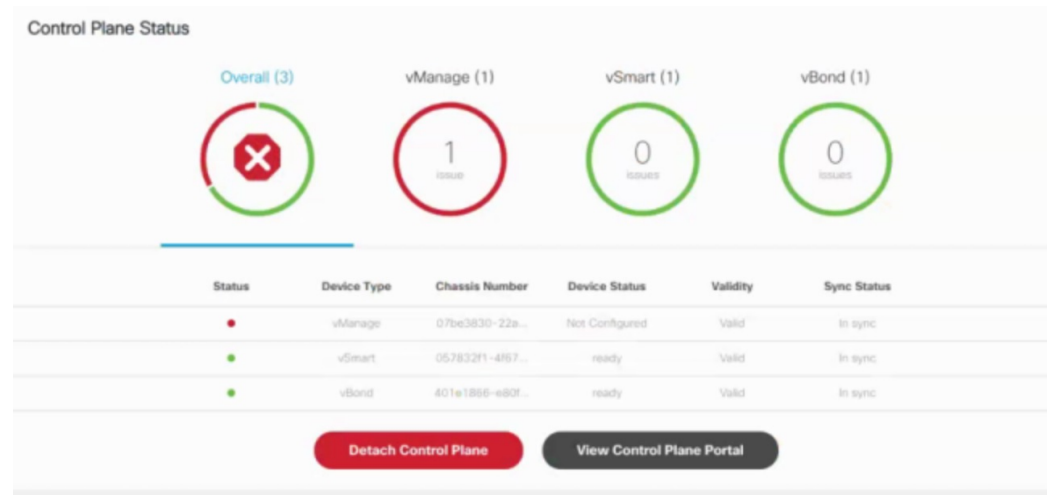
Parameter	Value	Description
id	0693072f-d25d-487c-89de-6dc10acf919c	VMS tenantId
controlPlaneCredDTO	{ "password": "dGFjdHJhaW5pbmc=", "username": "admin" }	SD-WAN Control Plane Cred DTO

Fixing Control Plane Device Status State

Problem

After adding a new control plane, the Control Plane (vManage) remains in 'Not Configured' state, as shown below:

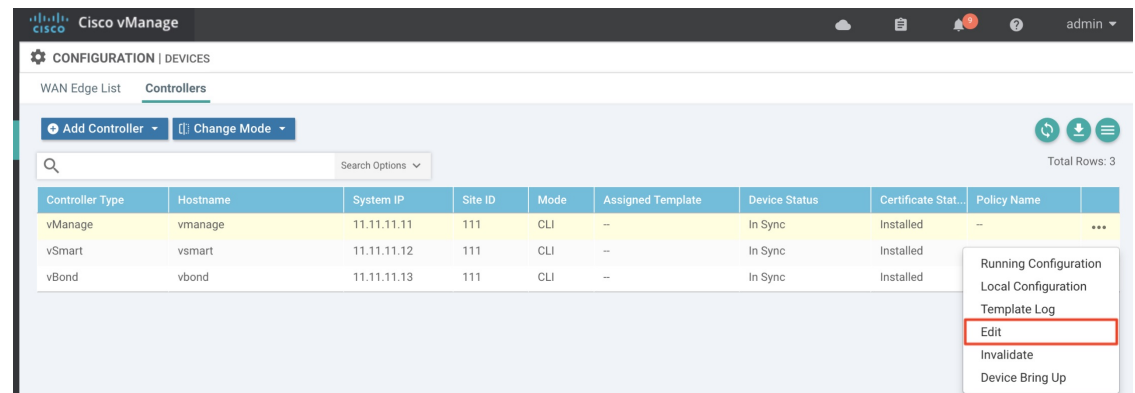
Figure 4: Control Plane Status



Reason

Incorrect way of changing the control plane password. This issue was due to changing the Control Plane password from **vManage Console > Configuration > Devices > Controllers**.

