

# Cisco Cloud Services Platform Configuration Guide, Release 2.8.0

---

**Last Modified:** 2020-08-18

## Configuring Cisco CSP

This guide describes how to configure various Cisco CSP features available in Release 2.4.1 and later releases.

## Information About Cisco Cloud Services Platform

Cisco Cloud Services Platform is a software and hardware platform for data center network functions virtualization. This open kernel virtual machine (KVM) platform, with Red Hat Enterprise Linux (RHEL) as the base operating system, is designed to host networking virtual services. Cisco CSP provides REST APIs, a web interface, and a CLI for creating and managing the virtual machine (VM) lifecycle.

## Supported Cisco Networking Services

Cisco CSP can host any Cisco or third-party VNF that is supported on KVM hypervisor. Some of the Cisco VNFs available include the following:

- Cisco Cloud Services Router (CSR) 1000V virtual router
- Cisco IOS® XRv 9000 Router
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower™ NGFW Virtual
- Cisco Prime® Virtual Network Analysis Module (vNAM)
- Cisco Virtual Wide Area Application Services (vWAAS)
- Cisco Web Security Virtual Appliance (WSAv)
- Cisco Identity Services Engine (ISE)
- Cisco Firepower Management Center (FMC)
- Cisco Virtual Security Gateway (VSG) for Cisco Nexus® 1000V Series Switch deployments
- Cisco Virtual Supervisor Module (VSM) for Cisco Nexus 1000V Series Switch deployments
- Cisco Data Center Network Manager (DCNM)

## Important Notes and Restrictions

Following are the important notes and restrictions for Cisco CSP.

### Configuration Limits

Use the following configuration limits for Cisco CSP.

Component	Supported Limits
Number of services in a node with hyperthreading disabled	<ul style="list-style-type: none"> <li>For Cisco CSP with 8 or less than 8 cores, you can deploy the following number of VM cores: <i>Number of Cores – 1</i> For example, for Cisco CSP with 8 cores, you can deploy 7 VM cores.</li> <li>For Cisco CSP with greater than 8 and less than or equal to 16 cores, you can deploy the following number of VM cores: <i>Number of Cores – 2</i> For example, for Cisco CSP with 16 cores, you can deploy 14 VM cores.</li> <li>For Cisco CSP with greater than 16 cores, you can deploy the following number of VM cores: <i>Number of Cores – 4</i> For example, for Cisco CSP with 36 cores, you can deploy 32 VM cores.</li> </ul>
Total number of nodes in a cluster	10
Number of vNICs per service	24

### Hyper-Threading Technology Support

Cisco CSP hardware supports Hyper-Threading (HTT). However by default, HTT is disabled and must be kept disabled, as it is not supported. This action avoids VNFs sharing same CPU cores, cache and memory bus that can result in stalls or latency issues, and VNF data plane performance degradation. The enablement or disablement of Hyper-Threading is done by CIMC on CSP 5000 hardware.

### Changing IP Address of the Management Interface for NFS Configurations

If NFS is configured on the system, note the following:

- Changing the management IP address causes an outage of the VNC console and stats collection for 15 to 30 minutes.
- Reboot of the system can take up to 30 minutes.

As a workaround, you can unconfigure the NFS mount before performing these operations and reconfigure the NFS mount after the operation is complete. You can also reboot the system from the Cisco CSP CIMC connection.

## Configuring Passthrough Interfaces

When a service has passthrough as well as non-passthrough vNICs, we recommend that you first define the non-passthrough vNICs and then define the passthrough vNICs.

## Run `config terminal` Command After Initial Setup

The `config terminal` command fails when you run it after performing the initial setup for a new installation. This happens because the admin user is not assigned to a group at the initial login. To run this command and configure Cisco CSP features, you must log out and then log in to Cisco CSP.

## Spectre and Meltdown Firmware Update

This release include fixes for spectre and meltdown issue in Cisco CSP software. For firmware update, update the CIMC version to 4.0(1a). See the Cisco UCS C-Series Software Release Notes for more information about CIMC version at,

[Release Notes for Cisco UCS C-Series Software, Release 4.0\(1\)](#).

# Configuring Management Interface

## Configuring Management Interface pNIC Mode

Cisco CSP provides support for configuring the shared or dedicated mode of the management interface pNIC. In shared mode, the management interface pNIC can be shared with any service VMs. The management interface pNIC carries the management traffic of Cisco CSP and the management and data traffic of any service using this pNIC. In dedicated mode, the management interface pNIC carries only the management traffic of Cisco CSP. In shared mode, you can change the management interface pNIC to any available pNIC. In dedicated mode, you can change the management interface pNIC only to a pNIC that is not associated with any service.



**Note** Changing the mode of the management interface pNIC to dedicated while a service is currently using it results into the `Management pNIC already in service use error`. Similarly, if the management interface pNIC is in dedicated mode and you try to create a service using the management pNIC, you get the `pNIC is dedicated to management error`.

You can configure the management interface pNIC mode during the initial Cisco CSP setup or later on by using the web interface, the CLI, or the REST API. For information about how to configure the management interface pNIC mode during initial setup, see the *Cisco Cloud Services Platform Quick Start Guide*.

## Management Interface pNIC Mode Configuration

Configuration Mode	Description
Web Interface	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; HOST</b>.</li> <li>2. Choose a mode from the <b>Management pNIC Mode</b> drop-down list.</li> <li>3. Click <b>Submit</b>.</li> </ol>

Configuration Mode	Description
CLI	Use the <b>resource csp-2100 mgmt_pnic_mode</b> <i>mgmt_pnic_mode</i> command.
REST API	Use the following REST API:  <b>curl -u user:password -X POST</b> <b>https://ip-address:port-number/api/running/resources/resource/csp-2100 -H</b> <b>"Content-type: application/vnd.yang.data+json" -d</b> <b>'{"mgmt_pnic_mode": "mgmt_pnic_mode"}'</b>

## Configuring ACL Access for the Management Interface

Cisco CSP provides support for enabling the ACL access for the management interface. When this feature is enabled, only specified source networks can access the management interface. While creating an ACL access rule, you must specify the IPv4 IP address of the source network along with the priority and the action to be taken for the packets received from the source network. You can also select a specific service type for the ACL access. You can configure this feature by using the web interface, the CLI, or REST API.

### ACL Access Configuration

Configuration Mode	Description
Web Interface	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; IP Receive ACL</b>.</li> <li>2. Click the add (+) button.</li> <li>3. Enter the IP address of the source network in the <i>ip-address/prefix</i> format in the <b>Source Network</b> field.</li> <li>4. Choose one or more services in the <b>Service</b> field.</li> <li>5. Choose an action in the value from the <b>Action</b> drop-down list.</li> <li>6. Enter a priority value for the ACL rule in the <b>Priority</b> field.</li> <li>7. Click <b>Submit</b>.</li> </ol>
CLI	Use the <b>resource csp-2100 ip-receive-acl</b> <i>source_ip_address</i> <b>service</b> <i>service</i> <b>priority</b> <i>priority</i> <b>action</b> <i>action</i> command.
REST API	Use the following REST API:  <b>curl -u user:password -X POST</b> <b>https://ip-address:port-number/api/running/resources/resource/csp-2100/ip-receive-acls</b> <b>-H "Content-type: application/vnd.yang.data+json" -d</b> <b>'{"host":{"ip-receive-acl":{"source": "source_ip_address", "service": "service",</b> <b>"priority": "priority", "action": "action"}}'</b>

## Resetting to Factory Default

Cisco CSP provides support for restoring to original factory defaults. This process is useful when you want to remove an undesirable configuration that is present in Cisco CSP and want to restore Cisco CSP to clean

install mode. The factory reset process deletes VMs and volumes, files including logs, images, certificates, and erases all configuration. Connectivity is lost, and the admin password is changed to factory default password.



