Monitor Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Devices

Cisco vManage displays the Cloud OnRamp for Colocation status at a cluster level that indicates the health of each device. The cluster level resources are displayed to indicate the resource availability, such as the CPU allocated and available. You can view service groups in the cluster. All the service groups under a cluster are shown in a table view that indicates the number of VMs in a service chain that are up or down. Also, you can view the diagram view of a service group. This diagram view displays all service chains and VMs in a service chain that allows you to look at the resources that are allocated to a VM. The view displays VLANs for each VNIC attached to the VM. You can look at the VNF view, which is in tabular form that displays VNF details. You can hover over VM and get information about management IP, CPU, Memory, disk, HA, and VM type.

The historical and real-time operational statistics such as CPU, memory, disk, and VNIC utilization charts are available for each VM and CSP device. The VNF view can be navigated from a device under the cluster view or from the services view. See Monitor Operational Status of Cloud OnRamp for Colocation Devices from Cisco Catalyst SD-WAN Manager, on page 1.

Monitor Operational Status of Cloud OnRamp for Colocation Devices from Cisco Catalyst SD-WAN Manager

Monitoring colocation devices is the process of reviewing and analyzing a device, such as Cloud Services Platform (CSP) devices and Cisco Colo Manager for health, inventory, availability, and other operation-related processes. You can also monitor the components of CSP devices such as CPU, memory, fan, temperature, and so on. For more information about theCisco SD-WAN Manager Monitoring screens, see the Cisco Catalyst SD-WAN Configuration Guides configuration guides.

All notifications are sent to the Cisco SD-WAN Manager notification stream. To use the notification stream command, see Cisco Catalyst SD-WAN Command Reference.

Procedure

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

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

If Cisco SD-WAN Manager can't reach the CSP devices and Cisco Colo Manager cannot reach the switches, the CSP devices and Cisco Colo Manager are shown as unreachable.

Step 2 Click a CSP device or a switch from the list by clicking the hostname.

By default, the VNF Status window appears.

Step 3 Click **Select Device** and to filter the search results for devices, use the Filter option in the search bar.

The following are the categories of information about the device that are displayed:

- VNF Status—Displays performance specifications, required resources, and component network functions for each VNF See View Information About VNFs from Cisco vManage, on page 3.
- Interface—Displays Interface status and statistics See the "View Interfaces" topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Control Connections—Displays status and statistics for control connections See the View Control Connections topic in the Cisco Catalyst SD-WAN Configuration Guides.
- System Status—Displays reboot and crash information, hardware component status, and CPU and memory usage. See the View Control Connections topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Cisco Colo Manager—Displays Cisco Colo Manager health status See View Cisco Colo Manager Health, on page 5.
- Events—Displays latest system logging (syslog) events. See the View Events topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Troubleshooting—Displays information about pings and traceroute traffic connectivity tools See the Troubleshoot a Device topic in the Cisco Catalyst SD-WAN Configuration Guides.
- Real Time—Displays real-time device information for feature-specific operational commands. See the View Real-Time Data topic in the Cisco Catalyst SD-WAN Configuration Guides.

Step 4 To monitor colocation clusters, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and click **Colocation Cluster**.

Cisco vManage Release 20.6.1 and earlier: To monitor colocation clusters, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Network** and click **Colocation Clusters**.

Step 5 Click the desired cluster name. See Monitor Cloud OnRamp Colocation Clusters, on page 5 for more information.

View Information About VNFs from Cisco vManage

Table 1: Feature History

Feature Name	Release Information	Description
VNF States and Color Codes	Cisco SD-WAN Release 20.1.1	This feature allows you to determine the state of a deployed VM using color codes, which you can view on the **Monitor** > **Devices** page.

Table 2: Feature History

Feature Name	Release Information	Description
Network Utilization Charts for SR-IOV Enabled NICs and OVS Switch	Cisco SD-WAN Release 20.1.1	This feature allows you to view network utilization charts of VM VNICs connected to both SR-IOV enabled NICs and OVS switch.

You can view performance specifications and required resources for each VNF. Reviewing this information can help you to determine which VNF to use when you're designing a network service. To view information about VNFs, perform the following steps:

Procedure

Step 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**.