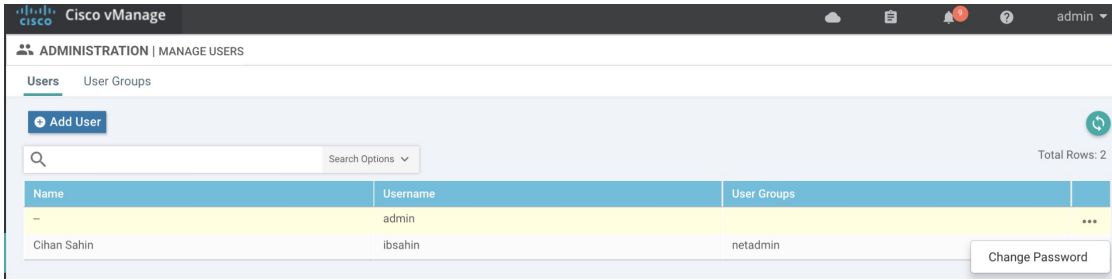
Figure 5: Changing the Control Plane Password from vManage



Solution

- Step 1** Change the Control Plane password from **vManage Console > Administration > Manage Users > Users**.

Figure 6: Changing the Control Plane Password from vManage



Step 2 Restart nms application server on vManage.

```
vmmanage# request nms application-server restart
```

Note The server takes a few minutes to start.

Data Plane Troubleshooting

Check the deployment status of the vEdge device:

1. Check NSO device status.
2. Check data plane deployment in the MSX Portal.

Check the reachability status (vEdge to control plane):

1. Check the vManage device state.
2. Check that the site status in SD-WAN is green.

Data Plane Deployment Status: NSO Device Status

Example:

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe agH89ZqVcqVObci6Pyv1jU56 plan
component state
```

NAME	STATE	STATUS	WHEN	ref	MESSAGE
self	init	reached	2017-11-12T04:55:12	-	
	ready	reached	2017-11-12T04:57:33	-	
agH89ZqVcqVObci6Pyv1jU56	init	reached	2017-11-12T04:55:12	-	
	pn-p-callhome	reached	2017-11-12T04:55:12	-	
	ready	reached	2017-11-12T04:56:10	-	Ready
vEdge_SD-Branch-vEdge	init	reached	2017-11-12T04:56:11	-	
	ready	reached	2017-11-12T04:56:34	-	Ready
vEdge_agH89ZqVcqVObci6Pyv1jU56	init	reached	2017-11-12T04:56:35	-	
	vm-deployed	reached	2017-11-12T04:56:50	-	
	vm-alive	reached	2017-11-12T04:57:33	-	
	ready	reached	2017-11-12T04:57:33	-	Ready

Data Plane Deployment Status (MSX Portal)

To view the data plane deployment status:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click **Dashboard**.
- Step 3** Select the tenant from the drop-down.
- Step 4** Click **SD-WAN**. The **SD-WAN Service Offer** screen appears.
- Step 5** Click **SD-WAN**.
- Step 6** Select the SD-WAN service. The **SD-WAN** screen appears.

Reachability Status: vManage Device State

To view the reachability status:

- Step 1** Log in to vManage.
- Step 2** In vManage, choose **Configuration > Devices**. The Configure | Devices window is displayed.

Figure 7: Reachability Status of the Devices

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP	Site ID	
✓	vEdge Cloud	104920e9-ee97-4f98-88d3-b385acbb03...	Token - 2fb5defbdabef...	-	-	-	Running Configuration
✓	vEdge Cloud	8b57277e-7790-4826-b85c-763a558ee...	Token - 9380b5a8f929c...	-	-	-	Local Configuration
⚠	vEdge Cloud	3aca2c89-6b97-4fc8-a741-be48ff5c448	Token - aa52101a1dc5...	-	-	-	Delete vEdge
✓	vEdge Cloud	e887118a-c434-46ab-9957-068c38cc6...	Token - c8423a838bd2...	Gap50	1.1.1.22	222	Copy Configuration
⚠	vEdge Cloud	346389cf-4009-4ca4-81a3-508e378ae2...	Token - 7724226c175d5...	-	-	-	Decommission vEdge
✓	vEdge Cloud	e0b0477b-9e4d-4832-8bdf-af6ae1e7de...	Token - d093d134f909...	-	-	-	Template Log
✓	vEdge Cloud	159483d1-d888-4116-bc05-1f30c88fe0...	c2620fas	DhruvSite	1.1.1.99	222	CLI
✓	vEdge Cloud	0bfb3774-0825-4591-b095-a1d97d6b33...	Token - cb8b37d7661ff...	montrealadwan	1.1.1.14	567	CLI
✓	vEdge Cloud	6978c2a4-8f5e-4489-8500-80e8048f60...	f44d3aee	-	-	-	CLI
✓	vEdge Cloud	94e8ffbc-288c-4c90-a06d-96719e818a...	Token - 6f76d6ec5bfe3...	-	-	-	CLI

- The **State** column indicates if the certificate is installed.
- In the **Serial No./Token** column, you should have a serial number and not a token.
- Click **Running Configuration** to view the configuration running on the device.

- If reachability is not achieved, then verify the variables that were passed during the site deployment (especially VPN_0).

Data Plane Reachability Status (MSX Portal)

To view the data plane reachability status:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click **Dashboard**.
- Step 3** Select the tenant from the drop-down.
- Step 4** Click **SD-WAN**. The **SD-WAN Service Offer** screen appears.
- Step 5** Click **SD-WAN**.
- Step 6** Select the SD-WAN service. The **SD-WAN** screen appears.

PnP Server Troubleshooting Commands

List of Devices in Contact with the PnP Server

