Configure Cisco SD-WAN Cloud onRamp for Colocation Solution Devices Using Cisco vManage

Add Cloud OnRamp Colocation Devices Using Cisco vManage

You can add CSP devices, switch devices, and VNFs using Cisco vManage. When you order the Cisco SD-WAN Cloud onRamp for Colocation solution product identifier (PID), the device information is available from the smart account that can be accessed by Cisco vManage.

Before you begin

Ensure that the setup details are as follows:

- Cisco SD-WAN setup details such as, Cisco vManage IP address and credentials, Cisco vBond IP address and credentials
- NFVIS setup details such as, Cisco CSP device CIMC IP address and credentials or UCSC CIMC IP address and credentials
- Able to access both the switch consoles

Step 1 From the Cisco vManage menu, choose **Tools** > **SSH Terminal** to start an SSH session with Cisco vManage.

Step 2 Choose a CSP device or a switch device.

Step 3 Enter the username and password for the CSP device or switch device, and click **Enter**.

Step 4 Get the PID and serial number (SN) of a CSP device.

The following sample output shows the PID for one of the CSP devices.

```
CSP# show pl
platform-detail hardware_info Manufacturer "Cisco Systems Inc"
platform-detail hardware_info PID CSP-5444
platform-detail hardware_info SN WZP224208MB
platform-detail hardware_info hardware-version 74-105773-01
platform-detail hardware_info UUID da39edec-d831-e549-b663-9e407afd5ac6
platform-detail hardware_info Version 4.6.0-15
```

The output shows both the CSP device PID and serial number.

Step 5 Get the serial number of both the Catalyst 9500 switch devices.

The following sample shows the serial number of the first switch.

```
Switch1# show version
Cisco IOS XE Software, Version 17.03.03
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 26-Feb-21 02:01 by mcpre
Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                  Technology-package
Current                       Type                     Next reboot
------------------------------------------------------------------------------
network-advantage    Smart License                  network-advantage
dna-advantage        Subscription Smart License     dna-advantage
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C9500-40X (X86) processor with 1331521K/6147K bytes of memory.
Processor board ID FCW2229A0RK
1 Virtual Ethernet interface
96 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-1:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-1:.

Base Ethernet MAC Address          : 00:aa:6e:f3:02:00
Motherboard Assembly Number        : 73-18140-03
Motherboard Serial Number          : FOC22270RF8
Model Revision Number              : D0
Motherboard Revision Number        : B0
Model Number                       : C9500-40X
System Serial Number               : FCW2229A0RK
CLEI Code Number                   :
```

From this output, you can know the Catalyst 9500 switch series and the serial number.

Step 6 Create a .CSV file with the PID and serial number records for all the CSP devices and Catalyst 9500 switches in a colocation cluster.

For example, from the information available from Steps 4,5, the CSV-formatted file can be as follows:

```
C9500-40,FCW2229A0RK CSP-5444,SN WZP224208MB
```

Note You can create a single .CSV file for all devices in a colocation cluster.

Step 7 Upload all the CSP and switch devices using Cisco vManage. For more information, see Uploading a device authorized serial number file.

After upload, you can see all the CSP and switch devices listed in the table of devices.

Delete Cloud OnRamp for Colocation Devices from Cisco vManage

To delete the CSP devices from Cisco vManage, perform the following steps:

Before you begin

Ensure that you consider the following:

- If any service chains are attached to a device that is deleted, detach service groups. See Attach or Detach a Service Group in a Cluster, on page 56.
- If a CSP device that is being deleted is hosting Cisco Colo Manager, see Recovery of Cisco Colo Manager.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Certificates**.

Step 2 For the desired device, click **…** and choose **Invalid**.

Step 3 In the **Configuration** > **Certificates** window, click **Send to Controller**.

Step 4 In the **Configuration** > **Devices** window, for the desired device, click **…** and choose **Delete WAN Edge**.

Step 5 Click **OK** to confirm the deletion of the device.

Deleting a device removes the serial and chassis numbers from the **WAN edge router serial number** list, and also permanently removes the configuration from Cisco vManage.

Manage Clusters in Cisco vManage

Use the Cloud onRamp for Colocation screen to configure a colocation cluster and service groups that can be used with the cluster.

The three steps to configure are:

- Create a cluster. See Create and Activate Clusters, on page 6.
- Create a service group. See Create Service Chain in a Service Group, on page 33.
- Attach a cluster with a service group. See Attach or Detach a Service Group in a Cluster, on page 56.

A colocation cluster is a collection of two to eight CSP devices and two switches. The supported cluster templates are:

- Small cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+2 CSP
- Medium Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+4 CSP
- Large Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+6 CSP
- X-Large Cluster—2 Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C+8 CSP

Note Ensure that you add a minimum of two CSP devices one-by-one to a cluster. You can keep adding three, four, and so on, up to a maximum of eight CSP devices. You can edit a Day-N configuration of any cluster, and add pairs of CSP devices to each site up to a maximum of eight CSP devices.

Ensure that all devices that you bring into a cluster have the same software version.

Note You can't use the CSP-5444 and CSP-5456 devices in the same cluster.

Following are the cluster states:

- Incomplete—When a cluster is created from the Cisco vManage interface without providing the minimum requirement of two CSP devices and two switches. Also, cluster activation is not yet triggered.
- Inactive—When a cluster is created from the Cisco vManage interface after providing the minimum requirement of two CSP devices and two Switches, and cluster activation is not yet triggered.
- Init—When the cluster activation is triggered from the Cisco vManage interface and Day-0 configuration push to the end devices is pending.
- Inprogress—When one of the CSP devices within a cluster comes up with control connections, the cluster moves to this state.
- Pending—When the Day-0 configuration push is pending or VNF install is pending.
- Active—When a cluster is activated successfully and NCS has pushed the configuration to the end device.
- Failure—If Cisco Colo Manager has not been brought up or if any of the CSP devices that failed to receive an UP event.

A cluster transitioning to an active state or failure state is as follows:

- **Inactive** > **Init** > **Inprogress** > **Pending** > **Active**—Success
- **Inactive** > **Init** > **Inprogress** > **Pending** > **Failure**—Failure

During a cluster creation, cluster clearing, and cluster deletion, ensure that you clean the configurations of both switches. See Troubleshoot Catalyst 9500 Issues for more information about cleaning switch configuration that has been used previously.

Provision and Configure Cluster

This topic describes about activating a cluster that enables deployment of service chains.

To provision and configure a cluster, perform the following:

1. Create a colocation cluster by adding two to eight CSP devices and two switches.

   CSP devices can be added to a cluster and configured using Cisco vManage before bringing them up. You can configure CSP devices and Catalyst 9K switches with the global features such as, AAA, default user (admin) password, NTP, syslog, and more.

2. Configure colocation cluster parameters including IP address pool input such as, service chain VLAN pool, VNF management IP address pool, management gateway, VNF data plane IP pool, and system IP address pool.

3. Configure a service group.

   A service group consists of one or more service chains.

Note You can add a service chain by selecting one of the predefined or validated service chain template, or create a custom one. For each service chain, configure input and output VLAN handoff and service chain throughput or bandwidth, as mentioned. The service chain is configured in Mbps, and you can assign as high as 10 Gbps, and as low as 10 M. The default service chain bandwidth is 10 Mbps. See the Ordering and Sizing of Network Hub Devices topic.

4. Configure each service chain by selecting each VNF from the service template. Choose a VNF image that is already uploaded to the VNF repository to bring up the VM along with required resources (CPU, memory, and disk). Provide the following information for each VNF in a service chain:

   - The specific VM instance behavior such as, HA, shared VM can be shared across service chains.
   - Day-0 configuration values for tokenized keys and not part of the VLAN pool, management IP address, or data HA IP address. The first and last VMs handoff-related information such as peering IP and autonomous system values must be provided. The internal parameters of a service chain are automatically updated by Cisco vBond Orchestrator from the VLAN, or Management, or Data Plane IP address pool provided.

5. Add the required number of service chains for each service group and create the required number of service groups for a cluster.

6. To attach a cluster to a site or location, activate the cluster after all configuration is complete.

   You can watch the cluster status change from In progress to active or error in the **Task View** window.

To edit a cluster:

1. Modify the activated cluster by adding or deleting service groups or service chains.

2. Modify the global features configuration such as, AAA, system setting, and more.

You can predesign a service group and service chain before creating a cluster. You can then attach the service group with a cluster after the cluster is active.

Create and Activate Clusters

This topic provides the steps on how you can form a cluster with CSP devices, Cisco Catalyst switches as a single unit, and provision the cluster with cluster-specific configuration.

Before you begin

- Ensure that you synchronize the clocks for Cisco vManage and CSP devices. To synchronize a clock for CSP devices, configure the NTP server for CSP devices when you enter information about cluster settings.
- Ensure that you configure the NTP server for Cisco vManage and Cisco vBond Orchestrator. To configure the NTP server, see the Cisco SD-WAN System and Interface Configuration Guide.
- Ensure that you configure the OTP for the CSP devices to bring up the CSP devices.
- Ensure that you power on both the Catalyst 9500 switches and ensure that they are operational.

Step 1 From the Cisco vManage menu, choose Cisco vManage, click **Configuration** > **Cloud OnRamp for Colocation**.

a) Click **Configure & Provision Cluster**.

b) Provide the following information:

Table 1: Cluster Information

Field	Description
Cluster Name	The cluster name can contain 128 alphanumeric characters.
Description	The description can contain 2048 alphanumeric characters.
Site ID	The overlay network site identifier. Ensure that the value you enter for Site ID is similar to the organizations Site ID structure for the other Cisco SD-WAN overlay elements.
Location	The location can contain 128 alphanumeric characters.
Cluster Type	To configure a cluster in a multitenant mode so that it can be shared across multiple tenants, choose **Shared**. **Note** In the single-tenant mode, the cluster type **Non Shared** is selected by default.

c) To configure switches, click a switch icon in the **Switches** box. In the **Edit Switch** dialog box, enter a switch name and choose the switch serial number from the drop-down list. Click **Save**.

The switch name can contain128 alphanumeric characters.

The switch serial numbers that you view in the drop-down list are obtained and integrated with Cisco vManage using the PnP process. These serial numbers are assigned to switches when you order Cisco SD-WAN Cloud onRamp for Colocation solution PID on the CCW and procure the switch devices.

Note You can keep the serial number field blank for switch devices and CSP devices, design your colocation cluster, and then edit the cluster later to add the serial number after you procure the devices. However, you can't activate a cluster with the CSP devices or switch devices without the serial numbers.

d) To configure another switch, repeat Step c.
e) To configure CSP devices, click a CSP icon in the **Appliances** box. The **Edit CSP** dialog box is displayed. Provide a CSP device name and choose the CSP serial number from the drop-down list. Click **Save**.

The CSP device name can contain 128 alphanumeric characters.

f) Configure OTP for the CSP devices to bring up the devices.
g) To add remaining CSP devices, repeat Step e.
h) Click **Save**.
After you create a cluster, on the cluster configuration window, an ellipsis enclosed in a yellow circle appears next to a device where the serial number isn't assigned for the device. You can edit a device to enter the serial numbers.
i) To edit a CSP device configuration, click a CSP icon, and perform the process mentioned in substep e.
j) To set the mandatory and optional global parameters for a cluster, on the cluster configuration page, enter the parameters for **Cluster Configuration**. See Cluster Configuration, on page 7.
k) Click **Save**.

You can view the cluster that you created in a table on the cluster configuration page.

Step 2 To activate a cluster,

a) Click a cluster from the cluster table.
b) For the desired cluster, click **…** and choose **Activate**.

When you activate the cluster, Cisco vManage establishes a DTLS tunnel with the CSP devices in the cluster, where it connects with the switches through Cisco Colo Manager. When the DTLS tunnel connection is running, a CSP device in the cluster is chosen to host the Cisco Colo Manager. Cisco Colo Manager starts up and Cisco vManage sends global parameter configurations to the CSP devices and Cisco Catalyst 9500 switches. For information about cluster activation progress, see Progress of Cluster Activation, on page 18.

Note In Cisco vManage Release 20.7.x and earlier releases, the Cisco Colo Manager (CCM) and CSP device configuration tasks time out 30 minutes after the tasks are created. In the case of long-running image installation operations, these configuration tasks may time out and fail, while the cluster activation state continues to be in a pending state.

From Cisco vManage Release 20.8.1, the CCM and CSP device configuration tasks time out 30 minutes after the last heartbeat status message that Cisco vManage received from the target devices. With this change, long-running image installation operations do not cause configuration tasks to fail after a predefined interval of time after task creation.

Cluster Configuration

The cluster configuration parameters are:

Login Credentials

1. On the **Cluster Topology** window, click **Add** next to **Credentials**. In the **Credentials** configuration window, enter the following:
   - (Mandatory) Template Name—The template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.
2. Click **New User**.
   - In the **Name** field, enter the username.
   - In the **Password** field, enter the password and confirm the password in the **Confirm Password** field.
   - In the **Role** drop-down list, select administrators.
3. Click **Add**.

   The new user with username, password, and role with action appears.
4. Click **Save**.

   The login credentials for the new user are added.
5. To cancel the configuration, click **Cancel**.
6. To edit the existing credential for the user, click **Edit** and save the configuration.

Resource Pool

Table 2: Feature History

Feature Name	Release Information	Description
Day-N Expansion of Cluster Resource Pools	Cisco vManage Release 20.9.1 Cisco NFVIS Release 4.9.1	This feature supports editing resource pool parameters when the cluster state is active.

Note Starting from Cisco vManage Release 20.9.1 you can edit resource pool parameters when the cluster state is active. This feature only supports expansion of active Day-N cluster resource pools. Reduction of IP and VLAN pools are not supported. All the IP Pools except the VNF Management IP Pool can have new subnets added in day-N edit.

You cannot edit the following fields: **Name**, **Description**, **Management Subnet Gateway**, **Management Mask**, and **Switch PNP Server IP**.

1. On the **Cluster Topology** window, click **Add** next to **Resource Pool**. In the **Resource Pool** configuration window, enter values for the following fields:
   - Name—The name of the IP address pool should contain 128 alphanumeric characters.
   - Description—The description can contain 2048 alphanumeric characters.

2. In the **DTLS Tunnel IP** field, enter the IP addresses to be used for the DTLS tunnel. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 172.16.0.180-172.16.255.190).
3. In the **Service Chain VLAN Pool** field, enter the VLAN numbers to be used for service chains. To enter multiple numbers, separate them by commas. To enter a numeric range, separate the numbers with a hyphen (for example, 1021-2021).

   Consider the following points when entering the VLAN information:

   1002-1005 are the reserved VLAN values, and they shouldn't be used in the cluster creation VLAN pool.

Note Valid VNF VLAN pool: 1010-2000 and 1003-2000

Invalid: 1002-1005 (shouldn't be used)

Caution 1002-1005 isn't allowed for configuration. The VLANs tht are allowed should be contiguous.

Example: Enter data VLAN pool as 1006-2006. Ensure that this VLAN range isn't used in the Input/Output VLAN during service chain creations.

4. In the **VNF Data Plane IP Pool** field, enter the IP addresses to be used for auto configuring data plane on a VNF interface. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 10.0.0.1-10.0.0.100).
5. In the **VNF Management IP Pool** field, enter the IP addresses to be used for the VNF. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 192.168.30.99-192.168.30.150).

Note These addresses are IP addresses for secure interfaces.