Cisco SD-WAN Manager displays the VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

Step 2 Click a CSP device from the table.

Step 3 From the left pane, click **VNF Status**.

Step 4 From the table, click the VNF name. Cisco SD-WAN Manager displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, and disk utilization to monitor the VNF resources utilization.

The following VNF information is displayed:

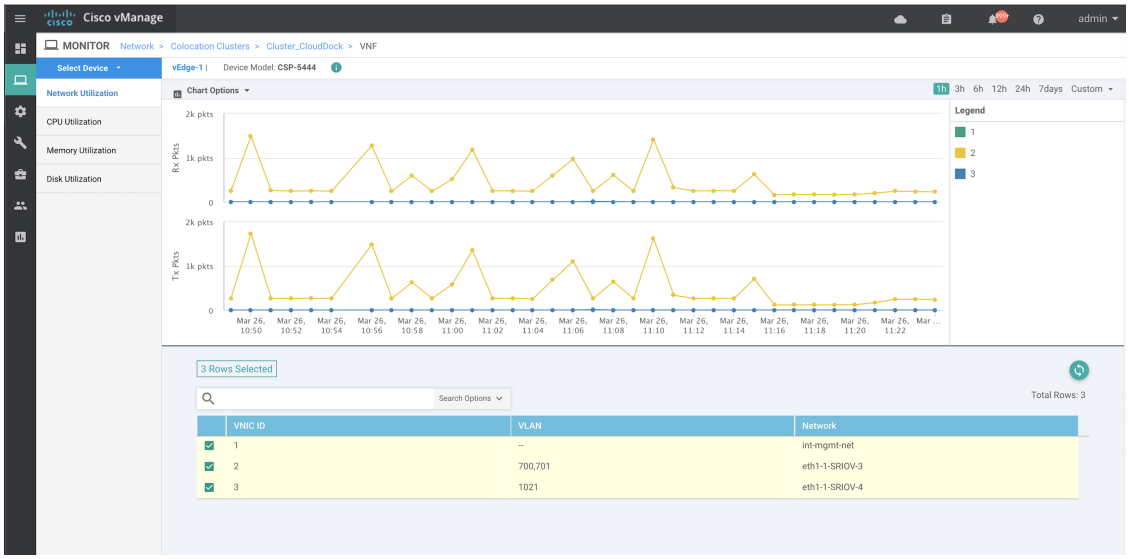
Table 3: VNF Information

Chart options bar	VNF information in graphical format	VNF information in color coded format
• Chart Options drop-down—Click Chart Options drop-down list to select the type of data to display. • Time periods—Click either a predefined time period, or a custom time period for which to display data.	Choose a VNF from the **Select Device** drop-down list to display information for the VNF.	The VNFs are shown in specific colors based on the following operational status of the VNF life cycle: • Green—VNF is healthy, deployed, and successfully booted up. • Red—VNF deployment or any other operation fails, or VNF stops. • Yellow—VNF is transitioning from one state to another.

The right pane displays the following:

- Filter criteria
- VNF table that lists information about all VNFs or VMs. By default, the first six VNFs are selected. The network utilization charts for VNICs connected to SR-IOV enabled NICs and OVS switch are displayed.

Figure 1: VNF Information



The graphical display plots information for the VNFs that you have selected by checking the check box.

- Click the check box at the left to select and deselect VNFs. You can select and display information for a maximum of six VNFs at a time.
- To change the sort order of a column, click the column title.

View Cisco Colo Manager Health

You can view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state. Reviewing this information can help you to determine which VNF to use when you're designing a network service chain. To view information about VNFs, perform the following steps:

Procedure

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

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

The information of all devices is displayed in a tabular format.

Step 2 Click a CSP device from the table.

Step 3 From the left pane, click **Colo Manager**.

The right pane displays information about the memory usage, CPU usage, uptime, and so on, of the Cisco Colo Manager.

