CONTENTS

CHAPTER 1

What's New for Cisco SD-WAN  1

What's New for Cisco IOS XE SD-WAN Release 16.12.1b, 16.12.1d, and 16.12.2r  1

What's New for Cisco SD-WAN Release 19.2.x  3

CHAPTER 2

Monitor and Analyze Cisco SD-WAN  5

ACL Log  5
Alarms  5
Audit Log  11
BFD Protocol  12
Events  14
Geography  15
Network  17
vAnalytics  33
  Overview of vAnalytics  33
  Enable vAnalytics  34
  vAnalytics Dashboard  34
  Monitor Network Performance  35
  Monitor Application Performance  36

CHAPTER 3

Maintain Cisco SD-WAN  39

Admin Tech Command  39
SSH Terminal  40
Rediscover Network  40
Reboot Your Device  41
Software Upgrade  44
  Upgrade CSP Device with NFVIS Upgrade Image  47
Contents

Software Repository  48
  Upload VNF Images  50
  Create Customized VNF Image  51
  View VNF Images  56
  Delete VNF Images  57
CHAPTER 1

What's New for Cisco SD-WAN

This chapter describes what's new in Cisco SD-WAN for each release.

- What's New for Cisco IOS XE SD-WAN Release 16.12.1b, 16.12.1d, and 16.12.2r, on page 1
- What's New for Cisco SD-WAN Release 19.2.x , on page 3


This section applies to Cisco XE SD-WAN devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td></td>
</tr>
<tr>
<td>Multitenancy support in Cisco XE SD-WAN Devices</td>
<td>Starting release Cisco IOS XE SD-WAN 16.12.2r, multitenancy is supported on the following platforms:</td>
</tr>
<tr>
<td></td>
<td>• Cisco ASR 1000 Series Aggregation Services Routers, Cisco ASR 1001X</td>
</tr>
<tr>
<td></td>
<td>• Cisco ISR 4000 Series Integrated Services Routers, Cisco ISR 4321, Cisco ISR 4461</td>
</tr>
<tr>
<td></td>
<td>• Cisco ISR 1000 Series Integrated Services Routers, Cisco ISR 1111-4P</td>
</tr>
<tr>
<td></td>
<td>• Cisco CSR 1000 Series Cloud Services Routers, Cisco 1000v</td>
</tr>
</tbody>
</table>

Multitenancy allows service providers to manage multiple customers or tenants.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant data backup solution in multitenant mode</td>
<td>Starting from Cisco IOS XE SD-WAN 16.12.2r, when databases are shared by multiple tenants in a multitenant mode, you can back up data for a specific tenant and restore it.</td>
</tr>
</tbody>
</table>

**Systems and Interfaces**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Support for NAT64 Devices</td>
<td>This release supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN routers. For related information, see Configure NAT64 CLI Equivalent on Cisco XE SD-WAN Routers.</td>
</tr>
<tr>
<td>Secure Shell Authentication Using RSA Keys</td>
<td>You can now configure RSA keys to secure communication between a client and a Cisco SD-WAN server. For related information, see SSH Authentication using vManage on Cisco XE SD-WAN Devices.</td>
</tr>
<tr>
<td>DHCP option support</td>
<td>You can now use DHCP server options 43 and 191 to configure vendor-specific information in client-server exchanges. For related information, see Configure DHCP.</td>
</tr>
<tr>
<td>Communication with an UCS-E Server</td>
<td>This feature provides an interface in the interface feature template list to configure an UCS-E interface to connect to an UCS-E server. For related information, see Create a UCS-E Template.</td>
</tr>
</tbody>
</table>

**Bridging, Routing, Segmentation, and QoS**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subinterface QoS</td>
<td>A physical interface may be treated as multiple interfaces by configuring one or more logical interfaces called subinterfaces. This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. For related information, see QoS on Subinterface.</td>
</tr>
</tbody>
</table>

**Policies**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Duplication for Noisy Channels</td>
<td>This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices. For related information, see Configure and Monitor Packet Duplication.</td>
</tr>
<tr>
<td>Integration with Cisco ACI</td>
<td>The SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix list and includes a VPN list to an SLA class that is provided by Cisco ACI. For related information, see Integration with Cisco ACI.</td>
</tr>
<tr>
<td>Encryption of Lawful Intercept Messages</td>
<td>Lawful intercept messages between a Cisco XE SD-WAN router and a Media Device can now be encrypted using static tunnel information. For related information, see Lawful Intercept.</td>
</tr>
</tbody>
</table>

**Security**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-Speed Logging for Zone-Based Firewalls</td>
<td>High-Speed Logging (HSL) allows a firewall to log records with minimum impact to packet processing. For related information, see Firewall High-Speed Logging.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Self zone policy for Zone-Based Firewalls</td>
<td>Self-zone is a default zone in the firewall that is associated with the VPN for punt and inject interface. You can define policies to impose rules on the incoming and outgoing traffic. For related information, see Configure Firewall Policies Using vManage.</td>
</tr>
<tr>
<td>Secure Communication Using Pairwise IPsec Keys</td>
<td>This feature enables support to create and install private pairwise IPsec session keys to secure communication between IPsec devices and its peers. For related information, see IPSec Pairwise Keys Overview.</td>
</tr>
</tbody>
</table>

**Network Optimization and High Availability**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Optimization</td>
<td>TCP optimization fine tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput. For related information, see TCP Optimization: Cisco XE SD-WAN Routers. This feature support was added in Cisco IOS XE SD-WAN Release 16.12.1d</td>
</tr>
</tbody>
</table>

**Commands**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback interface support for WAN (IPsec)</td>
<td>You can now configure a loopback transport interface on a Cisco IOS XE SD-WAN router to help in troubleshooting and diagnostics. For related information, see the bind command.</td>
</tr>
</tbody>
</table>

---

**What's New for Cisco SD-WAN Release 19.2.x**

This section applies to Cisco vEdge devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

**Table 2: What's New for Cisco vEdge Device**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td></td>
</tr>
<tr>
<td>Tenant data backup solution in multitenant mode</td>
<td>Starting from Cisco SD-WAN release 19.2.1, when databases are shared by multiple tenants in a multitenant mode, you can back up data for a specific tenant and restore it.</td>
</tr>
<tr>
<td>Systems and Interfaces</td>
<td></td>
</tr>
<tr>
<td>Secure Shell Authentication Using RSA Keys</td>
<td>This feature enables secure shell authentication between a client and a Cisco SD-WAN server using RSA keys. For related information, see SSH Authentication using vManage on Cisco XE SD-WAN Devices.</td>
</tr>
<tr>
<td>Policies</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Packet Duplication for Noisy Channels</td>
<td>This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices. For related information, see <strong>Configure and Monitor Packet Duplication</strong>.</td>
</tr>
<tr>
<td>Control Traffic Flow Using Class of Service Values</td>
<td>This feature lets you control the flow of traffic into and out of a Cisco vEdge device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. For related information, see <strong>Configure Localized Data Policy for IPv4 vManage</strong>.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
</tr>
<tr>
<td>IPSec Pairwise Keys</td>
<td>This feature enables support to create and install private pairwise IPSec session keys to secure communication between IPSec devices and its peers. For related information, see <strong>IPSec Pairwise Keys Overview</strong>.</td>
</tr>
<tr>
<td><strong>Network Optimization and High Availability</strong></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery for vManage</td>
<td>This feature helps you configure vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances. For detailed information, see <strong>Configure Disaster Recovery</strong>.</td>
</tr>
<tr>
<td>Share VNF Devices Across Service Chains</td>
<td>This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. For related information, see <strong>Share VNF Devices Across Service Chains</strong>.</td>
</tr>
<tr>
<td>Monitor Service Chain Health</td>
<td>This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. For related information, see <strong>Monitor Service Chain Health</strong>.</td>
</tr>
<tr>
<td>Manage PNF Devices in Service Chains</td>
<td>This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. For related information, see <strong>Manage PNF Devices in Service Chains</strong>.</td>
</tr>
</tbody>
</table>
Monitor and Analyze Cisco SD-WAN

- ACL Log, on page 5
- Alarms, on page 5
- Audit Log, on page 11
- BFD Protocol, on page 12
- Events, on page 14
- Geography, on page 15
- Network, on page 17
- vAnalytics, on page 33

**ACL Log**

Use the ACL Log screen to view logs for access lists (ACLs) configured on a vEdge router. Routers collect ACL logs every 10 minutes.

**Set ACL Log Filters**

To set filters for searching ACL logs:

1. Click the **Filter** drop-down menu.
2. In the VPN drop-down, select the entity for which you are collecting ACL logs. You can select only one VPN.
3. Click **Search** to search for logs that match the filter.

vManage NMS displays a log of activities in table format.

**Alarms**

Use the Alarms screen to display detailed information about alarms generated by controllers and routers in the overlay network.

**Set Alarm Filters**

To set filters for searching alarms generated by one or more Cisco SD-WAN devices:
1. Click the **Filter** drop-down menu.

2. In the **Severity** drop-down, select the alarm severity level. You can specify more than one severity level.

3. In the **Active** drop-down, select active, cleared, or both types of alarm. Active alarms are alarms that are currently on the device but have not been acknowledged.

4. Click the **Alarm Name** drop-down, select the name of the alarm. You can specify more than one alarm name.

5. Click **Search** to search for alarms that match the filter.

vManage NMS displays the alarms both in table and graphical format.

**Export Alarm Data in CSV Format**

To export data for all alarms to a file in CSV format, click the **Download** icon. This icon, which is a downward-pointing arrow, is located to the right of the Search box below the Alarms Histogram.

vManage NMS downloads all data from the alarms table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named Alarms.csv.

**View Alarm Details**

To view detailed information about any alarm:

1. Select the alarm row from the table.

2. Click the **More Actions** icon to the right of the row and click **Alarm Details**.

The Alarms Details window opens, displaying the possible cause of the alarm, impacted entities, and other details.

**Send Alarm Notifications**

To send email notifications when alarms occur:

1. In the **vManage Administration > Settings** screen, ensure that **Email Notifications** is enabled.

2. In the **Monitor > Alarms** screen, click **Email Notifications**. A list of configured notifications is displayed in the email notifications table.

3. Click **Add Email Notification**.

4. In the **Name** field, enter a name for the email notification. The name can be up to 128 characters and can contain only alphanumeric characters.

5. In the **Severity** drop-down, select one or more alarm severity levels, from Critical, Major, Medium, and Minor.

6. In the **Alarm Name** drop-down, select one or more alarms. The alarms generated for each severity level are listed in the section Alarms Generated on vManage NMS, below.

7. In **Account Details**, enter the email addresses to receive email notifications:
   a. Click **Add New Email List**.
   b. In the Email List pop up, click **Add Email**.
c. Enter the email address of a user.

d. Add additional email addresses as desired.

e. Click Save.

8. In the Email Threshold field, set the maximum number of emails to be sent per minute. The number can be a value from 1 through 30. The default is 5.

9. Click the Webhook box to trigger an HTTP callback when an alarm notification event occurs:
   a. Enter the username and password to authenticate the webhook server.
   b. Enter the URL of the webhook server.

