Troubleshoot Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution

Troubleshoot Colocation Multitenancy Issues

You can use the following commands to view the output and locate issues.

- To view an overview of the VNICs and VLANs of each VNF such as in which bridge they exist, use the `support ovs vsctl show` command.

  ```
  nfvis# support ovs vsctl show
  ```

- To verify the details of a service chain deployment with bridge, or network, or VLAN, use the `show service-chains` command.
- To view the data and HA VTEP IP addresses of a CSP device and the peer CSP devices in a colocation cluster, use the `show cluster-compute-details` command.
- To view the source and destination serial numbers of each HA bridge with the corresponding VLAN and VNID associations, use the `show vxlan tunnels` command.
- To view the data flows per tenant that you can identify by a user id with the VLAN, VNID mapping, use the `show vxlan flows` command.
- To view the VXLAN flow statistics, use the `support ovs ofctl dump-flows vxlan-br` command.
- To view the overall deployment status of VM life cycle, use the `show vm_lifecycle deployments` command.

End-to-end Ping Fails

1. Verify if the VMs are deployed by using the **show vm_lifecycle deployments all** command.
2. Verify that the service chains display the chain name attached to it by using the **show service-chains** command.
3. Verify notifications about events that have occurred on the Cisco SD-WAN device by using the **show notification stream viptela**
4. Ping the **data-vtep-ip** and **ha-vtep-ip** of the CSP peer device by using the **show cluster-compute-details** command.
5. Verify that the VLAN association per bridge, network, or VLAN is matching with the VNICs and VLANs of each VNF. Check the output from the **show service-chain** *chain-name* command matches with the output from the **support ovs vsctl show** command.
6. Contact Technical Support, if connection fails and you're unable to ping the peer CSP device.

Troubleshoot Catalyst 9500 Issues

This section covers some of the common Catalyst 9500 problems and how to troubleshoot them.

General Catalyst 9500 Issues

Switch devices are not calling home to PNP or Cisco Colo Manager

Verify the PNP list on Cisco Colo Manager to determine if the switch devices have not called home. The following are the good and bad scenarios respectively when the **show pnp list** command is used:

Devices have called home

```
admin@ncs# show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
------------------------------------------------------------------------------
FCW2223A3VN 192.168.10.40 true true true 2018-12-18 22:53:26
FCW2223A4B3 192.168.30.42 true true true 2018-12-11 00:41:19
```

Devices have not called home

```
admin@ncs# show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
------------------------------------------------------------------------------
```

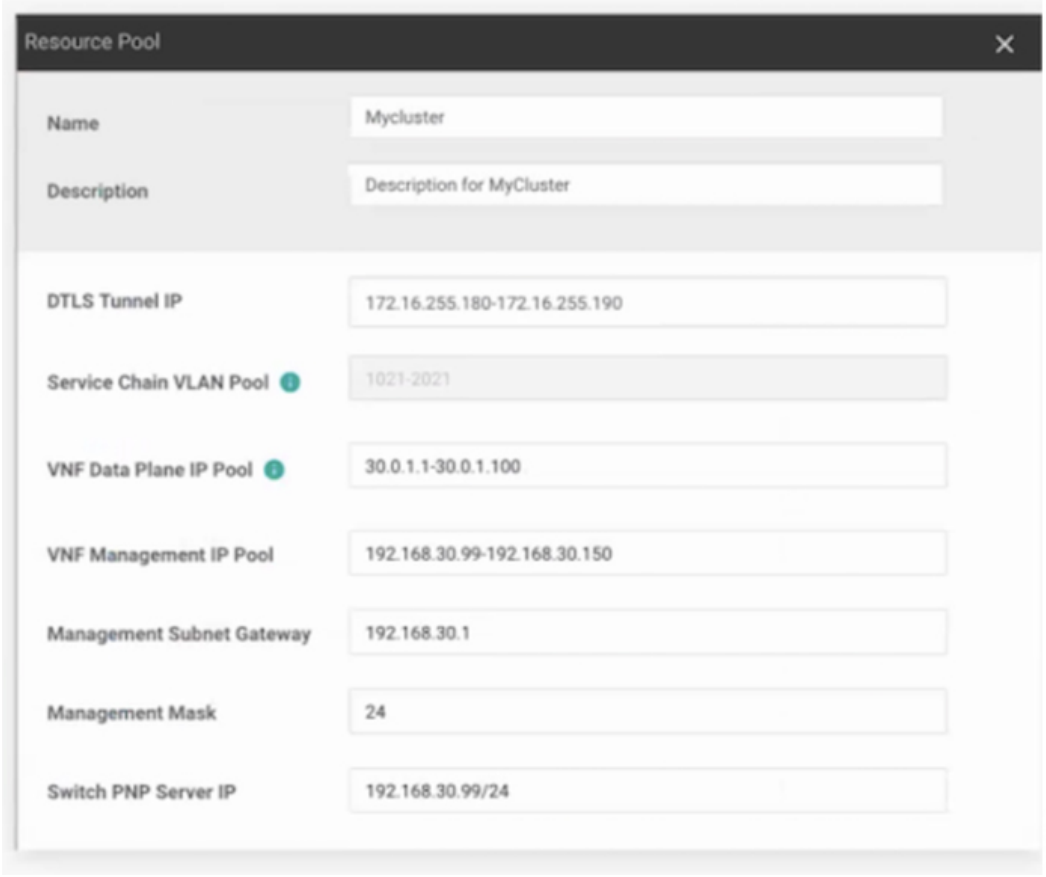
<– Empty list

Action:

1. Verify that the management interfaces on both the switches are not shut and have IP addresses.
2. Try running the **write erase** command on the switch and then reload. Verify that the IP address appears on the management interface.
3. Verify that the configuration for DHCP option 43 is valid. Here is a sample DHCP configuration where the PNP IP address is 192.168.30.99:

```
ip dhcp pool 192_NET network 192.168.30.0 255.255.255.0 dns-server 192.168.30.1
default-router 192.168.30.1 option 43 ascii "5A;B2;K4;I192.168.30.99;J9191" lease infinite
```

4. Verify that the PNP IP address provided on Cisco vManage for resource pool matches the IP address in DHCP configuration as follows:



5. Ping and determine whether both switches are reachable.

Catalyst 9500 failed to reach through DHCP option 43

Here Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state is in progress. If a cluster has already been activated, it shows that the cluster is in activation pending state. If a cluster has not been activated, it shows the cluster is not in activated state.

Action:

1. SSH into NFVIS as an admin user. Use the `ccm-console` command to log into Cisco Colo Manager. Run the `show pnp list` command.
2. If the PNP list is empty, verify the OOB status whether the Cisco Colo Manager IP address is correctly configured on the OOB switch.

Day-0 configuration push failed on both Catalyst 9500 switches

Here Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state is in progress. PnP configuration push fails with an error and Cisco Colo Manager is in-progress state.

Action:

1. Clean the Catalyst 9500 switches by using the **renumber** and **write erase** commands.
2. Deactivate and Reactivate the cluster again from Cisco vManage to repush the Day-0 configuration.

Day-0 configuration push fails on the secondary Catalyst 9K switch

Here Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state shows, "Failure." Cisco Colo Manager shows that only one switch is brought up successfully and cannot detect the secondary switch failure.

Action:

1. Clean the secondary Catalyst 9500 switch by using the **renumber** and **write erase** commands.
2. Deactivate and Reactivate the cluster again from vManage to repush the Day-0 configuration.

One of the Catalyst 9500 switches is up and running. The secondary switch is not in SVL configuration and SVL link cables are not connected

Here Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state shows, "Failure." Both switches are onboarded with an IP address. Cisco Colo Manager detects an error as both switches are connected, as the SVL link on he switches are missing. You can see both switches as "Green" in Cisco vManage.

Action:

1. Verify the SVL link cables.
2. Verify licenses of both Catalyst 9500 switches.

Day-0 configuration push fails and connectivity to switch is down

Here Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state shows, "Failure" until the next Day-0 configuration push. NSO sends notification of not being able to push configuration. You can see a switch as "Red" in Cisco vManage, which means connectivity is down.

Action:

1. Verify the health of the Catalyst 9500 switch.
2. Bring the switch back to online.
3. Start pushing Day-0 configuration again.

Unable to log into Catalyst 9500 after PNP from Cisco vManage

If Cisco vManage is not able to push more configuration to a Catalyst 9500 after PNP, you might have been locked out of the switch.

Action:

1. Log into NFVIS by using **admin** as the login name and **Admin123#** as the default password.

Note The system prompts you to change the default password at the first login attempt. Ensure that you set a strong password as per the on-screen instructions.

2. Use the **ccm console** command on Cisco NFVIS to log into Cisco Colo Manager. Run the following commands on Cisco Colo Manager to add a user to Catalyst 9500 switches.