Monitor Cloud OnRamp Colocation Clusters

Table 4: Feature History

Feature Name	Release Information	Description
Network Assurance –VNFs: Stop/Start/Restart	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature provides the capability to stop, start, or restart VNFs on Cisco CSP devices from the **Colocation Cluster** tab. You can easily perform the operations on VNFs using Cisco SD-WAN Manager.

You can view the cluster information and their health states. Reviewing this information can help you to determine which Cisco CSP device is responsible for hosting each VNF in a service chain. To view information about a cluster, perform the following steps:

Procedure

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

Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 To monitor clusters, click **Colocation Cluster**.

Cisco vManage Release 20.6.1 and earlier: Click **Colocation Clusters**.

All clusters with relevant information are displayed in a tabular format. Click a cluster name. You can monitor cluster by clicking **Config. View** and **Port Level View**.

- **Config. View**: The primary part of the window displays the CSP devices and switch devices that form the cluster. In the right pane, you can view the cluster information such as the available and total CPU resources, available and allocated memory, and so on, based on colocation size.

  The detail part of the window contains:

  - Search: To filter the search results, use the Filter option in the search bar.
  - A table that lists information about all devices in a cluster (Cisco CSP devices, PNFs, and switches).

    Click a Cisco CSP device. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, number of CPUs, memory consumption, and other core parameters that define performance of a network service chain. See View Information About VNFs from Cisco vManage, on page 3 .

    To start, stop, or reboot a VNF, for the desired VNF, click **...** and choose one of the following operations:

    - **Start**.
    - **Stop**.
    - **Restart**.

Note
Ensure that service chain provisioning is complete and VMs are deployed, before issuing start, stop, restart operations on any of the VNFs in the service chain.

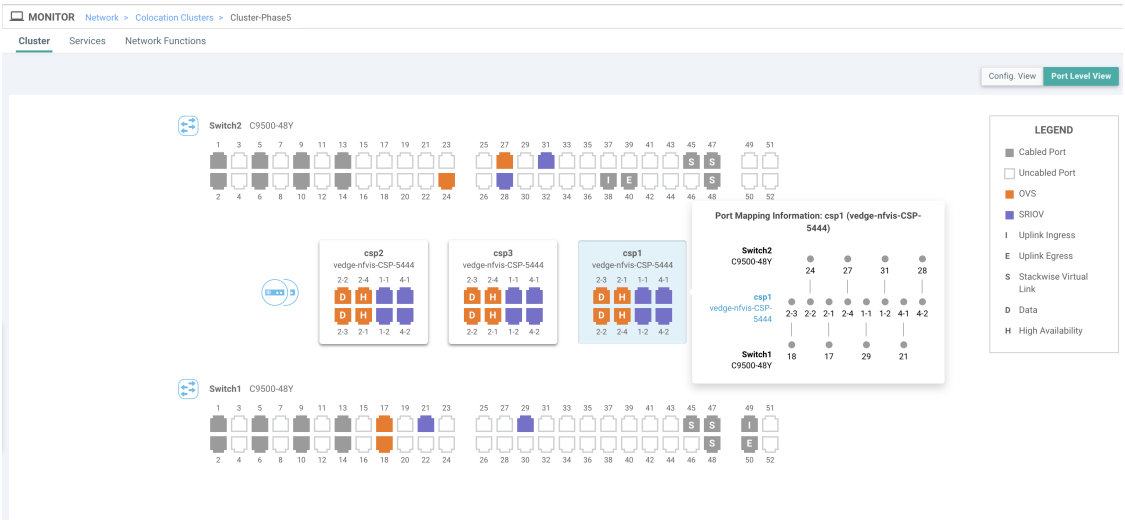
After you choose an operation on a VNF, wait until the operation is complete before you issue another operation. You can view the progress of an operation from the **Task View** window.

- **Port Level View**: After you activate the cluster, to view the port connectivity details, click **Port Level View**.

  You can view detailed port connectivity information for the switches and CSP devices in a color coded format based on the SR-IOV and OVS modes.

  To view the mapping of ports between the Catalyst 9500 switches and CSP devices, click or hover over a CSP device.

Figure 2: Monitor Port Connectivity Details of a Cluster



Step 3 Click **Services**.