6. In the **Management Subnet Gateway** field, enter the IP address of the gateway to the management network. It enables DNS to exit the cluster.
7. In the **Management Mask** field, enter the mask value for the failover cluster. For example, /24 and not 255.255.255.0
8. In the **Switch PNP Server IP** field, enter the IP address of the switch device.

Note The IP address of the switch is automatically fetched from the management pool, which is the first IP address. You can change it if a different IP address is configured in the DHCP server for the switch.

9. Click **Save**.

Port Connectivity

Table 3: Feature History

Feature Name	Release Information	Description
Support for SVL Port Configuration on 100G Interfaces	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1 Cisco NFVIS Release 4.8.1	With this feature, you can configure SVL ports on 100-G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.
Common Port Channel for Ingress and Egress Traffic	Cisco vManage Release 20.9.1 Cisco NFVIS Release 4.9.1	This feature introduces a common port channel for ingress and egress traffic from the time of creation of a colocation cluster. This feature facilitates an uninterrupted traffic flow by bringing all connected member links into a single port channel, which in turn load balances the traffic. The ingress port number is used to create a single port channel.

Common Port Channel for Ingress and Egress Traffic

In Cisco vManage Release 20.8.1 and earlier releases the ingress and egress port channels are separate. You can use the same VLAN for both ingress and egress port channels and service chanining. This results in Spanning Tree Protocol (STP) loop and shuts down one of the port channel causing traffic disruption.

Starting from Cisco vManage Release 20.9.1 a single port channel is used for ingress and egress traffic in Stackwise Virtual Switch Link (SVL) switches. If you create and activate the cluster or upgrade the cluster to Cisco vManage Release 20.9.1, Cisco Colocation Manager will automatically combine the two port channels to a single port channel. After the upgrade or activation of the cluster, both the ingress and egress VLAN handoffs are configured in a single port channel. When you create a cluster in Cisco vManage, you can continue to select the respective ports for ingress and egress. This feature facilitates an uninterrupted traffic flow by bringing all connected member links into a single port channel, which in turn load balances the traffic.

After you upgrade to Cisco vManage Release 20.9.1 ensure that you change the topology configuration for devices such as Cisco 1000 Series Aggregation Services Routers or Cisco Nexus 9000 Series Switches to bundle all the four links into a single port-channel using Link Aggregation Group (LAG) and configure VLANs appropriately. You can continue to add both the ingress and egress ports in Cisco vManage and the software will combine it into a single port channel in the backend before sending to the device.

The following is a sample configuration that combines the four links into a single port-channel:

```
switch1#show running-config int twe1/0/35

interface TwentyFiveGigE1/0/35
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe2/0/35
Building configuration...
```

```
Current configuration : 177 bytes
!
interface TwentyFiveGigE2/0/35
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe1/0/37
Building configuration...

Current configuration : 177 bytes
!
interface TwentyFiveGigE1/0/37
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end

switch1#show running-config int twe2/0/37
Building configuration...

Current configuration : 177 bytes
!
interface TwentyFiveGigE2/0/37
description vManaged-SVL Complete
switchport trunk allowed vlan 2001-2004,3001-3004
switchport mode trunk
channel-group 35 mode active
end
```

You will see the following warning in the Cisco vManage screen:

Starting from 20.9.1, Single port channel with members of I & E (four interfaces) will be formed and configured with both Ingress/Egress VLAN handoffs of the service chains - Please make sure the next hop device (router.switch) configuration matches the port channel config and VLAN config when activating or upgrading the cluster to 20.9.1.

Prerequisites for Configuring SVL and Uplink Ports

- When configuring the SVL and uplink ports, ensure that the port numbers you configure on Cisco vManage match the physically cabled ports.
- Ensure that you assign serial numbers to both the switches. See Create and Activate Clusters.

Configure SVL and Uplink Ports

- On the **Cluster Topology** window, click **Add** next to **Port Connectivity**.

  In the **Port Connectivity** configuration window, both the configured switches appear. Hover over a switch port to view the port number and the port type.

Change Default SVL and Uplink Ports

Before you change the default port number and port type, note the following information about Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches:

- From Cisco vManage Release 20.8.1, you can configure two SVL ports and one Dual-Active Detection (DAD) port when creating a colocation cluster with two Cisco Catalyst 9500-40X switches or two Cisco Catalyst 9500-48Y4C switches.
- To ensure that SVL and DAD ports are configured correctly for Cisco Catalyst 9500-48Y4C switches, note the following information:
  - Configure the SVL ports on same-speed interfaces, that is, either 25-G interfaces or 100-G interfaces. Ensure that both switches have the same configuration.
  - Configure the DAD port only on 25-G interfaces on both switches.
  - In case of an existing cluster, you can change the SVL ports only if it is inactive.
  - A cluster created in releases earlier than Cisco vManage Release 20.8.1 automatically displays two SVL ports and one DAD port after the upgrade to Cisco vManage Release 20.8.1.
- In case of Cisco Catalyst 9500-40X switches, you must configure the SVL and DAD ports on 10-G interfaces on both switches.
- The following are the default SVL, DAD, and uplink ports of Cisco Catalyst 9500 switches:

  Cisco Catalyst 9500-40X

  - SVL ports: Te1/0/38-Te1/0/39, and Te2/0/38-Te2/0/39

    In Cisco vManage Release 20.7.x and earlier releases, the default SVL ports are Te1/0/38-Te1/0/40 and Te2/0/38-Te2/0/40.
  - DAD ports: Te1/0/40 and Te2/0/40
  - Uplink ports: Te1/0/36, Te2/0/36 (input VLAN handoff), Te1/0/37, and Te2/0/37 (output VLAN handoff)

  Cisco Catalyst 9500-48Y4C

  - SVL ports: Hu1/0/49-Hu1/0/50 and Hu2/0/49-Hu2/0/50

    In Cisco vManage Release 20.7.x and earlier releases, the default SVL ports are Twe1/0/46-Twe1/0/48 and Twe2/0/46-Twe2/0/48.
  - DAD ports: Twe1/0/48 and Twe2/0/48
  - Uplink ports: Twe1/0/44, Twe2/0/44 (input VLAN handoff), Twe1/0/45, and Twe2/0/45 (output VLAN handoff) for 25-G throughput.
- I, E, and S represent the ingress, egress, and SVL ports, respectively.
- Ensure that the physical cabling is the same as the default configuration, and click **Save**.

To change the default ports when the connectivity is different for SVL and uplink ports, perform the following:

1. If both the switches are using the same ports:
   a. Click a port on a switch that corresponds to a physically connected port.
   b. To add the port configuration to the other switch, check the **Apply change** check box.

   If both the switches aren't using the same ports:

a. Click a port on **Switch1**.

b. Choose a port type from the **Port Type** drop-down list.

c. Click a port on **Switch2** and then choose the port type.

2. To add another port, repeat step 1.
3. Click **Save**.
4. To edit port connectivity information, in the **Cluster Topology** window, click **Edit** next to **Port Connectivity**.

Note You can modify the SVL and uplink ports of a cluster when the cluster hasn't been activated.

5. To reset the ports to default settings, click **Reset**.

The remaining ports (SR-IOV and OVS) on the Cisco CSP devices and the connections with switches are automatically discovered using Link Layer Discovery Protocol (LLDP) when you activate a cluster. You don't need to configure those ports.

Cisco Colo Manager (CCM) discovers switch neighbor ports and identifies whether all Niantic and Fortville ports are connected. If any port isn't connected, CCM sends notifications to Cisco vManage that you can view in the task view window.

NTP

Optionally, configure the NTP server for the cluster:

1. On the **Cluster Topology** window, click **Add** next to **NTP**. In the **NTP** configuration window, enter the following:
   - Template Name—Name of the NTP template should be in alphanumeric characters and the name should contain upto 128 characters.
   - Description—The description should be in alphanumeric characters and can be upto 2048 characters.
2. In the **Preferred server** field, enter the IP address of the primary NTP server.
3. In the **Backup server** field, enter the IP address of the secondary NTP server.
4. Click **Save**.

   The NTP servers are added.
5. To cancel the NTP server configuration, click **Cancel**.
6. To edit the NTP server configuration details, click **Edit**.

Syslog Server

Optionally, configure the syslog parameters for the cluster:

1. On the **Cluster Topology** window, click **Add** next to **Syslog**. In the **Syslog** configuration window, enter the following:

- Template Name—Name of the system template should be in alphanumeric characters and the name can contian upto 128 characters.
- Description—The description can be up to 2048 characters and can contain only alphanumeric characters.

2. In the **Severity** drop-down list, choose the severity of syslog messages to be logged.
3. To add a new syslog server, click **New Server**.

   Type the IP address of a syslog server.
4. Click **Save**.
5. To cancel the configuration, click **Cancel**.
6. To edit the existing syslog server configuration, click **Edit** and save the configuration.

TACACS Authentication

Table 4: Feature History

Feature Name	Release Information	Description
TACACS Authentication	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature allows you to configure the TACACS authentication for users accessing the Cisco CSP and Cisco Catalyst 9500 devices. Authenticating the users using TACACS validates and secures their access to the Cisco CSP and Cisco Catalyst 9500 devices.

The TACACS authentication determines the valid users who can access the Cisco CSP and Cisco Catalyst 9500 devices after a cluster is active.

Points to consider

- By default, the admin users with Role-based access control (RBAC) are authorized to access the Cisco CSP and Cisco Catalyst 9500 devices.
- Do not configure the same user with different passwords when configuring using TACACS and RBAC. If same user with a different password is configured on TACACS and RBAC, the RBAC user and password authentication is used. For information about how to configure RBAC on the devices, see Login Credentials, on page 8.

To authenticate users:

1. To add TACACS server configuration, on the **Cluster Topology** window, click **Other Settings** > **Add** next to **TACACS**.

   To edit TACACS server configuration, in the **Cluster Topology** window, click **Other Settings** > **Edit** next to **TACACS**.

   In the **TACACS** configuration window, enter information about the following:

   - Template Name—The TACACS template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.

2. To add a new TACACS server, click **+ New TACACS SERVER**.
   - In **Server IP Address**, enter the IPv4 address.

     Use IPv4 addresses for hostnames of TACACS server.
   - In **Secret** enter the password and confirm the password in **Confirm Secret**.
3. Click **Add**

   The new TACACS server details are listed in the **TACACS** configuration window.

Note You can add a maximum of four TACACS servers.

4. To add another TACACS server, repeat step 2 to step 3.

   When authenticating users, if the first TACACS server is not reachable, the next server is verified until all the four servers are verified.
5. Click **Save**.
6. To delete a TACACS server configuration, choose a row from the TACACS server details list and click **Delete** under **Action**.

Note To modify an existing TACACS server information, ensure to delete a TACACS server and then add a new server.

7. To view the TACACS server configuration, in Cisco vManage, click **Configuration** > **Devices**.

   For the desired Cisco CSP device or Cisco Catalyst 9500 switch, click **...** and choose **Running Configuration**.

Backup Server Settings

Points to Consider

- If you don't use an NFS server, Cisco vManage can’t successfully create backup copies of a CSP device for future RMA requirements.
- The NFS server mount location and configurations are same for all the CSP devices in a cluster.
- Don't consider an existing device in a cluster as the replacement CSP device.

Note If a replacement CSP device isn’t available, wait until the device appears in Cisco vManage.

- Don't attach further service chains to a cluster after you identify that a CSP device in the cluster is faulty.
- The backup operation on a CSP device creates backup files containing NFVIS configuration and VMs (if VMs are provisioned on the CSP device). You can use the following information for reference.

- An automated backup file is generated and is in the format:

  serial_number + "_" + time_stamp + ".bkup"

  For example,

  `WZP22180EW2_2020_06_24T18_07_00.bkup`

- An internal state model is maintained that specifies the status of the overall backup operation and internal states of each backup component:
  - NFVIS: A configuration backup of the CSP device as an xml file, config.xml.
  - VM_Images: All VNF tar.gz packages in `data/intdatastore/uploads` which are listed individually.
  - VM_Images_Flavors: The VM images such as, img_flvr.img.bkup.
  - Individual tar backups of the VNFs: The files such as, vmbkp.
- The backup.manifest file contains information of files in the backup package and their checksum for verification during restore operation.

To create backup copies of all CSP devices in a cluster, perform the following steps:

1. On the **Cluster Topology** window, click **Add** next to **Backup**.

   To edit backup server settings, on the **Cluster Topology** window, click **Edit** next to **Backup**

   In the **Backup** configuration window, enter information about the following fields:

   - Mount Name—Enter the name of the NFS mount after mounting an NFS location.
   - Storage Space—Enter the disk space in GB.
   - Server IP: Enter the IP address of the NFS server.
   - Server Path: Enter the folder path of the NFS server such as, `/data/colobackup`
   - Backup: Click **Backup** to enable it.
   - Time: Set a time for scheduling the backup operation.
   - Interval: Choose from the options to schedule a periodic backup process.
     - Daily: The first backup is created a day after the backup configuration is saved on the device, and everyday thereafter.
     - Weekly: The first backup is created seven days after the backup configuration is saved on the device, and every week thereafter.
     - Once: The backup copy is created on a chosen day and it's valid for the entire lifetime of a cluster. You can choose a future calendar date.

2. Click **Save**.
3. To view the status of the previous five backup operations, use the **show hostaction backup status** command. To know about the backup status configuration command, see Backup and Restore NFVIS and VM Configurations. To use this command:

a. In Cisco vManage, click the **Tools** > **SSH Terminal** screen to start an SSH session with Cisco vManage.

b. Choose the CSP device.

c. Enter the username and password for the CSP device and click **Enter** to log in to the CSP device and run the **show hostaction backup status** command.

Restore CSP Device

You can perform the restore operation only by using the CLI on the CSP device that you're restoring.

1. Use the **mount nfs-mount storage** command to mount NFS:

   For more information, see Network File System Support.

Note To access the backup file, the configuration for mounting an NFS file system should match the faulty device. You can view this information from other healthy CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view and capture the information, you can do one of the following:

- In the **Cluster Topology** window, click **Add** next to **Backup**.
- Use the **show running-config** command to view the active configuration that is running on a CSP device. See Prerequisites and Restrictions for Backup and Restore of CSP Devices.

   mount nfs-mount storage { *mount-name* | **server_ip** *server_ip* | **server_path** *server_path* | **storage_space_total_gb** *storage_space_total_gb* | **storage_type** *storage_type* }

   For example, `mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path /data/colobackup/ storage_space_total_gb 100.0 storagetype nfs`

2. Restore the backup information on a replacement CSP device using the **hostaction restore** command:

   For example,

   ```
   hostaction restore except-connectivity file-path
   nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
   ```

Note Specify the except-connectivity parameter to retain the connectivity with the NFS server mounted in Step 2.

3. Use the **show hostaction backup status** command to view the status of the previous five backup images and their operational status.

   Also, you can view the backup images from the notifications available on the Cisco vManage **Monitor** > **Logs** > **Events** page.

Note In Cisco vManage Release 20.6.x and earlier releases, you can view the backup images from the notifications available on the Cisco vManage **Monitor** > **Events** page.

4. Use the **show hostaction restore-status** command on the CSP device to view the status of the overall restore process and each component such as system, image and flavors, VM and so on.
5. To fix any failure after viewing the status, perform a factory default reset of the device.

Note The factory default reset sets the device to default configuration. Therefore, before performing the restore operation from Steps 1-4 on the replacement device, verify that all the restore operation prerequisites are met. See Prerequisites and Restrictions for Backup and Restore of CSP Devices, on page 27.