   - ```
     config t
     cluster <cluster-name>
     system rbac users user admin password
     $9$yYkZqj7lQcrRL3$sZ23jqv5buK4lYCkt0dCbO6xYEfxRHQJiQnrlFdYHBg
     ```

Note Ensure that you set password as a scrypt string.

Now the corresponding user is added to Catalyst 9500 switches and you can SSH to the switches by using user and password.

Issues with a cluster activation, admin and password cannot be pushed to Catalyst 9500

Action:

1. If a cluster activation is in still in pending state, verify if colo-config-status is in IN-PROGRESS state. If state is In-Progress, the synchronization has not been done and no new configurations can be pushed. This process can take up to 20 minutes.
   a. If Cloud OnRamp for Colocation configuration status is In-progress state for a long time, SSH into NFVIS as an admin user. Use the **ccm-console** command to log into Cisco Colo Manager. Run the **show pnp list** command. Verify if two switches are added.
   b. If only one switch is displayed, ensure that the other switch configuration is cleaned by using the **write erase** command and reloaded. The secondary switch startup configuration must be erased and returned to its initial state.
   c. Ensure switch connectivity with PNP server in Cisco Colo Manager.
2. If a cluster has been activated successfully, verify if colo-config-status is in "SUCCESS" state. If status is displayed as Success, your admin password must have been pushed to a switch. If not, on Cisco vManage, add a new credential to the switch and then push new configurations.
3. If a cluster activation fails and colo-config-status is in "FAILED" state, use the RBAC to push a new authentication from ccm-console. In the following example, the password is encryption of "Cisco-123."

   cluster cluster system rbac users user Alpha password 9Z9Sr2VOuwjwC74$qEYAmxgoaW4m07.UjPGR9gL2ksFkcCIgIcEYOUWxDFo role administrators

Note You cannot push any RBAC configuration if a cluster is in active state. Cisco vManage does not allow out of bound change to Cisco Colo Manager.
     ```

Clean switches configuration and reset switches to factory defaults

During a cluster creation, cluster clearing, cluster deletion, the configurations of both switches must be cleaned. To clean switches configuration, perform the following steps:

Action:

1. Use the **show switch** command to determine the switch number and whether the provisioned switch exists in the switch stack. If the switch number is two, use the **switch 2 renumber 1** command.

Note The switch renumbering is essential for SVL stack mode.

2. To erase the switch startup configuration and return it to its initial state, use the **write erase** command.
3. To reload the switch with a new configuration, use the following command in privileged EXEC mode and type n for not saving the modified configuration:

```
switch(config)#reload
```

4. Perform steps 2 and 3 on the second switch device after the switch stack reloading has been completed on the first switch.

To verify addition of switch devices from Cisco Colo Manager, perform the following steps:

1. Log into Cisco Colo Manager and use the **show pnp list** command.

   The two switch devices are displayed. PNP pushes the Day-0 configuration, adds switch devices into the Cisco Colo Manager device tree, and synchronizes the device configuration with Cisco Colo Manager. If any of the switch devices cannot be viewed, the PNP of the missing switch device may be misconfigured or network may be down.

   SVL configuration that is pushed to switches issues a reboot command to switches, after the reboot. Both switch devices are up and become one stack.

2. On Cisco Colo Manager, trigger a timer for around 14 minutes to perform another synchronization on the primary device.
3. To view the device configuration and current status, use the **show cluster** *cluster-name* command.

   If status is displayed as "GREY," the switch devices are not yet added to the Cisco Colo Manager device list. If status is displayed as "RED," the switch devices are not reachable. If status is displayed as, "GREEN," the device is currently connected. Also, you can view which is the primary switch device.

4. To view the devices status in a colocation, use the **show colo-config-status** command. If status is in "In-progress," the switch devices are not yet synchronized and Cisco vManage cannot send any further configuration. See Chapter, Monitor Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Devices for more information about Cisco Colo Manager state transitions.

   After the timer reaches its duration (for example, 14 minutes), Cisco Colo Manager tries to synchronize again with the primary Catalyst 9500 device.

   After the second synchronization has been completed, Cisco Colo Manager state is displayed as, "SUCCESS".

Configuration on switch after QoS policy is applied

When QoS policy is applied, the following configuration appears on the switch device after you set the bandwidth for a service chain and deploy it:

```
class ASAvOnly_chain1_VLAN_210police 2000000000class ASAvOnly_chain1_VLAN_310police
2000000000policy-map
service-chain-qosclass ASAvOnly_chain1_VLAN_210police 2000000000class
ASAvOnly_chain1_VLAN_310police 2000000000
```

Troubleshoot Cisco Cloud Services Platform Issues

This section covers some of the common Cloud Services platform (CSP) problems and how to troubleshoot them.

RMA of Cisco CSP Devices

Use the **admin tech** command for the CSP device from Cisco vManage to collect the log information for the device on the **Tools** > **Operational Commands** screen. Verify the following log files:

- `nfvis_config.log`: Displays the device configuration-related logs
- `escmanager.log`: Displays VM deployment-related logs.
- `Tech-support-output`: Use the following show commands that are available from the CSP device.
  - `cat/proc/mounts`: Displays mount information
  - `show hostaction backup status`: Displays the status of the last five backups taken on the CSP device
  - `show hostaction restore-status`: Displays the status of the overall restore process and each component such as device, image and flavors, VM, and so on
  - `show vm_lifecycle deployments`: Displays the deployment name and the VM group name.

The following is an example of the mount operation on the NFS server:

```
nfvis# show running-config mount
mount nfs-mount storage sujathast/
storagetype            nfs
storage_space_total_gb 5000.0
server_ip              192.168.0.1
server_path            /NFS/colobackup
```

The following is an example of the operational status output for the last five backup operations and notifications on Cisco vManage for the last backups:

```
eventTime 2021-02-02T04:02:25.577705+00:00
viptela
severity-level minor
host-name nfvis
system-ip 10.0.0.1
user_id admin
config_change false
transaction_id 0
status SUCCESS
status_code 0
status_message Backup configuration-only to nfs:test_storage/test_config_only.bkup completed
```