Here, you can view the following:

- Complete information of a service chain. The first two columns display the name and description of the service chain in the service group and the remaining columns mention about the VNF, PNF statuses, monitoring service enablement, and the overall health of a service chain. You can also view the colocation user group associated with a service chain. The various health statuses and their representations are:
  - Healthy—An up arrow in green. A service chain is in 'Healthy' status when all the VNF, PNF devices are running and are in healthy state. Ensure that you configure the routing and policy correctly.
  - Unhealthy—A down arrow in red. If one of the VNFs or PNFs are in unhealthy state, the service chain is reported to be in 'Unhealthy' status. For example, after deploying a service chain, if one of the network function IP address changes on the WAN or LAN side, or the firewall policy isn't configured to let the traffic pass through, then unhealthy state is reported. This is because the network function or overall service chain is Unhealthy or both are in Unhealthy state.
  - Undetermined—Down arrow in yellow. This state is reported when the health of the service chain can't be determined. This state is also reported when there's no status such as healthy or unhealthy available for the monitored service chain over a time period. You can't query or search a service chain with undetermined status.

    If a service chain consists of a single PNF and PNF is outside the reachability of Cisco SD-WAN Manager, it can't be monitored. If a service chain consists of a single network function, the firewall that has VPN termination on both sides which can't be monitored, then it's reported as Undetermined.

    Note
    If the status of a service chain is undetermined, you can't choose the service chain to view the detailed monitoring information.

- If you had configured a service chain by enabling the monitoring field, then click a service group that is in Healthy or Unhealthy state. The primary part of the service chain monitoring window contains the following elements:

  Graphical display that plots the latency information of the service chain, VNFs, PNFs.

  The detail part of the service chain monitoring window contains:
  - Search: To filter the search results, use the Filter option in the search bar.
  - A table that lists information about all service chains, VNFs, PNFs, their health status, and types.
    - Check the service chain, VNF, PNF check boxes for the service chains, VNFs, PNFs you want to choose.
    - To change the sort order of a column, click the column title.

  The status details column indicates the monitored data path and it provides the per hop analysis.
- Click **Diagram** and view the service group with all the service chains and VNFs in the design view window.
- Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
- Choose a service group from the **Service Groups** drop-down. The design view displays the selected service group with all the service chains and VNFs.

Step 4 Click **Network Functions**.

Here, you can view the following:

- All the virtual or physical network functions in a tabular format. Use the **Show** button, and choose to display either a VNF or PNF.

  VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, colocation user groups, CPU use, memory consumption, and other core parameters that define performance of network service. To view more information about the VNF, click a VNF name. See View Information About VNFs from Cisco vManage, on page 3 .

- PNF information is displayed in tabular format. The table includes information such as the serial number and PNF type. To view and note configuration of a specific PNF, click the desired PNF serial number. Ensure that you manually note all the configuration of the PNFs and then configure the PNF devices. For example, the following are some of the PNF configuration where you position the PNF at various locations in the service chain. See the ASR 1000 Series Aggregation Services Routers Configuration Guides and Cisco Firepower Threat Defense Configuration Guides to configure the PNFs manually.