10. Select the routers to which the alarm notification applies, either All Devices or a custom list. If you select Custom, a device list is displayed:
   a. In the Available Devices table on the left, select one or more devices.
   b. Click the right-point arrow to move the devices to the Selected Devices table on the right.

11. Click Add.

View an Email Notification
1. Click Email Notifications.
2. For the desired email notification, click the View icon to the right of the row.
3. When you are done viewing the notification, click OK.

Edit an Email Notification
1. Click Email Notifications.
2. For the desired email notification, click the Pencil icon to the right of the row.
3. When you are done editing the notification, click Update.

Delete an Email Notification
1. Click Email Notifications.
2. For the desired email notification, click the Trash Bin icon to the right of the row.
3. In the confirmation pop up, click OK.

Alarms Generated on vManage NMS

The table below lists the alarms that the vManage NMS software generates. The software generates alarms when a state or condition changes, such as when a software component starts, transitions from down to up, or transitions from up to down. The severity indicates the seriousness of the alarm. When you create email notifications, the severity that you configure in the notification determines which alarms you can receive email notifications about.
<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Admin Password Change</td>
<td>Critical</td>
<td>The password for the AAA user <strong>admin</strong> changed on a router or controller.</td>
</tr>
<tr>
<td>BFD Between Sites Down</td>
<td>Critical</td>
<td>All BFD sessions on all routers between two sites are in the Down state. This means that no data traffic can be sent to or transmitted between those two routers.</td>
</tr>
<tr>
<td>BFD Between Sites Up</td>
<td>Medium</td>
<td>A BFD session on a router between two sites transitioned to the Up state.</td>
</tr>
<tr>
<td>BFD Node Down</td>
<td>Critical</td>
<td>All BFD sessions for a router are in the Down state. This means that no data traffic can be sent to or transmitted from that router.</td>
</tr>
<tr>
<td>BFD Node Up</td>
<td>Medium</td>
<td>A BFD session for a router transitioned to the Up state.</td>
</tr>
<tr>
<td>BFD Site Down</td>
<td>Critical</td>
<td>All BFD sessions for all vEdge routers in a site are in the Down state. This means that no data traffic can be sent to or transmitted from that site.</td>
</tr>
<tr>
<td>BFD Site Up</td>
<td>Medium</td>
<td>A BFD session on a router in a site transitioned to the Up state.</td>
</tr>
<tr>
<td>BFD TLOC Down</td>
<td>Major</td>
<td>All BFD sessions for a TLOC (transport tunnel identified by a color) are in the Down state. This means that no data traffic can be sent to or transmitted from that transport tunnel.</td>
</tr>
<tr>
<td>BFD TLOC Up</td>
<td>Medium</td>
<td>A BFD session for a TLOC transitioned to the Up state.</td>
</tr>
<tr>
<td>BGP Router Down</td>
<td>Critical</td>
<td>All BGP sessions on a router are in the Down state.</td>
</tr>
<tr>
<td>BGP Router Up</td>
<td>Medium</td>
<td>A BGP session on a router transitioned to the Up state.</td>
</tr>
<tr>
<td>Clear Installed Certificate</td>
<td>Critical</td>
<td>All certificates on a controller or device, including the public and private keys and the root certificate, have been cleared, and the device has returned to the factory-default state.</td>
</tr>
<tr>
<td>Cloned vEdge Detected</td>
<td>Critical</td>
<td>A duplicate router that has the same chassis and serial numbers and the same system IP address has been detected.</td>
</tr>
<tr>
<td>Cloud onRamp</td>
<td>Major</td>
<td>The Cloud onRamp service was started on a router.</td>
</tr>
<tr>
<td>Control All vSmarts Down</td>
<td>Critical</td>
<td>All control connections from all vSmart controllers in the overlay network are in the Down state. This means that the overlay network cannot function.</td>
</tr>
<tr>
<td>Control Node Down</td>
<td>Critical</td>
<td>All control connections for a vEdge router are in the Down state.</td>
</tr>
<tr>
<td>Control Node Up</td>
<td>Medium</td>
<td>At least one control connection for a vEdge router transitioned to the Up State.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Severity</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Control Site Down</td>
<td>Critical</td>
<td>All control connections from all Cisco SD-WAN devices in a site are in the Down state. This means that no control or data traffic can be sent to or transmitted from that site.</td>
</tr>
<tr>
<td>Control Site Up</td>
<td>Medium</td>
<td>A control connection from the vManage NMS and the vBond orchestrator in the site transitioned to the Up state.</td>
</tr>
<tr>
<td>Control vBond State Change</td>
<td>Critical Major</td>
<td>A control connection on a vBond orchestrator transitioned to the Down state (Critical) or the Up state (Major).</td>
</tr>
<tr>
<td>Control TLOC Down</td>
<td>Major</td>
<td>All control connections for a TLOC are in the Down state.</td>
</tr>
<tr>
<td>Control TLOC Up</td>
<td>Medium</td>
<td>A control connection for a TLOC is in the Up state.</td>
</tr>
<tr>
<td>Control vManage Down</td>
<td>Critical</td>
<td>All control connections from a vManage NMS are in the Down state.</td>
</tr>
<tr>
<td>Control vManage Up</td>
<td>Medium</td>
<td>A control connection from a vManage NMS transitioned to the Up state.</td>
</tr>
<tr>
<td>Control vSmart Down</td>
<td>Critical</td>
<td>All control connections from a vSmart controller in the overlay network are in the Down state.</td>
</tr>
<tr>
<td>Control vSmart Up</td>
<td>Medium</td>
<td>A control connection from a vSmart controller in the overlay network transitioned to the Up state.</td>
</tr>
<tr>
<td>Control vSmarts Up</td>
<td>Medium</td>
<td>Control connection from all vSmart controllers in the overlay network transition to the Up state.</td>
</tr>
<tr>
<td>CPU Load</td>
<td>Critical Medium</td>
<td>The CPU load on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality.</td>
</tr>
<tr>
<td>Default App List Update</td>
<td>Major</td>
<td>The default application and application family lists, which are used in application-aware routing policy, have changed.</td>
</tr>
<tr>
<td>Device Activation Failed</td>
<td>Critical</td>
<td>Activation of a software image on a controller or device failed.</td>
</tr>
<tr>
<td>Device Upgrade Failed</td>
<td>Critical</td>
<td>The software upgrade on a router failed.</td>
</tr>
<tr>
<td>DHCP Server State Change</td>
<td>Major</td>
<td>The state of a DHCP server changed.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Critical Major</td>
<td>The disk usage load on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality.</td>
</tr>
<tr>
<td>Domain ID Change</td>
<td>Critical</td>
<td>A domain identifier in the overlay network changed.</td>
</tr>
<tr>
<td>Interface Admin State Change</td>
<td>Critical Medium</td>
<td>The administrative status of an interface in a controller or router changed from up to down (Critical) or down to up (Medium).</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Severity</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface State Change</td>
<td>Medium</td>
<td>The administrative or operational status of an interface changed.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Critical</td>
<td>The memory usage on a controller or device has reached a critical level that could impair or shut down functionality, or a medium level that could impair functionality.</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>New CSR Generated</td>
<td>Critical</td>
<td>A controller or router generated a certificate signing request (CSR).</td>
</tr>
<tr>
<td>OMP All vSmarts Down</td>
<td>Critical</td>
<td>All OMP connections from all vSmart controllers in the overlay network are in the Down state. This means that the overlay network cannot function.</td>
</tr>
<tr>
<td>OMP vSmarts Up</td>
<td></td>
<td>At least one OMP connection from all vSmart controllers in the overlay network is in the Up state.</td>
</tr>
<tr>
<td>OMP Node Down</td>
<td></td>
<td>All OMP connections for a vEdge router are in the Down state.</td>
</tr>
<tr>
<td>OMP Node Up</td>
<td>Medium</td>
<td>At least one OMP connection for a vEdge router is in the Up state.</td>
</tr>
<tr>
<td>OMP Site Down</td>
<td>Critical</td>
<td>All OMP connections to vSmart controllers from all nodes in the overlay network are in the Down state. This means that the site cannot participate in the overlay network.</td>
</tr>
<tr>
<td>OMP Site Up</td>
<td>Medium</td>
<td>At least one OMP connection to vSmart controllers from all nodes in the site is in the Up state.</td>
</tr>
<tr>
<td>OMP State Change</td>
<td>Critical</td>
<td>The administrative or operational state of an OMP session between a vSmart controller and a vEdge router has changed, from Up to Down (Critical) or Down to Up (Medium).</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>OMP vSmarts Up</td>
<td>Medium</td>
<td>OMP connection from all vSmart controllers in the overlay network transition to the Up state.</td>
</tr>
<tr>
<td>Org Name Change</td>
<td>Critical</td>
<td>The organization name used in the certificates for all overlay network devices changed.</td>
</tr>
<tr>
<td>OSPF Router Down</td>
<td>Critical</td>
<td>All OSPF connections on a router are in the Down state.</td>
</tr>
<tr>
<td>OSPF Router Up</td>
<td>Medium</td>
<td>An OSPF connection on a router transitioned to the Up state.</td>
</tr>
<tr>
<td>PIM Interface State Change</td>
<td>Major</td>
<td>The state of a PIM interface changed.</td>
</tr>
<tr>
<td>Process Restart</td>
<td>Critical</td>
<td>A process (daemon) on a controller or router restarted.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Severity</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pseudo Commit Status</td>
<td>Minor</td>
<td>The vManage NMS has started pushing a device configuration template to a controller or router. The NMS pushes a tentative configuration (called the pseudo commit) to the device and starts the rollback timer. If, with the new configuration, the control connections between the device and the vManage NMS come up, the tentative configuration becomes permanent. If the control connections do not come up, the tentative configuration is removed, and the device's configuration is rolled back to the previous configuration (that is, to the last known working).</td>
</tr>
<tr>
<td>Root Cert Chain Installed</td>
<td>Critical</td>
<td>The file containing the root certificate key chain was installed on a controller or router.</td>
</tr>
<tr>
<td>Root Cert Chain Uninstalled</td>
<td>Critical</td>
<td>The file containing the root certificate key chain was removed from a controller or router.</td>
</tr>
<tr>
<td>Site ID Change</td>
<td>Critical</td>
<td>A site identifier in the overlay network changed.</td>
</tr>
<tr>
<td>System IP Change</td>
<td>Critical</td>
<td>The system IP address on a controller or router changed.</td>
</tr>
<tr>
<td>System IP Reuse</td>
<td>Critical</td>
<td>The same system IP address is being used by more than one device in the overlay network.</td>
</tr>
<tr>
<td>System Reboot Issued</td>
<td>Critical</td>
<td>A device rebooted, either initiated by the device (Critical) or by a user (Medium).</td>
</tr>
<tr>
<td>Template Rollback</td>
<td>Critical</td>
<td>The attaching of a device configuration template to a router did not succeed in the configured rollback time, and as a result, the configuration on the device was not updated, but instead was rolled back to the previous configuration.</td>
</tr>
<tr>
<td>Unsupported SFP Detected</td>
<td>Critical</td>
<td>The software detected an unsupported transceiver in a hardware router.</td>
</tr>
<tr>
<td>vEdge Serial File Uploaded</td>
<td>Critical</td>
<td>The WAN Edge serial number file was uploaded to the vManage server.</td>
</tr>
<tr>
<td>vSmart/vManage Serial File Uploaded</td>
<td>Critical</td>
<td>A vManage NMS uploaded the file containing certificate serial numbers for the vManage NMSs and vSmart controllers in the overlay network.</td>
</tr>
<tr>
<td>ZTP Upgrade Failed</td>
<td>Critical</td>
<td>A software upgrade using ZTP failed on a controller or router.</td>
</tr>
</tbody>
</table>

**Audit Log**

Use the Audit Log screen to display a log of all activities on Cisco SD-WAN devices.
Set Audit Log Filters
To set filters for searching audit logs:

1. Click the **Filter** drop-down menu.
2. In the Module drop-down, select the entity for which you are collecting audit logs. You can select more than one entity.
3. Click **Search** to search for logs that match the filter.

vManage NMS displays a log of activities both in table and graphical format.