```
 successfully with operational status: BACKUP-COMPLETED-PARTIALLY
details NA
event_type BACKUP_SUCCESS
severity INFO
host_name nfvis
 !
```

The following example shows that status of the device after using the `show hostaction restore-status` command:

```
nfvis# show hostaction restore-status
hostaction restore-status 2021-03-19T20:53:15-00:00
source nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status RESTORE-ERROR
components NFVIS
status      RESTORE-ERROR
last update 2021-03-19T21:02:11-00:00
details     "Unable to load configuration Editing of storage definitions is not allowed"
components nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status      VERIFICATION-SUCCESS
```

Clear Status of VNICs and PNICs

1. To view the PNIC stats, use the **show pnic stats** command.
2. To view the VNIC stats, use either of the following commands:
   - **show vm_lifecycle vnic_stats** for all VMs
   - **show vm_lifecycle vnic_stats** *vm-name* for a single VM
3. To clear the stats of one or more VMs, run the following commands:

   ```
   clear counters vm all
   clear counters vm vm-name vnic vnic-id
   clear counters vm vm-name vnic all
   ```

4. To clear the stats of all PNICs and VNICs, use the **clear counters all** command.

When CSP reboots, all PNIC and VNIC counters are erased and the counters are cleared. If the stats of VNICs and PNICs aren't displayed, you can use the following commands to view the stats:

```
show pnic-clear-counter
show vm_lifecycle tx_rx_clear_counters
```

Issues in Cisco CSP Device Onboarding

1. To verify that the device has established a secure control connection with the SD-WAN controllers, use the **show control connections** command.
2. To verify the device properties used to authenticate the devices, use the **show control local-properties** command.

   From the displayed output, make sure:

   - 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 vBond IP address or DNS
- **system-ip** is configured, **chassis-num/unique-id**, and **serial-num/token** is available on the device

3. To view the reason for failure, if a device fails to establish connection with the Cisco SD-WAN controllers, use the**show control connections-history** command. View the **LOCAL ERROR** and **REMOTE ERROR** column to gather error details.

   The following are the reasons the Cisco CSP device fails to establish control connections with the Cisco SD-WAN controllers.

   - CRTVERFL – the error state indicates that the device authentication is failing because of a root-ca certificate mismatch between the device and the Cisco SD-WAN controller. Use the **show certificate root-ca-cert** on Cisco CSP devices to confirm that the same certificates are installed on the device and the Cisco SD-WAN controllers.
   - CTORGNMMIS - the error state indicates that the device authentication is failing because of a mismatch organization-name, compared with the organization-name configured on the Cisco SD-WAN controller. Use show **sdwan control local-properties** on CSP devices to confirm all the SD-WAN components are configured with same organization-name.
   - NOVMCFG – the error status indicates that the device hasn't been attached with a device template in Cisco vManage. This status is seen when onboarding the device using automated deployment options, which is the PnP.
   - VB_TMO, VM_TMO, VP_TMO, VS_TMO – the error indicates that the device has lost reachability to the Cisco SD-WAN controllers.

Failure in Cluster Activation

In CCM, verify if the SVL formation of switches is complete and the devices are onboarded by viewing CCM notifications status.

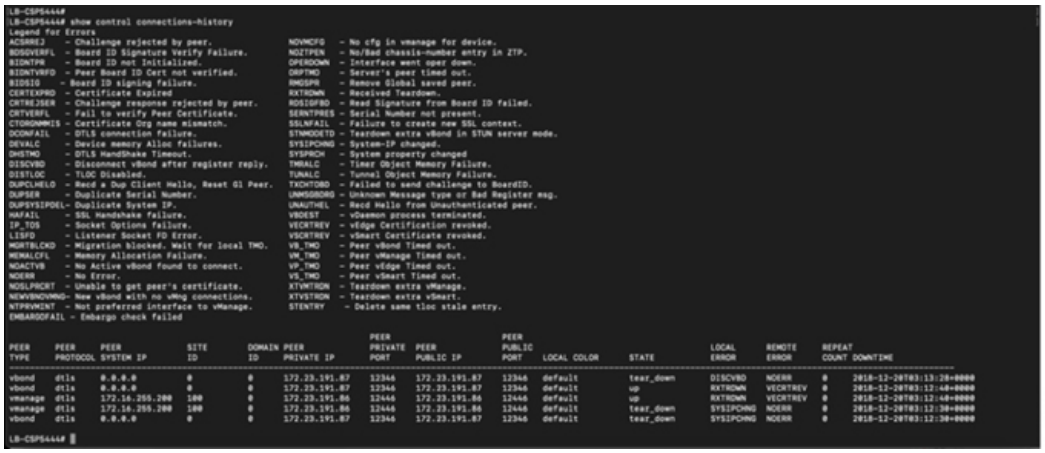
1. Ensure that all the SR-IOV and OVS ports are cabled correctly to the Catalyst 9500 switches and the interfaces are in link-up state.
2. Determine the SR-IOV and OVS ports using the **show lldp neighbors** command on a CSP device and verifying the wiring between the CSP devices and Catalyst 9500 switches.

   Ensure that the **show lldp neighbors** command displays all eight ports are powered up and reports about the neighbors.
3. Ensure that the Catalyst 9500 switches are in SVL mode and the interfaces have the description, "SVL Complete."

Failures with Certificate installation

Use the **show control connections-history** command to determine certificate installation failures.

Figure 1: Certificate Installation Failure



Action:

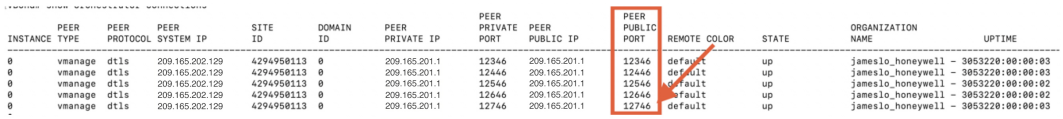
The following are the verifications that you can perform based on errors that you might encounter:

- vbond with error SERNTPRES–This error is caused, if the serial or token on device don't match with vBond serial or token. Check vManage to ensure that the device is in "valid" state and it was decommissioned properly.
- Cisco vManage with error NOVMCFG–This error is caused if the template wasn't attached to the device. Activating the cluster resolves this issue.
- On vBond, verify that the **show orchestrator valid-vedges** command shows the device correctly. This means that the device is valid with the same token that you had used.
- Ensure that the clocks on Cisco vManage and CSP devices are synchronized.

Failures with Control Connection

The **show control connections-history** displays DCONFAIL. Open the firewall to view the ports that need to be opened.

Figure 2: Failure with Control Connection, DCONFAIL



Action:

The following ports need to be opened:

Table 1: UDS and TCP Ports to be Opened

Core Number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core0	12346	23456
Core1	12446	23556

Core Number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

CSP doesn't have a DHCP IP address

The CSP device doesn't get displayed in Cisco vManage as a connected device.

Action:

1. Connect to a CSP through the CIMC interface.
2. Verify if the CSP has an IP address by running the **`show system:system settings`** command on the Cloud OnRamp for Colocation management port.
3. Verify if the DHCP server has IP addresses. To assign a static IP address and configure DHCP sticky IP, see DHCP IP Address Assignment, on page 14.
4. Verify that the PNP server is reachable by a ping.
5. From the PNP server, verify if the CSP device can be contacted and claimed, or redirection is successful. In the PNP portal, if it shows Pending Redirection for the device, verify if the serial number is same as CSP devices.
6. Use the **`show platform-details`** command on CSP to determine the serial number.
7. In the PNP portal, verify if it shows Connected.

CSP hasn't established connectivity with Cisco vManage

The CSP device doesn't get displayed in Cisco vManage as a connected device.

Action:

1. Verify if the CSP device has root CA installed from PNP by using the **`show certificate installed`** and **`show certificate root-ca-cert`**.
2. Verify if CSP can ping the vBond IP address. Then, attain the vBond IP by using the **`show running-config viptela-system:system`**
3. If ping to vBond fails, verify the network connectivity on the management interface.
4. If ping to vBond goes through, use the **`running-config vpn 0`** to view the configuration for control connection.
5. If the control connection configuration exists, verify Cisco vManage settings.

6. In Cisco vManage, verify if a cluster is activated and device OTP information has been included by using the **show control connections** and **show control local-properties** commands.
7. Verify if the CSP token number has been manually entered by using the **request vedge-cloud activate chassi-number token-number** command. Rerun the command with the correct OTP.

Factory reset of CSP device

To reset a CSP device to factory default, use the following command.

CSPxx# factory-default-reset all

The command deletes VMs and volumes, files including logs, notifications, images, and certificates. It erases all configuration. The connectivity is lost, admin password is changed to the factory default password. The system is rebooted automatically after reset and you must not perform any operation for 15- 20 minutes when factory reset is in progress. You can continue when prompted to proceed with the factory reset process.

CSP with a bad storage disk

The control connection is brought up and cluster is activated. The Cisco vManage monitoring screen displays all the eight CSP disks are available and one of the disks that is faulty.

Action:

Replace the faulty disk.

CSP device has less memory or CPU

The control connection is brought up and cluster is activated. The Cisco vManage monitoring screen displays that the memory threshold has reached.

Action:

Upgrade the specific CSP device that matches the minimum requirements.

I/O cards on CSP device are on wrong slots

Action:

Verify the slot details from CIMC inventory.

Colo Manager is not healthy on a CSP device

Action:

1. To verify Cisco Colo Manager state:
   a. Verify the health of the container by using the **show container ColoMgr** command. See Troubleshoot Cisco Colo Manager Issues, on page 15.
   b. View notifications about events from the Viptela device by using the **show notification stream viptela** command
2. To access Cisco Colo Manager, run the **ccm console** command on the CSP device where Cisco Colo Manager has been enabled.

This action takes you to the Cisco Colo Manager CLI. Run the **show running-config cluster** *cluster name* command.

3. Get the logs from Cisco vManage by using the **admin-tech** command. Alternatively, you can get the logs from the device directly. See Log Collection from CSP, on page 19.

Day-0 configuration push to CSP fails

The failure can be either due to CSP not having the correct hardware or Day-0 configuration of VNF has wrong input.

Action:

1. Verify the hardware configuration of CSP and ensure that it's a supported configuration.
2. Verify service chain Day-0 configuration, and then retrigger configuration push.

CSP doesn't get added to a cluster

Cluster state in the **vManage** > **Cofigurationn** > **Cloud OnRamp for Colocation** interface shows, "FAILED." The added CSP is depicted as "RED" in the Cloud OnRamp for Colocation graphical representation.

Action:

1. Verify the hardware configuration of CSP and ensure that it's supported.
2. Retry activating the cluster again

IP connectivity with CSP can't be retained

When CSP devices renew its DHCP IP, the IP connectivity to the CSP can't be retained.

Action:

For DHCP IP address allocation, ensure that the DHCP server is always on the same subnet as the CSP devices.

CSP devices aren't able to reach Cisco vManage

Action:

Perform the following steps:

1. Install Cisco NFVIS on the CSP device by using the KVM console. See the Cisco Enterprise NFV Infrastructure Software Configuration Guide for information about installing NFVIS.
2. Log in to the NFVIS system and ping gateway

   If it's not pinging or reachable, ensure OOB switch ports that are connected to the switch has port-channel configuration that is done.

   a. If port-channel configuration on a switch is missing, run the nfvis# **support ovs appctl bond-show mgmt-bond** command. The output is as follows:

```
--- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
```

```
next rebalance: 3479 ms
lacp_status: configured
active slave mac: 00:00:00:00:00:00(none)
slave eth0-1: disabled
                may_enable: false
slave eth0-2: disabled
                may_enable: false
```

b. If the port channel on a switch is configured, but eth0-2 isn't connected to the switch, run the nfvis# **support ovs appctl bond-show mgmt-bond** command. The following ouput now shows that eth0-2 isn't connected to switch:

```
---- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 4938 ms
lacp_status: off
active slave mac: 50:2f:a8:c7:64:c2(eth0-1)


slave eth0-1: enabled
active slave
may_enable: true
hash 195: 2 kB load


slave eth0-2: disabled
may_enable: false
```

Note Cisco vManage manages the CSP devices and therefore OOB configuration through NETCONF or REST API or CLI causes devices to be out of synchronization with Cisco vManage. Cisco vManage deletes this configuration when the next configuration is pushed from it. For any troubleshooting, to configure the Cisco CSP or NFVIS, use configuration only in shared mode or in NETCONF target candidate followed by commit. This configuration is required as in the Confd database, CDB is in a candidate mode on Cisco NFVIS for Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution. If the **confg t** CLI mode or NETCONF target running is used, the CDB database might not be in synchronization and cause strange behavior on the CSP devices and results into an unusable cluster.

DHCP IP Address Assignment

To configure a static IP address:

1. After clean installation of the DHCP server, run **confd cli**.
2. Verify the existing configuration by using the nfvis# **show running-config vm_lifecycle** command.

   For example,

   nfvis# **show running-config vm_lifecycle networks**

   ```
   vm_lifecycle networks network int-mgmt-net
   !
   ```

3. Set up a static IPv4 address by using the nfvis# **config shared** command.

   For example,

   nfvis# **config shared**

```
Entering configuration mode terminal
nfvis(config)# vm_lifecycle networks network int-mgmt-net subnet int-mgmt-net-subnet
address <host-ip> gateway <host-ip-gateway> netmask <your-host-ip-netmask>  dhcp false
nfvis(config-ip-receive-acl-0.0.0.0/0)# commit
Commit complete.
nfvis(config-ip-receive-acl-0.0.0.0/0)# end
nfvis#
```

Configure DHCP Sticky IP

For sticky DHCP IP, configure the DHCP servers. Ensure that you have the serial number of the device readily available.

1. If you use CentOS 7.4 as the DHCP server, ensure that you have the following similar configuration in `/etc/dhcp/dhcpd.conf`.

```
host abcxxxx175 {
option dhcp-client-identifier <serial number>;
}
```

2. If you use IOS as the DHCP server, ensure that you have the following similar configuration in an IOS DHCP server or pool.