Figure 3: PNF in the First Position with Service Chain Side Parameters

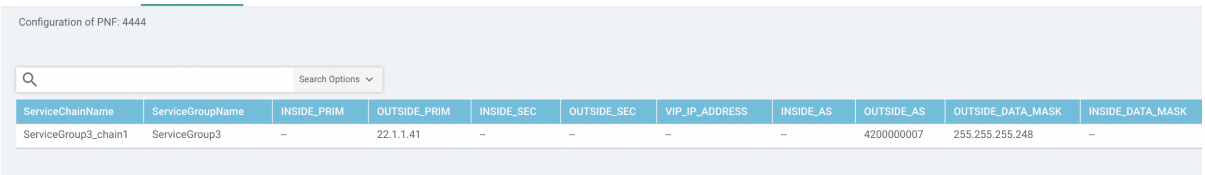


Figure 4: PNF in the First Position with Outside Neighbor Information

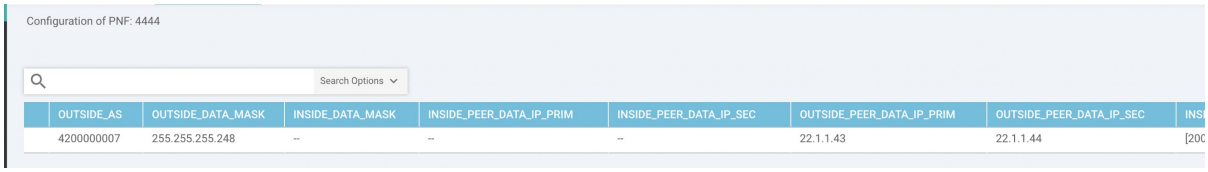


Figure 5: PNF Shared Across Two Service Chains

The ServiceGroup2_chain3 is a PNF-only service chain and therefore no configuration gets generated. The PNF is in the last position of the ServiceGroup2_chain1, so only INSIDE variables gets generated.

Figure 6: PNF Shared Across Two Service Chains with Outside Neighbor Information

Packet Capture for Cloud OnRamp Colocation Clusters

Table 5: Feature History

Feature Name	Release Information	Description
Packet Capture for Cloud OnRamp Colocation Clusters	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature lets you capture packets at either the physical network interface card (PNIC) level or the virtual network interface card (VNIC) level on a Cloud Services Platform (CSP) device of a colocation cluster. You can capture packets on one or more PNIC or VNIC on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format, and helps in application analysis, security, and troubleshooting.

You can capture packets flowing to, through, and from a CSP device of a colocation cluster. You can capture packets at either the PNIC or the VNIC level on the CSP device.

Supported Ports for Packet Capture for Cloud OnRamp Colocation Clusters

Packet capture is supported for the following ports:

Table 6: Supported Ports for Packet Capture

Mode	VNIC Level	PNIC Level
Single Tenancy	OVS-DPDK, HA-OVS-DPDK, SR-IOV, OVS-MGMT	SR-IOV, MGMT
Multitenancy (Role-Based Access Control)	OVS-DPDK, HA-OVS-DPDK, OVS-MGMT	MGMT

Enable Packet Capture on Cisco SD-WAN Manager

Enable the packet capture feature on Cisco SD-WAN Manager before capturing packets at the PNIC or VNIC level on a CSP device of a colocation cluster:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Data Stream**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable data stream.

Capture Packets at PNIC Level

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

2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. In the left pane, click **Packet Capture**.
5. From the **PNIC ID** drop-down list, choose a PNIC.
6. (Optional) Click **Traffic Filter** to filter the packets that you want to capture based on the values in their IP headers.

   Table 7: Packet Capture Filters

Field	Description
Source IP	Source IP address of the packet.
Source Port	Source port number of the packet.
Protocol	Protocol ID of the packet. The supported protocols are: ICMP, IGMP, TCP, UDP, ESP, AH, ICMP Version 6 (ICMPv6), IGRP, PIM, and VRRP.
Destination IP	Destination IP address of the packet.
Destination Port	Destination port number of the packet.

7. Click **Start**.

   The packet capture begins, and its progress is displayed:

   - Packet Capture in Progress: Packet capture stops after the file size reaches 20 MB, or 5 minutes after you started packet capture, or when you click **Stop**.
   - Preparing file to download: Cisco SD-WAN Manager creates a file in libpcap format (a .pcap file).
   - File ready, click to download the file: Click the download icon to download the generated file.

Capture Packets at VNIC Level

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. Choose a VNF, and then click **Packet Capture** in the left pane.
5. Alternatively, choose **Monitor** > **Devices** > **Colocation Cluster**. Next, choose a cluster and click **Network Functions**, choose a VNF, and then click **Packet Capture** in the left pane.
6. From the **VNIC ID** drop-down list, choose a VNIC.
7. (Optional) Click **Traffic Filter** to filter the packets to capture based on values in their IP headers. For more information on these filters, see the above section.