**Note** Do not perform any operation for around 15 to 20 minutes while the factory reset process is in progress. The time taken for the factory reset process is almost the same as rebooting Cisco CSP.

After factory reset process is complete, Cisco CSP reboots automatically, and you are prompted with the configuration services questionnaire similar to clean installation. For more information about how to set up your Cisco CSP through clean installations, see the *Cisco Cloud Services Platform Quick Start Guide*.

You can restore Cisco CSP to factory default configuration by using the CLI, or the REST API.

Configuration Mode	Description
CLI	Perform a factory reset of Cisco CSP to factory defaults by using the <b>factory-default-reset all</b> command.  <b>Note</b> Select <b>Yes</b> when you are prompted with the factory default warning message.
REST API	Use the following REST API:  <b>curl -k -u user:password -X POST https://ip-address:port-number/api/operations/factory-default-reset/all -H "Content-type: application/vnd.yang.data+json"</b>

## Configuring Dedicated Service Management Interface

Cisco CSP provides support for configuring a pNIC or a port channel to be used as the dedicated service management interface. You can configure the dedicated service management interface during the initial Cisco CSP setup or later on by using the CLI, or the REST API. For information about how to configure the dedicated service management interface during initial setup, see the *Cisco Cloud Services Platform Quick Start Guide*.

### Guidelines for Dedicated Service Management Interface

Following are the guidelines for configuring the dedicated service management interface:

- Only one dedicated service management interface can be active at a time.
- The specified pNIC cannot be a member of a port channel.
- The specified pNIC cannot be same as the Cisco CSP management pNIC (**mgmt\_pnic**).
- The dedicated service management interface can be changed only when it is not in use. In addition, the port or the port channel that you are planning to assign as the dedicated service management interface should not be in use.
- The dedicated service management interface can be used by multiple services and on multiple vNICs in the same service.
- The dedicated service management interface is deleted only when it is not in use.

## Dedicated Service Management Interface Configuration

Configuration Mode	Description
Web Interface	<p>Configure the dedicated service management interface by performing the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Configuration &gt; pNICs</b> or <b>Configuration &gt; Port Channel</b>.</li> <li>2. Under the <b>Action</b> column, click <b>Enable Service Management</b>.</li> </ol> <p>To use the configured dedicated service management interface with a service, check the <b>Service Management Interface</b> check box while configuring a service vNIC. For detailed information about how to create a service using the web interface, see the <i>Cisco Cloud Services Platform 2100 Quick Start Guide</i>.</p>
CLI	<p>Configure the dedicated service management interface by using the <b>resource csp-2100 service-mgmt-pnic</b> <i>pnic_name</i> command.</p> <p>To use the configured dedicated service management interface with a service, use the <b>service name vnic nic_num mgmt-vnic true</b> command.</p>
REST API	<p>Configure the dedicated service management interface by using the following REST API:</p> <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/resources/resource/csp-2100 -H "Content-type: application/vnd.yang.data+json" -d '{"service-mgmt-pnic": "pnic_name"}</pre> <p>To use the configured dedicated service management interface with a service, use the following REST API:</p> <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/services -H "Content-type: application/vnd.yang.data+json" -d '{"service": {"name": "name" "vnics": {"vnic": [{"nic": "nic_num "mgmt-vnic": "true"}]}}}'</pre>

## Configuring AAA Authentication Mode

You can select the server to be used for AAA authentication by using the web interface, the CLI, or the REST API. You can select a TACACS+ or a RADIUS server.

Configuration Mode	Description
Web Interface	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; AAA</b>.</li> <li>2. In the <b>AAA Authentication Mode</b> field, select a server.</li> </ol>
CLI	<p>Use the <b>aaa authentication authentication_server rest_req_caching_tmout rest_req_caching_tmout</b> command.</p>

Configuration Mode	Description
REST API	Use the following REST API: <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/security_servers/aaa -H "Content-type: application/vnd.yang.data+json" -d '{"aaa":{"authentication":" authentication_server : {"rest_req_caching_tmout": rest_req_caching_tmout }}}'</pre>

## Configuring a TACACS+ Server

You can configure a TACACS+ server by using the web interface, the CLI, or the REST API.



**Note** When the TACACS+ feature is enabled, use port 2024 to connect to the Cisco CSP through SSH; for example, `ssh -p 2024 username@csp_ipaddress`.

Configuration Mode	Description
Web Interface	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; AAA &gt; TACACS</b>.</li> <li>2. Click the add (+) button.</li> <li>3. Enter a name in the <b>TACACS Server</b> field.</li> <li>4. Choose a key type from the <b>Key Type</b> drop-down list.</li> <li>5. Enter a shared secret in the <b>Shared Secret</b> field.</li> <li>6. Choose a value from the <b>Insert First</b> drop-down list.</li> <li>7. Click <b>Submit</b>.</li> </ol>
CLI	Use the <code>tacacs-server host hostname key key_value shared-secret shared-secret</code> command.
REST API	Use the following REST API: <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/security_servers/tacacs-server -H "Content-type: application/vnd.yang.data+json" -d '{"host":{"server":"hostname", "secret":{"key":"key_value", "shared-secret ":"shared-secret"}}}'</pre> <p><b>Note</b> If you are configuring a TACACS+ server for the first time through REST API, use your Cisco CSP user account credentials. After configuring a TACACS+ server, use your configured TACACS+ server's user account credentials with the REST APIs.</p>

## Configuring a RADIUS Server

You can configure a RADIUS server by using the web interface, the CLI, or the REST API. You can also specify the global configuration settings for the RADIUS server such as the timeout duration and the retransmit count.

Configuration Mode	Description
Web Interface	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; AAA &gt; RADIUS</b>.</li> <li>2. Click the add (+) button.</li> <li>3. Enter a name in the <b>RADIUS Server</b> field.</li> <li>4. Choose a key type from the <b>Key Type</b> drop-down list.</li> <li>5. Enter a shared secret in the <b>Shared Secret</b> field.</li> <li>6. Enter a port number in the <b>Authentication Port</b> field.</li> <li>7. Enter a port number in the <b>Accounting Port</b> field.</li> <li>8. Click <b>Submit</b>.</li> </ol>
CLI	Use the <b>radius-server host</b> <i>hostname</i> <b>key</b> <i>key_value</i> <b>shared-secret</b> <i>shared-secret</i> <b>acct-port</b> <i>acct-port</i> <b>auth-port</b> <i>auth-port</i> command.
REST API	<p>Use the following REST API:</p> <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/security_servers/radius-server -H "Content-type: application/vnd.yang.data+json" -d '{"host":{"server":"hostname", "secret":{"key":"key_value", "shared-secret":"shared-secret"}, "auth-port":"auth-port", "acct-port":"acct-port"}}</pre>

## Configuring SR-IOV Support

The SR-IOV support is configurable on per-pNIC basis. You can configure the SR-IOV support on 10G and 40G interfaces by using the web interface, the CLI, or the REST API.