To know more about how to configure the restore operation on CSP devices, see Backup and Restore NFVIS and VM Configurations.

Progress of Cluster Activation

Table 5: Feature History

Feature Name	Release Information	Description
Monitor Cluster Activation Progress	Cisco SD-WAN Release 20.1.1	This feature displays the cluster activation progress at each step and shows any failures that may occur during the process. The process of activating a cluster takes approximately 30 minutes or longer, and you can monitor the progress using the Cisco vManage task view window and events from the Monitoring page.

To check cluster activation status after activating a cluster, view the progress on the task view window:

Note In Cisco vManage Release 20.7.x and earlier releases, Cisco Colo Manager (CCM) bring up and activation progress is reported as part of the CLOUD ONRAMP CCM task. This task shows the seven steps in the CCM bring up and activation sequence and indicates whether the sequence was successfully completed or not. The Push Feature Template Configuration task shows the status of the RBAC settings configuration push.

From Cisco vManage Release 20.8.1, CLOUD ONRAMP CCM task is completed when Cisco vManage receives CCM Healthy from the target CSP device. The Push Feature Template Configuration task shows the seven steps in the CCM bring up and activation sequence and indicates whether the sequence was successfully completed or not, along with the status of the RBAC settings configuration push.

Figure 1: Cluster Activation (Cisco vManage Release 20.7.x and earlier)

Figure 2: CLOUD ONRAMP CCM Task (Cisco vManage Release 20.8.1 and later)

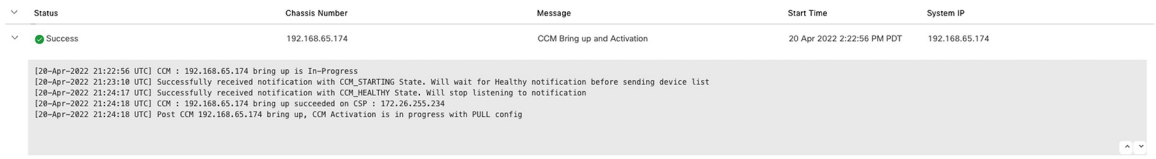
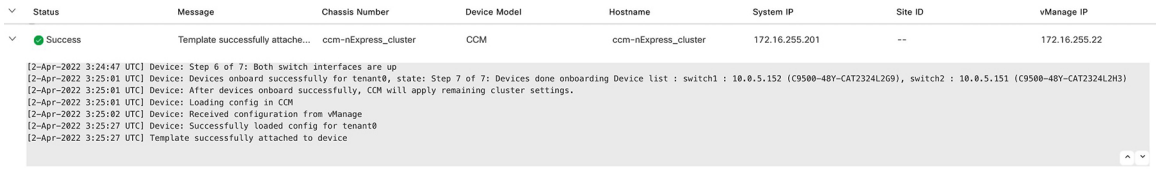


Figure 3: Push Feature Template Configuration Task (Cisco vManage Release 20.8.1 and later)



Perform the following verification steps:

1. To view cluster state and change the state:
   a. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for Colocation**. For the cluster that is goes into a "PENDING" state, click **...**, and choose **Sync**. This action moves a cluster back to an "ACTIVE" state.
   b. To view if a cluster moves back to an "ACTIVE" state, you can view the successful activation for the cluster.
2. To view the service groups present on CSP devices, from the Cisco vManage menu, choose **Monitor** > **Devices** > **Colocation Cluster**.

   Cisco vManage Release 20.6.x and earlier: To view the service groups present on CSP devices, from the Cisco vManage menu, choose **Monitor** > **Network** > **Colocation Clusters**.

   Choose a cluster and then choose a CSP device. You can choose and view other CSP devices.
3. To check if cluster is activated from a CSP device:
   a. From the Cisco vManage menu, choose **Configuration** > **Devices**.
   b. View device status of all the CSP devices and ensure that they are in synchronization with Cisco vManage.
   c. View the state of CSP devices and verify that the certificates are installed for CSP devices.

Note If the state of CSP devices doesn't show "cert installed" for more than five minutes after CSP activation through OTP, see Troubleshoot Cisco Cloud Services Platform Issues .

After a cluster is activated from a CSP device, the Cisco Colo Manager (CCM) performs the cluster activation tasks on the Cisco NFVIS host.

4. To view if CCM is enabled for a CSP device,
   a. From the Cisco vManage menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.

   b. Click **Colocation Cluster**.

      Cisco vManage Release 20.6.x and earlier: Click **Colocation Clusters**.

      View whether CCM is enabled for specific CSP devices.

5. To monitor CCM health,
   a. From the Cisco vManage menu, choose **Monitor** > **Devices**.

      Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.

   b. Click **Colocation Cluster**.

      Cisco vManage Release 20.6.x and earlier: Click **Colocation Clusters**.

      View whether CCM is enabled for the desired CSP devices.

   c. For the CCM-enabled CSP device, click the CSP device.

   d. To view CCM health, click **Colo Manager**.

   If the Cisco Colo Manager status doesn't change to "HEALTHY" after "STARTING", see Troubleshoot Cisco Colo Manager Issues .

   If the status of Cisco Colo Manager changes to "HEALTHY" after "STARTING" but the status of Cisco Colo Manager shows IN-PROGRESS for more than 20 minutes after the switch configurations are already complete, see Switch devices are not calling home to PNP or Cisco Colo Manager .

View Cluster

To view cluster configuration, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 For the desired cluster, click **...** and choose **View**.

The **Cluster** window displays the switch devices and CSP devices in the cluster and shows the cluster settings that are configured.

You can only view the global parameters of a cluster, configuration of switch devices and CSP devices.

Step 3 Click **Cancel** to return to the **Cluster** window.

Edit Cluster in Cisco vManage

To modify any existing cluster configuration such as global parameters, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **Edit**.

The **Cluster** window displays the switch devices and CSP devices in the cluster and shows the cluster settings that are configured.

Step 3 In the cluster design window, you can modify some of the global parameters. Based on whether a cluster is in active or inactive state, you can perform the following operations on a cluster:

a. Inactive state:

- Edit all global parameters, and the Resource Pool parameter.
- Add more CSP devices (up to eight).
- Can’t edit the name or serial number of a switch or CSP device. Instead, delete the CSP or switch and add another switch or CSP with a different name and serial number.
- Delete an entire cluster configuration.

b. Active state:

- Cisco vManage 20.8.1 and earlier releases: Edit all global parameters, except the Resource Pool parameter.

  Note You can't change the Resource pool parameter when the cluster is active. However, the only option to change the Resource Pool parameter is to delete the cluster and recreate it with the correct Resource Pool parameter.

- From Cisco vManage 20.9.1: Edit all global parameters and some Resource Pool parameters.

  Note Expansion of active Day-N cluster resource pools is supported. Reduction of IP and VLAN pools are not supported. All the IP Pools except the VNF Management IP Pool can have new subnets added in day-N edit.

  You cannot edit the following Resource Pool parameters:

  - **Name**
  - **Description**
  - **Management Subnet Gateway**
  - **Management Mask**
  - **Switch PNP Server IP**

- Can’t edit the name or serial number of a switch or CSP device.
- Can’t delete a cluster in an active state.

- Add more CSP devices (up to eight).

Step 4 Click **Save Cluster**.

Add CSP Device to Cluster

You can add and configure the CSP devices using Cisco vManage.

Before you begin

Ensure that the Cisco NFVIS version that you use is same for all the CSP devices in the cluster.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **Add/Delete CSP**.

Step 3 To add a CSP device, click **+ Add CSP**. The **Add CSP** dialog box appears. Enter a name and choose the CSP device serial number. Click **Save**.

Step 4 To configure a CSP device, click the CSP icon in the CSP box. The **Edit CSP** dialog box appears. Enter a name and choose the CSP device serial number. Click **Save**.

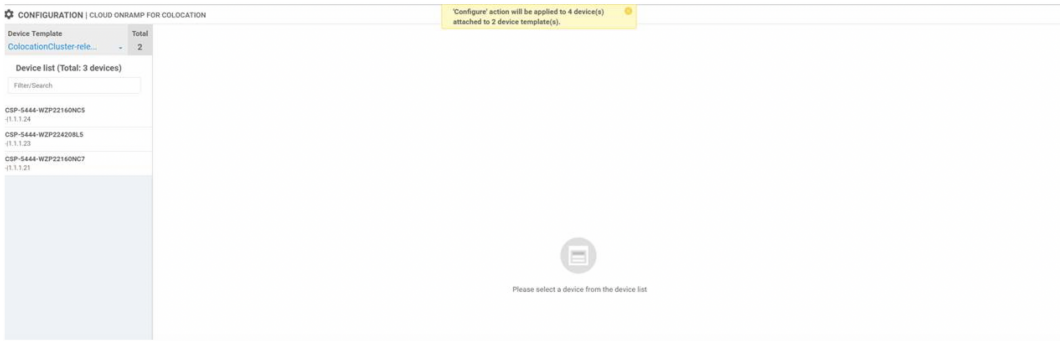
The name can contain 128 alphanumeric characters.

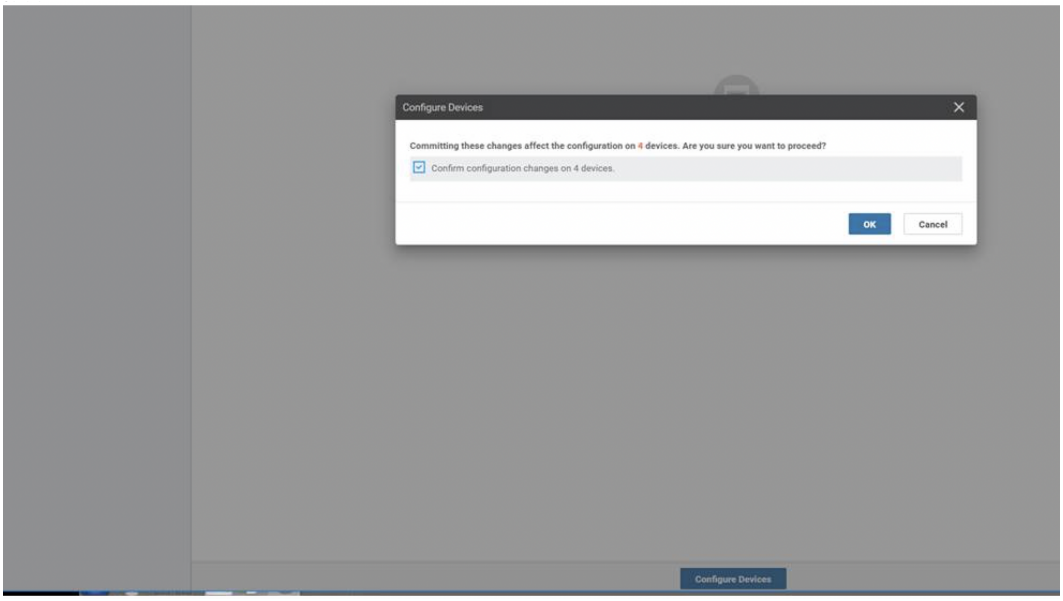
Note To bring up the CSP devices, ensure that you configure the OTP for the devices.

Figure 4: Add a CSP Device

Step 5 Click **Save**.

Step 6 After saving, perform the onscreen configuration instructions as shown in the following images:





Step 7 To check whether the CSP device is added, use the **Task View** window that displays a list of all running tasks.

Delete CSP Devices from Cluster

You can delete CSP devices using Cisco vManage.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

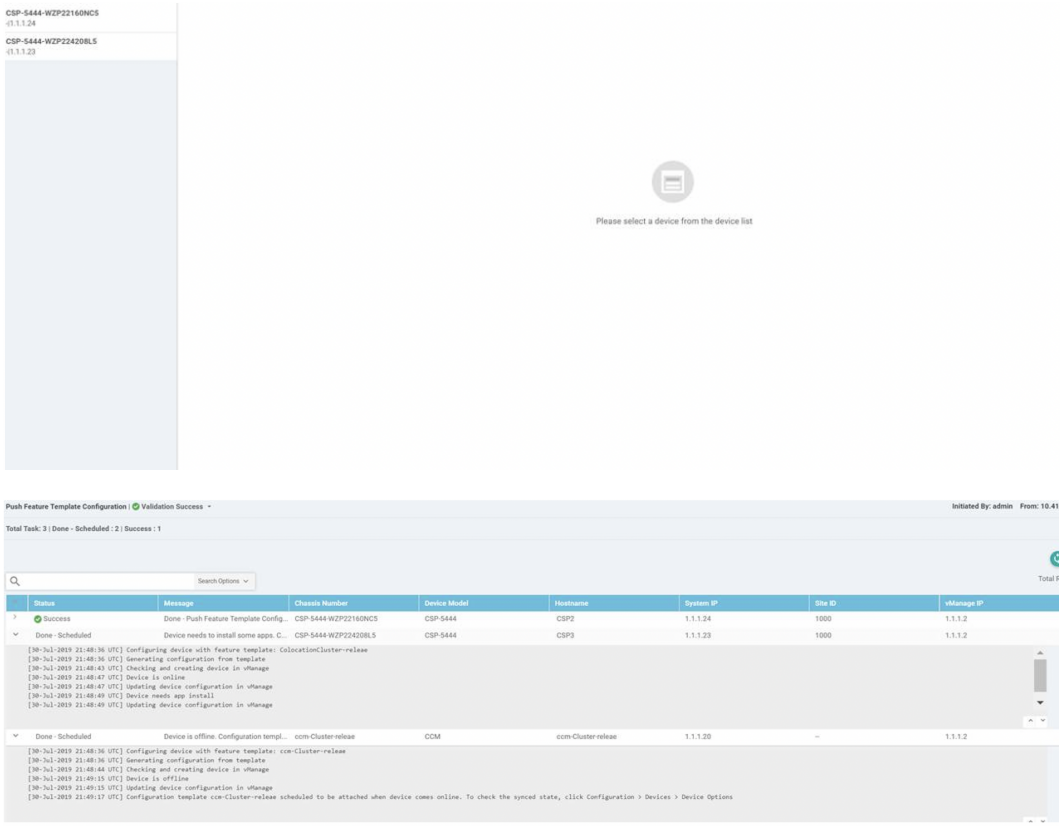
Step 2 For the desired cluster, click **...** and choose **Add/Delete CSP**.

Step 3 To delete a CSP device, click the CSP icon from the **Appliances** box.

Step 4 Click **Delete**.

Step 5 Click **Save**.

Step 6 Perform the onscreen instructions to proceed with the deletion as shown in the following images.



Step 7 Reset the CSP devices to factory-default settings. See Factory reset of CSP device.

Step 8 To decommission invalid CSP devices, from the Cisco vManage menu, choose **Configuration** > **Devices**.

Step 9 For the CSP devices that are in the deactivated cluster, click the **...** and choose **Decommission WAN Edge**.

This action provides new tokens to the devices.

If an HA service chain is deployed on a CSP device that is deleted, the corresponding HA service chains are deleted from the CSP device that hosts the HA instances.