8. Click **Start**. The packet capture begins, and displays its progress.

Cisco Colo Manager States for Switch Configuration

The various Cisco Colo Manager (CCM) states and transitions when you trigger various processes from Cisco vManage are:

- INIT state—When the Cisco Colo Manager container is successfully initialized.
- IN-PROGRESS state—When any configuration push is not possible.
- SUCCESS state—When the Cisco Colo Manager container has successfully translated and pushed the intent that is received from Cisco vManage to Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches.
- FAILURE state—If there is any failure in processing or configuration push in Cisco Colo Manager.

When Cisco vManage pushes the Cloud OnRamp for Colocation configuration intent to the CCM for the first time, it moves from INIT to IN-PROGRESS state. After Cisco Colo Manager pushes the configuration, it goes back to the SUCCESS or FAILURE state. For every incremental configuration push, it goes to IN-PROGRESS state. If any of the configurations pushes fail, Cisco Colo Manager goes into FAILURE state.

Note A notification is sent when Cisco Colo Manager state changes. See Cisco Colo Manager Notifications, on page 12.

Cisco Colo Manager States and Transitions from Host

Cisco vManage depends on various CSP hosts state for the Cisco Colo Manager to be brought up, which are:

- Starting—When Cisco Colo Manager is brought up and health check script hasn't been run. During this phase, Cisco vManage waits for CSP state to change to Healthy.
- Healthy—When the health check script has been run and it has passed the checks. This state implies that the operational model for configuration status can be queried or configuration can be pushed. During this phase, if Cisco Colo Manager is in INIT state, Cisco vManage pushes the device list. If Cisco Colo Manager isn't in INIT state, Cloud OnRamp for Colocation may be in degraded state and recovery flow should start.
- Unhealthy—When all the necessary packages in Network Services Orchestrator (NSO) aren't up. This state can be due to various reasons such as, NSO didn't come up, Cisco Colo Manager package didn't come up, or other reasons. This state implies that the configuration status operation isn't up and configuration can't be pushed.

Cisco Colo Manager Notifications

You can view the Cisco Colo Manager notifications from Cisco Colo Manager console by using the **show notification stream viptela** command.

The various Cisco Colo Manager internal states are:

Table 8: CCM Notifications

Cisco Colo Manager States	Notification Trigger	Notification Output Example

INIT	Init: Cloud OnRamp for Colocation is activated and Cisco vManage brings up Cisco Colo Manager on Cisco CSP.
	Note The Cisco Colo Manager state must be in "Init" only when the docker container is initially brought up and must not be in this state unless container is deleted and brought up again.
		`admin@ncs# show notification stream viptela last 50`
		`notification`
		` eventTime 2019-04-08T17:15:15.982292+00:00`
		` ccmEvent`
		`  severity-level minor`
		`  host-name ccm`
		`  user-id vmanage_admin`
		`  config-change false`
		`  transaction-id 0`
		`  status SUCCESS`
		`  status-code 0`
		`  status-message init`
		`  details Initializing CCM`
		`  event-type CCM-STATUS`
		 `!`
		`!`

IN-PROGRESS	Cisco vManage pushes intent and Cisco Colo Manager moves to in-progress state.
	Note Cisco Colo Manager generates multiple in-progress notifications for the switches that are up.
		`notification`
		` eventTime 2019-04-08T17:37:54.536953+00:00`
		` ccmEvent`
		`  severity-level minor`
		`  host-name ccm`
		`  user-id vmanage_admin`
		`  config-change false`
		`  transaction-id 0`
		`  status SUCCESS`
		`  status-code 0`
		`  status-message IN-PROGRESS`
		`  details Received configuration from vManage`
		`  event-type CCM-STATUS`
		 `!`

Cisco Colo Manager States	Notification Trigger	Notification Output Example
SUCCESS	During cluster activation, after Cisco Catalyst 9500 switches have been successfully onboarded, status moves to SUCCESS. For any incremental configuration, status moves to SUCCESS only if configuration has been saved successfully in the switch devices.	notification eventTime 2019-04-08T17:51:48.044286+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message SUCCESS details Devices done onboarding event-type CCM-STATUS ! ! admin@ncs#