### Guidelines for SR-IOV Support

Following are the guidelines for configuring the SR-IOV support:

- SR-IOV support cannot be configured on the management interface.
- SR-IOV feature is supported only with 10G and 40G interfaces.
- SR-IOV support cannot be disabled if any existing service is already using this feature.
- VF interfaces come up only when the physical pNIC is up and running.
- VF interfaces are used in the passthrough mode.
- Up to 63 VFs are supported on a 10G interface and up to 64 VFs are supported on a 40G interface.



- To add more VFs to a pNIC, you must disable the SR-IOV support and then enable it.
- Only one VLAN can be configured on a VF.
- Port channels are supported only on Intel X520 (Niantic) NICs.

## Configuring Port Channels on SR-IOV

Cisco CSP provides support for configuring a port channel on SR-IOV VFs inside a VNF. This feature is currently supported only on Intel X520 (Niantic) NICs. To configure port channels on SR-IOV, do the following:

### Procedure

**Step 1** Create a VNF with two VFs. These VFs should be from two different SR-IOV-enabled pNICs.

**Step 2** Create a port channel inside the VM by using the VFs from Step 1.

**Step 3** Configure a port channel on the upstream switches with two Cisco CSP pNIC ports.

**Note** The two pNIC ports on the Cisco CSP can only be used for port channels. VFs from either of the pNICs cannot be used by a VM in isolation.

## SR-IOV Support Configuration

Configuration Mode	Description
Web Interface	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Configuration &gt; SRIOV</b>.</li> <li>2. On the <b>SRIOV Configuration</b> page, under the <b>Action</b> column, click <b>Enable SRIOV</b>.</li> <li>3. Enter a value in the <b>Number of VFs</b> field.</li> <li>4. Choose a value from the <b>Switch Mode</b> drop-down list.</li> <li>5. Click <b>Configure</b>.</li> </ol>
CLI	Use the <b>pnic name sr-iov numVFs numVFs switchMode switchmode</b> command.
REST API	Use the following REST API: <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/pnics/pnic -H "Content-type: application/vnd.yang.data+json" -d '{"pnic":{"name":"name", "sr-iov": {"numVFs":"numVFs", "switchMode ":"switchMode"}}}'</pre>

## Configuring SNMP

### Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for monitoring and managing devices in a network. SNMP supports IPv4 and IPv6 addresses. The SNMP framework consists of following parts:

- An SNMP manager: The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent: The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems.
- An MIB: The collection of managed objects on the SNMP agent.

Cisco CSP supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

### Configuring SNMP Support

You can configure the SNMP support in Cisco CSP by using the web interface, the CLI, or the REST API. The procedure for configuring SNMP version 2 is different from the procedure for configuring SNMP version 3. When you configure SNMP versions 1 and 2, you can optionally create or modify views for community strings to limit which MIB objects an SNMP manager can access.

Use the **snmp-server** commands to enable the supported versions of SNMP.




---

**Note** The first **snmp-server** command that you enter enables the supported versions of SNMP. All other configurations are optional.

---

### Creating or Modifying an SNMP View Record

You can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view or create your own view. If you are using a predefined view or no view at all, skip this task.

Perform the following steps to create or modify an SNMP view record:

#### Procedure

---

**Step 1** Enter global configuration mode.

**Step 2** Create a view record.

**Note** You can use the **snmp-server view** command multiple times to create the same view record. If a view record for the same OID value is created multiple times, the latest entry of the object identifier takes precedence.

**Step 3** Exit global configuration mode.

- Step 4** (Optional) Display a view of the MIBs associated with SNMP by using the **show running-config snmp-server view** command.
- 

### Configuring Community Strings

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the device. Optionally, you can specify one or more of the following characteristics associated with the string:

- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

Perform the following steps to create or modify a community string:

#### Procedure

---

- Step 1** Enter global configuration mode.
- Step 2** Define the community access string.
- Note** You can configure one or more community strings.
- Step 3** Exit global configuration mode.
- Step 4** (Optional) Display the community access strings configured for the system with **show running-config snmp-server community**.
- 

### Configuring a Recipient of an SNMP Trap Operation

SNMP traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender does not know if the traps were received. However, an SNMP entity that receives an inform acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform can be sent again. Thus, informs are more likely to reach their intended destination.

To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you do not enter a **snmp-server host** command, no notifications are sent. If you enter the command without keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and type of notification, each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Perform the following steps to configure a device to send SNMP notifications:

**Procedure**

- 
- Step 1** Enter global configuration mode.
  - Step 2** Specify whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.
  - Step 3** Exit global configuration mode.
  - Step 4** (Optional) Display the SNMP notifications sent as traps, the version of SNMP, and the host IP address of the notifications using **show running-config snmp-server host**.
- 

**Specifying SNMP-Server Group Names**

You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Perform the following steps to specify a new SNMP group or a table that maps SNMP users to SNMP views:

**Procedure**

- 
- Step 1** Enter global configuration mode.
  - Step 2** Configure a new SNMP group on a remote device.
  - Step 3** Exit global configuration mode.
  - Step 4** (Optional) Display information about each SNMP group on the network using the **show running-config snmp-server group** command.
- 

**Configuring SNMP Server Users**

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

For the *priv-password* and *auth-password* arguments, the minimum length is eight characters, and should include both letters and numbers.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You must configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain text password or a localized MD5 digest.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain text password. The digest should be formatted as aabbccdd...ff where aa, bb, and cc are hexadecimal values. Also, the digest should be 16 octets for MD5 and 20 octets for SHA.




---

**Note** Changing the engine ID after configuring the SNMP user does not allow the removal of the user. To remove the configurations, you need to first reconfigure all the SNMP configurations.

---

Perform the following steps to add a new user to an SNMP group:

**Procedure**

- 
- Step 1** Enter global configuration mode.
  - Step 2** Configure the SNMP engine ID.
  - Step 3** Configure a new user to an SNMP group.
  - Step 4** Exit global configuration mode.
  - Step 5** (Optional) Display information about the configured characteristics of an SNMP user.
  - Step 6** (Optional) Display information about the SNMP engine ID configured for an SNMP user using the **show running-config snmp-server user** command.
- 

**Setting the Agent Contact, Location, and EngineID Information**

You can set the system contact, location, and engineID of the SNMP agent so that these descriptions can be accessed through the configuration file.