Export Audit Log Data in CSV Format
To export data for all audit logs to a file in CSV format, click the **Download** icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria.

vManage NMS downloads all data from the audit logs table to an Excel file in CSV format. The file is downloaded to your browser’s default download location and is named Audit_Logs.csv.

View Audit Log Details
To view detailed information about any audit log:

1. Select the audit log row from the table.
2. Click the **More Actions** icon to the right of the row and click **Audit Log Details**.

The Audit Log Details pop up window opens, displaying details of the audit log.

View Changes to a Configuration Template
When you push a template configuration to a device, you can view changes between the old and the new configuration template. To view changes made to a configuration template:

1. Select the audit log row from the table. The Message column of the audit log row will contain a message to the effect that the template is successfully attached to the device.
2. Click the **More Actions** icon to the right of the row and click **CLI Diff**.

The CLI Diff pop up window opens, with the Config Diff tab selected by default. This window displays a side-by-side view of the differences between the configuration that was on the device and the changes made to the configuration. To view the changes inline, click the **Inline Diff** button located to the right of the window.

To view the updated configuration on the device, click the **Configuration** tab located to the left of the window.

BFD Protocol

The Role of BFD in Cisco SD-WAN Solution
The BFD protocol detects links failures between routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.
For data plane resiliency, the Cisco SD-WAN software implements the BFD protocol, which runs automatically on the secure IPsec and GRE connections between routers. These connections are used for the data plane, and for data traffic, and are independent of the DTLS tunnels used by the control plane.

BFD is enabled by default on all connections between Cisco vEdge devices. You cannot disable BFD. However, you can adjust the Hello packet and dead time intervals. If the timers on the two ends of a BFD link are different, BFD negotiates to use the lower value. See Configure BFD using vManage for information on configuring BFD for application-aware routing and configuring BFD on transport tunnels.

**How BFD Works**

After a Cisco vEdge device comes up and control connections are established, the Cisco vSmart Controller advertises peer TLOC information to the Cisco vEdge device. Based on this TLOC information and other configuration, Cisco vEdge devices establish BFD sessions with all or some of the peer TLOCs.

BFD sends Hello packets periodically (by default, every 1 second) to determine whether the session is still operational. If a certain number of the Hello packets are not received, BFD considers that the link has failed and brings the BFD session down (the default multiplier time is 7 seconds). When BFD sessions goes down, any route that points to a next hop over that IPsec tunnel is removed from the forwarding table (FIB), but it is still present in the route table (RIB).

**Interpret BFD States to Troubleshoot Connection Loss Between TLOCs**

If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the `show bfd sessions` or the `show bfd history` commands to check the status of your BFD sessions. These commands help you understand whether all the BFD sessions that should have been established, have indeed been established.

BFD sessions have three valid states: Down, Init, and Up.

- **Down**: Non-operational connections with other Cisco vEdge devices in the network.
- **Init**: Connections that are reachable but not up yet.
- **Up**: Operational connections with other Cisco vEdge devices in the network.

Each device sends an echo-request to its peer and also an echo-response for the request it receives. In the echo response, the device sends its current BFD state. Based on this, the peer changes its BFD state if required.

For information on BFD alarms generated by vManage, see the Alarms topic in the Monitor and Maintain Guide.

**Changes in Session States Based on Echo Response from Peers**

The following table shows how the BFD session states on a device change based on the session states that the peer responds with.

<table>
<thead>
<tr>
<th>BFD Session State on Device</th>
<th>BFD State sent by Peer in Echo Response</th>
<th>BFD Status Change on Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Up or Init</td>
<td>Up (no change)</td>
</tr>
<tr>
<td>Up</td>
<td>Down</td>
<td>Down</td>
</tr>
<tr>
<td>Init</td>
<td>Up or Init</td>
<td>Up</td>
</tr>
<tr>
<td>Init</td>
<td>Down</td>
<td>Init (no change)</td>
</tr>
</tbody>
</table>

Monitor and Analyze Cisco SD-WAN BFD Protocol
Events

Use the Events screen to display detailed information on events generated by Cisco SD-WAN devices.

**Set Event Filters**

To set filters for searching events generated on one or more Cisco SD-WAN devices:

1. Click the **Filter** drop-down menu.

2. In the **Severity** drop-down, select the event severity level. Events generated by Cisco SD-WAN devices are collected by vManage NMS and classified as:
   - Critical—indicates that action needs to be taken immediately.
   - Major—indicates that the problem needs to be looked into but is not critical enough to bring down the network.
   - Minor—is informational only.

You can specify more than one severity level.

1. In the **Component** drop-down, select the configuration component that caused the event. You can select more than one configuration component.

2. In the **System IP** drop-down, select the system IP of the devices for which to view generated events.

3. In the **Event Name** drop-down, select the event name for which to view generated events. You can select more than one event name.

4. Click **Search** to search events that match the filter.

vManage NMS displays the events both in table and graphical format.

**Export Event Data in CSV Format**

To export data for all events to a file in CSV format, click the **Download** icon. This icon, which is a downward-pointing arrow, is located to the right of the Search box below the Events Histogram.

vManage NMS downloads all data from the events table to an Excel file in CSV format. The file is downloaded to your browser’s default download location and is named Events.csv.

**View Device Details**

To view detailed information about a device on which an event was generated:

1. Select the event row from the table.

2. Click the **More Actions** icon to the right of the row and click **Device Details**.
The Device Details pop up window opens, displaying the hostname of the device originating the event and other details.

**Geography**

Use the Geography screen to view information about the Cisco SD-WAN devices and links in the overlay network. The Geography screen provides a map displaying the geographic location of the Cisco SD-WAN devices.

Note: The browser on which you are running vManage NMS must have Internet access. If you do not have Internet access, ensure that the browser has access to "*.openstreetmaps.org."

**Set Map Filters**

To select the devices and links you want to display on the map:

1. Click the **Filter** button to display a pull-down menu.
2. Select the device group from the pull-down menu which includes all configured device groups. By default, the group "All" is selected and displays all Cisco SD-WAN devices in the overlay network. The group "No Groups" includes the devices that are not part of a device group. If all devices are in a group, the "No Groups" group is not displayed.
3. Select the Cisco SD-WAN devices to display on the map. By default, the map displays all device types including vEdge, vEdge-vBond, vSmart, and vManage.
4. Select the state of control and data links. By default, the map displays all control and data connections.
5. Close the Filter box by moving the cursor outside the box.

The map is dynamically updated to reflect your selections. Also, as you make the device group, device type, and link selections, the tabs next to the Filter button are updated.

**View Device Information**

To display basic information for a device, hover over the device icon. A hover box displays the system IP, hostname, site ID, device type, and device status.

To display detailed information for a device, double-click the device icon to open the View More Details hover box. Click **Device Dashboard**, **Device Details**, **SSH Terminal**, or **Links** to get further details for the device.

**View Link Information**

By default, control and data connections are not displayed on the map. To see control and data connections for a device:

1. Double-click the device icon to open a hover box with details about the device.
2. Click **Links**.

Note the following:

- An active control connection between two devices is displayed on the map as a thin blue line. Multiple active connections between devices are displayed by a bold blue line. A control connection that is down
is displayed on the map as a dotted red line. Multiple control connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.

• An active data connection between two devices is displayed on the map as a thin green line. Multiple active data connections are displayed by a bold green line. A data connection that is down is displayed on the map as a dotted red line. Multiple data connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.

• An active consolidated control and data connection between two devices is displayed on the map as a thick grey line.

Configure Geographic Coordinates for a Device

To configure the geographic coordinates for a device, use the Configuration > Templates > System feature template.

If the Cisco SD-WAN device is not attached to a configuration template, you can configure the latitude and longitude directly on the device:

1. Select the Tools > SSH Terminal screen.
2. Select the device from the left pane. The SSH Terminal screen opens in the right pane.
3. Enter the username and password to log in to the device.
4. Determine whether the device is attached to a configuration template:

   Device# show system status

   Check the values in the vManaged and Configuration template output fields. For example:

   ...
   Personality: vedge
   Model name: vedge-cloud
   Services: None
   vManaged: false
   Commit pending: false
   Configuration template: None

   If the vManaged field is false, the device is not attached to a configuration template, and the Configuration template field says None. For such a device, you can configure the GPS coordinates directly from the CLI. If the vManaged field is true, the device's configuration has been downloaded by the vManage server, and the Configuration template field shows the name of the configuration template. For such a device, you cannot configure the GPS coordinates directly from the CLI. If you attempt to do so, the validate or commit command fails, with the following message:

   Aborted: 'system is-vmanaged': This device is being managed by the vManage. Configuration through the CLI is not allowed.

5. Enter configuration mode:

   Device# config
   Device(config) #

6. Configure the latitude and longitude on the device:

   Device(config)# system gps-location latitude degrees.minutes.seconds
   Device(config-system)# gps-location longitude degrees.minutes.seconds
7. Save the configuration:

```
Device(config-system)# commit
Device(config-system)#
```

## Network

Use the Network screen to display a list of Cisco SD-WAN devices in the overlay network and to display detailed information about individual devices.

### View List of Devices

The Network screen lists the Cisco SD-WAN devices in the overlay network. When you first come to the Network screen, the device group "All" is selected, and the screen shows status information for all Cisco SD-WAN devices in the overlay network.

To see a list of devices in a particular group, select that device group.

To filter the devices by reachability, hostname, system IP address, site ID, and device model, select from the sort options in the drop-down or type a string in the Search box.

To display information about an individual device, click its hostname.

### Export Device Data in CSV Format

To export data for all devices to a file in CSV format, click the Download button. This button is located to the right of the filter criteria.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your browser’s default download location and is named viptela_download.csv.

### View Information about a Device

To view high-level information about a device, select the device from the Monitor > Network screen:

1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.

2. Select the device by clicking its hostname. The left pane lists the information categories about the device. In the right pane, the System Status category is selected, which displays status information about the device.