Cisco Colo Manager States	Notification Trigger	Notification Output Example
FAILURE	If onboarding of switches fails during cluster activation, CCM status moves to FAILURE. If any incremental configurations are not saved, CCM status moves to FAILURE. **Note** The failure state cannot transition to another state without end-user intervention.	notification eventTime 2019-04-08T18:01:44.943198+00:00 ccmEvent severity-level critical host-name ccm user-id vmanage_admin config-change false transaction-id 0 status FAILURE status-code 0 status-message FAILURE details SVL bringup not successful. Could not sync TenGigabitEthernet2/0/* interfaces. event-type CCM-STATUS ! ! admin@ncs#
	Onboarding of switches fails during cluster activation due to wiring errors in flexible connections, and CCM status moves to FAILURE.	admin@ncs# show notification stream viptela last 100 | include Step notification details Step 5 of 7: Device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) connected after SVL reload. details Step 6 of 7: Started sync-from for primary device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) details Step 6 of 7: Sync-from done for primary device switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM) Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2) details Step 6 of 7: Devices ready for LLDP query Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2) details Step 6.1 of 7: LLDP Query Details: csp2 has 8/8 interfaces connected, 2/4 sriov, 2/4 fortville to primary switch; 2/4 sriov, 2/4 fortville to secondary switch; Found devices with not optimum connections:- csp1 has 6/8 interfaces connected, 2/4 sriov, 2/4 fortville to primary switch; 2/4 sriov, 0/4 fortville to secondary switch; Minimum Requirement is to have 8/8 interfaces per CSP in cluster. Recommended action: Please refer to recommended topologies and minimum requirements details Step 7 of 7: Devices done onboarding Device list : switch1 : 192.168.100.21 (C9500-48Y4C-CAT2324L2HM), switch2 : 192.168.100.19 (C9500-48Y4C-CAT2316L2F2)

VM Alarms

The following are VM alarms and you can view them from Cisco vManage, when Cisco vManage receives the alarms.

Table 9: Alarms

Alarm	Trigger Condition	Syslog Messages
INTF_STATUS_CHANGE	interface status change	nfvis %SYS-6-INTF_STATUS_CHANGE: Interface eth0, changed state to up
VM_STOPPED	vm stopped	nfvis %SYS-6-VM_STOPPED: VM stop successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_STARTED	vm started	nfvis %SYS-6-VM_STARTED: VM start successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_REBOOTED	vm rebooted	nfvis %SYS-6-VM_REBOOTED: VM reboot successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_INIT	vm recovery initiation	nfvis %SYS-6-VM_RECOVERY_INIT: VM recovery initiation successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_REBOOT	vm recovery reboot	nfvis %SYS-6-VM_RECOVERY_REBOOT: VM recovery reboot successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_RECOVERY_COMPLETE	vm recovery complete	nfvis %SYS-6-VM_RECOVERY_COMPLETE: VM recovery successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_MONITOR_UNSET	vm monitoring unset	nfvis %SYS-6-VM_MONITOR_UNSET: Unsetting VM monitoring successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c
VM_MONITOR_SET	vm monitoring set	nfvis %SYS-6-VM_MONITOR_SET: Setting VM monitoring successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c

See Cisco NFVIS Configuration Guide for more information about syslog support and VM alarms.

VM States

The following are the operational status of deployed VM life cycle. In Cisco Catalyst SD-WAN, you can view and monitor the VM states from Cisco SD-WAN Manager.

Table 10: VM States

VM States	Description
VM_UNDEF_STATE	VM or VNF is transitioning from one state to another.
VM_INERT_STATE	VM or VNF is deployed but not alive.
VM_ALIVE_STATE	VM or VNF is deployed and successfully booted up or alive.
VM_ERROR_STATE	VM or VNF is in error state when deployment or any other operation fails.

Cloud Services Platform Real-Time Commands

Table 11: Real-Time Commands

System Information
Container status
show control connections
Control connection history
Control local properties
Control summary
Control statistics
Control valid vEdges
valid vManage ID
HW Alarms
HW Environments
PNICs
System Status

Host System Mgmt Info
Host System settings
Host System processes
Resource CPU allocation
RBAC Authentication
Resource CPU VNFs
Hardware Inventory
Hardware Temperature thresholds
Control affinity stats