Perform the following steps, as required:

**Procedure**

- 
- Step 1** Enter global configuration mode.
  - Step 2** Set the system contact string.
  - Step 3** Set the system location string.
  - Step 4** Configure a name for local SNMP engine on CSP.
  - Step 5** Exit global configuration mode.
  - Step 6** (Optional) Display the contact strings configured for the system using **show running-config snmp-server contact** command.
  - Step 7** (Optional) Display the location string configured for the system using **show running-config snmp-server location** command.
  - Step 8** (Optional) Display the identification of the local SNMP engine configured on CSP using **show running-config snmp-server engineID** command.
- 

**Configuring SNMP Notifications**

Perform this task to configure the device to send traps or informs to CSP 2100 host.



- 
- Note** Many snmp-server commands use the keyword **traps** in their command syntax. Unless there is an option within the command to specify either traps or informs, the keyword **traps** should be taken to mean traps, informs, or both. Use the **snmp-server host** command to specify whether you want SNMP notifications to be sent as traps or informs.
-

### Procedure

---

- Step 1** Enter global configuration mode.
- Step 2** Specify the name of a local copy of SNMP.
- Step 3** Configure a local or remote user to be associated with the remote host created in Step 2.
- Note** You cannot configure a remote user for an address without first configuring the engine ID of the remote host. Otherwise, you receive an error message, and the command is not executed.
- Step 4** Configure an SNMP group.
- Step 5** Specify whether you want the SNMP notifications to be sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.
- The **snmp-server host** command specifies which hosts will receive SNMP notifications, and whether you want the notifications sent as traps or informs.
- Step 6** Enable sending of general SNMP notifications.
- Step 7** Exit global configuration mode.
- 

## Configuring SNMP Version 2

To configure SNMP version 2, do the following:

### Procedure

---

- Step 1** Use the default SNMP engine ID or modify the engine ID.
- Note** The engine ID can be modified only if you have not yet configured the SNMP community, group, or user. After configuring the SNMP community, group, or user, you cannot modify the engine ID.
- Step 2** Create an SNMP community.
- Step 3** Create an SNMP group with group version as **2**, group security level as **noAuthNoPriv**, and group context prefix as **snmp**.
- The group context prefix must be specified as **snmp**. No other value is supported for group context prefix.
- Step 4** Create an SNMP user. The name of this user must be exactly same as the community name created in Step 2 and the name of the user group must be exactly same as the group created in Step 3.
- 

## Configuring SNMP Version 3

To configure SNMP version 3, do the following:

### Procedure

---

- Step 1** Use the default SNMP engine ID or modify the engine ID.

**Note** The engine ID can be modified only if you have not yet configured the SNMP community, group, or user. After configuring the SNMP community, group, or user, you cannot modify the engine ID.

**Step 2** Create an SNMP group with group version as **3**, group security level as **authNoPriv** or **authPriv**, and group context prefix.

**Note** Starting with Release 2.2.2, you can specify any group context prefix. You can also configure null context to run an SNMPv3 query without specifying the context name. To configure the null context, use the `\"` character sequence. In Release 2.2.1 and earlier releases, only **snmp** prefix is supported with SNMPv3.

**Step 3** Create an SNMP user and specify the same group name as created in Step 2. In addition, specify the values for the following fields or parameters: **auth-protocol** (MD5 or SHA), **priv-protocol** (des or aes), and **passphrase**.

## SNMP Support Configuration

Configuration Mode	Description
Web Interface	Click <b>Administration &gt; SNMP</b> and then click on the relevant tabs to configure SNMP agent, group, community, users, and server (host).
CLI	Use the following SNMP commands: <ul style="list-style-type: none"> <li>• <b>snmp agent engineID</b> <i>engine_id</i></li> <li>• <b>snmp community name community-access</b> <i>community-access</i></li> <li>• <b>snmp group name group_context_prefix</b> {1   2   3} {noAuthNoPriv   authNoPriv   authPriv} <b>read</b> <i>readview</i> <b>write</b> <i>writeview</i> <b>notify</b> <i>notifyview</i></li> <li>• <b>snmp user username auth-protocol</b> {md5   sha} <b>priv-protocol</b> {aes   des} [<b>passphrase</b> <i>passphrase</i>] [<b>user-group</b> <i>groupname</i>] <b>user-version</b> {1   2   3}</li> <li>• <b>snmp host hostname host-ip-address</b> <i>ip_address</i> <b>host-version</b> <i>version</i> <b>host-security-level</b> <i>securitylevel</i> <b>host-user-name</b> <i>username</i> <b>host-port</b> <i>port</i></li> </ul>

Configuration Mode	Description
REST API	<p>Use the following REST APIs:</p> <ul style="list-style-type: none"> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp/agent -H "Content-type: application/vnd.yang.data+json" -d '{"engineID": "engine_id"}'</b></li> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp/communities -H "Content-Type: application/vnd.yang.data+json" -d '{"community": {"community-name": "name", "community-access": "access"}}'</b></li> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp/groups -H "Content-type: application/vnd.yang.data+json" -d '{"group": {"group-name": "name", "group-context-prefix": "group_context_prefix", "group-version": version, "security-level": "security-level", "read": "readview", "write": "writeview", "notify": "notifyview"}}'</b></li> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp/users -H "Content-Type: application/vnd.yang.data+json" -d '{"user": {"user-name": "username", "auth-protocol": "authprotocol", "priv-protocol": "privprotocol", "passphrase": "passphrase", "user-group": "groupname", "user-version": version}}'</b></li> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp/hosts -H "Content-Type: application/vnd.yang.data+json" -d '{"host": {"host-name": "hostname", "host-ip-address": "ip-address", "host-version": "version", "host-security-level": "securitylevel", "host-user-name": "username", "host-port": "port"}}'</b></li> </ul>

## SNMP Server Support Configuration

Configuration Mode	Description
Web Interface	Click <b>Administration &gt; SNMP</b> and then click on the relevant tabs to configure SNMP server agent, group, community, users, and host.



Configuration Mode	Description
CLI	<p>Use the following SNMP server commands:</p> <ul style="list-style-type: none"> <li>• <b>snmp-server contact</b> <i>contact-string</i></li> <li>• <b>snmp-server location</b> <i>location-string</i></li> <li>• <b>snmp-server view</b> <i>view-name oid-enum {included   excluded}</i></li> <li>• <b>snmp-server community</b> <i>community-name [ view view-name ] [ro   rw ]</i></li> <li>• <b>snmp-server engineID</b> {<b>local</b> <i>engineid-string</i>}</li> <li>• <b>snmp-server user</b> <i>user-id group-id [remote] {v1   v2c   v3 [encrypted] [auth {md5   sha} auth-password]} [priv {aes   des} priv-password] engineID engine-id</i></li> <li>• <b>snmp-server group</b> <i>group-name {v1   v2c   v3 {auth   noauth   priv}}</i> [ <i>read readview</i> ] [ <i>write writeview</i> ] [ <i>notify notifyview</i> ]</li> <li>• <b>snmp-server host</b><i>host-name [traps   informs] [ version {1  2c 3 {auth   noauth   priv } }]</i> <i>remote-id [ udp-port port-number]</i></li> <li>• <b>snmp-server enable traps</b> [<b>snmp</b> ]</li> </ul>