```
admin@ncs-sm-SD-Branch> show pnp list
SERIAL          IP ADDRESS      CONFIGURED  ADDED  SYNCED  LAST CONTACT
-----
FTX1738AJME     173.36.207.85   true        true   true    2017-10-24 23:44:44
FTX1738AJMG     173.36.207.81   true        true   true    2017-10-24 23:43:50
FTX1740ALBX     173.36.207.80   true        true   true    2017-10-24 23:44:21
SSI184904LG     173.36.207.82   true        true   true    2017-10-24 23:43:56
SSI185104LT     173.36.207.84   true        true   true    2016-10-24 23:43:57
[ok] [2016-10-24 23:45:49]
```



Note

- The Last Contact column displays the last date and time when the PnP server was in contact with the CPE. If the CPE has not been in recent contact with the PnP server, it may be due to connectivity or reachability issues between the PnP server and the CPE.
- Identify the active NSO instance using the following command:

```
curl -v http://consul.service.consul:8500/v1/catalog/service/nso-ha | python -m json.tool
```

CPE in Contact with the PnP Server (Without a Service)

```
admin@ncs-sm-SD-Branch> show branch-infra:branch-infra branch-cpe
```

```
%No entries found
[ok] [2016-10-24 23:45:49]
```

CPE in Contact with the PnP Server (With a Service)

```
admin@ncs-sm-SD-Branch> show branch-infra:branch-infra-status branch-cpe
amXqvXDO9zW2IZ1leho2cOBrD plan component state status
NAME STATE STATUS
-----
self init reached
ready reached
amXqvXDO9zW2IZ1leho2cOBrD init reached
pnp-callhome reached
ready reached
[ok] [2017-10-25 14:20:40]
```

CPE in Contact with the PnP Server (Detailed)

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe amXqvXDO9zW2IZ1leho2cOBrD plan
component
plan component self
type self
state init
status reached
when 2017-10-25T14:15:20
message ""
state ready
status reached
when 2017-10-25T14:16:57
message ""
real-name amXqvXDO9zW2IZ1leho2cOBrD
plan component amXqvXDO9zW2IZ1leho2cOBrD
type branch-cpe
state init
status reached
when 2017-10-25T14:15:20
message ""
state pnp-callhome
status reached
when 2017-10-25T14:16:22
message ""
state ready
status reached
when 2017-10-25T14:16:57
message Ready
real-name amXqvXDO9zW2IZ1leho2cOBrD
provider CiscoSystems
device amXqvXDO9zW2IZ1leho2cOBrD_ENCS
[ok] [2017-10-25 14:23:10]
```

View CPE Details

```
vmsnso@ncs> show pnp list
```

SERIAL	IP ADDRESS	CONFIGURED	ADDED	SYNCED	LAST CONTACT
FGL21388017	10.85.189.20	true	true	true	2017-10-25 14:24:07

```

FGL2138801A 10.85.189.23 false false false 2017-10-25 14:21:16
FGL2138801E 10.85.189.24 false false false 2017-10-25 14:21:40

[ok][2017-10-25 14:24:20]
vmsnso@ncs> configure

Entering configuration mode private
[ok][2017-10-25 14:24:31]

[edit]
vmsnso@ncs% show branch-infra:branch-infra branch-cpe serial FGL21388017
branch-cpe amXqvXDO9zW2IZ1eho2cOBrD {
  provider CiscoSystems;
  type ENCS;
  serial FGL21388017;
  var SD-Branch_DEVICE_TYPE {
    val ENCS;
  }
  var contact {
    val Customer;
  }
  var email {
    val abc@example.ocm;
  }
  var phone {
    val null;
  }
}
[ok][2017-10-25 14:24:34]
[edit]
vmsnso@ncs% exit
[ok][2017-10-25 14:24:53]

```

IPsec Tunnel Cannot be Established

Problem

Device fails to establish secure VPN tunnel between NFVIS and CSR Mgmt hub router.