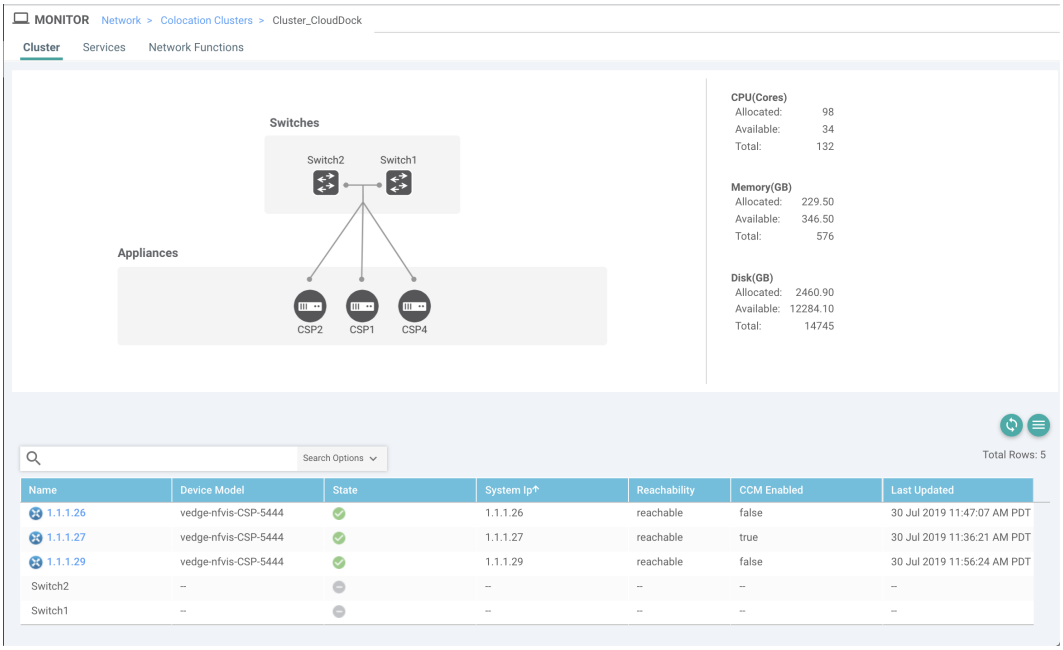
Delete CSP with CCM

Step 1 Determine the CSP device that hosts the CCM.

Step 2 If **CCM Enabled** is true on a CSP device and you decide to delete this CSP device, for the device, click **...** and choose **Add/Delete CSP**.

From the **Montior** window, you can view whether CCM is enabled. The following image shows how where you can view the CCM status.

Figure 5: CSP Device with CCM



When the CSP device that you choose to remove from a cluster, runs the service chain monitoring service and CCM, ensure that you click **Sync** for the cluster. Clicking the sync button starts the service chain health monitoring service on a different CSP device and continues monitoring the existing service chain health.

Ensure that Cisco vManage has control connections to all the CSP devices for a cluster so that it can bring up CCM instance on another CSP device.

Note For Cisco vManage Release 20.8.x and earlier releases, if you delete a CSP device hosting a CCM instance, you have to add a CSP device to bring up the CCM instance on one or more of the CSP devices.

After you delete a CSP device with CCM, the CCM instance starts on another CSP device on the cluster.

Note The service chain monitoring is disabled until the CCM instance doesn't start in any of the remaining CSP devices.

Replace Cisco CSP Devices After RMA

SUMMARY STEPS

1. From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**
2. For the desired cluster, click **...** and choose **RMA**.
3. Do the following in the **RMA** dialog box:

DETAILED STEPS

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 For the desired cluster, click **...** and choose **RMA**.

Step 3 Do the following in the **RMA** dialog box:

a) Select Appliance: Choose a CSP device that you want to replace.

All CSP devices in a specific colocation cluster are displayed in the format, CSP Name-<Serial Number>.

b) Choose a serial number for a new CSP device from the drop-down list.

c) Click **Save**.

After saving, you can view the configuration.

Return of Materials of Cisco CSP Devices

Table 6: Feature History

Feature Name	Release Information	Description
RMA Support for Cisco CSP Devices	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature allows you to replace a faulty CSP device by creating backup copies of the device, and then restoring the replacement device to a state it was in before the replacement. The VMs running in HA mode operate uninterrupted with continuous flow of traffic during device replacement.

You can now create backup copies and restore NFVIS configurations and VMs.

Points to Consider

- You can use Network File Storage (NFS) servers to create regular backup copies of the CSP devices.
- If you're using an external NFS server for the backup operation, ensure that you maintain and clean the NFS directory regularly. This maintenance ensures that the NFS server has sufficient space for the incoming backup packages.
- If you don't use NFS servers, don't configure the backup server settings using Cisco vManage. However, if you're not configuring the backup server settings, you can't restore the replacement device. You can use delete CSP to remove the faulty device, add a new CSP device, and then start provisioning the service chains onto the added CSP device.

RMA Process for Cisco CSP Devices

Ensure that you perform the Return of Materials (RMA) process in the following order:

1. Create a backup copy of all the CSP devices in a cluster using Cisco vManage. See Backup Server Settings, on page 15.

Note During CSP device replacement, create a backup copy of the device in the NFS server when creating a cluster using Cisco vManage. Perform one of the following if you're bringing up a cluster or editing an existing cluster.

- Bring up a colocation cluster: At the time of cluster creation and activation, provide information about the NFS storage server and backup intervals. If the backup task fails on a CSP device, the device returns an error, but the cluster activation continues. Ensure that you update the cluster after addressing the failure and wait for a successful cluster activation.
- Edit a colocation cluster: For an existing active cluster, edit the cluster and provide information about the NFS storage server and backup intervals.

2. Contact Cisco Technical Support to get a replacement CSP device. See Cisco Cloud Services Platform 5000 Hardware Installation Guide for more information about replacing a CSP device.
3. Rewire the replacement Cisco CSP device with the Cisco Catalyst 9500 switches to move the wiring of the faulty device to the replacement device. See Wiring Requirements.
4. Verify that the Cisco CSP ISO image running on the replacement device is the same that was running on the faulty device.
5. Restore the replacement device using CLI.

Prerequisites and Restrictions for Backup and Restore of CSP Devices

Prerequisites

Backup Operation

- The connectivity to the NFS server from CSP devices should be established before configuring the backup server settings using Cisco vManage.
- The backup directory on the NFS server should have write permission.
- The external NFS server should be available, reachable, and maintained. The maintenance of the external NFS server requires you to check the available storage space and network reachability regularly.
- The schedule for the backup operation should be synced with the local date and time on the CSP device.

Restore Operation

- The replacement device should have the same resources as the faulty device. These resources are, Cisco NFVIS image version, CPU, memory and storage as the faulty CSP device.
- The connectivity between the replacement device and switch ports should be same as the faulty device and switches.
- The PNIC wiring of the replacement device should match the faulty device on the Catalyst 9500 switches.

  For example,

  If slot-1/port-1 (eth1-1) on the faulty device is connected to switch-1 and port, 1/0/1, then connect slot-1/port-1 (eth1-1) of the replacement device to the same switch port, such as switch-1 and port, 1/0/1.

- The onboarding of the replacement device should be completed using the PnP process for CSP devices.
- To prevent the loss of backup access during the restore operation, the configuration for mounting an NFS server to access the backup package should match the configuration on the faulty device.

  You can view configuration information from other CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view the active configuration that is running on a healthy CSP device, use the **show running-config** command. Use this active configuration information when creating a mount point during the restore operation.

  For example,

```
nfvis# show running-config mount
mount nfs-mount storage nfsfs/
storagetype            nfs
storage_space_total_gb 123.0
server_ip              172.19.199.199
server_path            /data/colobackup/
!
```

- The authentication of the replacement device with the Cisco SD-WAN controllers using the OTP process should be completed after restoring the replacement device.

Note Use the **request activate chassis-number** *chassis-serial-number* **token** *token-number* command to authenticate a device by logging in to Cisco NFVIS.

- The replacement device shouldn't have any configuration other than the configuration of the faulty device.

Restrictions

Backup Operation

- The periodic backup operation doesn't start during the upgrade of a CSP device.
- If the NFS folder path isn't available on the NFS server, the backup operation doesn't start.
- Only one backup operation can occur at a specific time.
- The backup operation fails if the available disk space on the NFS server is less than the combined size of the VM export size and tar.gz VM packages.
- The backup device information can only be restored on a replacement CSP device and not on any existing device that is already part of the cluster.
- The NFS mount configurations can’t be updated after they are configured for a CSP device. To update, delete the NFS configuration and reapply an updated configuration to the NFS server and reconfigure the backup schedule. Perform this update when the backup operation isn't in progress.

Restore Operation

- Only one restore operation can occur at a specific time.
- If a backup file doesn’t exist in the NFS server, the restore operation doesn't start.

- The restore operation isn't supported when you convert a cluster from a single tenant mode to multitenant mode, and conversely.

Remove PNF Devices from Cluster

Step 1 Detach all service groups and service chains that has the PNF.

Step 2 (Optional) Delete the service groups.

If the deleted PNF is an ASR router, which is orchestrated using Cisco vManage, invalidate and decommission the device from the **Device** window.

Step 3 Remove the cables that connect the PNF with the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches and manually remove the VLAN configuration from the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C corresponding interfaces.

Remove Cluster from Cisco vManage

To decommission an entire cluster from Cisco vManage, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Certificates**.

Step 2 Verify the **Validate** column for the CSP devices that you wish to delete, and click **Invalid**.

Step 3 For the invalid devices, click **Send to Controllers**.

Step 4 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 5 For the cluster that has invalid CSP devices, click **...** and choose **Deactivate**.

If the cluster is attached to one or more service groups, a message appears that displays the service chains hosting the VMs that are running on the CSP device and whether you can continue with the cluster deletion. However, although you confirm the deletion of a cluster, you're not allowed to remove the cluster without detaching the service groups that are hosted on this CSP device. If the cluster isn't attached to any service group, a message appears that gets a confirmation from you about the cluster deletion.

Note You can delete the cluster, if necessary, or can keep it in deactivated state.

Step 6 To delete the cluster, choose **Delete**.

Step 7 Click **Cancel** if you don't wish to delete the cluster.

Step 8 To decommission invalid devices, from the Cisco vManage menu, choose **Configuration** > **Devices**.

Step 9 For the devices that are in the deactivated cluster, click **...** and choose **Decommission WAN Edge**.

This action provides new tokens to your devices.

Step 10 Reset the devices to the factory default by using the command:

factory-default-reset all

Step 11 Log into Cisco NFVIS by using **admin** as the login name and **Admin123#** as the default password.

Step 12 Reset switch configuration and reboot switches. See Clean switches configuration and reset switches to factory defaults .

Remove and Replace Switch

The Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C series of switches are used in the data path for switching traffic between the different VNF devices in a service chain. There are two switches that are stacked by using Stackwise Virtual (SVL) technology.

To achieve a redundant stack, the switches use a set of two stackwise virtual links (SV links) and one dual active detection (DAD link). For prescriptive connections on Cisco Catalyst 9500-40X, ports 38, 39 are SVL links and port 40 is the DAD link. For prescriptive connections on Cisco Catalyst 9500-48Y4C, ports 46, 47 are SVL links and port 48 is the DAD link.

In a stack, there are two switches in which one of the switches is active and the other is the standby. The control plane databases are synchronized between the switches. Each switch is assigned a switch number as part of the stack. The switches are numbered 1 and 2 in the current scenario. For more information on SVL redundancy, see High Availability Switch Configuration Guide.

Note In the case of a switch failure, ensure that you know the switch number that failed. This switch can be used to set up as the replacement.

To replace a switch in the stack:

Step 1 On the switch 1 console, use the **show switch** command to view the configuration.

```
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Member   0000.0000.0000     0      V01     Removed
```

Note Here, the switch number that is removed is two. This switch number is required when configuring the new switch.

Step 2 On the switch that replaces the failed unit, ensure that the switch number is one. This is achieved by using the **show switch** command again on the new unit.

```
Switch# show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*1       Active   5486.bc78.c900     1      V01     Ready
```

Step 3 If the new switch is numbered two, ensure that you renumber it to 1 and then reload the switches. Use the following commands to view the switch number and then renumber the switch to 1:

```
Switch# show switch
Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*2       Active   5486.bc78.c900     1      V01     Ready


Switch# switch 2 renumber 1
WARNING: Changing the switch number may result in a configuration change for that switch.  The
interface configuration associated with the old switch number will remain as a provisioned
configuration. New Switch Number will be effective after next reboot. Do you want to continue?[y/n]?
 [yes]:
Switch#reload

System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

Jun 17 19:41:01.793: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command
```

Step 4 Connect the required cables for SVL; which are ports 38, 39, and 40 from the first Cisco Catalyst 9500-40X switch to the second switch.

Step 5 On the second switch, configure and save the configuration.

```
Switch(config)#
stackwise-virtual
domain 10
!
interface TenGigabitEthernet1/0/38
stackwise-virtual link 1
!
interface TenGigabitEthernet1/0/39
stackwise-virtual link 1
!
interface TenGigabitEthernet1/0/40
stackwise-virtual dual-active-detection
```

Step 6 Renumber the new unit to be the same as the one it's replacing, and then reload the box.

```
Switch# switch 1 renumber 2
WARNING: Changing the switch number may result in a configuration change for that switch.  The
interface configuration associated with the old switch number will remain as a provisioned
configuration. New Switch Number will be effective after next reboot. Do you want to continue?[y/n]?
 [yes]: yes
Switch# reload
```

After the new switch comes up, it joins the stack and synchronizes with the configuration.

Here's the sample output from the **show switch** command.

```
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Member   5486.bc78.c900     1      V01     Ready
```

```
Switch#
*Jun 17 21:00:57.696: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Jun 17 21:00:57.694: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))

*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Jun 17 21:01:53.686: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Jun 17 21:01:54.688: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
Switch#
Switch# show switch
Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------------------------
*1       Active   c4b3.6a71.0b00     1      V01     Ready
 2       Standby  5486.bc78.c900     1      V01     Ready
```

Reactivate Cluster from Cisco vManage

To add new CSP devices or when CSP devices are considered for RMA process, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Devices**.

Step 2 Locate the devices that are in a deactivated cluster.

Step 3 Get new token from Cisco vManage for the devices.

Step 4 Log into Cisco NFVIS using **admin** as the login name and **Admin123#** as the default password.

Step 5 Use the **request activate chassis-number** *chassis-serial-number* **token** *token-number* command.

Step 6 Use Cisco vManage to configure the colocation devices and activate the cluster. See Create and Activate Clusters, on page 6.

If you've deleted the cluster, recreate and then activate it.

Step 7 From the Cisco vManage menu, choose **Configuration** > **Certificates**. Locate and verify status of the colocation devices.

Step 8 For the desired device that should be valid, click **Valid**.

Step 9 For the valid devices, click **Send to Controllers**.

Manage Service Groups

A service group consists of one or more service chains. You can configure a service group using Cisco vManage. A service chain is the structure of a network service, and consists of a set of linked network functions.

VNF Placement for Service Chains in Cisco vManage

The service chain placement component chooses a CSP device that hosts each VNF in service chains. The placement decision is based on available bandwidth, redundancy and computation resources (CPUs, memory,

and storage) availability. The placement logic returns an error if the bandwidth, CPU, memory, and storage needs of all the VNFs in the service chains that are configured for a Cloud OnRamp for Colocation aren't met. You receive notifications if the resources aren't available and service chains aren't deployed.

Create Service Chain in a Service Group

A service group consists of one or more service chains.

Table 7: Feature History

Feature Name	Release Information	Feature Description
Monitor Service Chain Health	Cisco SD-WAN Release 19.2.1	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.

From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

a) Click **Service Group** and click **Create Service Group**. Enter the service group name, description, and colocation group.

   The service group name can contain 128 alphanumeric characters.

   The service group description can contain 2048 alphanumeric characters.