```
ip dhcp pool P_112
host 209.165.201.12 255.255.255.0
client-identifier 4643.4832.3xxx.3256.3xxx.48
```

   In this example, the IP address, 209.165.201.12 is the DHCP sticky IP for a client with identifier: 4643.4832.3xxx.3256.3xxx.48. Then, you can find out the client-identifier.

3. To find the client identifier, on an IOS DHCP server, turn on **debug ip dhcp server packet**.

   From the debug console output, you can view DHCP client-identifier of the SD-WAN Cloud OnRamp for Colocation device.

Troubleshoot Cisco Colo Manager Issues

This section covers some of the common Cisco Colo Manager problems and how to troubleshoot them.

General Cisco Colo Manager Issues

Verify Port Connectivity when SVL Formation Fails

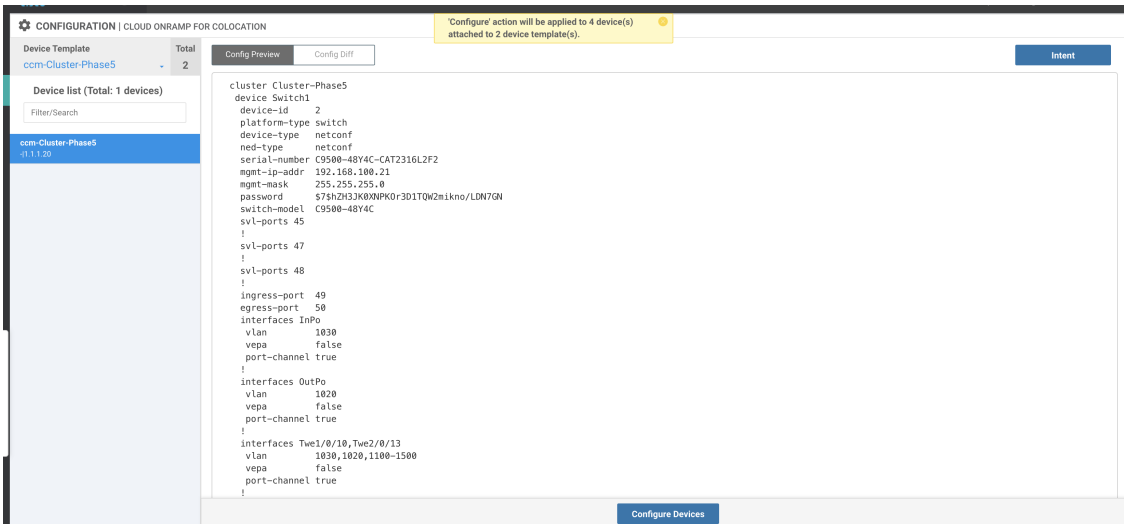
After activating a cluster, to verify the SVL and uplink ports from CCM, perform the following steps:

1. From Cisco SD-WAN Manager, click **Configuration** > **Cloud OnRamp for Colocation**.
2. To verify the port connectivity of a cluster, choose the cluster from the table, click the **More Actions** icon to the right of the row, and then choose **Sync**.
3. Under **Device Template**, click the colocation cluster, and then choose the CCM cluster from the drop-down list.

4. To view the CCM configuration, click the CCM cluster.

   You can now view port connectivity details of both the switch devices in the cluster and determine the connectivity issues.

   Figure 3: Verification of SVL and Uplink Ports



Failure in Cisco Catalyst 9500 SVL Formation

1. Establish an SSH session with Cisco NFVIS as an admin user. Use the **ccm-console** command to log into Cisco Colo Manager and run the **`show colo-config-status`** command.

   ```
   admin@ncs# show colo-config-status
   ```

   Displays the recommended action.

   ```
   colo-config-status status failure
   colo-config-status description "Step 4 of 7:
   Device c9500-2 : 192.168.6.252 (CAT2324L42L)
   SVL ports specified by vmanage does not match with
   actual cabled svl ports. Recommended action: Correct
   the configured svl ports specified in cluster
   configuration by vmanage in accordance with switch
   SVL port cabling" colo-config-status severity critical
   ```

2. Ensure that the ports you choose for SVL on Cisco vManage match the physically cabled ports, and that they are detected by the Cisco Catalyst 9500 switches.

Cisco Colo Manager is unhealthy while activating a cluster for Day-0, or Cisco CSP is deleted when Cisco Colo Manager is running. Also, the new Cisco Colo Manager on the newly added Cisco CSP device fails to instantiate or becomes unhealthy

Here Cisco Colo Manager is in unhealthy state at the host end, and Cisco Colo Manager internal state shows, "FAILURE." Cisco vManage monitoring also shows Cisco Colo Manager in "UNHEALTHY" state.

Action:

1. Verify the Cisco Colo Manager state on the newly added Cisco CSP device by running the **show container ColoMgr** command.