Solution

To establish secure VPN tunnel:

Step 1 Log in to the device and run the following command:

Example:

```
vmsnso@ncs% show pnp day0-common | display set
```

Step 2 Ensure day0-common has correct values specified for the following parameters:

Example:

```

INT_MGMT_SUBNET_DHCP set to false
INT_MGMT_SUBNET_GW <GW IP address>
INT_MGMT_SUBNET_INVERSE_MASK <subnet mask>
INT_MGMT_SUBNET_IP <subnet value>
INT_MGMT_SUBNET_IPVERSION <IPv4 or ipv6>
INT_MGMT_SUBNET_NETMASK <subnet netmask value>

```



```

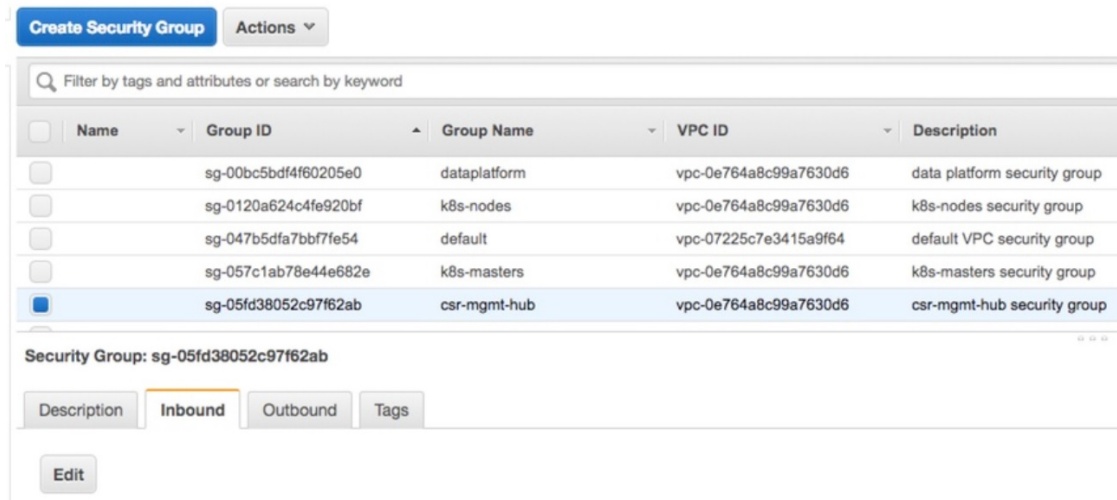
LOCAL_PRESHARED_KEY <Pre-shared key for VPN authentication on the ENCS>
MGMHUB_OVERLAY_IP_ADDR <IP address of the interface connecting to MSX internal host on the CSR mgmt
hub>
MGMHUB_OVERLAY_NET <Supernet of the subnets on MSX side>
MGMT_HUB_IP <Public IP address of the CSR mgmt hub>
REMOTE_ID <Local identity configured on the CSR mgmt hub's VPN configuration>
REMOTE_PRESHARED_KEY <Pre-share key for VPN authentication on the CSR mgmt hub>
SECURE_OVERLAY_NAME
SOURCE-BRIDGE
    
```

Step 3 Ensure CSR Hub VPN configuration matches NFVIS's.

Step 4 Edit CSR Hub's Security group and ensure the following ports are open. The following ports are used for communication from MSX to the NFVIS via the CSR mgmt hub VPN.

- 22022 - 22024: VNF ports
- 21045: VNF port
- 830: Netconf port
- 443: Metric collection from the ENCS

Figure 8: Editing the Security Group



Step 5 Configure route to NFVIS's secure IP. The default is 10.128.0.0/16 (Assigned by SD-Branch). This can be changed using:

- SD-Branch_variables.yml file at the install time
- SD-Branch settings API