To select a different device, either click the Select Device drop-down located at the top of the left pane, or click Network in the title bar and then select a device by clicking its hostname.

After you select a device by clicking its hostname, the screen changes and displays the elements.

### View Device Status Summary

To view summary status information about a device:

1. From the Monitor > Network screen, select a device.

2. From the Select Device bar, click the More Info drop-down located to the right of the bar. vManage NMS opens a drop box with summary information about the device.
To close the device status summary, click More Info again or click anywhere on the screen outside the drop-down.

**View DPI Flows**

To view DPI flow information on a vEdge router:

1. From the Monitor > Network screen, select a device.
2. Click Applications in the left pane. The right pane displays DPI flow information for the device.

The upper part of the right pane contains:

- Filter bar—Located directly under the device name, this bar includes the Filter icon and time periods. Click the Filter icon to display a drop-down menu to select the desired VPN and TLOC. Click a predefined or custom time period for which to display data.
- DPI flow information in graphical format.
- DPI flow graph legend—Select an application family to display information for just that flow. Click the Total Network Traffic check box to display flow information as a proportion of total network traffic.

The lower part of the right pane contains:

- Filter criteria.
- DPI flow information table that lists all application families sorted by usage. By default, the top six application families are selected. The graphical display in the upper part of the right pane plots the flow and usage of the selected application families.
  - Click the check box to the left to select and deselect application families. You can select and display information for a maximum of six application families at one time.
  - Click an application family to display applications within the family.
  - Click an application to display the source IP addresses of the devices accessing the application. The Traffic per TLOC pie chart next to the graph displays traffic distribution per TLOC (color).
  - To re-arrange the columns, drag the column title to the desired position.
  - To return to the list of application families, click Applications in the title bar or click the Back button in the browser.

**View VNF Status**

To view performance specifications, required resources for each VNF, and component network functions for each VNF. Reviewing this information can help you to determine which VNF to use when you are designing a network service.

1. In vManage, click Monitor > Network.
   The right pane displays 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.
2. Click a CSP device from the table.
3. From the left pane, click VNF Status.
4. In the table, click the VNF name. The right pane displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, disk utilization to monitor the resources utilization of a VNF.

The primary part of the right pane contains:

- Chart Options bar that includes the following options:
  - Chart Options drop-down—Click **Chart Options** 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.
  - VNF information in graphical format.
  - VNF graph legend—Select a VNF to display information for just that VNF.

The detail part of the right pane contains:

- Filter criteria
- VNF table that lists information about all VNFs. By default, the first six VNFs are selected. The graphical display in the upper part of the right pane plots information for the selected VNFs.
  - Check or uncheck the check box at the left to select and deselect VNFs. You can select and display information for a maximum of six VNFs at one time.
  - To change the sort order of a column, click the column title.

**View Interfaces**

To view information about interfaces on a device:

1. From the **Monitor > Network** screen, select a device.

2. Click **Interface** in the left pane. The right pane displays interface information for the device.

The upper part of the right pane contains:

- Chart Options bar—Located directly under the device name, this bar includes:
  - Chart Options drop-down—Click **Chart Options** to select the type of data to display.
  - IPv4 & IPv6 drop-down—Click **IPv4 & IPv6** to select the type of interfaces to display. The information is displayed in graphical format. By default, the graph is Combined, showing interfaces on which both IPv4 and IPv6 addresses are configured. To display IPv4 and IPv6 interfaces in separate graphs, select the Separated toggle button.
  - Time periods—Click either **Real Time**, a predefined time period, or a custom time period for which to display data.
  - Interface information in graphical format.
  - Interface graph legend—Select an interface to display information for just that interface.

The lower part of the right pane contains:
• Filter criteria.
• Interface table that lists information about all interfaces. By default, the first six interfaces are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  • Click the check box to the left to select and deselect interfaces. You can select and display information for a maximum of 30 interfaces at one time.
  • To re-arrange the columns, drag the column title to the desired position.
  • For cellular interfaces, click the interface name to display a screen that shows detailed information about the cellular interface.

View QoS Information
1. From the Monitor > Network screen, select a device.
2. Click QoS in the left pane. The following details display:
  • Options bar—Located directly under the device name, this bar includes:
    • Interface Name—Select the interface for which to display data.
    • Time periods—Real Time, a predefined time period, or a custom time period.
    • Chart Options—Post Policy Rate lets you display post policy rate data in Kbps (default) or Pps. Post Policy Counter lets you display post policy counter data in bytes (default) or for packets.
  • QoS information in graphical format.
  • Legend—Select a queue for which to display information.
  • Queue table that displays QoS information for each queue and aggregate information for all queues. To re-arrange the columns, drag the column title to the desired position.

View TCP Optimization Information
If TCP optimization is enabled on a router, you can view information about how the optimization is affecting the processing and throughput of TCP data traffic on the router:
1. From the Monitor > Network screen, select a vEdge router.
2. Click TCP Optimization–WAN Throughput in the left page. The right pane displays the WAN throughput, in megabits per second.

The upper part of the right pane contains the following elements:
• Chart Options bar—Located directly under the device name, this bar includes the Filter Options drop-down and time periods. Click Filter to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
• Average optimized throughput information in graphical format.
• WAN graph legend—Identifies non-optimized and TCP optimized packet throughput.
The lower part of the right pane shows the hourly average throughput and the total optimized throughput, both in megabits per second.

Click **TCP Optimization–Flows** in the left pane to display information about TCP-optimized traffic flows. The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Filter drop-down and time periods. Click **Filter** to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.

- Average optimized throughput information in graphical format.

- Flows graph legend—Identifies traffic flows.

The lower part of the right pane contains the following elements:

- Set perspective—Select the flow direction.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.

- Flow table that lists the flow destination, usage, and percentage of total traffic for all TCP-optimized flows. By default, the first six flows are selected. Click the check box to the left to select and deselect flows to display. The graphical display in the upper part of the right pane plots information for the selected flows.

Click **TCP Optimization–Connections** in the left pane to display status information about all the tunnels over which the most TCP-optimized traffic is flowing. The upper part of the right pane contains the following elements:

- TCP Optimization Connections in graphical format.

- Connection State boxes—Select the connection state or states to display TCP optimization information about.

The lower part of the right pane contains the following elements:

- Filter criteria.

- Flow table that lists information about each of the tunnels, including the tunnel's connection state.

**View TLOC Loss, Latency, and Jitter Information**

To view information about TLOC loss, latency, and jitter:

1. From the **Monitor > Network** screen, select a device.

2. Click **WAN–TLOC** in the left pane. The right pane displays the aggregated average loss or latency/jitter information for all TLOC colors.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.

- TLOC information in graphical format. The time interval in the graph is determined by the value of the BFD application-aware routing poll interval.
• TLOC graph legend—Select a TLOC color to display information for just that TLOC.

The lower part of the right pane contains the following elements:

• Search box—Includes the Search Options drop-down, for a Contains or Match.

• TLOC color table that lists average jitter, loss, and latency data about all TLOCs. By default, the first six colors are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  • Click the check box to the left to select and deselect TLOC colors. You can select and display information for a maximum of 30 TLOCs at one time.
  • Click Application Usage to the right to display DPI flow information for that TLOC.

View Tunnel Connections

To view all tunnel connections for a device:

1. From the Monitor > Network screen, select a device.

2. Click WAN–Tunnel in the left pane. The right pane displays information about all tunnel connections.

The upper part of the right pane contains the following elements:

• Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.

• Tunnel information in graphical format.

• Tunnel graph legend—Select a tunnel to display information for just that tunnel.

The lower part of the right pane contains the following elements:

• Search box—Includes the Search Options drop-down, for a Contains or Match.

• Tunnel table that lists average latency, loss, and jitter data about all tunnel end points. By default, the first six tunnels are selected. The graphical display in the upper part of the right pane plots information for the selected tunnels.
  • Click the arrow to the left to view the tunnel end points for that TLOC color.
  • Click the check box to the left to select and deselect tunnels. You can select and display information for a maximum of 30 tunnels at one time.
  • Click Application Usage to the right to display DPI flow information for that TLOC.

View WiFi Configuration

To view WiFi configuration for Cisco SD-WAN routers that support wireless LANs (WLANs), such as the vEdge 100wm routers:

1. From the Monitor > Network screen, select a device.

2. Click WiFi in the left pane. The right pane displays information about WiFi configuration on the router.
The upper part of the right pane contains the following elements:

- AP Information bar—Located directly under the device name, it displays access point information and the Clients Details button. Click the Clients Details button to view information about clients connected to the WiFi access point during the selected time period.
- Radio frequency parameters for access points.
- SSID parameters for virtual access points (VAPs).

The lower part of the right pane contains the following elements:

- VAP receive and transmit statistics bar—Includes the time periods. Click a predefined or custom time period for which to display data.
- VAP receive and transmit statistics information in graphical format.
- VAP statistics graph legend—Select a VAP interface to display information for just that interface. Click the VAP interface again to return to the previous display.

**View Client Details**

To view details of clients connected to the WiFi access point, click the **Clients Details** button on the WiFi screen.

The upper part of the Clients Info right pane contains the following elements:

- Clients Details title bar—Includes the Clients Usage tab.
- Time periods—Click a predefined or custom time period for which to display data.
- Information of clients connected to the WiFi access point in graphical format. Select a column to display information for just those clients in tabular format in the lower part of the screen.

The lower part of the Clients Info right pane contains the following elements:

- Filter criteria.
- Table of clients connected to the WiFi access point.

**View Client Usage**

To view data usage details of all clients connected to the WiFi access point, click the **Clients Usage** tab.

The upper part of the Clients Usage right pane contains the following elements:

- Time periods—Click a predefined or custom time period for which to display data.
- Data usage of all clients connected to the WiFi access point in graphical format.
- Data usage information graph legend—Select a client MAC address to display information for just that client.

The lower part of the Clients Usage right pane contains the following elements:

- Filter criteria.
- Data usage information table. By default, the first six clients are selected.
View Control Connections

To view all control connections for a device:

1. From the **Monitor > Network** screen, select a device. If you select a controller device—a vBond orchestrator, a vManage NMS, or a Smart controller—the Control Connections screen opens by default.

2. If you select a vEdge router, click Control Connections in the left pane. The right pane displays information about all control connections that the device has with other controller devices in the network.

The upper part of the right pane contains the following elements:

- Expected and actual number of connections.
- Control connection data in graphical format. If the device has multiple interfaces, vManage NMS displays a graphical topology of all control connections for each color.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- Control connections data in tabular format. By default, the first six control connections are selected. The graphical display in the upper part of the right pane plots information for the selected control connections.
  - Click the arrow to the left to view the control connections for that TLOC color.
  - Click the check box to the left to select and deselect control connections. You can select and display information for a maximum of six control connections at one time.

View System Status

To view system status about a device:

1. From the **Monitor > Network** screen, select a device. When you select a vEdge router, the System Status screen opens by default.