Configuration Mode	Description
REST API	<p>Use the following REST APIs:</p> <ul style="list-style-type: none"> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"contact" : "contact"}'</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"location" : "location"}'</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"view" : {"name" : "view-name", "rule" : [{"mibs" : "oid-enum-string", "included-opt" : "included/excluded"}]}'</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"community" : {"name" : "community-name", "view" : "view-name", "access" : "access-type"}'}</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"engineID" : {"local" : "engineID"}'}</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"user" : {"name" : "user-name", "group-name" : "group-name", "remote" : "remote-host", "encrypted" : "null string", "security-model" : "security-model", "auth" : "auth-protocol", "auth-password" : "auth-password", "priv" : "priv-protocol", "priv-password" : "priv-password", "engineID" : "engineID-string"}'}</b></li> <li>• <b>curl -ku user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"group" : {"name" : "group-name", "security-model" : "security-model", "security-level" : "security-level", "read" : "readview", "write" : "writeview", "notify" : "notifyview"}'}</b></li> <li>• <b>curl -u user:password -X POST</b>  <b>https://ip-address:port-number/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"name" : "name", "inform-type" : "inform-type", "version" : "version", "security-level" : "security-level", "username" : "username", "remote-community" : "remote-community", "udp-port" : "udp-port"}'}</b></li> </ul>

## Creating and Deleting Port Channels

### Creating a Port Channel

You can create a port channel by using the web interface, the CLI, or the REST APIs.

Configuration Mode	Description
Web Interface	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Configuration &gt; Port Channel</b>.</li> <li>2. Click the add (+) button.</li> <li>3. On the <b>Port Channel Configuration</b> page, in the <b>Port Channel Members</b> field, select at least two pNICs.</li> <li>4. Enter a name in the <b>Enter Port Channel Name</b> field.</li> <li>5. Enter a VLAN range in the <b>Enter VLAN Trunk Range</b> field.</li> <li>6. Choose a bond mode from the <b>Choose Bond Mode</b> drop-down list.</li> <li>7. Choose a LACP type from the <b>Choose LACP Type</b> drop-down list.</li> <li>8. Click <b>Submit</b>.</li> </ol>
CLI	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Create a port channel by using the <b>pnict portchannel_name</b> command.</li> <li>2. Assign two or more pNIC members to this port channel by using the <b>pnict name member_of portchannel_name</b> command.</li> </ol>
REST API	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Create a port channel by using the following REST API:  <pre>curl -u user:password -X POST https://ip-address:port-number/api/running/pnics -H "Content-type: application/vnd.yang.data+json" -d '{"pnict":{"name":"name", "type":"port_channel", "bond_mode":"bond_mode", "lact_type":"lact_type", "trunks":"vlan_num"}}'</pre> </li> <li>2. Assign two or more pNIC members to this port channel by using the following REST API:  <pre>curl -u user:password -X PATCH https://ip-address:port-number/api/running/pnics/pnictname -H "Content-type: application/vnd.yang.data+json" -d '{"pnict":{"member_of":"portchannel_name"}}'</pre> </li> </ol>

### Deleting a Port Channel

You can delete a port channel by using the web interface, the CLI, or the REST APIs.

Configuration Mode	Description
Web Interface	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Configuration &gt; Port Channel</b>.</li> <li>2. On the <b>Port Channel Configuration</b> page, under the <b>Action</b> column, click <b>Delete</b>.</li> <li>3. In the Port Channel Removal dialog box, click <b>Remove</b>.</li> </ol>
CLI	Do the following: <ol style="list-style-type: none"> <li>1. Unassign the pNICs assigned to a port channel by using the <b>pnict name no member_of</b> command.</li> <li>2. Delete the port channel by using the <b>no pnict portchannel_name</b> command.</li> </ol>
REST API	Do the following: <ol style="list-style-type: none"> <li>1. Unassign the pNICs assigned to a port channel by using the following REST API:  <code>curl -u user:password -X DELETE https://ip-address/api/running/pnics/pnict/name member_of</code> </li> <li>2. Delete the port channel by using the following REST API:  <code>curl -u user:password -X DELETE https://ip-address/api/running/pnics/pnict/name.</code> </li> </ol>

## Managing User Accounts

### Information About User Accounts

Cisco CSP supports the local and remote users. A local user is configured in the Cisco CSP and is authenticated by the Cisco CSP. A remote user is configured on a remote TACACS+ server and is authenticated by a configured TACACS+ server. If the same username is configured both locally and remotely, the remote TACACS+ server is used for authentication.




---

**Note** Only local users can log in to Cisco CSP by using CIMC console. Remote TACACS+ users cannot log in to Cisco CSP by using CIMC console.

---

### Supported User Groups

Cisco CSP provides the following user groups to configure role-based access control (RBAC):

- **admin-group:** The members of this group have complete read and write access to Cisco CSP. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is 15. The members of this group can do the following:
  - Create new users.

- Delete users.
- Modify existing users.
- Copy core, certificates, or log files to and from Cisco CSP.
- Create, delete, and manage services.
- Access all support commands.

The initial local user **admin** belongs to this group.

- **service-group**: The members of this group have complete read and write access to Cisco CSP services. For TACACS+ or RADIUS configuration, privilege level (priv-lvl) or class that is assigned to this user group is 7. The members of this group can do the following:
  - Create, delete, and manage services.
  - Change their own password.
  - Copy core or log files to and from Cisco CSP.
  - Access some of the support commands.
- **operator-group**: The members of this group have only read access to Cisco CSP. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is 1. The members of this group can change their own password and access limited number of support commands.
- **vnf-operator-group**: The members of this group have operator role access to CSP, and also have access to VNC console to log into VMs. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is a string with a vnf-operator-group name.
- **user-created-group**: A custom group that you can create. For TACACS+ and RADIUS configuration, privilege level (priv-lvl) or class that is assigned to this user group is a string with a group name.

## Rules for User Passwords

The user passwords must meet the following requirements:

- Must be 8 to 64 characters long.
- Must contain a digit.
- Must contain a special character. Following characters are allowed: "\_", "-", "@", "=", "+", "^", "#".
- Must contain an uppercase character and a lowercase character.
- Must not contain two or more repeating characters.
- Must not contain dictionary words.

## Configuring User Accounts

You can create, delete, or modify a user by using the web interface, the CLI, or the REST API.

Configuration Mode	Description
Web Interface	<p>To create a user, do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; User</b>.</li> <li>2. Click the add (+) button.</li> <li>3. Enter a name in the <b>User Name</b> field.</li> <li>4. Choose a group from the <b>User Group</b> drop-down list.</li> <li>5. Enter a password in the <b>Password</b> field.</li> <li>6. Enter the password again in the <b>Confirm Password</b> field.</li> <li>7. Click <b>Submit</b>.</li> </ol> <p>To modify or delete a user, under the <b>Action</b> column, click <b>Edit</b> or <b>Delete</b>.</p>
CLI	<p>To create or modify a user, use the <b>csp-users users user username password password group group</b> command.</p>
REST API	<p>To create a user, use the following REST API:</p> <pre><b>curl -u user:password -X POST</b> <b>https://ip-address:port-number/api/running/csp_users/users/user -H</b> <b>"Content-Type:application/vnd.yang.data+json" -d '{"user": {"name":</b> <b>"username", "Password":"Password", "group":"group"}}'</b></pre> <p>To modify a user, use the following REST API:</p> <pre><b>curl -u user:password -X PATCH</b> <b>https://ip-address:port-number/api/running/csp_users/users/user -H</b> <b>"Content-Type:application/vnd.yang.data+json" -d '{"user": {"name":</b> <b>"username", "Password":"Password", "group":"group"}}'</b></pre> <p>To delete a user, use the following REST API:</p> <pre><b>curl -u user:password -X DELETE</b> <b>https://ip-address:port-number/api/running/csp_users/users/user/username</b></pre>

## Configuring VNF User Groups

The CSP admin users can configure VNF user groups, add users to the VNF groups, and associate VNFs (service VMs) to those users. The users within VNF group have access to the VNFs associated with their groups and do not have access to other VNFs. You can create maximum of 10 VNF user groups.