   For a multitenant cluster, choose a colocation group or a tenant from the drop-down list. For a single-tenant cluster, the colocation group **admin** is chosen by default.

b) Click **Add Service Chain**.

c) In the **Add Service Chain** dialog box, enter the following information:

Table 8: Add Service Chain Information

Field	Description
Name	The service chain name can contain 128 alphanumeric characters.
Description	The service chain description can contain alphanumeric 2048 characters.
Bandwidth	The service chain bandwidth is in Mbps. The default bandwidth is 10 Mbps and you can configure a maximum bandwidth of 5 Gbps.
Input Handoff VLANS and Output Handoff VLANS	The Input VLAN handoff and output VLAN handoff can be comma-separated values (10, 20), or a range from 10–20.

Field	Description
Monitoring	A toggle button that allows you to enable or disable service chain health monitoring. The service chain health monitoring is a periodic monitoring service that checks health of a service chain data path and reports the overall service chain health status. By default, the monitoring service is disabled. A service chain with subinterfaces such as, SCHM (Service Chain Health Monitoring Service) can only monitor the service chain including the first VLAN from the subinterface VLAN list. The service chain monitoring reports status based on end-to-end connectivity. Therefore, ensure that you take care of the routing and return traffic path, with attention to the Cisco SD-WAN service chains for better results. **Note** • Ensure that you provide input and output monitoring IP addresses from input and output handoff subnets. However, if the first and last VNF devices are VPN terminated, you don't need to provide input and output monitoring IP addresses. For example, if the network function isn't VPN terminated, the input monitoring IP can be 192.0.2.1/24 from the inbound subnet, 192.0.2.0/24. The inbound subnet connects to the first network function and the output monitoring IP can be, 203.0.113.11/24 that comes from outbound subnet, 203.0.113.0/24 of the last network function of a service chain. • If the first or last VNF firewall in a service chain is in transparent mode, you can't monitor these service chains.
Service Chain	A topology to choose from the service chain drop-down list. For a service chain topology, you can choose any of the validated service chains such as, Router - Firewall - Router, Firewall, Firewall - Router. See You can also create a customized service chain. See Create Custom Service Chain, on page 42.

d) In the **Add Service Chain** dialog box, click **Add**.
Based on the service chain configuration information, a graphical representation of the service group with all the service chains and the VNFs automatically appear in the design view window. A VNF or PNF appears with a "V" or "P" around the circumference for a virtual a physical network function. It shows all the configured service chains within each service group. A check mark next to the service chain indicates that the service chain configuration is complete.

After you activate a cluster, attach it with the service group and enable monitoring service for the service chain, when you bring up the CSP device where CCM is running. Cisco vManage chooses the same CSP device to start the monitoring service. The monitoring service monitors all service chains periodically in a round robin fashion by setting the monitoring interval to 30 minutes. See Monitor Cloud onRamp Colocation Clusters.

e) In the design view window, to configure a VNF, click a VNF in the service chain.
The **Configure VNF** dialog box appears.

f) Configure the VNF with the following information and perform the actions, as appropriate:

Note The following fields are available from Cisco vManage Release 20.7.1:

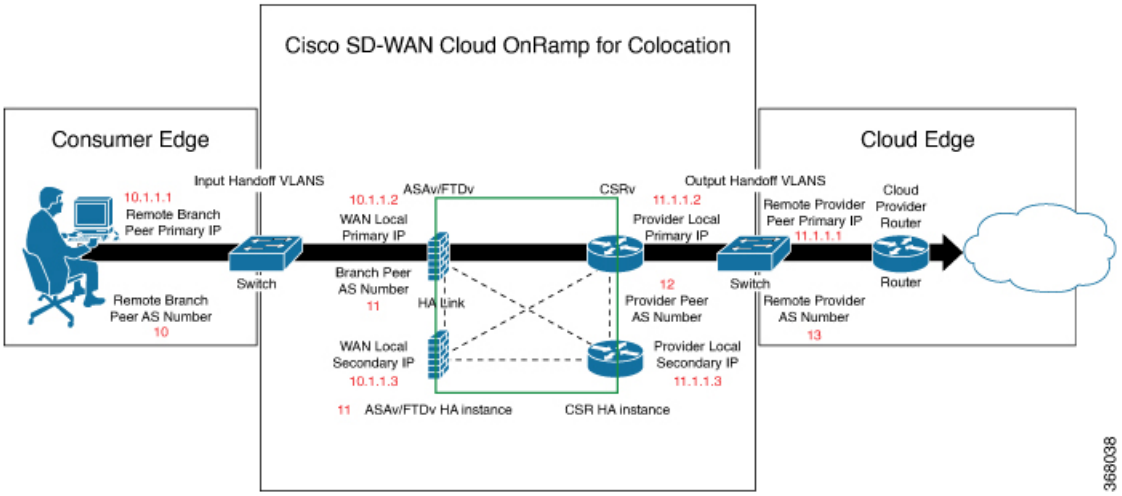
- **Disk Image/Image Package (Select File)**
- **Disk Image/Image Package (Filter by Tag, Name and Version)**
- **Scaffold File (Select File)**
- **Scaffold File (Filter by Tag, Name and Version)**

Table 9: VNF Properties of Router and Firewall

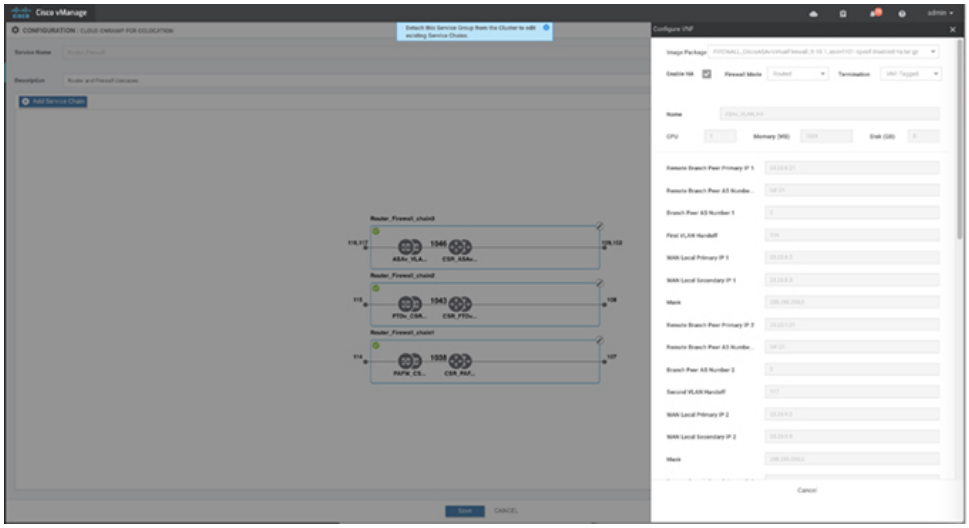
Field	Description
Image Package	Choose a router, firewall package.
Disk Image/Image Package (Select File)	Choose a tar.gz package or a qcow2 image file.
Disk Image/Image Package (Filter by Tag, Name and Version)	(Optional) Filter an image or a package file based on the name, version, and tags that you specified when uploading a VNF image.
Scaffold File (Select File)	Choose a scaffold file. **Note** • This field is mandatory if a qcow2 image file has been chosen. It is optional if a tar.gz package has been chosen. • If you choose both a tar.gz package and a scaffold file, then all image properties and system properties from the scaffold file override the image properties and system properties, including the Day-0 configuration files, specified in the tar.gz package.
Scaffold File (Filter by Tag, Name and Version)	(Optional) Filter a scaffold file based on the name, version, and tags that you specified when uploading a VNF image.
Click **Fetch VNF Properties**. The available information for the image is displayed in the **Configure VNF** dialog box.	
Name	VNF image name
CPU	(Optional) Specifies the number of virtual CPUs that are required for a VNF. The default value is 1 vCPU.
Memory	(Optional) Specifies the maximum primary memory in MB that the VNF can use. The default value is 1024 MB.
Disk	(Optional) Specifies disk in GB required for the VM. The default value is 8 GB.

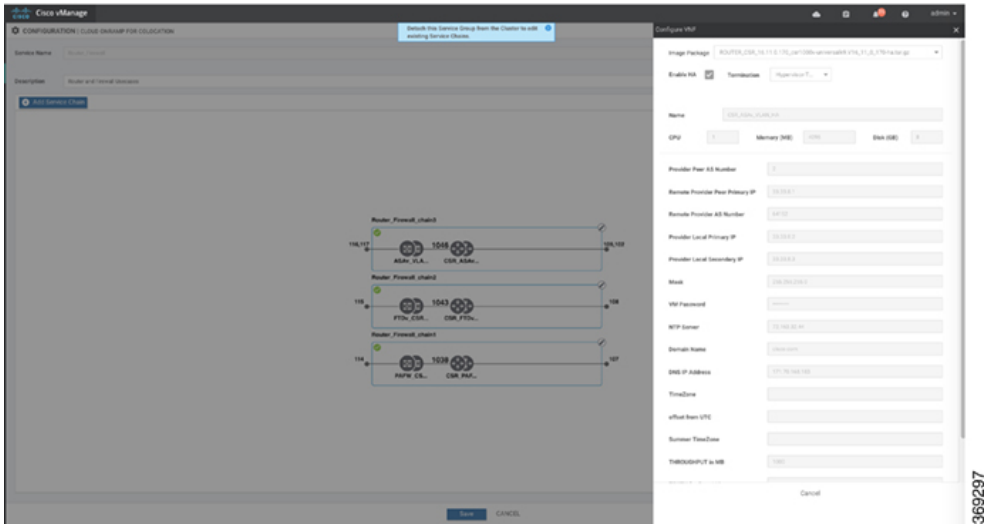
Field	Description
A dialog box with any custom tokenized variables from Day-0 that requires your input appears. Provide the values.	

In the following image, all IP addresses, VLAN, and autonomous system within the green box are system-specific information that is generated from the VLAN, IP pools provided for the cluster. The information is automatically added into the Day-0 configurations of VMs.



The following images are a sample configuration for VNF IP addresses and autonomous system numbers, in Cisco vManage.





If you're using a multitenant cluster and a comanged scenario, configure the Cisco SD-WAN VM by entering the values for the following fields and the remaining fields, as required for the service chain design:

Note To join the tenant overlay network, the provider should provide correct values for the following fields.

Field	Description
Serial Number	The authorized serial number of a Cisco SD-WAN device. The service provider can get the device serial number from the tenant before creating the service chain.
OTP	The OTP of the Cisco SD-WAN device that is available after authenticating it with Cisco SD-WAN Controllers. The service provider can get the OTP for the corresponding serial number from the tenant before creating the service chain.
Site Id	The identifier of the site in the tenant Cisco SD-WAN overlay network domain in which the Cisco SD-WAN device resides, such as a branch, campus, or data center. The service provider can get the site Id from the tenant before creating the service chain.
Tenant ORG Name	The tenant organization name that is included in the Certificate Signing Request (CSR). The service provider can get the organization name from the tenant before creating the service chain.
System IP connect to Tenant	The IP address to connect to the tenant overlay network. The service provider can get the IP address from the tenant before creating the service chain.
Tenant vBond IP	The IP address of the tenant Cisco vBond Orchestrator. The service provider can get the Cisco vBond Orchestrator IP address from the tenant before creating the service chain.

For edge VMs such as first and last VM in a service chain, you must provide the following addresses as they peer with a branch router and the provider router.

Table 10: VNF Options for First VM in Service Chain

Field	Mandatory or Optional	Description
Firewall Mode	Mandatory	Choose Routed or Transparent mode. **Note** Firewall mode is applicable to firewall VMs only.
Enable HA	Optional	Enable HA mode for the VNF.

Termination	Mandatory	Choose one of the following modes:
		• L3 mode selection with subinterfaces that are in trunk mode
		`<type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val>`
		• L3 mode with IPSEC termination from a consumer-side and rerouted to the provider gateway
		`<val help="L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW" display="Tunneled">vpn</val>`
		• L3 mode with access mode (nontrunk mode)
		`<val help="L3 Mode In Access Mode (Non-Trunked)" display="Hypervisor-Tagged">routed</val>`

g) Click **Configure**. The service chain is configured with the VNF configuration.
h) To add another service chain, repeat the procedure from Steps b-g.
i) Click **Save**.

The new service group appears in a table under the **Service Group**. To view the status of the service chains that are monitored, use the **Task View** window, which displays a list of all running tasks along with the total number of successes and failures. To determine the service chain health status, use the **show system:system status** command on the CSP device that has service chain health monotioring enabled.

QoS on Service Chains

Table 11: Feature History

Feature Name	Release Information	Description
QoS on Service Chains	Cisco SD-WAN Release 20.1.1	This feature classifies the network traffic based on the Layer 2 virtual local-area network (VLAN) identification number. The QoS policy allows you to limit the bandwidth available for each service chain by applying traffic policing on bidirectional traffic. The bidirectional traffic is the ingress side that connects Cisco Catalyst 9500-40X switches to the consumer and egress side that connects to the provider.

Prerequisites

- Ensure that you use the Quality of Service (QoS) traffic policing on service chains that do not have shared VNF and PNF devices.

Note You cannot apply QoS policy on service chains with shared VNF devices where input and output VLANs are same for multiple service chains.

- Ensure that you use the following versions of software for QoS traffic policing:

Software	Release
Cisco NFVIS Cloud OnRamp for Colocation	4.1.1 and later
Catalyst 9500-40X	16.12.1 and later

The QoS policing policy is applied on the network traffic based on the following workflow:

1. Cisco vManage saves the bandwidth, input, or output VLAN information to VNF and PNF devices. To provide bandwidth and VLAN information, see Create Service Chain in a Service Group, on page 33.
2. CCM saves the bandwidth, input, or output VLAN values information to the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches.
3. CCM creates corresponding class-maps and policy-maps in Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches based on VLAN match criteria.
4. CCM applies input service-policy on the ingress and egress ports.

Note From Cisco vManage Release 20.7.1, the QoS traffic policy on service chains is not supported for Cisco Catalyst 9500 switches.

- If an active cluster is upgraded to Cisco vManage Release 20.7.1 and CSPs 4.7.1, and if there are service chains provisioned prior to upgrade, the QoS configuration will be removed from switches during the upgrade automatically.
- When new service chains are provisioned in Cisco vManage Release 20.7.1, the QoS policy will not be configured on switches.
- Similarly, new clusters created in Cisco vManage Release 20.7.1 will not configure QoS configuration for service chains on switches.

Clone Service Groups

Table 12: Feature History

Feature Name	Release Information	Description
Clone Service Groups in Cisco vManage	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature allows you to create copies of service groups for different RBAC users, without having to enter the same configuration information multiple times. By cloning a service group, you can easily create service chains by leveraging the stored service chain templates.

When you clone or create copies of service chains, remember the following:

- Cisco vManage copies all configuration information of a service group to a cloned service group regardless of whether the cloned service group is attached to a cluster.
- Verify the CSV file and ensure that configuration information has a matching service group name during CSV file upload. Otherwise, an unmatched service group name can result in an error message during CSV file upload.
- To get an updated list of service group configuration values, always download service group configuration properties from the service group design view.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 Click **Service Group**.
The service group configuration page appears and all the service groups are displayed.

Step 3 For the desired service group, click **...** and choose **Clone Service Group**.

A clone of the original service group appears in the service group design view. Note the following points:

- By default, the cloned service group name and VM names are suffixed with a unique string.
- To view any VM configuration, click a VM in service chains.