2. Click **System Status** in the left pane. The right pane displays information about the device.

The right pane contains the following elements:

- Reboot—Number of times the device has rebooted. For details about each reboot, click **Reboot**. The Reboot screen opens and contains the following elements:
  - Search box—Includes the Search Options drop-down, for a Contains or Match.
  - Table listing all the reboots on the device along with the time and reason for the reboot. If the device is down for 90 seconds or longer, the reason shows as "Unknown". The Last Updated column displays the time when the vManage NMS retrieved the reboot data from the device.

- Crash—Number of times the device has crashed. For details about each crash, click **Crash**. The Crash screen opens and contains the following elements:
  - Search box—Includes the Search Options drop-down, for a Contains or Match.
  - Table listing all the crashes on the device along with the time of crash and name of the core file created as a result of the crash.
• Status of hardware components, applicable only if the selected device is a hardware vEdge router:
  • Module
  • Temperature sensors
  • USB
  • Power supply
  • Fans

The status of a hardware component is represented in one of the following ways:
  • Green check mark—Component is operational.
  • Red circle with an X—Component is down.
  • Orange triangle with an exclamation point—Component has an error.
  • N/A—Not applicable since the selected device is not a hardware vEdge router.
  • CPU & Memory—To the right are the time periods. Click a predefined or custom time period for which
to display data.
    • CPU usage—Displays the CPU usage, as a percentage of available CPU, over the selected time
      range.
    • Memory usage—Displays the memory usage, as a percentage of available memory, over the selected
      time period.

View Cisco Colo Manager Health

To view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state.

1. In vManage, click Monitor > Network.

   The right pane displays 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.

2. Click a CSP device from the table.

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 colo manager.

**View Events**

To view the number of critical, major, or minor events on a device:

1. From the Monitor > Network screen, select a device.

2. Click Events in the left pane. The right pane displays information about all events on the device.

The upper part of the right pane contains the following elements:

- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching events by severity, component, and event name. Click a predefined or custom time period for which to display data.

- Events Histogram—Displays a graphical representation of all events. To hide the events histogram, click the Events Histogram title or the down angle bracket to the right of it.

The lower part of the right pane has the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.

- Events table.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

**View ACL Logs**

To view logs for access lists (ACLs) configured on a vEdge router:

1. From the Monitor > Network screen, select a vEdge router.

2. Click ACL Logs in the left pane. The right pane displays information about all localized data policy (ACL) logs on the router. You configure these logs by including the log action in an ACL.

The upper part of the right pane contains the following elements:

- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching logs by VPN. Click a predefined or custom time period for which to display data.

- Search box—Includes the Search Options drop-down, for a Contains or Match.

The lower part of the right pane contains the following elements:

- Logs table.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.
Troubleshoot a Device

You can troubleshoot connectivity or traffic health for all devices in the overlay network.

Check Device Connectivity

To troubleshoot connectivity for a device in the network, you can do the following:

• Check device bringup
• Ping the device
• Run a speed test
• Run a traceroute
• View control connections in real time

Check Device Bringup

To verify the status of a device bringup (available on vEdge routers only):

1. From the Monitor > Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Device Bringup.

The Device Bringup screen opens and displays:

• Troubleshooting drop-down—Located to the right of the Select Device drop-down. Click an option to view troubleshooting information. To close the drop-down, click the Troubleshooting button again.

• Device bringup state—Indicated by one of the following states:
  • Green check mark—Indicates that the device has successfully established control-plane connections with the controller devices in the network and is up and running.
  • Gray check mark—Indicates that ZTP was disabled in the Administration > Settings screen when the device initially came up. You will see this state for the Software Image Update box only.
  • Red check mark—Indicates that the device failed to establish control-plane connections with the controller devices in the network and is not up and running.
  • Yellow exclamation point—Indicates that vManage NMS could not find the reason for a failure on the device.

Ping a Device

To verify that a device is reachable on the network, ping the device to send ICMP ECHO_REQUEST packets to it:

1. From the Monitor > Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Ping.
4. In the Destination IP field, enter the IP address of the device to ping.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send the ping packets.
7. In the Probes field, select the protocol type to use to send the ping packets.
8. In the Source Port field, enter the number of the source port.
9. In the Destination Port field, enter the number of the destination port.
10. In the Type of Service field, enter the value for the type of service (ToS) field to include in the ping packets.
11. In the Time to Live field, enter the round-trip time for sending this ping packet and receiving a response, in milliseconds.
12. Click the Don’t Fragment slider to set the Don’t Fragment bit in the ping packets.
13. Click Advanced Options to specify additional parameters:
   a. In the Count field, enter the number of ping requests to send. The range is 1 through 30. The default is 5.
   b. In the Payload Size field, enter the size of the packet to send. The default is 64 bytes, which comprises 56 bytes of data and 8 bytes of ICMP header. The range for data is 56 through 65507 bytes.
   c. Click the Rapid slider to send 5 ping requests in rapid succession and to display statistics only for packets transmitted and received, and the percentage of packets lost.
14. Click Ping.

Run a Speed Test
To check the actual bandwidth of a circuit from one device to another:
1. In the Administration > Settings screen, ensure that Data Stream is enabled.
2. From the Monitor > Network screen, select the device.
3. Click Troubleshooting in the left pane.
4. From the Connectivity pane, click Speed Test.
5. In the Source Circuit drop-down, select the color of tunnel interface on the local device.
6. In the Destination Device drop-down, select the remote device by the device's name and system IP address.
7. In the Destination Circuit drop-down, select the color of the tunnel interface on the remote device.
8. Click Start Test. The speed test sends a single packet from the source to the destination and receives the acknowledgment from the destination.

The middle part of the right pane reports the results of the speed test. The clock reports the circuit's speed based on the round-trip time. The download speed shows the speed from the source to the destination, and the upload speed shows the speed from the destination to the source, both in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.
When a speed test completes, the test results are added to the table at the lower part of the right pane.

**Run a Traceroute**

To display the path that packets take to reach a host or IP address on the network:

1. From the **Monitor > Network** screen, select the device.
2. Click **Troubleshooting** in the left pane.
3. From the Connectivity pane, click **Trace Route**.
4. In the Destination IP field, enter the IP address of a device on the network.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send traceroute probe packets.
7. Click **Advanced Options**.
8. In the Size field, enter the size of the traceroute probe packets, in bytes.
9. Click **Start** to trigger a traceroute to the requested destination.

The lower part of the right pane displays:

- Output—Raw output of the path the traceroute probe packets take to reach the destination.
- Graphical depiction of the path the traceroute probe packets take to reach the destination.

**View Control Connections in Real Time**

To display a real-time view the control plane connections on a vEdge router:

1. From the **Monitor > Network** screen, select the device. The device must be a vEdge router.
2. Click **Troubleshooting** in the left pane.
3. From the Connectivity pane, click **Control Connections**.

The control plane connection screen is updated automatically, every 15 seconds.

The upper part of the right pane shows figures illustrates the operational control plane tunnels between the vEdge router and vManage and vSmart controllers.

The lower part of the lower pane contains a table that shows details for each of the control plane tunnels, including the remote device's IP address and the status of the tunnel end points, including the reason for the failure of an end point.

**Check Traffic Health**

To check traffic health for a vEdge router in the network:

- View tunnel health
- View traffic path information
- Packet capture
- Simulate flows
**View Tunnel Health**

To view the health of a tunnel from both directions (available on vEdge routers only):

1. From the **Monitor > Network** screen, select the device.
2. Click **Troubleshooting** in the left pane.
3. From the Traffic pane, click **Tunnel Health**.
4. From the Local TLOC drop-down, select a source TLOC.
5. From the Remote Device drop-down, select a remote device.
6. From the Remote TLOC drop-down, select a destination TLOC.
7. Click **Go**. The lower part of the screen displays:
   - Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
   - App-route data (either loss, latency, or jitter) in graphical format for all tunnels between the two devices in each direction.
   - App-route graph legend—Identifies selected tunnels from both directions.

Select a TLOC to display information for just that TLOC.

**Check Application-Aware Routing Traffic**

To check application-aware routing traffic from the source device to the destination device (available on vEdge routers only):

1. From the **Monitor > Network** screen, select the device.
2. Click **Troubleshooting** in the left pane.
3. From the Traffic pane, click **App Route Visualization**.
4. From the Remote Device drop-down, select a destination device.
5. Click **Go**. The lower part of the screen displays:
   - Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
   - Application-aware routing data (either loss, latency, or jitter), along with octets, in graphical format for all tunnels between the two devices.
   - Application-aware routing graph legend—Identifies source and destination TLOC.

**Capture Packets**

To capture control plane and data plane packets in real time, similar to a UNIX tcpdump operation, and to save these packets to a file (available on vEdge routers only):

1. From the **Monitor > Network** screen, select the device.
2. Click **Troubleshooting** in the left pane.

3. From the Traffic pane, click **App Packet Capture**.

4. From the VPN drop-down, select the VPN in which to capture packets.

5. From the Interface drop-down, select the interface over which to capture packets.

6. Optionally, click **Traffic Filter** to filter the packets to capture based on values in their IP headers. Enter values for one or more of these fields:
   a. In Source IP, enter the packets' source IP address.
   b. In Source Port, enter the packets' source port number.
   c. In Protocol, enter the packets' protocol number.
   d. In Destination IP, enter the packets' destination IP address.
   e. In Destination Port, enter the packets' destination port number.

7. Click **Start**. The packet capture begins, and displays its progress:
   a. Packet Capture in Progress—Packet capture stops after 5 minutes, after the file of collected packets reaches 5 MB, or when you click the Stop button.
   b. Preparing file to download—vManage NMS creates a file in libpcap format (a .pcap file).
   c. File ready, click to download the file—Click the download icon to download the generated file.

**Simulate Flows**

To display the next-hop information for an IP packet (available on vEdge routers only):

1. From the **Monitor** > **Network** screen, select the vEdge router.

2. Click **Troubleshooting** in the left pane.

3. From the Traffic pane, click **Simulate Flows**.

4. To specify the data traffic path, select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are: • VPN—VPN in which the data tunnel is located. • Source Interface—Interface from which the cflowd flow originates. • Source IP—IP address from which the cflowd flow originates. • Destination IP—Destination IP address of the cflowd flow. • Protocol (under Advanced Options)—Number of the protocol being used to transmit the cflowd flow. The optional fields are: • Application—Application running on the router. • Source Port (under Advanced Options)—Port from which the cflowd flow originates. • Destination Port (under Advanced Options)—Destination port of the cflowd flow. • DSCP (under Advanced Options)—DSCP value in the cflowd packets.

5. Click **Advanced Options**:
   a. In the Path toggle field, select whether the data traffic path information comes from the service side of the router or from the tunnel side.
   b. Select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are: • Protocol—Number of the protocol being used to transmit the cflowd flow. The optional fields are: • Source Port—Port from which the cflowd flow originates. • Destination Port—Destination port of the cflowd flow. • DSCP—DSCP value in the cflowd packets.
Check the All Paths check box to display all possible paths for a packet.

6. Click Simulate to determine the next hop that a packet with the specified headers would take.

Check Device Syslog Files
To display the contents of a device's syslog files:
1. In the Administration > Settings screen, ensure that Data Stream is enabled.
2. From the Monitor > Network screen, select the vEdge router.
3. Click Troubleshooting in the left pane.
4. From the Logs pane, click Debug Log.
5. In the Log Files field, select the name of the log file. The lower part of the screen displays the log information.