You can create, delete, or modify a VNF user group by using the web interface, the CLI, or the REST API.

Configuration Mode	Description
Web Interface	<p>To create a user, do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; User</b>.</li> <li>2. Click the add (+) button.</li> <li>3. Enter a name in the <b>User Name</b> field.</li> <li>4. Choose a group from the <b>VNF User Group</b> drop-down list.</li> <li>5. Enter a password in the <b>Password</b> field.</li> <li>6. Enter the password again in the <b>Confirm Password</b> field.</li> <li>7. Click <b>Submit</b>.</li> </ol> <p>To modify or delete a user, under the <b>Action</b> column, click <b>Edit</b> or <b>Delete</b>.</p>
CLI	<p>To create or modify a VNF user group, use the <code>csp-users groups group groupname type grouptype</code> command.</p>
REST API	<p>To create a new VNF user group, use the following REST API:</p> <pre>curl -ku user:password -X POST https://ip-address:port-number/api/running/csp_users/groups -H "Content-Type:application/vnd.yang.data+json" -d '{"group": {"name": "VNF group name", "type": grouptype}}'</pre> <p>To associate with a VNF user group, use the following REST API:</p> <pre>curl -ku user:password -X POST https://ip-address:port-number/api/running/csp_users/groups -H "Content-Type:application/vnd.yang.data+json" -d '{"service": {"name": "VMname", "Power":"mode", "iso_name":"VMimage ", "vnf-group":"VNF user group"}}'</pre> <p>To delete a VNF user group, use the following REST API:</p> <pre>curl -ku user:password -X DELETE https://ip-address:port-number/api/running/csp_users/groups/group/group-name</pre>

## Recovering Password for the admin User

To recover the password for the **admin** user, do the following:

### Procedure

- Step 1** Using the CIMC KVM console, reboot Cisco CSP ISO image.  
The following menu is displayed.

```
Red Hat Enterprise Linux 7.2
Install CSP-2100
```

```
Test this media & install CSP-2100
Troubleshooting >
```

- Step 2** Choose **Troubleshooting**.
- Step 3** Choose **Rescue a CSP-2100 Password**.
- Step 4** Choose **Continue**.
- Step 5** Press **Return** to get a shell.
- Step 6** Run the **chroot /mnt/sysimage** command.
- Step 7** Run the **csp-2100-password-reset** command.  
This command resets the password to **admin**.
- Step 8** Enter **exit** twice.  
The CD-ROM is ejected and Cisco CSP is rebooted.
- Step 9** Log in to Cisco CSP by using the default credentials **admin/admin**.  
After you log in to Cisco CSP, you are prompted to enter a new password.
- Step 10** Enter a new password.
- Step 11** Retype the new password.  
You are connected to Cisco CSP and the following message is displayed:  
\*\*\*admin password has been changed\*\*\*
- 

## Saving and Loading Configurations

### Saving and Loading the Running Configuration

To save the running configuration and then load the saved configuration, do the following:

#### Procedure

---

- Step 1** Save the running configuration by using one of the following methods:
- **save config-file filename** command
  - **curl -u user:password -X POST https://ip-address:port-number/api/running/save-load/save -H "Content-Type: application/vnd.yang.data+json" -d '{"input":{"config-file":"filename"}}' REST API**
- The configuration file is saved in Cisco CSP repository.
- Step 2** Copy the ISO files, the banner files, and the saved configuration file to the repository of the Cisco CSP where the saved configuration is going to be loaded.
- Step 3** Load the saved configuration by using one of the following methods:
- **load config-file filename** command



- **curl -u user:password -X POST https://ip-address:port-number/api/running/save-load/load -H "Content-type: application/vnd.yang.data+json" -d '{"input": {"config-file": "filename"}}'** REST API

## Saving and Loading the Running Configuration with Service Data

To save the running configuration and then load the saved configuration along with the service data, do the following:

### Procedure

- Step 1** Save the running configuration by using one of the following methods:
- **save config-file filename** command
  - **curl -u user:password -X POST https://ip-address:port-number/api/running/save-load/save -H "Content-Type: application/vnd.yang.data+json" -d '{"input":{"config-file":"filename"}}'** REST API
- The configuration file is saved in Cisco CSP repository.
- Step 2** Set the power mode of the service that you want to export to off by using one of the following methods:
- **service name power off** command.
  - **curl -u user:password -X POST https://ip-address:port-number/api/running/services/service/name -H "Content-Type: application/vnd.yang.data+json" -d '{"service": {"power": "off"}}'** REST API
- Step 3** Export the service by using one of the following methods:
- **service name export exported\_service\_name exported\_name** command
  - **curl -u user:password -X POST https://ip-address:port-number/api/running/services/service/name/\_operations/export -H "Content-Type: application/vnd.yang.data+json" -d '{"input": {"exported\_service\_name": "exported\_name"}}'** REST API
- A file named *exported\_name.tar.gz* or *service\_name-clone.tar.gz* is created in Cisco CSP repository. It takes few minutes to create this file.
- Step 4** Copy the ISO files, the banner files, the exported service file, and the saved configuration file to the repository of Cisco CSP where the saved configuration is going to be loaded.
- Step 5** Edit the saved configuration file and specify the name of the exported service file in the *iso\_name* parameter of a service.
- Note** For all other parameters, specify the values that the exported service used.
- Step 6** Load the saved configuration by using one of the following methods:
- **load config-file filename** command

- **curl -u user:password -X POST https://ip-address:port-number/api/running/save-load/load-H "Content-type: application/vnd.yang.data+json" -d '{"input": {"config-file": "filename"}}' REST API**

## Configuring Clusters

### Guidelines for Cluster Configuration


The following are the guidelines and prerequisites for cluster configuration:

- The CSP cluster is a GUI feature, where you can configure two or more CSP nodes in a single cluster up to a maximum of 10 nodes.
- Cluster configuration through REST API and CLI are not supported for CSP version 2.5.0.
- Cluster configuration through REST API is supported for CSP version 2.8.0.
- A cluster on CSP can only be configured by the local user, admin.
- For every local user on cluster nodes, ensure that the passwords and usernames are same on every node in the cluster, otherwise cluster node creation or addition fails.
- For external TACACS or RADIUS users, ensure that you configure the same TACACS or RADIUS on all cluster nodes. However, if you do not configure the same TACACS or RADIUS, the cluster node creation or addition does not fail.
- Each CSP can be part of only one cluster at a time.
- Ensure to configure NTP on all cluster members for the lifetime of the cluster and the clock timezone should be the same across all nodes.
- To enable all cluster nodes share and access the same NFS storage, ensure to configure the NFS mount to the same storage location on all cluster nodes.
- The CSP cluster can be modified from any node in the cluster after creation.
- With the new cluster infrastructure, an upgrade from earlier CSP versions to CSP version 2.5.0 and later with cluster configured is not supported. You must delete the existing cluster prior to upgrade and recreate it after upgrading to CSP, Release 2.5.0 and later.
- All cluster members must be upgraded to the same version before starting to create a cluster.
- The admin users and externally authenticated TACAS and RADIUS users can perform a file copy between cluster members.
- The load option does not support adding cluster from configuration files prior to CSP, Release 2.5.0. Before loading the configuration, if the cluster configuration exists in the saved configuration file, the cluster configuration must be automatically deleted from the configuration file before applying it in 2.5.0 and later.
- To change the management IP of a CSP node in the cluster, remove the node from the cluster, change the management IP and then add the node back to the cluster.
- Ensure that each CSP node is reachable before and during cluster creation or addition of a node, otherwise the creation or addition process fails.

- If the cluster state for members goes to a failed state, the cluster state can be stabilized by deleting the member that is in failed state or deleting the cluster and recreating it.
- In a cluster with two members, if one of the members become unreachable, the cluster does not permit add operations. The cluster can recover either if the unreachable member becomes reachable, or if the cluster is deleted and reconfigured with another member.
- If **factory default reset** or **clean-install** operations are executed on a member of a cluster, the cluster configuration gets cleaned up from that member. After that CSP is brought up and is running, no cluster configuration is present on it. On the other members of the cluster, the node is still present in the cluster with its cluster state as "not\_present."
- The new nodes can only be added to a cluster if every node is in "deployed" state. If the nodes are not in "deployed" state, the only delete cluster or delete node operations can be performed on a cluster.
- For a cluster with two members, deleting one of the cluster members results in deletion of the entire cluster.
- A cluster uses default CA certificates for HTTPS communication across cluster nodes. If desired, the default CA certificates can be replaced by custom certificate, however the infrastructure requires that every node in the cluster have the certificate generated from the same CA to ensure connectivity
- If NAT is configured, ensure that only CSP management IP addresses are used to log in to the GUI. NAT addresses are not supported for cluster creation or modification operations.

## Creating Clusters

You can create a cluster by using the web interface and REST API.

Configuration Mode	Description
Web Interface	<p>To create a cluster, perform the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; Cluster</b>.</li> <li>2. In the Cluster configuration page, to create a new cluster, click .</li> <li>3. In the <b>Cluster Name</b> field, enter a string.</li> <li>4. In the <b>Number of Nodes</b> drop-down list, select the number of applicable nodes.</li> <li>5. In <b>Management IPs or FQDN</b>, enter the management IP of each node in the <b>Cluster Node</b> fields.  The local node is already populated with an IP address.</li> <li>6. Click <b>Create Cluster</b>.</li> </ol>
REST API	<p>To create a cluster, use the following REST API:</p> <pre>curl -ku user:password -X POST https:// ip-address:port-number /api/new_post_cluster/clusters -H "Content-Type: application/vnd.yang.data+json" -d '{"cluster" : [{"name": " name, "nodes":{"node":[{"member_ip": member_ip },{ "member_ip": member_ip }]}]}'</pre>

## Deleting Clusters

You can delete a cluster by using the web interface and REST API.

Configuration Mode	Description
Web Interface	<p>To delete a cluster, perform the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; Cluster &gt; .</b></li> <li>2. In the Cluster configuration page, to delete a cluster, click <b>Delete Cluster</b> at the right side.</li> </ol> <p><b>Note</b> You cannot delete a cluster, if VMs are deployed in gluster.</p>
REST API	<p>To delete a cluster, use the following REST API:</p> <pre>curl -ku user:password -X POST https://ip-address:port-number /api/delete_cluster/ name -H "Content-Type:application/vnd.yang.data+json"</pre>

## Adding Nodes to Cluster

You can add node to a cluster by using the web interface and REST API.

Configuration Mode	Description
Web Interface	<p>To add a node to the cluster, perform the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; Cluster</b>.</li> <li>2. In the Cluster configuration page, to add a node, click <b>+</b> under the cluster name.</li> <li>3. In the Add Cluster Member page, enter a value for the <b>Number of Nodes</b> that should be added to the existing cluster.</li> <li>4. In <b>Management IPs or FQDN</b>, enter the management IP for each node in the <b>Cluster Node</b> field.</li> <li>5. Click <b>Add Node</b>.</li> </ol>
REST API	<p>To add a node, use the following REST API:</p> <pre>curl -ku user:password /api/add_cluster_node/running/clusters -H "Content-Type:application/vnd.yang.data+json" -d '{"cluster":{"name": name, "nodes":{"node":{"memeber_ip" : member_ip}}}}'</pre>

## Deleting Nodes from Cluster

You can delete nodes to a cluster by using the web interface and REST API.

Configuration Mode	Description
Web Interface	To delete a cluster, perform the following: <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; Cluster</b>.</li> <li>2. In the Cluster configuration page, to delete a node from a cluster, click the <b>Action</b> icon against a node, and choose <b>Delete</b> for the node that you want to remove from the cluster.</li> </ol>
REST API	To delete a node, use the following REST API: <b>curl -ku user:password /api/delete_cluster_node/name /ip-addresss -H "Content-Type:application/vnd.yang.data+json"</b>

## Copying Files between Cluster Members

### Procedure

- 
- Step 1** Create a cluster. See [Creating Clusters, on page 27](#).
- Step 2** Click **Configuration > Repository**.
- Step 3** Click the **Action** icon against the file row that needs to be copied, and choose either **Copy To** or **Copy From** depending on the file destination.
- 

## Replacing Node from Cluster

To replace a node when a CSP device needs to go through an RMA process, please contact Cisco Technical Assistance Center (TAC).


## Enabling Storage Virtualization

Storage virtualization is an add-on functionality to the existing cluster functionality. You can enable the storage virtualization using the web interface.

Ensure that you note the following points before enabling storage virtualization:

- To enable storage network, ensure to add a minimum of three nodes to a cluster.
- A maximum of one node failure in a cluster is supported.
- Distributed storage network isn't available on nodes; 5, 7, and 9 of a cluster.


You can enable the storage virtualization by using the web interface and REST API.

