Appendix A: 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>
<thead>
<tr>
<th>Color</th>
<th>Green</th>
<th>Red</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Status</td>
<td>Provisioned</td>
<td>Provisioned-Failed: See Troubleshooting notes Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Deployment Errors.</td>
<td>Checks that VNF(s) is fully deployed and in active state.</td>
</tr>
<tr>
<td>Reachability Status</td>
<td>Reachable</td>
<td>Not Reachable: See Troubleshooting notes Troubleshooting Cisco SD-WAN vEdge Reachability Errors.</td>
<td>Checks the connectivity between the deployed vEdge and Cisco SD-WAN Control Plane.</td>
</tr>
</tbody>
</table>

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 axj9AUv5A06MXXSSWSAAA {
    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;
    }
    vnfd 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:**
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-vEdge 6 running
```

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

```
show control connections
```
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
```

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/sdwnservice.log"/>
```
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.

```bash
-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:

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

```bash
  "configuredLevel": "<LOG_LEVEL>"
}'
```

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.sdwanservice)

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:

```bash
```

Where:

- Replace `<MSX_URL>` by real MSX URL
- Replace `<service>` by service endpoint (for example: sdwanservice)
- 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.
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**

<table>
<thead>
<tr>
<th>osorch</th>
<th>Show/Hide</th>
<th>List Operations</th>
<th>Expand Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /osorch/alive</td>
<td>Show/Hide</td>
<td>List Operations</td>
<td>Expand Operations</td>
</tr>
<tr>
<td>GET /osorch/v1/vims</td>
<td>Get all VMs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}</td>
<td>Get a VIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/validate</td>
<td>Check a VIM config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/flavors</td>
<td>Get a list of flavors on a VIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/flavors/{flavorName}</td>
<td>Get a flavor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/images</td>
<td>Get a list of images on a VIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/images/{imageName}</td>
<td>Get an image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/volumes</td>
<td>Get a list of volumes on a VIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/vims/{vimID}/volumes/{volumeName}</td>
<td>Get an volume</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/cps</td>
<td>Get all Control Planes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/cps/cpsID</td>
<td>Get a Control Plane</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/jobs</td>
<td>Get all Jobs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/jobs/jobID</td>
<td>Get a Job by ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/templates</td>
<td>List all the Avisibe templates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET /osorch/v1/templates/{templateName}</td>
<td>Get a Template by Name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
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:

```bash
kubectl -n vms get po
```

**Step 3**  To log in to the container, execute the given command:

```bash
kubectl -n vms exec -it <osorch_log_name> bash
```

**Step 4**  To check the logs, execute the given command:

```bash
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*

<table>
<thead>
<tr>
<th>PUT</th>
<th>/v1/controlplanemanagers/{id}/credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implementation Notes</strong></td>
<td>Update tenant control plane credentials in VMS system</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td>id</td>
<td>0693072f-d23d-4b7c-89de-9dc10ac918c</td>
</tr>
<tr>
<td>controlPlaneCredDTO</td>
<td>{ &quot;password&quot;: &quot;GFJvJw5tW2Wkmc&quot;, &quot;username&quot;: &quot;admin&quot; }</td>
</tr>
</tbody>
</table>

## 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:
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.

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.

vmanage# 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:

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

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>STATUS</th>
<th>WHEN</th>
<th>ref</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>self</td>
<td>init</td>
<td>reached</td>
<td>2017-11-12T04:55:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
<td>2017-11-12T04:57:33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>agH89ZqVcqVObci6Pyv1jU56</td>
<td>init</td>
<td>reached</td>
<td>2017-11-12T04:55:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
<td>2017-11-12T04:56:34</td>
<td></td>
<td>Ready</td>
</tr>
<tr>
<td>vEdge_SD-Branch-vEdge</td>
<td>init</td>
<td>reached</td>
<td>2017-11-12T04:56:35</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
<td>2017-11-12T04:57:33</td>
<td></td>
<td>Ready</td>
</tr>
<tr>
<td>vEdge_agH89ZqVcqVObci6Pyv1jU56</td>
<td>vm-deployed</td>
<td>reached</td>
<td>2017-11-12T04:56:50</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vm-alive</td>
<td>reached</td>
<td>2017-11-12T04:57:33</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
<td>2017-11-12T04:57:33</td>
<td></td>
<td>Ready</td>
</tr>
</tbody>
</table>
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, select the Configuration > Devices. The Configure | Devices screen appears.

Figure 7: Reachability Status of the Devices

- 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

<table>
<thead>
<tr>
<th>SERIAL</th>
<th>IP ADDRESS</th>
<th>CONFIGURED</th>
<th>ADDED</th>
<th>SYNCHED</th>
<th>LAST CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTX1738AJME</td>
<td>173.36.207.85</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2017-10-24 23:44:44</td>
</tr>
<tr>
<td>FTX1738AJMG</td>
<td>173.36.207.81</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2017-10-24 23:43:50</td>
</tr>
<tr>
<td>FTX1740ALBX</td>
<td>173.36.207.80</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2017-10-24 23:44:21</td>
</tr>
<tr>
<td>SSI184904LG</td>
<td>173.36.207.82</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2017-10-24 23:43:56</td>
</tr>
<tr>
<td>SSI185104LT</td>
<td>173.36.207.84</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2016-10-24 23:43:57</td>
</tr>
</tbody>
</table>

[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)

<table>
<thead>
<tr>
<th>SERIAL</th>
<th>IP ADDRESS</th>
<th>CONFIGURED</th>
<th>ADDED</th>
<th>SYNCHED</th>
<th>LAST CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTX1738AJME</td>
<td>173.36.207.85</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>FTX1738AJMG</td>
<td>173.36.207.81</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>FTX1740ALBX</td>
<td>173.36.207.80</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>SSI184904LG</td>
<td>173.36.207.82</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>SSI185104LT</td>
<td>173.36.207.84</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

[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

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>init</td>
<td>reached</td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
</tr>
<tr>
<td>amXqvXDO9zW2IZIzeho2cOBrD</td>
<td>init</td>
<td>reached</td>
</tr>
<tr>
<td></td>
<td>pnp-callhome</td>
<td>reached</td>
</tr>
<tr>
<td></td>
<td>ready</td>
<td>reached</td>
</tr>
</tbody>
</table>

CPE in Contact with the PnP Server (detailed)

vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe amXqvXDO9zW2IZIzeho2cOBrD plan component self

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 amXqvXDO9zW2IZIzeho2cOBrD
plan component amXqvXDO9zW2IZIzeho2cOBrD

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 amXqvXDO9zW2IZIzeho2cOBrD
provider CiscoSystems
device amXqvXDO9zW2IZIzeho2cOBrD_ENCS

View CPE Details

vmsnso@ncs> show pnp list

<table>
<thead>
<tr>
<th>SERIAL</th>
<th>IP ADDRESS</th>
<th>CONFIGURED</th>
<th>ADDED</th>
<th>SYNCED</th>
<th>LAST CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGL21388017</td>
<td>10.85.189.20</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>2017-10-25 14:24:07</td>
</tr>
</tbody>
</table>
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:**

```
vmsns@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>
```
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