View Real-Time Data
To view real-time data for a device:
1. From the Monitor > Network screen, select a device.
2. Click Real Time. The right pane displays system information about the device.

The right pane contains the following elements:

• Device Options—Located directly under the device name, this drop-down allows you to select a feature-specific operational command to display real-time device information for the selected command. The commands in the drop-down are listed alphabetically. The commands available vary depending on the device selected. When you first select Real Time, the System Information command is selected, and real-time system information about the device is displayed in tabular format. For some commands, you can add filters to speed up the display of information. When you select these commands from the drop-down, the Select Filter window is displayed prompting you to either Show Filters or Do Not Filter.
  • Show Filters—Displays the available filters. Fill in the desired fields and click Search to display real-time device information corresponding just to those fields. Clicking Search without filling any of the fields displays the entire information for the selected command.
  • Do Not Filter—Displays the entire real-time device information for the selected command.

• Filter criteria.

• Table with real-time information for the selected command.

• To re-arrange the columns, drag the column title to the desired position.

• To change the sort order in a column, click the Up or Down arrow in the column title.

View Colocation Cluster Information
To view the cluster information and their health states. Reviewing this information can help you to determine which CSP device is responsible for hosting each VNF in a service chain.
1. In vManage, click **Monitor > Network**.

2. To monitor clusters, click the **Colocation Clusters** tab.

All clusters with relevant information are displayed in a tabular format. Click a cluster name.

From the primary part of the left pane, you can view the cluster topology. 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 Cloud OnRamp for Colocation size.

The detail part of the left pane contains:

- Filter criteria—select the fields to be displayed from the search options drop-down.
- A table that lists information about all devices in the cluster (CSP devices and switches).

Click a CSP cluster. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, and other core parameters that define performance of a network service.

3. Click the **Services** tab.

In this tab, you can view:

- All service groups that are attached to the cluster in a tabular format. The first two columns display the name and description of the service chain within the service group.
- Click the **Diagram** button and view the service group with all its 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.
- Select a service group from the **Service Groups** drop-down. The design view displays the selected service group with all its service chains and VNFs.

---

### vAnalytics

#### Overview of vAnalytics

Cisco vAnalytics is a cloud-based service that offers insights into the performance of applications and the underlying SD-WAN network infrastructure. It offers the following details over an extended period of time:

- **Network performance**
  - Uptime (or availability) of your devices and WAN circuits
  - Key performance parameters of your data tunnels—latency, loss, and jitter

- **Application performance**
  - Top applications and their bandwidth usage
  - Quality of Experience (QoE) for your applications
By default, the vAnalytics dashboard displays data for the past day. You can drill further to view data for the past week, past month, or custom time period of up to one year.

From the dashboard, you can navigate to individual screens and see more data by either clicking the **Network** tab or the **Applications** tabs on the top menu bar, or by clicking on individual screen elements directly.

---

**Enable vAnalytics**

Open a support case with Cisco, [https://mycase.cloudapps.cisco.com/case](https://mycase.cloudapps.cisco.com/case), and provide the following information:

- Customer name
- Organization Name (as configured in Cisco vManage)
- Cisco Sales or SE contact
- Subscription or license type
- Approved by (customer contact)
- Customer email
- Approved by customer on (specify date)

Customer approval is needed, as vAnalytics collects network and application flows related metadata, and this data is stored in the US-West region in the Amazon Web Services cloud.

After receiving this information, Cisco takes approximately 24 to 48 hours to ready the backend set up and provide the appropriate log-on credentials for vAnalytics.

After you receive log-on credentials for vAnalytics, navigate to the Cisco vManage dashboard, click on the **Administration Settings** tab, and then enable vAnalytics.

After vAnalytics is enabled, you can launch vAnalytics directly from the Cisco vManage console.

---

**Note**

In case you have an on-premises Cisco vManage installation, then ensure that your firewall allows for communication from your Cisco vManage (interface VPN 0) to Cisco’s data collection server `us-west.des.viptela.net` on port 443. You can use the `cURL -k` command from your Cisco vManage CLI to verify reachability to this server. You may also need to disable IP tables in Cisco vManage (`Configuration > System > no iptables-enable`).

---

**vAnalytics Dashboard**

The vAnalytics dashboard offers a quick summary of network and application performance.

The top left corner of the dashboard displays a menu icon for expanding and collapsing the vAnalytics menu options, and the vAnalytics product name. The top right corner displays the number of icons and the user profile drop-down.

**Network Pane**

The Network pane displays performance of various network elements.
• Network Availability—The Network Availability pane displays network-wide availability of all devices and circuits in the last 24 hours. Each box displays uptime as a percentage and total downtime in minutes.

Click in the Device box or the Circuit box to navigate to the Display Network Availability screen.

• Tunnel Performance—The Tunnel Performance box displays the performance of the top ten worst performing tunnels for the last 24 hours.

Click on the individual tunnel bar to navigate to the Display Latency, Loss, or Jitter screen.

• Carrier Performance—The Carrier Performance box displays loss, latency, or jitter performance of all the tunnels terminating on that location on a geographical map.

Navigate to the Display Performance By Carrier screen for more information.

Applications Pane

The Applications pane displays the top ten applications by bandwidth consumption, and by best or worst performing QoE score. It also lists top anomalies in application behavior.

• Best or Least Performing Applications—vAnalytics computes a Quality of Experience (QoE) score to assess end-user experiences with various applications. This score ranges from zero to ten, with zero being the worst performance, and ten being the best. The QoE score combines scores for latency, loss, and jitter, customizing the calculation for the needs of each application.

• Top Ten Applications By Bandwidth—The Applications Consuming Most Bandwidth box displays the top ten applications consuming the most bandwidth in the network.

Hover over a data bar in the graph to open a hover box with details about that application.

Click on the data bar to navigate to the Display Bandwidth Utilization screen.

• Top Anomalous Sites—The Anomalous Sites box displays application families using more bandwidth than their baseline.

Hover over a bar in the graph to display a hover box with details about that application family.

Click to navigate to the Anomaly screen.

Monitor Network Performance

Use the Network screens to monitor the health of data tunnels and the availability of network devices and circuits.

Screen Elements

• Title bar—Includes the title of the screen.

• Health—Displays latency, loss, and jitter performance.

• Availability—Displays downtime information for the Cisco SD-WAN edge devices and circuits.
Display Network Availability

To display downtime for Cisco SD-WAN edge devices and circuit at each site:
1. Select an edge device or circuit view to see the respective downtime.
2. Adjust length of time: Day, Week, Month, or Custom Period.
3. Select **Aggregated Downtime by Sites**.
4. Click on individual data elements to see downtime information for a specific site.
5. Click a Cisco SD-WAN edge device or circuit to display details about that downtime event.

Display Network Health

Use the Network Health screen to monitor the performance of tunnels over time in your overlay network over time.

The tunnel statistics may be displayed in one of three views: by edge device, by tunnel, or by carrier.

To display performance through Cisco SD-WAN edge device view:
1. Click **vEdge**.
2. Select an individual color to filter the view.
3. Select a Cisco vEdge device to display latency, loss, and jitter on all the tunnels on that device.

To display graphs for latency, loss, and jitter on each tunnel in your overlay network:
1. Click **Tunnel**. Select an individual carrier, color, or both to filter the view.
2. Hover over a point on a line to open a hover box with details for that point in time.
3. Click a local Cisco SD-WAN device to display average latency, loss, or jitter on all the tunnels on that device.
4. Click a remote Cisco SD-WAN device to display latency, loss, or jitter on the tunnels between two Cisco SD-WAN devices.

To display performance by carrier on a geographical map of the overlay network:
1. Click **Carrier**. Circles on the map represent each carrier. The legend to the right indicates the color of each carrier.
2. Select **Latency**, **Loss**, or **Jitter** to change the data displayed.
3. Click on individual data elements to select specific carriers to view.
4. Hover over a carrier's circle to display a hover box with details for that location.
5. Click a circle on the map to display loss, latency, or jitter of all the tunnels terminating on that location.
6. Click a carrier on the graph to see performance by individual edge devices on that carrier.

Monitor Application Performance

Use the Applications screen to monitor application families and individual applications in your network.
Screen Elements

- Title bar—Includes the title of the screen and the time period. Select a desired time interval.
- Bandwidth—Displays bandwidth utilization by application families and individual applications.
- Performance—Displays Quality of Experience (QoE) values for application families and applications.
- Anomaly—Displays anomalies in application bandwidth consumption over baselines.
Display Bandwidth Utilization

To display bandwidth utilization for application families:

1. Click Bandwidth.
2. Click on individual data elements to select a specific application family to view.
3. Hover over an item in any chart to open a hover box with details about that item.
4. Select a view: By Summary, By Time, or By Sites:
   - By Summary displays a summary by application family. Click an application family to display applications in that family. Click an application to see that application's bandwidth utilization over time.
   - By Time displays a timeline of application family bandwidth utilization. Click an application family to display utilization for the applications in that family. Click an application to display utilization at each site running the application.
   - By Sites displays bandwidth utilization on each Cisco SD-WAN edge device. Click a site to display a timeline of application family bandwidth utilization at that site. Click an application family to display utilization for applications in that family at that time.

Display QoE Values

To display QoE values for each application family:

1. Click Performance.
2. Click on individual data elements to select a specific application family to view.
3. Hover over an application family in the chart to open a hover box with details for that application family.
4. Click an application family to display QoE, average latency, loss, and jitter for each application in that family:
   a. Click an application to display that application's performance on each device in the tunnel.
   b. Click a tunnel to display an hourly summary of that application on that tunnel.

Display Anomaly from Baseline Utilization

The vAnalytics platform computes daily averages and standard deviations for application families at every site in a rolling window of seven days. An anomaly occurs if an application family's bandwidth utilization exceeds the average plus two times the standard deviation.

To display deviations from baseline values of bandwidth utilization for application families:

1. Click Anomaly.
2. Click on individual data elements to select a specific application family to view.
3. Hover over an application family in the chart to open a hover box with details for that application family.
4. Click a site to see a timeline of anomalies for that site.
5. Click an hour on the timeline to see anomalous behavior of individual applications in that hour.
CHAPTER 3

Maintain Cisco SD-WAN

- Admin Tech Command, on page 39
- SSH Terminal, on page 40
- Rediscover Network, on page 40
- Reboot Your Device, on page 41
- Software Upgrade, on page 44
- Software Repository, on page 48

Admin Tech Command

Use the Admin Tech command to collect system status information for a device in a tar file to aid in troubleshooting and diagnostics.