- Cisco vManage marks the service chains that require configuration as **Unconfigured**, next to the edit button of the service chain.

Step 4 Modify the service group name, if required. Provide a description for the service group.

Step 5 To configure a service chain, use one of the following methods:

- Click the edit button for a service chain, enter the values, and then click **Save**.
- Download the configuration values from a CSV file, modify the values, upload the file, and then click **Save**. See Steps 6, 7, 8 on how to download, modify, and upload a CSV file.

The cloned service group appears on the service group configuration page. You can now download the updated service group configuration values.

Step 6 To download the cloned service group configuration values, do one of the following:

Note The download and upload of a CSV file is supported for creating, editing, and cloning of the service groups that aren't attached to a cluster.

- On the service group configuration page, click a cloned service group, click **More Actions** to the right of the service group, and choose **Download Properties (CSV)**.
- In the service group design view, click **Download CSV** in the upper right corner of the screen.

Cisco vManage downloads all configuration values of the service group to an Excel file in CSV format. The CSV file can consist of multiple service groups and each row represents configuration values for one service group. To add more rows to the CSV file, copy service group configuration values from existing CSV files and paste them in this file.

For example, ServiceGroup1_Clone1 that has two service chains with one VM in each of the service chains is represented in a single row.

Note In the Excel file, the headers and their representation in the service chain design view is as follows:

- sc1/name represents the name of the first service chain.
- sc1/vm1/name represents the name of the first VNF in the first service chain.
- sc2/name represents the name of the second service chain.
- sc2/vm2/name represents the name of the second VNF in the second service chain.

Step 7 To modify service group configuration values, do one of the following:

- To modify the service group configuration in the design view, click a cloned service group from the service group configuration page.

  Click any VM in service chains to modify the configuration values, and then click **Save**.

- To modify the service group configuration using the downloaded Excel file, enter the configuration values in the Excel file manually. Save the Excel file in CSV format.

Step 8 To upload a CSV file that includes all the configuration values of a service group, click a service group in the service group configuration page, and then click **Upload CSV** from the right corner of the screen.

Click **Browse** to choose a CSV file, and then click **Upload**.

You can view the updated values displayed for the service group configuration.

Note You can use the same CSV file to add configuration values for multiple service groups. But, you can update configuration values for a specific service group only, when uploading a CSV file using Cisco vManage.

Step 9 To know the representation of service group configuration properties in the CSV file and Cisco vManage design view, click a service group from the service group configuration page.

Click **Show Mapping Names**.

A text appears next to all the VMs in the service chains. Cisco vManage displays this text after mapping it with the configuration properties in the CSV file.

Create Custom Service Chain

You can customize service chains,

- By including extra VNFs or add other VNF types.
- By creating new VNF sequence that isn't part of the predefined service chains.

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 33.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down. An empty service chain in the design view window is available.

Step 3 To add a VNF such as a router, load balancer, firewall, and others, click a VNF icon and drag the icon to its proper location within the service group box. After adding all required VNFs and forming the VNF service chain, configure each of the VNFs. Click a VNF in the service group box. The **Configure VNF** dialog box appears. Enter the following parameters:

a) Choose the software image to load from the **Disk Image/Image Package** (**Select File**) drop-down list.

Note You can select a qcow2 image file from Cisco vManage Release 20.7.1.

b) Choose a scaffold file from the **Scaffold File** (**Select File**) drop-down list if you have chosen a qcow2 image file.

Note This option is available from Cisco vManage Release 20.7.1.

c) Optionally, filter an image, a package file, or a scaffold file based on the name, version, and tags that you specified when uploading a VNF image.

Note This option is available from Cisco vManage Release 20.7.1.

d) Click **Fetch VNF Properties**.
e) In the **Name** field, enter a name of the VNF.
f) In the **CPU** field, enter the number of virtual CPUs required for the VNF.
g) In the **Memory** field, enter the amount of memory in megabytes to be allocated for the VNF.
h) In the **Disk** field, enter the amount of memory for storage in gigabytes to be allocated for the VNF.
i) Enter VNF-specific parameters, as required.

Note These VNF details are the custom variables that are required for Day-0 operations of the VNF.

j) Click **Configure**.

k) To delete the VNF or cancel the VNF configuration, click **Delete** or **Cancel** respectively.

The customized service chains are added to a service group.

Note You can customize a VNF sequence with only up to four VNFs in a service chain.

Physical Network Function Workflow

This topic outlines the sequence of operations that you require to create shared PNF devices, configure, and monitor them. To ensure that the PNF workflow is effective, ensure that cabling is accurate, and VLAN ports are on the right ports of Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C.

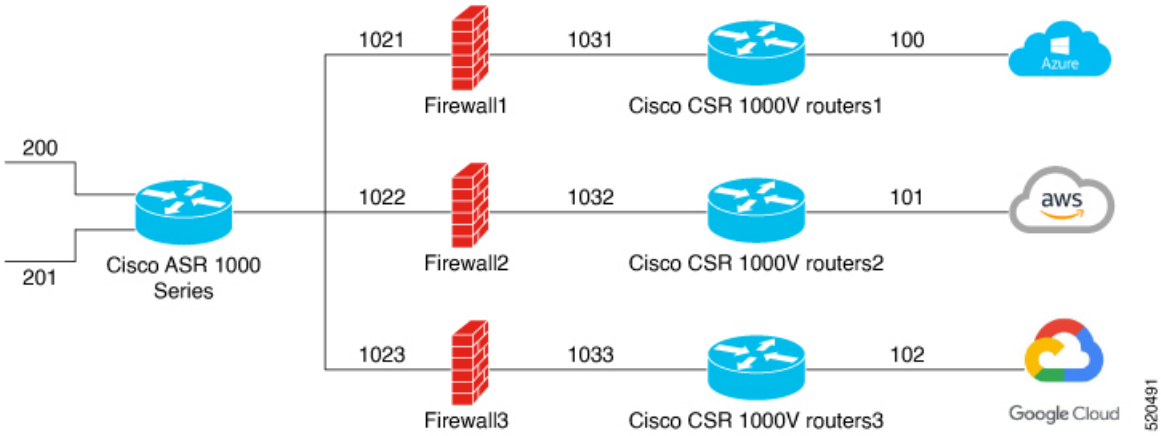
1. Connect the PNF devices to Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switch devices.
2. To make Cisco ASR 1000 Series router managed by Cisco vManage, upload WAN edge router authorized serial numbers from the Cisco Smart Account. See the "Upload WAN Edge Router Serial Numbers from Cisco Smart Account" section in the System and Interfaces Configuration Guide.
3. Create service chains by using the added PNF devices. See Custom Service Chain with Shared PNF Devices, on page 44.
4. Attach the service group to a cluster and check the configuration parameters that are generated. See Attach or Detach a Service Group in a Cluster, on page 56.
5. Configure the PNF and the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switch devices according to the configuration parameters generated. See Configure PNF and Cisco Catalyst 9500 Switches, on page 47.

In the following image, the first PNF is shared with multiple service chains. These service chains access different cloud applications in Microsoft Azure, AWS, and Google Cloud. The traffic from VLAN 200 enters the Cisco ASR 1000 series PNF based on SD-WAN policy definition and fetches the next hop firewall based on VRF configuration and corresponding destination application. The return traffic should traverse the same path for each application traffic.

To configure the PNF,

1. Log into the ASR1000 Series device, and configure it based on the VLAN and IP address information available from Cisco vManage.
2. To allow specific VLANs on both inbound and outbound traffic, configure the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switch ports where the PNF devices are connected.

Figure 6: PNF Shared with Multiple Service Chains



Custom Service Chain with Shared PNF Devices

You can customize service chains by adding supported PNF devices.

Caution Ensure that you don't share PNF devices across colocation clusters. A PNF device can be shared across service chains, or across service groups. However, a PNF device can now be shared only across a single cluster.

Table 13: Feature History

Feature Name	Release Information	Feature Description
Manage PNF Devices in Service Chains	Cisco SD-WAN Release 19.2.1	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.

Before you begin

To create a customized service chain by adding a router or firewall to an existing service chain, ensure that you note the following points:

- If a PNF device needs to be managed by Cisco vManage, ensure that the serial number is already available in Cisco vManage, which can then be available for selection during PNF configuration.
- The FTD device can be in any position in a service chain.
- An ASR 1000 Series Aggregation Services Routers can only be in the first and last position in a service chain.
- PNF devices can be added across service chains and service groups.

- PNF devices can be shared across service groups. They can be shared across service groups by entering the same serial numbers.
- PNF devices can be shared across a single colocation cluster, and can't be shared across multiple colocation clusters.

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 33.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down list. An empty service chain in the design view window is available. At the left, a set of VNF devices and PNF devices that you can add into the service chain appears. The 'V' in the circumference of VNF devices represents a VNF and 'P' in the circumference of PNF devices represent a PNF.

Note Ensure that you choose the **Create Custom** option for creating service chains by sharing PNF devices.

Step 3 To add a PNF such as physical routers, physical firewalls in a service chain, click the required PNF icon, and drag the icon to the proper location within the service chain box.

After adding all required PNF devices, configure each of them.

a) Click a PNF device in the service chain box.

The **Configure PNF** dialog box appears. To configure a PNF, enter the following parameters:

b) Check **HA Enabled** if HA is enabled for the PNF device.

c) If the PNF is HA enabled, ensure that you add the HA serial number in **HA Serial**.

If the PNF device is FTD, enter the following information.

1. In the **Name** field, enter a name of the PNF.
2. Choose Routed or Transparent mode as the **Firewall Mode**.
3. In the **PNF Serial** field, enter the serial number of the PNF device.

If the PNF device is ASR 1000 Series Aggregation Services Routers, enter the following information.

1. Check the **vManaged** check box if the device is managed by Cisco vManage.
2. Click **Fetch Properties**.
3. In the **Name** field, enter a name of the PNF.
4. In the **PNF Serial** field, enter the serial number of the PNF device.

d) Click **Configure**.

Step 4 To add service chains and share PNF devices, repeat from Step 2.

Step 5 To edit an existing PNF configuration, click the PNF.

Step 6 In the **Share NF To** drop-down list, choose the service chains with which the PNF should be shared.

After a PNF is shared, if you hover over a PNF, the respective shared PNF devices are highlighted in blue color. However, the PNFs from different service groups aren’t highlighted in blue color. After you choose an NF to be shared, a blue color

rim appears. If the same PNF is shared across multiple service chains, it can be used in different positions by dragging and placing the PNF icons in a specific positon.

Figure 7: Single PNF in a Service Chain

The following image shows a service chain that consists of a single PNF, Ftd_Pnf (not shared with other service chains).

Figure 8: Two PNF Devices in Service Chains

The following image shows service chains that consist of two PNFs, FTdv_PNF shared across service chain 1 (SC1) and service chain 2 (SC2) and ASR_PNF (non-shared).

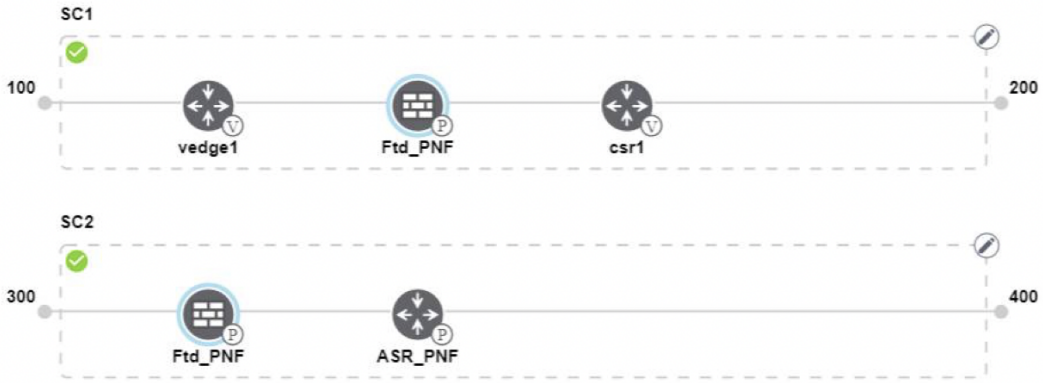
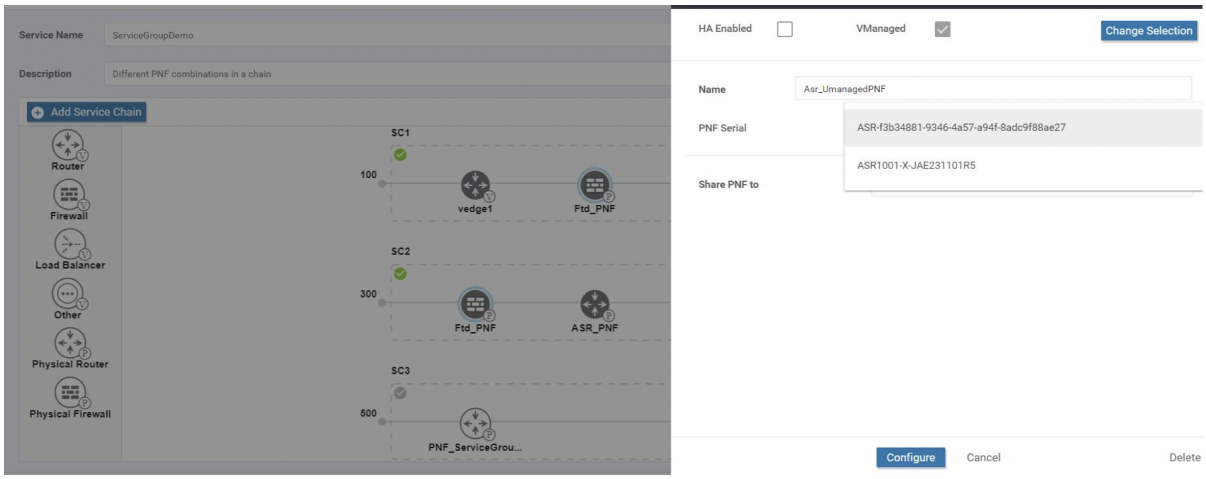


Figure 9: Three PNF Devices in Service Chains

The following image shows service chains that consist of three PNF devices in two different positions along with Cisco vManage configuration.



Step 7 To delete or cancel a Network Function configuration, click **Delete** or **Cancel** respectively.

You must attach the service groups to a colocation cluster. After attaching service groups that contain PNF devices, the PNF configuration isn't automatically pushed to the PNF devices unlike VNF devices. Instead, you must manually configure the PNF device by noting configuration that is generated on the Monitor window. The VLANs must be also configured on the Cisco Catalyst 9500-40X switch devices. See the ASR 1000 Series Aggregation Services Routers Configuration Guides and Cisco Firepower Threat Defense Configuration Guides for more information about the specific PNF configuration.

Configure PNF and Cisco Catalyst 9500 Switches

Step 1 Identify ports from the switches where the PNF devices should be added, which are part of a service chain. To verify the availability of the ports, see .

Step 2 Connect with Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C by using either the terminal server of any of the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches or use the **vty session** command with the IP address of the active switch.

Step 3 Configure VLANs from the generated configuration parameters on Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches with interfaces that are connected to the PNF. See the Monitor screen for the generated VLAN configuration.

Step 4 To configure an FTD or an ASR 1000 Series device, note the configuration from the **Monitor** window and then manually configure it on a device.

Custom Service Chain with Shared VNF Devices

You can customize service chains by including supported VNF devices.