```
CSP1# show container ColoMgr
container ColoMgr
 uuid       57b9b8646ff1066ba24707415b5449111d915664629f56221e141c1171ee283d
 ip-address 172.31.232.182
 netmask    24
 default-gw 172.31.232.2
 bridge     int-mgmt-net-br
 state      healthy
 error
CSP1#
```

2. Verify the reason for Cisco Colo Manager being in unhealthy state by looking at the error field as shown in the previous step.
3. For failures that are related to pinging the gateway, verify the Cisco Colo Manager parameters such as, IP address, mask and gateway IP address are valid. Also, verify the physical connection reachability to the gateway.
4. If any of the parameters are incorrect, fix them from Cisco vManage, and then retry activating cluster or synching.
5. If reason for Cisco Colo Manager being unhealthy are package errors, contact Technical Support.

Troubleshoot Service Chain Issues

This section covers some of the common service chain problems and how to troubleshoot them.

General Service Chain Issues

Service chain addition or deletion in to a service group fails

- Action:
- Cisco Colo Manager is in healthy state at the host end, and Cisco Colo Manager internal state shows, "FAILURE" for the configuration push. The configuration push fails, Cisco Colo Manager is in "FAILURE" state, and cluster is in "FAILURE" state.

  Action:

  1. To access Cisco Colo Manager, run the **`ccm console`** command on the CSP device where Cisco Colo Manager has been enabled.

     This action takes you to the CLI on Cisco Colo Manager. Run the following commands:

     a. **`show colo-config-status`**

        This action enables you to view the reason for failure in the description.

     b. If more information is required to debug the failure, collect logs by using the **`admin-tech`** command on CSP hosting Cisco Colo Manager. Alternatively, you can get the logs from the device directly. See Log Collection from CSP, on page 19.

  2. Verify the Day-0 configuration of VNF service chains.
  3. Provision the VNF service chain again.

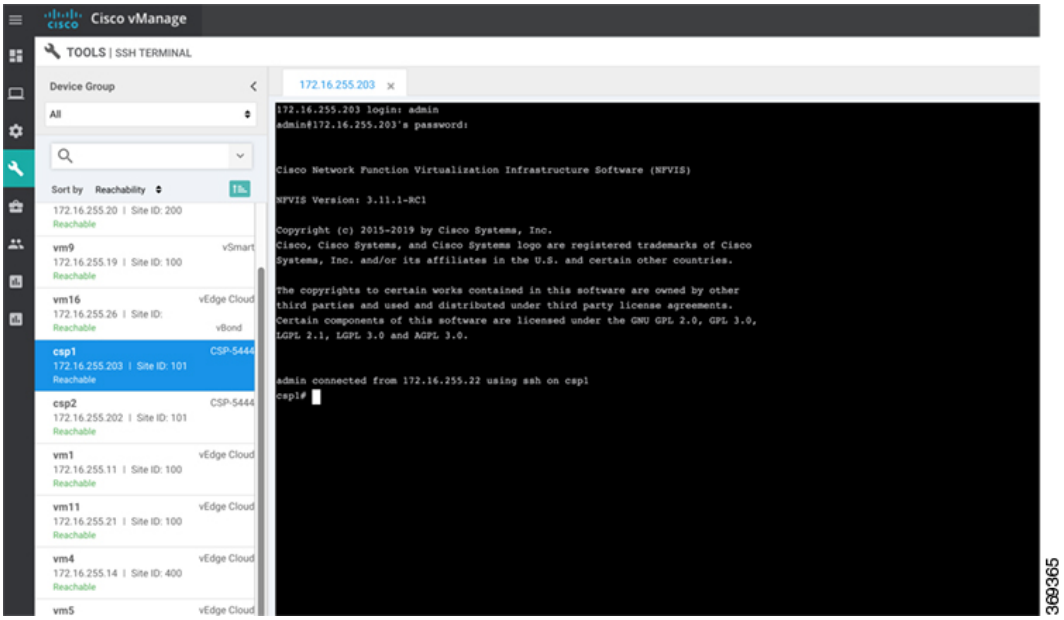
Note If service chain addition or deletion results in a failure on Cisco Colo Manager, there is an option to synchronize.

During service chain addition, VNF goes into error state

VNF is shown as down on Cisco vManage.

Action:

1. Verify the Day-0 configuration of VNF.
2. SSH from Cisco vManage to go to the CSP hosting the VNF.



3. Run the following commands:

   nfvis# show system:system deployments

   nfvis# get the VNF ID

   For example,

   NAME ID STATE

   Firewall2_SG-3 40 running

   nfvis# support show config-drive content 40

Ensure that all variables are properly replaced with key, value pairs.

Troubleshoot Physical Network Function Management Issues

To troublehsoot the sharing of PNF devices, ensure that the following are considered:

1. Cabling of PNF devices to Catalyst 9500 is correct and VLAN configurations are on the right ports of Catalyst 9500.
2. Verifying the LLDP enablement. By default, LLDP is enabled on Catalyst 9500. Ensure that you enable LLDP on PNF and check the LLDP neighbor and neighbor interface to confirm connectivity.
3. Verifying the missing configurations on PNF.

Log Collection from CSP

If CSP is not reachable from Cisco vManage, and logs need to be collected for debugging, use the **tech-support** command from CSP.

The following example shows the usage of the tech-support command:

```
nfvis# tech-support
nfvis# show system:system file-list
system:system file-list disk local 1
 name          nfvis_scp.log
 path          /data/intdatastore/logs
 size          2.1K
 typ
```

To secure copying a log file from the Cisco NFVIS to an external system or from an external system to Cisco NFVIS, the admin user can use the scp command in privileged EXEC mode. The following example shows the scp techsupport command:

```
nfvis# scp techsupport:NFVIS_nfvis_2019-04-11T15-33-09.tar.gz
cisco@172.31.232.182:/home/cisco/.
```

Troubleshoot Cisco vManage Issues

Use the following location to troubleshoot Cisco vManage issues,

SD-WAN Techzone Knowledge Base