1. From the device table, select the device.
2. Next, go to More Actions > Admin Tech.
3. In the Generate admin-tech File window, limit the contents of the Admin Tech tar file if desired:
   a. The Include Logs checkbox is selected by default. Deselect this checkbox to omit any log files from the compressed tar file. Log files are stored in the /var/log/directory on the local device.
   b. Select the Include Cores checkbox to include any core files. Core files are stored in the /var/crash directory on the local device.
   c. Select the Include Tech checkbox to include any files related to device processes (daemons) and operations. These files are stored in the /var/tech directory on the local device.
4. Click Generate. A tar file is created which contains the contents of various files on the local device. This file has a name similar to 20150709-032523-admin-tech.tar.gz, where the numeric fields are the date and time.
5. Send the admin-tech.tar.gz file to your Cisco SD-WAN customer support contact.

Interface Reset Command

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.
1. From the device table, select the device.
2. Next, go to More Actions > Interface Reset.
3. In the Interface Reset window, select the desired interface.
4. Click Reset.

**SSH Terminal**

Use the SSH Terminal screen to establish an SSH session to a Cisco vEdge device. From an SSH session, you can issue CLI commands on a Cisco vEdge device.

**Establish an SSH Session to a Device**

To establish an SSH session to a device:

1. From the left pane, select the device on which to collect statistics:
   a. Select the device group to which the device belongs.
   b. If needed, sort the device list by its status, hostname, system IP, site ID, or device type.
   c. Click on the device to select it.

2. Enter the username and password to log in to the device.

You can now issue CLI commands to monitor or configure the device.

**Rediscover Network**

Use the Rediscover Network screen to locate new devices in the overlay network and synchronize them with the vManage NMS.

**Screen Elements**

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Rediscover Network.
- Rows Selected—Displays the number of rows selected from the table.
  - Rediscover button—Click to rediscover the devices in the network.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
• Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.

Rediscover the Network
To locate new devices in the overlay network, click the Rediscover button located directly beneath the title bar. Cisco vManage redisCOVERs every device and link and displays updated information about the network.

Synchronize Device Data
To synchronize the data on a specific device with the vManage NMS:

1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.

2. Select the device.

3. Click Rediscover to confirm re-synchronization of the device data.

Reboot Your Device
Use the Device Reboot screen to reboot one or more Cisco SD-WAN devices.

Reboot Devices
To reboot Cisco SD-WAN devices in the overlay network:

1. In the title bar, click vEdge > Controller > vManage.
2. Choose one or more devices.
3. Click the Reboot button.

View Active Devices

To view a list of devices on which the reboot operation has been performed:
1. Click the Tasks icon that is located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

Reload Security Application

The reload service button enables you to recover a security application from an inoperative state. See Determine Security Applications in Inoperative State, on page 44. For more information about a security application, see Configuring Security Application.

Note

The reload service can recover some security applications from an inoperative state. Make sure to use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 44.

Ensure that a security application has already been installed on the device which is chosen from the device table. To reload one or more security applications:

1. In the WAN Edge tab, check against a Cisco SD-WAN device to reload the security application
2. Click Reload Services.

The Reload Container dialog box appears.
3. If the security application version is correct, check the box against the version of the security app. See the topic Upgrade a Security Virtual Image in Configuring Security Application for more information about an application version.
4. Click Reload.
   
   The security application is stopped, uninstalled, reinstalled, and started again.

**Reset Security Application**

The reset service button enables you to recover a security application from an inoperative state. See Determine Security Applications in Inoperative State, on page 44. For more information about a security application, see Configuring Security Application.

When the virtual network configuration of a security application changes such as the virtual port group configuration on a device, use the reset service button.

---

**Note**

The reset service can recover some security applications from an inoperative state, and therefore ensure to use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 44.

- Ensure that a security application has already been installed on the device which is chosen from the device table.
- Ensure that the chosen security application is in a running state.

To reset one or more security applications:

1. Go to the **WAN Edge** tab, check against a Cisco SD-WAN device to reload the security application.
2. Click **Reset Services**.
   
   The Reset Container dialog box appears.
3. If the security application version is correct, check the box against the version of the device. See the topic Upgrade the Security Virtual Image in Configuring Security Application for more information about an application version.

4. Click Reset.
   The security application is stopped, and then restarted.

Determine Security Applications in Inoperative State

To determine if a security application is in inoperative state:

1. In vManage NMS, click Monitor > Network.

2. In the MONITOR|NETWORK screen, click a Cisco SD-WAN device from Hostname.

3. In the left pane, click Real Time.
   The real time device information appears in the right pane.

4. Choose App Hosting Details from the Device Options drop-down.
   A table appears with the device-specific application hosting information. In the table, if the state of the device is "ACTIVATED," "DEPLOYED," or "STOPPED," perform a reload or reset operation on the security application.

   If the state of the device is "RUNNING," the security application is in an operative state.

   A table appears with the device-specific application data plane information. In the table, if the SN Health of the device is "yellow," or "red," perform a reload or reset operation on the security application.

   If the SN Health of the device is "green," the security application is in an operative state.

Software Upgrade

Use the Software Upgrade screen to download new software images and to upgrade the software image running on a Cisco SD-WAN device.

From a centralized vManage NMS, you can upgrade the software on Cisco SD-WAN devices in the overlay network and reboot them with the new software. You can do this for a single device or for multiple devices simultaneously.

When you upgrade a group of vBond orchestrators, vSmart controllers, and vEdge routers, the software upgrade and reboot is performed first on the vBond orchestrator, next on the vSmart controllers, and finally
on the vEdge routers. For vEdge routers, up to five routers can be upgraded and rebooted in parallel at the same time.

You cannot include the vManage NMS in a group software upgrade operation. You must upgrade and reboot the vManage server by itself.

It is recommended that you perform all software upgrades from the vManage NMS rather than from the CLI.

**View Software Images**

To view a list of software images in the repository on the vManage server or on a remote server, from the Device List drop-down, click **Repository**.

**Upgrade a Software Image**

To upgrade the software image on a device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices on which to upgrade the software image.
3. Click the **Upgrade** button. The Software Upgrade dialog box opens.
4. Select the software version to install on the device. If the software is located on a Remote Server, select the VPN in which the software image is located.
5. To automatically activate the new software version and reboot the device, select the Activate and Reboot checkbox.
6. Click **Upgrade**. A progress bar indicates the status of the software upgrade.

If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Cisco SD-WAN devices to come up after a software upgrade is 5 minutes, except for vEdge 100 routers, which have a default time of 12 minutes.

---

**Note**

If you upgrade the vEdge software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the vEdge software.

**Activate a New Software Image**

If you did not select the Activate and Reboot checkbox when upgrading the software image, the device continues to use the existing configuration. To activate the new software image:

1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which to activate the new software image.
3. Click the **Activate** button. The Activate Software dialog box opens.
4. Select the software version to activate on the device.
5. Click **Activate**. vManage NMS reboots the device and activates the new software image.
If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Cisco SD-WAN devices to come up after a software upgrade is 5 minutes, except for the vEdge 100 routers, which have a default time of 12 minutes.

**Upgrade CSP device with NFVIS Upgrade Image**

See Upgrade CSP Device with NFVIS Upgrade Image, on page 47.

**Delete a Software Image**

To delete a software image from a Cisco SD-WAN device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices from which to delete a software image.
3. Click the **Delete Available Software** button. The Delete Available Software dialog box opens.
4. Select the software version to delete.
5. Click **Delete**.

**Set the Default Software Version**

You can set a software image to be the default image on a Cisco SD-WAN device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on the device and in your network.

To set a software image to be the default image on a device:

1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which you wish to change the default software image.
3. Click the **Set Default Version** button. The Set Default Version dialog box opens.
4. From the Version drop-down, select the software image to use as the default.
5. Click **Set Default**.

**Export Device Data in CSV Format**

To export data for all devices to a file in CSV format, click the Export button. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named `viptela_download.csv`.

**View Log of Software Upgrade Activities**

To view the status of software upgrades and a log of related activities:

1. Click the **Tasks** icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click on the arrow to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

Upgrade CSP Device with NFVIS Upgrade Image

**Before you begin**

Ensure that the NFVIS software versions are the files that have .nfvispkg extension.

---

**Step 1** In the **Maintenance > Software Upgrade > WAN Edge** screen, view the list of all CSP devices along with their current and available versions.

**Step 2** Select one or more devices, and click **Upgrade**.

**Step 3** Choose a CSP device on which to upgrade the NFVIS software image.

**Step 4** Click the **Upgrade** button. The **Software Upgrade** dialog box appears.

**Step 5** Choose the NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

**Step 6** To automatically upgrade and activate with the new NFVIS software version and reboot the CSP device, check the **Activate and Reboot** checkbox.

If you do not check the **Activate and Reboot** checkbox, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new NFVIS software version by selecting the device again and clicking the **Activate** button on the **Software Upgrade** page. For more information about activation, see the "Activate a New Software Image" topic in the Cisco SD-WAN Configuration Guides.

**Step 7** Click **Upgrade**.

To view the status of software upgrades, the task view page displays a list of all running tasks along with total number of successes and failures. The page periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status page by clicking the Tasks icon located in the vManage toolbar.

**Note** If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happen in a sequence.
Set the Default Software Version option is not available for NFVIS images.

The CSP device reboots and the new NFVIS version is activated on it. This reboot happens during the Activate phase. The activation can either happen immediately after upgrade if you check the Activate and Reboot check box, or by manually selecting the activate button after selecting the device again.

To verify if CSP device has rebooted and is running, vManage polls your entire network every 90 seconds up to 30 times.

You can delete an NFVIS software image from a CSP device if the image version is not the active version that is running on the device.

Software Repository

Use the Software Repository screen to download software images to the vManage software repository.

View Software Images

When you open the Software Repository screen, the images in the repository are displayed in the table. To filter the list, search or type a string in the Search box.

The Software Version column lists the version of the software image, and the Controller Version column lists the version of controller software that is equivalent to the software version. The controller version is the minimum supported vManage controller version. The software image can operate with the listed controller version or with a higher controller version. In the following example:

<table>
<thead>
<tr>
<th>Software Version</th>
<th>Controller Version</th>
<th>Software Location</th>
<th>Version Type Name</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.8.55</td>
<td>18.1.x</td>
<td>vmanage</td>
<td>software</td>
<td></td>
</tr>
</tbody>
</table>

The software version is 16.8.55, and the controller version is 18.1.x. Reading these two columns together tells you that software version 16.8.55 is compatible with vManage controller software versions 18.1.x and later. This means that devices running version 16.8.55 can operate with vManage servers running Releases 18.1, 18.2, and 18.3, and with later software releases, and they cannot operate with vManage servers running Release 17.2 or Release 17.1.
The Software Location column indicates where the software images are stored, either in the repository on the vManage server or in a repository in a remote location.

The Available Files column lists the names of the software image files.

The Update On column shows when the software image was added to the repository.

In the More Actions column, you can delete a software image from the repository.

**Add Software Images to the Repository**

Before you can upgrade the software on a vEdge router, vSmart controller, or vManage NMS to a new software version, you need to add the software image to the vManage software repository. The repository allows you to store software images on the local vManage server and on a remote file server.

The vManage software repository allows you to store images in three ways:

- **On the local vManage server, to be downloaded over a control plane connection**—Here, the software images are stored on the local vManage server, and they are downloaded to the Cisco SD-WAN devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.