Table 14: Feature History

Feature Name	Release Information	Feature Description
Share VNF Devices Across Service Chains	Cisco SD-WAN Release 19.2.1	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation.

Before you begin

Ensure that you note the following points about sharing VNF devices:

- You can share only the first, last, or both first and last VNF devices in a service chain.
- You can share a VNF with a minimum of one more service chain and maximum up to five service chains.
- Each service chain can have a maximum of up to four VNF devices in a service chain.
- You can share VNF devices only in the same service group.

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 33.

Step 2 In the **Add Service Chain** dialog box, enter the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, monitoring health information of a service chain, and service chain configuration. Click **Add**.

For the service chain configuration, choose **Create Custom** from the drop-down list. An empty service chain in the design view window is available. At the left, a set of VNF devices and PNF devices that you can add into the service chain appears. The 'V' in the circumference of VNF devices represents a VNF and 'P' in the circumference of PNF devices represent a PNF.

Note Ensure that you choose the **Create Custom** option for creating a shared VNF package.

Step 3 To add a VNF such as a router, load balancer, firewall, and others, click a VNF icon from the left panel, and drag the icon to a proper location within the service chain box.

After adding all required VNF devices, configure each of them.

a) Click a VNF in the service chain box.

The **Configure VNF** dialog box appears. To configure VNF, enter the following parameters:

b) From the **Image Package** drop-down list, choose the software image to load.

To create a customized VNF package from Cisco vManage, see Create Customized VNF Image.

c) Click **Fetch VNF Properties**.
d) In the **Name** field, enter a name of the VNF.
e) In the **CPU** field, enter the number of virtual CPUs required for the VNF.
f) In the **Memory** field, enter the amount of memory in megabytes to be allocated for the VNF.
g) In the **Disk** field, enter the amount of memory for storage in gigabytes to be allocated for the VNF.
h) Enter VNF-specific parameters, as required. See Create Service Chain in a Service Group, on page 33 for more information about VNF-specific properties.

These VNF-specific parameters are the custom user variables that are required for Day-0 operations of a VNF.

For a complete information about the list of user and system variables for different VNF types when located at various positions, see Shared VNF Use Cases, on page 49 and Custom Packaging Details for Shared VNF .

Note Ensure that you enter the values of the user variables if they are defined as mandatory, and the system variables are automatically set by Cisco vManage.

i) Click **Configure**.

Step 4 To share VNF devices, repeat from Step 2.

Step 5 To edit an existing VNF configuration, click the VNF.

Step 6 Scroll down the VNF configuration to find the **Share NF To** field. From the **Share NF To** drop-down list, choose the service chains with which the VNF should be shared.

After a VNF is shared, if you hover over a VNF, the specific shared VNF devices are highlighted in blue color. After you choose an NF to be shared, a blue rim appears on it.

Step 7 To delete a VNF or cancel the VNF configuration, click **Delete** or **Cancel** respectively.

You must attach service groups to a cluster.

Shared VNF Use Cases

The following are the sample images for some of the shared VNF use cases and their predefined variable list:

Figure 10: Shared–Cisco vEdge Router VNF in First Position

The Cisco vEdge Router VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor (ASAv firewall) is in HA mode.

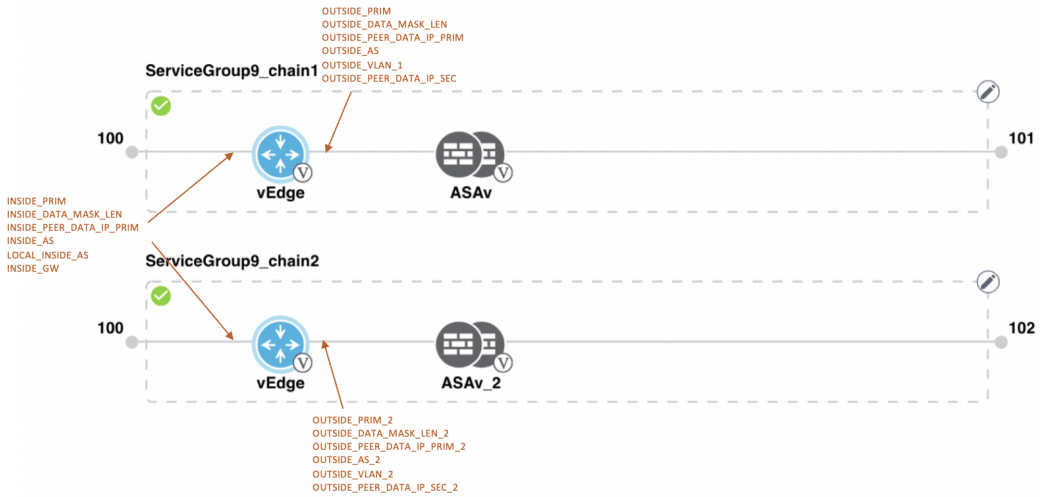


Figure 11: Shared–Cisco vEdge Router VNF in First Position

The Cisco vEdge Router VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

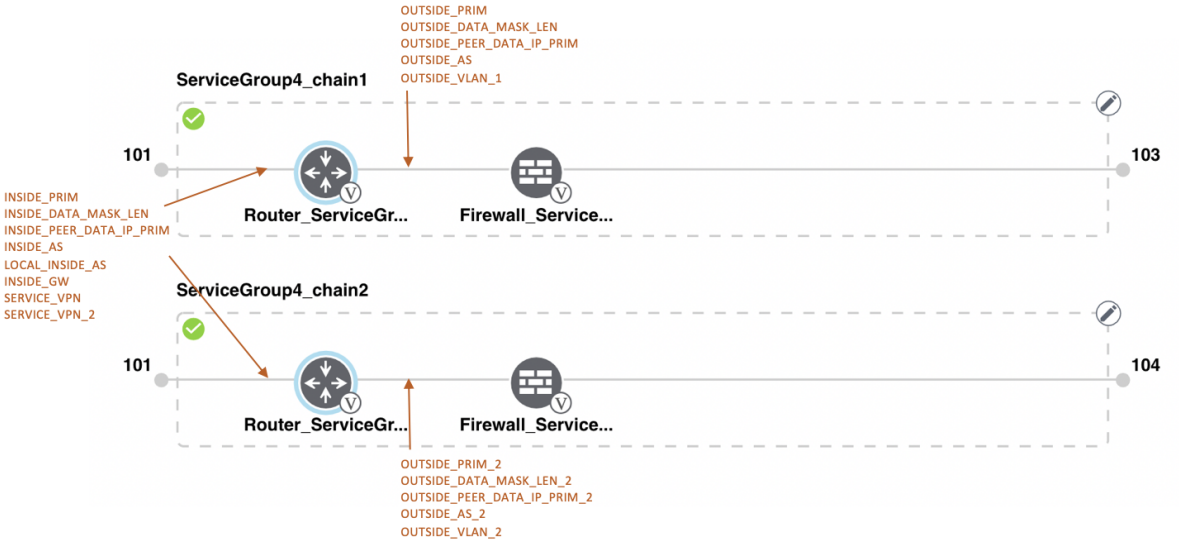


Figure 12: Shared–Cisco vEdge Router VNF in First Position

The Cisco vEdge Router VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in trunk mode (VNF-tagged) and the neighbor is in StandAlone mode.

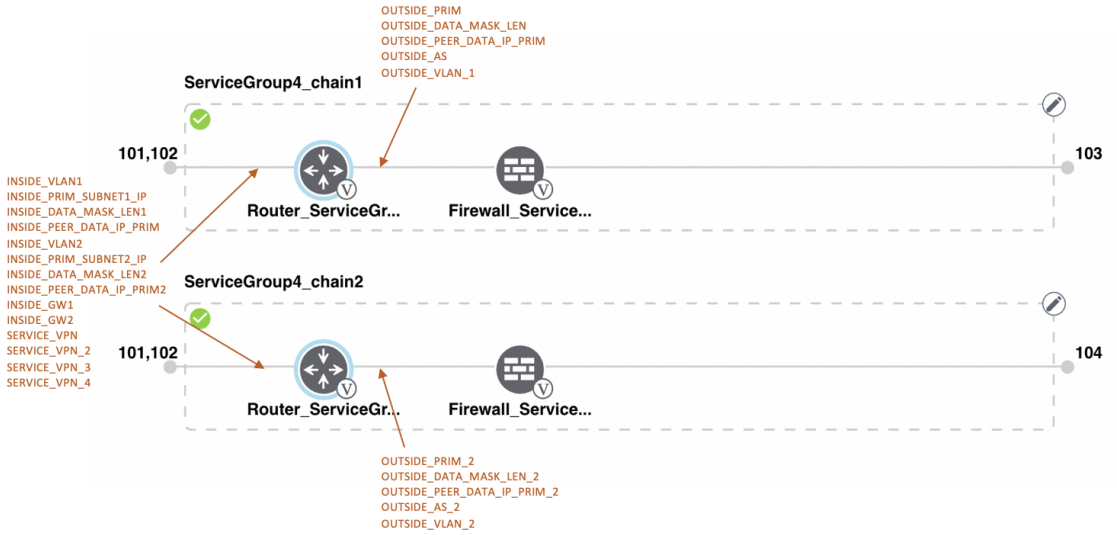


Figure 13: Shared–Cisco vEdge Router VNF in First Position

The Cisco vEdge Route VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in trunk mode (VNF-tagged) and the neighbor is in HA mode.

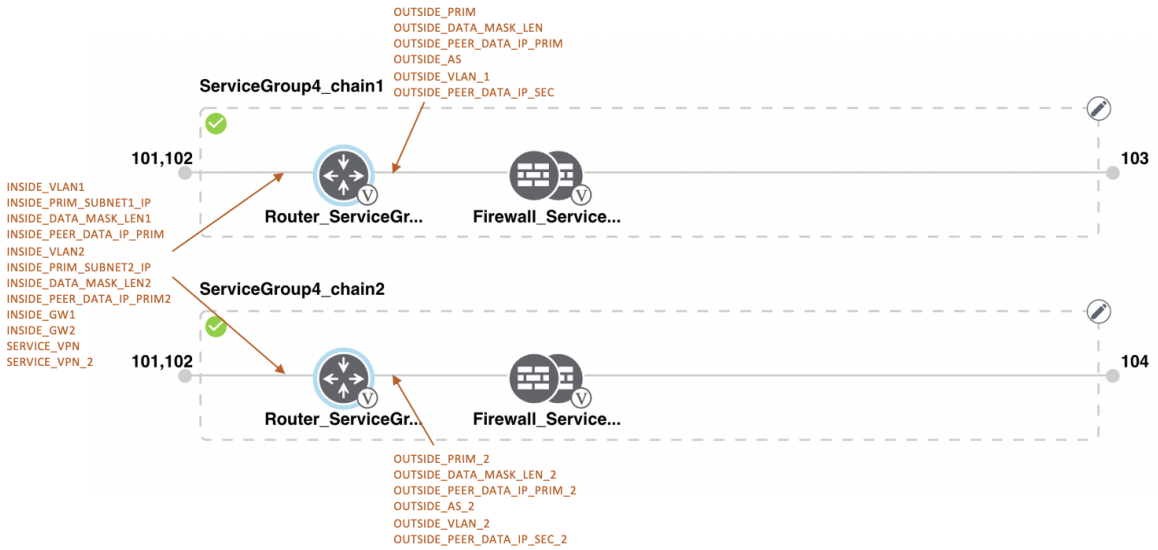


Figure 14: Shared-Cisco CSR1000V VNF in Last Position

The Cisco CSR1000V VNF in the last position is shared with the second service chain in the second position. The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor (ASAv firewall) is in StandAlone mode.

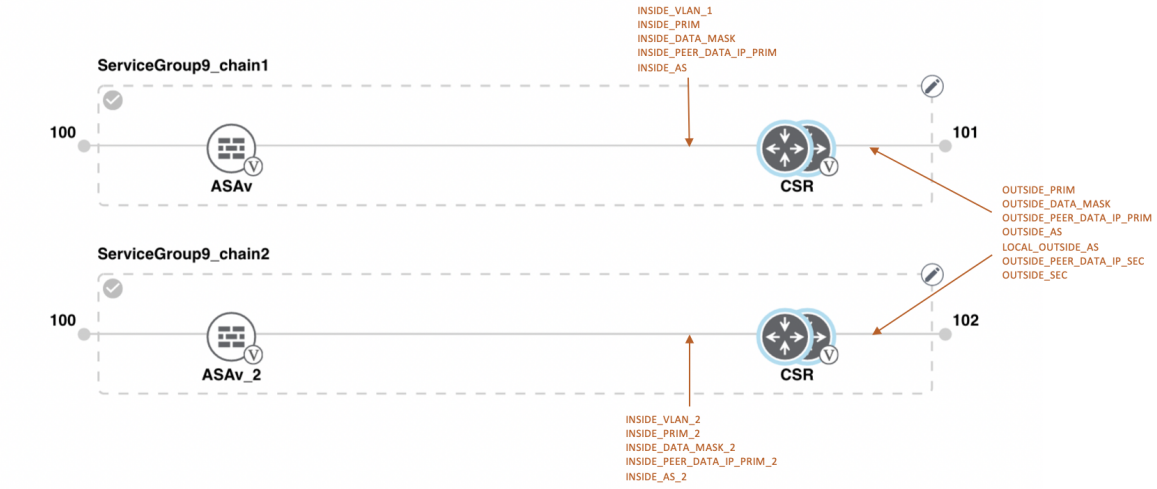


Figure 15: Shared–Cisco CSR1000V VNF in Last Position

The Cisco CSR1000V VNF in the last position is shared with the second service chain in the second position. The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

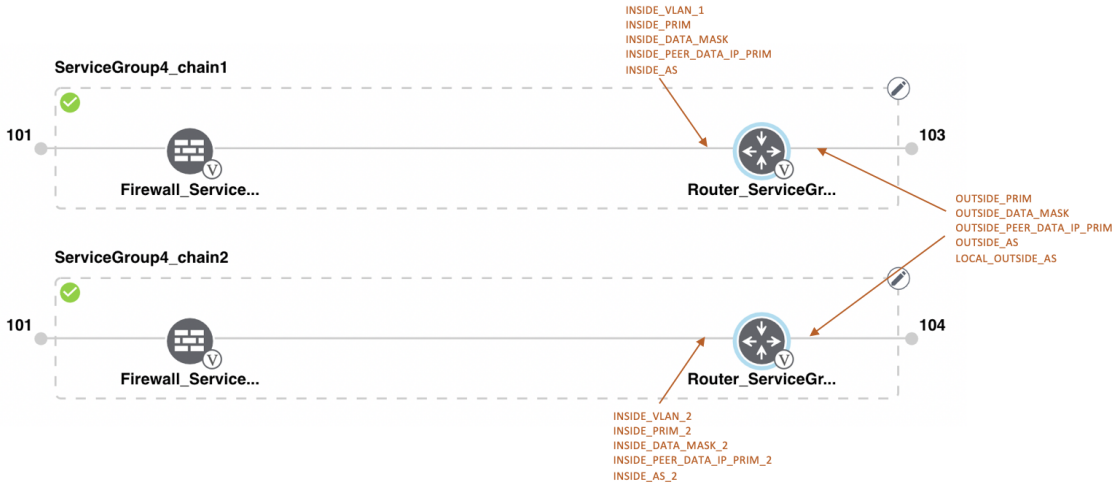


Figure 16: Shared–Cisco CSR1000V VNF in Last Position

The Cisco CSR1000V VNF in the last position is shared with the second service chain in the second position. The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor (Firewall_Service) is in HA mode.