Configuration Mode	Description
Web Interface	<p>To enable the storage virtualization using the web interface, perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Administration &gt; Cluster</b>.</li> <li>2. In the Cluster configuration page, to create a new cluster, click .</li> <li>3. In the <b>Cluster Name</b> field, enter a string.</li> <li>4. In the <b>Number of Nodes</b> drop-down list, select the number of applicable nodes.</li> <li>5. In <b>Management IPs or FQDN</b> enter the management IP of each node in the <b>Cluster Node</b> fields.</li> <li>6. In the <b>Cluster Advance Setting</b>, check <b>Enable Storage Network</b>. You can replace the cluster nodes after the storage network is enabled. However, you cannot add or delete cluster nodes when the storage network is enabled.</li> <li>7. In the <b>Gluster Disk Allocation</b>, enter the <b>Gluster Disk Allocation Capacity</b> in percentage. The default disk capacity value is 80% and the remaining disk capacity is allocated for the local storage.</li> <li>8. Click <b>Create Cluster</b>.</li> </ol>
REST API	<p>To enable the storage virtualization, use the following REST API:</p> <pre>curl -ku user:password -X POST https:// ip-address:port-number /api/new_post_cluster/running/clusters -H "Content-Type:application/vnd.yang.data+json" -d '{"cluster":{"name":"name","enable-storage-network": enable-storage-network,"gluster-disk-allocation": gluster-disk-allocation,"nodes":{"node":[{"member_ip": member_ip },{ "member_ip": member_ip } {"member_ip": member_ip } ]}}}'</pre>

## Deploying a Service in Gluster

To deploy a service in gluster, perform the following steps:

### Procedure

- 
- Step 1** Click the **Configuration** tab and then choose **Services**.
- Step 2** In the **Service** page, click .
- Step 3** From the **Target Host Name** drop-down list, choose the target host.
- Step 4** From the **Image Name** drop-down list, choose an image file for the service.
- You can use an ISO, OVA, QCOW, tar.gz or zip file to create the service.

- Step 5** In the **Number of Cores** field, specify the number of cores. Make sure that the new value does not exceed the available resources.
- Step 6** In the **RAM (MB)** field, specify the RAM. Make sure that the new value does not exceed the available resources.
- Step 7** In the **Disk Space (GB)** field, specify the disk space. Make sure that the new value does not exceed the available resources.
- Step 8** In the **Disk Type** field, specify the disk type. Valid choices are IDE or VIRTIO.
- Step 9** In the **Disk Storage** field, select **Gluster** to deploy a service in gluster.

## Node Failure Detection and Migration of VNFs to Alive Node

With node level redundancy in a cluster, if a node in a CSP is down, you can detect the node failure and then automatically deploy all the VNFs in the failed node to the other live nodes in a cluster.

### Procedure

- Step 1** To detect a node failure, click **Dashboard > Overview**  
Under Cluster resources section, you can view the status of each of the nodes.
- Step 2** To deploy all VNFs in the failed node to other live nodes, click **Administration > Cluster**.
- Step 3** In the CSP Cluster page, to add a cluster member, click the add (+) button.
- Step 4** In the Add Cluster Member page, provide the values for number of nodes, cluster node 1 name or IP.
- Step 5** Under the Advance Setting section, to enable node level redundancy for the new cluster, check **Enable Node Redundancy**.  
To enable node redundancy for an existing cluster, check **Enable Node Redundancy** for a node name or IP. You can enable node redundancy for an existing cluster using REST API. For more information, see the *Cisco Cloud Services Platform REST API Guide*.
- Step 6** Set **Eviction Timeout** in seconds.  
By setting the timeout, the eviction of VMs on the down node does not begin until the timeout expires.  
**Note** The VMs are not deployed on a node that has a VM High Availability pair.
- Step 7** To enable distributed storage network, check **Enable Storage Network**. Enter the **Gluster Disk Allocation** in percentage.  
The VNFs are deployed in the gluster location using the distributed storage network for the cluster.  
**Note** The default disk capacity value of the gluster is 80% and the remaining disk capacity is allocated for the local storage.  
You can recover the VNFs deployed in the gluster location during Day-N configuration, when the storage network is enabled. You can enable storage network for an existing cluster using REST API. For more information, see the *Cisco Cloud Services Platform REST API Guide*.
- Step 8** Click **Create**.
- Step 9** To view the migration of deploying VNFs in a failed node to a live node, click **Dashboard > Cluster Redundancy > Migration Report**.

Ensure that there are a minimum of three nodes in a cluster to enable the node level redundancy functionality.

- Step 10** During upgrade, delete the cluster, and recreate it when all nodes are upgraded.  
For VMs in HA mode, you must configure ha-key to include two VMs in HA.

---

### What to do next

If a node in a cluster is down, and cluster settings are edited, the affected node cannot synchronize with the latest cluster settings. To avoid this issue, edit cluster settings only when all nodes in a cluster are up and working. If a node is down, delete that node from the cluster. All nodes in a cluster should have same settings for cpu-pinning and ovs-dpdk. For detailed information about these commands, see the *Cisco Cloud Services Platform Command Reference Guide*.

## On Demand VNF Migration

For the services deployed in gluster, the VMs in the powered off or shut down mode with Day-N configuration are migrated between the cluster nodes on demand. You can migrate the VNF service to any other node of the cluster or enable **Auto Selection** to allow the CSP to select the available node in the cluster for migration.

To enable on demand VNF migration, perform the following steps:

### Procedure

- 
- Step 1** Click the **Configuration** tab, and choose **Services**.  
The **Service Configuration** page appears.
- Step 2** In the **Service configuration** page, click the **Action** icon against a deployed service, and choose **Migrate VM**.  
The **Virtual Service Migration** page appears.
- Step 3** In the **Virtual Service Migration** page, from the **Destination Host IP** drop-down list:
- **Auto Selection**—Allows the CSP to select the available node in the cluster.
  - **IP address**—Enables you to select from the available IP address list.

**Note** If storage virtualization is enabled and the VNF service is deployed in gluster, then the VNF service is migrated with Day-N configuration, otherwise the VNF service is migrated with day-0 configuration.

---

## Monitoring VM

Cisco CSP supports VM monitoring. When you bring up VNF, you can configure the monitoring service to monitor the VNF by verifying that it is responding to a ping. During failure, monitoring service can be configured to recover the VM by rebooting the VNF.



## Guidelines for VM Monitoring Support

Following are the guidelines for configuring the VM monitoring support:

- VM IP config is mandatory if monitoring is enabled.
- VM must have L3 connectivity from CSP management interface.
- VM IP can be edited without powering off the VNF, whereas other VM monitoring parameters can be edited after powering off the VM.
- VM monitoring can be paused or resumed for a VM that has monitoring enabled, and is powered on.
- The monitoring status can be viewed in the services page on the web interface or the show service command on the CLI.

## VM Monitoring Support Configuration

Configuration Mode	Description
Web Interface	To configure monitoring for a particular VNF, perform the following: <ol style="list-style-type: none"> <li>1. Click <b>Configuration &gt; Services</b>.</li> <li>2. On the <b>Service</b> page, click the add (+) button. The <b>Create Service page</b> is displayed.</li> <li>3. On the <b>Create Service page</b>, configure VM monitoring configuration as part of the service creation.</li> <li>4. To view the VM details, click the <b>VM Name</b> and expand the VM details.</li> <li>5. View the operational status of monitoring for a VM under <b>VM Monitoring</b>.</li> </ol>
CLI	To monitor the VNF, configure the monitoring service by using the Service command. For information about the VM monitoring command, see the Cisco Cloud Services Platform Command Reference Guide.
REST API	For VM monitoring, use the Services API. For information about the VM monitoring REST API, see the Cisco Cloud Services Platform REST API Guide.