- **On the local vManage server, to be downloaded over an out-of-band connection**—Here, the software images are stored on the local vManage server, and they are downloaded to the Cisco SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the vManage server is able to monitor the software installation.

- **On a remote server**—Here, the software images remain on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the vManage server sends this URL to the Cisco SD-WAN device, which then establishes a connection to the file server over which to download the software images.

To add software images to the vManage software repository:

1. Click **Add New Software**.

2. Select the location to store the software image:
   a. To store the software image on the local vManage server and have it be downloaded to Cisco SD-WAN devices over a control plane connection, select vManage. The Upload Software to vManage dialog box opens.
      1. Drag and drop the software image file to the dialog box, or click **Browse** to select the software image from a directory on the local vManage server.
      2. Click **Upload** to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

**Note**

The local vManage server is available for storing NFVIS upgrade images and no other locations are available.
b. To store the software image on a remote server, select **Remote Server**. The Location of Software on Remote Server dialog box opens.

1. In the Version box, enter the version number of the software image.
2. In the URL box, enter the FTP or HTTP URL of the software image.
3. Click **Add** to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

c. To store the image on a remote vManage server and have it be downloaded to Cisco SD-WAN devices over an out-of-band management connection, select **Remote Server - vManage**. The Upload Software to Remote Server - vManage dialog box opens.

1. In the vManage Hostname box, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).
2. Drag and drop the software image file to the dialog box, or click **Browse** to select the software image from a directory on the local vManage server.
3. Click **Upload** to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

---

**Upload VNF Images in Software Repository**

See [Upload VNF Images](#), on page 50.

**Create Customized VNF Image**

See [Create Customized VNF Image](#), on page 51.

**View VNF Images**

See [View VNF Images](#).

**Delete a Software Image from the Repository**

To delete a software image from the vManage software repository:

1. In the software repository table, select the software image.
2. In the More actions icon to the right of the line, click **Delete**.

If a software image is being download to a router, you cannot delete the image until the download process completes.

**Delete VNF Image**

See [Delete VNF Images](#).

---

**Upload VNF Images**

The VNF images are stored in software repository. These VNF images are referenced during service chain deployment, and then they are pushed to NFVIS during service chain attachment.
In vManage, click **Maintenance > Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To add a prepackaged VNF image, click the **Virtual Images** tab, and then click the **Upload Virtual Images** button.

b) Choose the location to store the virtual image.

   - To store the virtual image on the local vManage server and then get it downloaded to CSP devices over a control plane connection, click **vManage**. The **Upload Software to vManage** dialog box appears.

     1. Drag and drop the virtual image file to the dialog box or click **Browse** to choose the virtual image from the local vManage server. For example, CSR.tar.gz, ASAv.tar.gz.

     2. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

   - To store the image on a remote vManage server and then get it downloaded to CSP devices over an out-of-band management connection, click **Remote Server - vManage**. The **Upload Virtual Image to Remote Server - vManage** dialog box appears.

     1. In **vManage Hostname/IP Address**, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).

     2. Drag and drop the virtual image file to the dialog box, or click **Browse** to choose the virtual image from the local vManage server.

     3. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

c) Click **Submit**.

You can have multiple VNF entries such as a firewall from same or different vendors. Also, different versions of VNF that are based on the release of the same VNF can be added. However, ensure that the VNF name is unique.

**Create Customized VNF Image**

**Before you begin**

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.

- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
• Day-0 configuration files–system and tokenized custom variables
• VM configuration–CPU, memory, disk, NICs
• HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link
• Additional Storage–If additional storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Table 4: VNF Package Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Name</td>
<td>Mandatory</td>
<td>Specifies the filename of the target VNF package. It is the NFVIS image name with .tar or .gz extensions.</td>
</tr>
<tr>
<td>App Vendor</td>
<td>Mandatory</td>
<td>Specifies whether Cisco VNFs or third-party VNFs.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Specifies name of the VNF image.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional</td>
<td>Specifies version number of the program.</td>
</tr>
<tr>
<td>Type</td>
<td>Mandatory</td>
<td>Choose VNF type. Supported VNF types are: Router, Firewall, Load Balancer, and Other.</td>
</tr>
</tbody>
</table>

Step 1
In the Maintenance > Software Repository screen, click the Add Custom VNF Package button from the Virtual Images tab.

Step 2
Configure the VNF with the following VNF package properties and click Save.

Step 3
To package a VM qcow2 image, click File Upload under Image, and browse to choose a qcow2 image file.

Step 4
To choose a bootstrap configuration file for VNF, if any, click the Bootstrap Files button under Day 0 Configuration, click File Upload, and then browse to choose a bootstrap file.

Include the following Day-0 configuration properties:

Table 5: Day-0 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount</td>
<td>Mandatory</td>
<td>Specifies the path where the bootstrap file gets mounted.</td>
</tr>
<tr>
<td>Parseable</td>
<td>Mandatory</td>
<td>Specifies whether a Day-0 configuration file can be parsed or not. Options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>are: true or false. By default, it is true.</td>
</tr>
</tbody>
</table>
Choose high availability of a Day-0 configuration file. Supported values are: Standalone, HA Primary, HA Secondary.

**Note** If any bootstrap configuration is required for a VNF, you must create *bootstrap-config* or *day0-config*.

**Step 5**

To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** against the configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

**Note** The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the topic, Additional References in Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide for the list of system variables that must be added for different VNF types.

- a) To add a system variable, in the **CLI configuration** dialog box, select and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
- b) Choose a system variable from the **Variable Name** drop-down, and click **Done**. The highlighted property is replaced by the system variable name.
- c) To add a custom variable, in the **CLI configuration** dialog box, select and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
- d) Enter custom variable name and choose a type from **Type** drop-down.
- e) To set the custom variable attribute, do the following:
  - To ensure that the custom variable is mandatory when creating a service chain, check the **Type** check box against **Mandatory**.
  - To ensure that a VNF includes both primary and secondary Day-0 files, check the **Type** check box against **Common**.
- f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

**Step 6**

To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an additional qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

**Note** Ensure that you do not combine ephemeral disks and storage volumes when uploading extra VM images.

**Step 7**

To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

### Table 6: Storage Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Mandatory</td>
<td>Specifies the disk size that is required for the VM operation. The maximum disk size can be 256 if the size unit is GiB.</td>
</tr>
</tbody>
</table>
To add VNF image properties, expand **Image Properties** and provide the following image information.

**Table 7: VNF Image Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-IOV Mode</td>
<td>Mandatory</td>
<td>Specifies enabling or disabling SR-IOV support. By default, it is enabled.</td>
</tr>
<tr>
<td>Monitored</td>
<td>Mandatory</td>
<td>VM health monitoring for those VMs that can be bootstrapped. Options are: enable or disable. By default, it is enabled.</td>
</tr>
<tr>
<td>Bootup Time</td>
<td>Mandatory</td>
<td>Specifies monitoring timeout period for a monitored VM. By default, it is 600 seconds.</td>
</tr>
<tr>
<td>Serial Console</td>
<td>Optional</td>
<td>Specifies serial console that is supported or not. Options are: enable or disable. By default, it is disabled.</td>
</tr>
<tr>
<td>Privileged Mode</td>
<td>Optional</td>
<td>Allows special features like promiscuous mode and snooping. Options are: enable or disable. By default, it is disabled.</td>
</tr>
</tbody>
</table>
Step 9

To add VM resource requirements, expand **Resource Requirements** and provide the following information.

**Table 8: VM Resource Requirements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Cores</td>
<td>Mandatory</td>
<td>Facilitates allocation of a dedicated resource (CPU) to supplement a VM’s low latency (for example, router and firewall). Otherwise, shared resources are used. Options are: enable or disable. By default, it is enabled.</td>
</tr>
<tr>
<td>Default CPU</td>
<td>Mandatory</td>
<td>Specifies CPUs supported by a VM. The maximum numbers of CPUs supported are 8.</td>
</tr>
<tr>
<td>Default RAM</td>
<td>Mandatory</td>
<td>Specifies RAM supported by a VM. The RAM can range from 2–32.</td>
</tr>
<tr>
<td>Disk Size</td>
<td>Mandatory</td>
<td>Specifies disk size in GB supported by a VM. The disk size can range from 4–256.</td>
</tr>
<tr>
<td>Max number of VNICs</td>
<td>Optional</td>
<td>Specifies maximum number of VNICs allowed for the VM. The number of VNICs can range from 8–32 and the default value is 8.</td>
</tr>
<tr>
<td>Management VNIC ID</td>
<td>Mandatory</td>
<td>Specifies the management VNIC ID corresponding to the management interface. Valid range is from 0 to maximum number of VNICs.</td>
</tr>
<tr>
<td>Number of Management VNICs ID</td>
<td>Mandatory</td>
<td>Specifies number of VNICs.</td>
</tr>
<tr>
<td>High Availability VNIC ID</td>
<td>Mandatory</td>
<td>Specifies VNIC IDs where high availability is enabled. Valid range is from 0–maximum number of VNICs. It should not conflict with management VNIC Id. The default value is 1.</td>
</tr>
<tr>
<td>Number of High Availability VNICs ID</td>
<td>Mandatory</td>
<td>Specifies maximum number of VNIC IDs where high availability is enabled. Valid range is 0–(maximum number of VNICs-number of management VNICs-2) and default value is 1.</td>
</tr>
</tbody>
</table>
**Step 10**

To add Day-0 configuration drive options, expand **Day0 Configuration Drive options** and provide the following information.

**Table 9: Day-0 Configuration Drive Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Label</td>
<td>Mandatory</td>
<td>Displays the volume label of the Day-0 configuration drive. Options are: V1 or V2. By default, it is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.</td>
</tr>
<tr>
<td>Init Drive</td>
<td>Optional</td>
<td>Mounts the Day-0 configuration file as a disk. The default drive is CD-ROM.</td>
</tr>
<tr>
<td>Init Bus</td>
<td>Optional</td>
<td>Choose an init bus. Supported values for a bus are: virtio, scsi, and ide. By default, it is ide.</td>
</tr>
</tbody>
</table>

The Software Repository table displays the customized VNF image, and it is available for choosing while creating a custom service chain.

**View VNF Images**

In vManage, click **Maintenance > Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To view VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To view VNF images, click the **Virtual Images** tab. The images in the repository are displayed in the table.

b) To filter the list, search or type a string in the Search box.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. It can be stored either in the repository on the vManage server or in a repository in a remote location.

The Version Type Name column provides the type of firewall.

The Available Files column lists the names of the VNF image files.

The Update On column displays when the software image was added to the repository.

c) To view details of a VNF image, click a VNF image, click the **More Actions** icon, and click **Show Info** against the VNF image.
Delete VNF Images

In vManage, click **Maintenance > Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VM images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To delete a VM image, click the **Virtual Images** tab. The images in the repository are displayed in the table.
b) In the repository table, click a VM image.
c) Click the **More Actions** icon to the right of its row, and click **Delete** against the VM image.

**Note**
If a VNF image is being download to a router, you cannot delete the VNF image until the download process completes.

**Note**
If the VNF image is referenced by a service chain, it cannot be deleted.