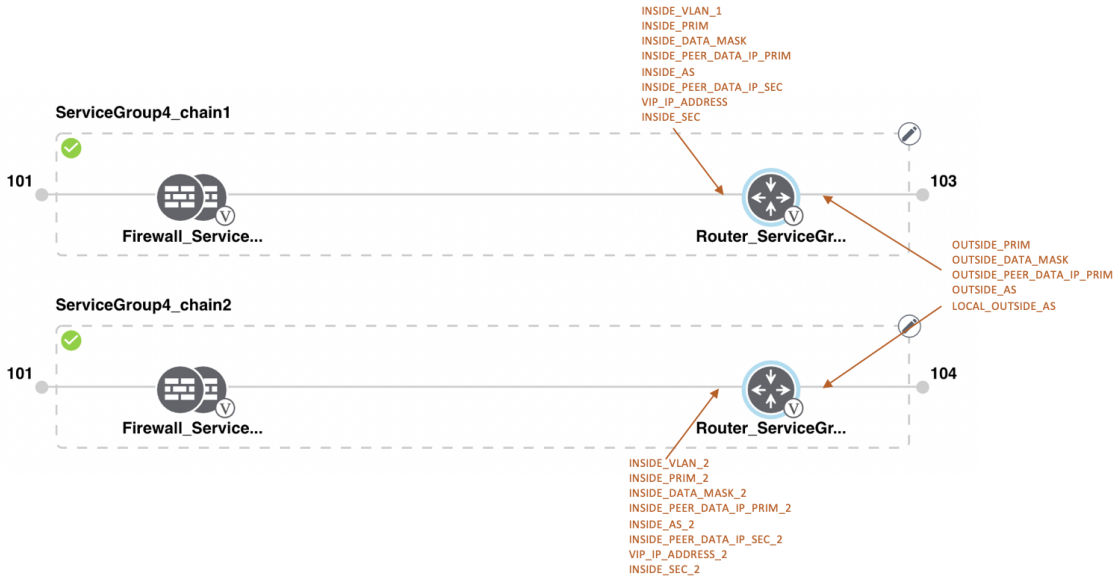


Figure 17: Shared–Cisco CSR1000V VNF in Last Position

The Cisco CSR1000V VNF in the last position is shared with the second service chain in the second position. The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor (Firewall_Service) is in HA mode.

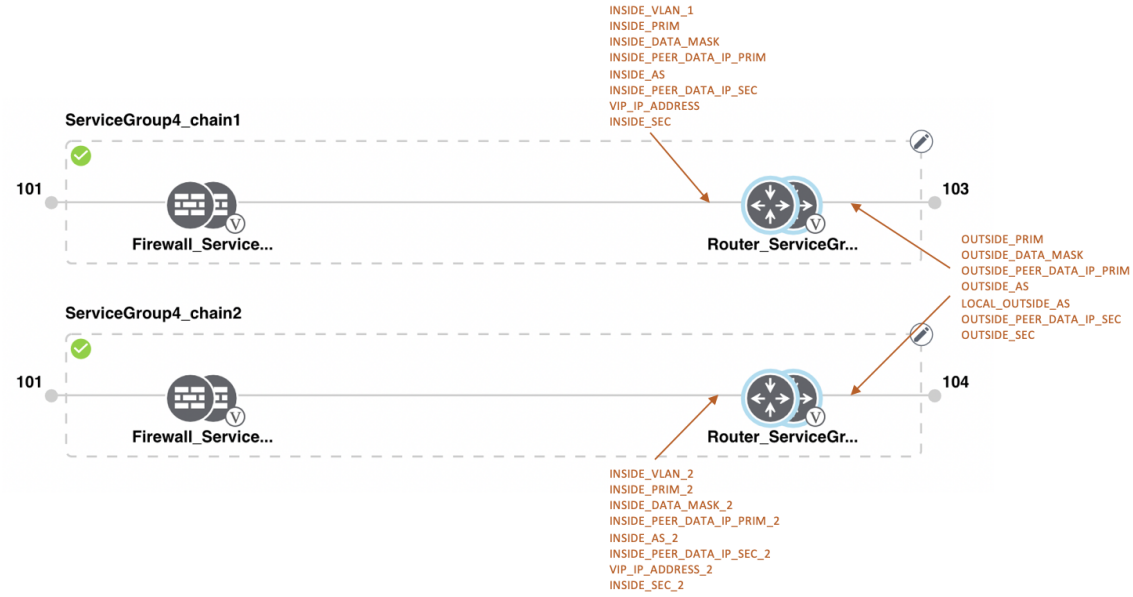


Figure 18: Shared–ASAv VNF in First Position

The ASAv VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in redundant mode.

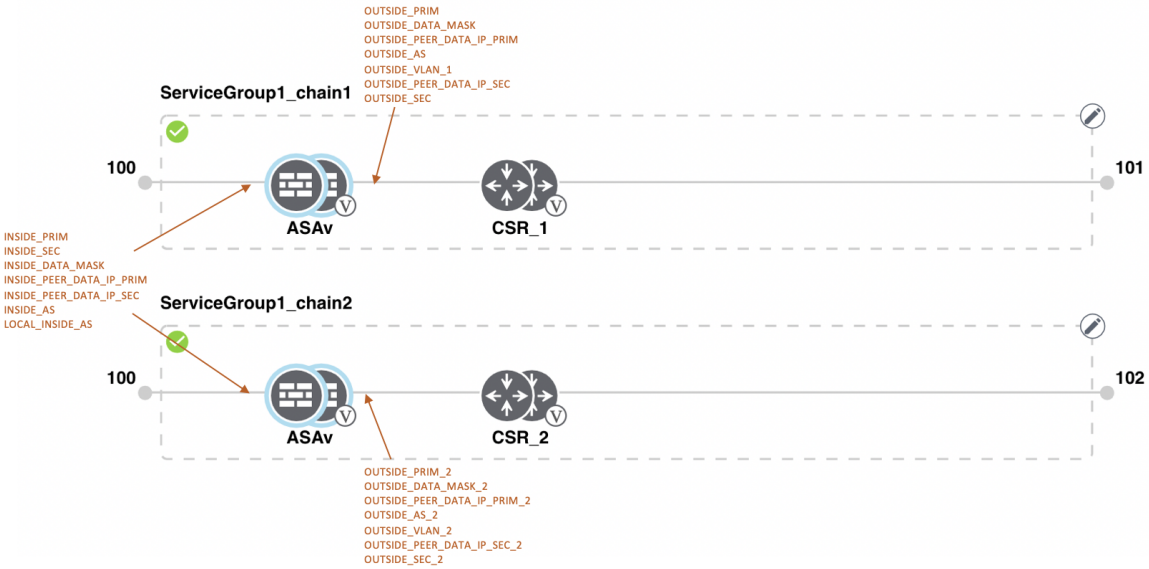


Figure 19: Shared–ASAv VNF in First Position

The ASAv (Firewall_Service) VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

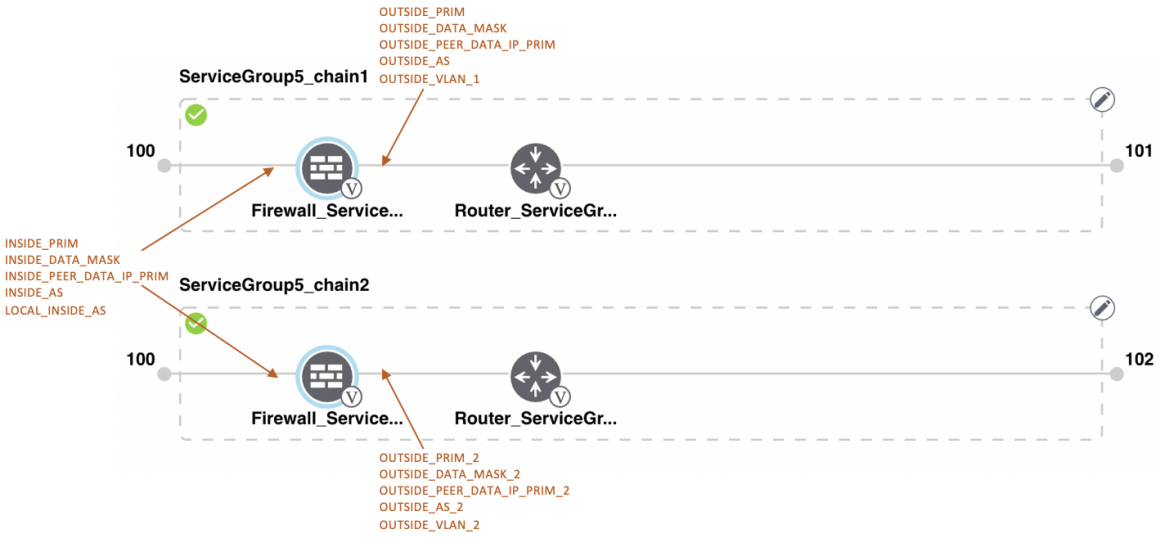


Figure 20: Shared–ASAv VNF in First Position

The ASAv (Firewall_Service) VNF in the first position is shared with the second service chain in the first position. The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor, which is a router is in redundant mode.

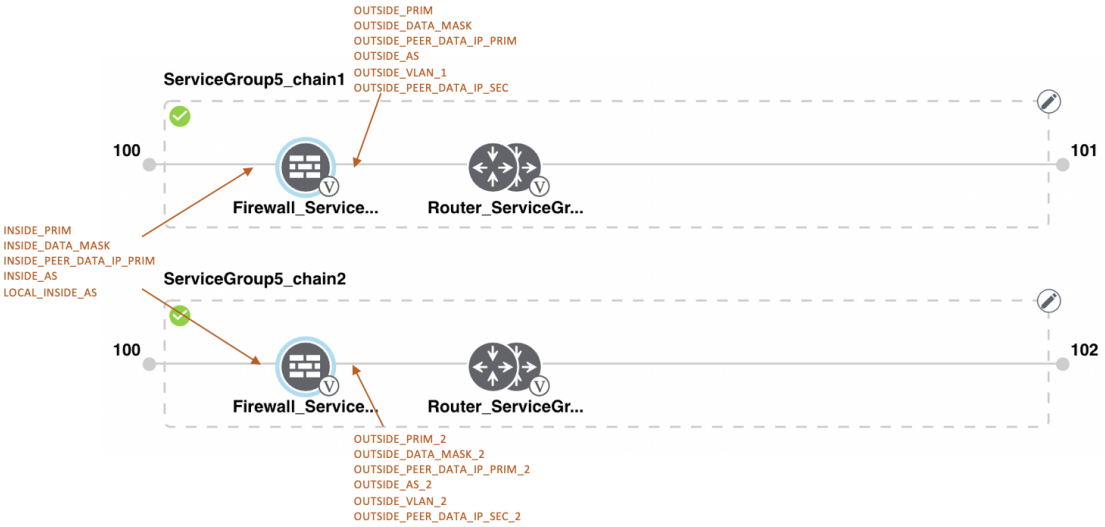
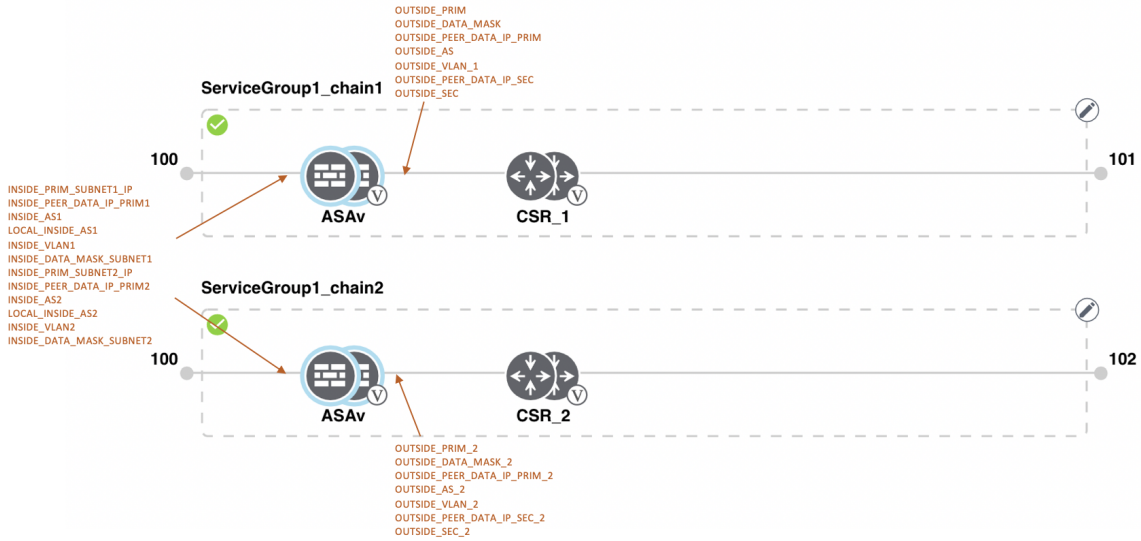


Figure 21: Shared–ASAv VNF in First Position

The ASAv VNF in the first position in HA mode is shared with the second service chain in the first position. The input to the first VNF is in trunk mode (vnf-tagged) and the neighbor is in redundant mode.



View Service Groups

To view service groups, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 Click **Service Group**.

Step 3 For the desired service group, click **...** and choose **View**.

You can view the service chains in the design window.

Edit Service Groups

Before attaching a service group with a cluster, you can edit all parameters. After attaching a service group with a cluster, you can only edit monitoring configuration parameters. Also, after attaching a service group, you can only add new service chains but not edit or attach a service chain. Hence, ensure that you detach a service group from a cluster before editing an existing service chain. To edit and delete a service group, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 Click **Service Group**.

Step 3 For the desired service group, click **...** and choose **Edit**.

Step 4 To modify either service chain configuration or modify a VNF configuration, click a router or firewall VNF icon.

Step 5 To add new service chains, click **Add Service Chain**.

Attach or Detach a Service Group in a Cluster

To complete the Cisco SD-WAN Cloud onRamp for Colocation configuration, you must attach service groups to a cluster. To attach or detach a service group to and from a cluster, perform the following steps:

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**.

Step 2 Click **...** adjacent to the corresponding cluster and choose **Attach Service Groups**.

Step 3 In the **Attach Service Groups** dialog box, choose one or more service groups in **Available Service Groups** and click **Add** to move the selected groups to **Selected Service Groups**.

Step 4 Click **Attach**.

Step 5 To detach a service group from a cluster, click **...** adjacent to the corresponding cluster and choose **Detach Service Groups**.

You can't attach or detach a single service chain within a service group.

Step 6 In the **Config Preview** window that is displayed, click **Cancel** to cancel the attach or detach task.

Note .

Step 7 To verify if service groups are attached or detached, you can view the status using Cisco vManage. Note the following points:

- If the status of the tasks in the **Task View** window is displayed as **FAILURE** or in **PENDING** for a long duration, see Troubleshoot Service Chain Issues .
- If a Cisco Colo Manager task fails, see Troubleshoot Cisco Colo Manager Issues.

If a colocation cluster moves to **PENDING** state, for a cluster, click **...**, and choose **Sync**. This action moves the cluster back to **ACTIVE** state. The **Sync** option keeps Cisco vManage synchronized with the colocation devices.

Day-N Configuration Workflow of Cisco SD-WAN Cloud onRamp for Colocation Solution

The following is the background process for a Day-N configuration.

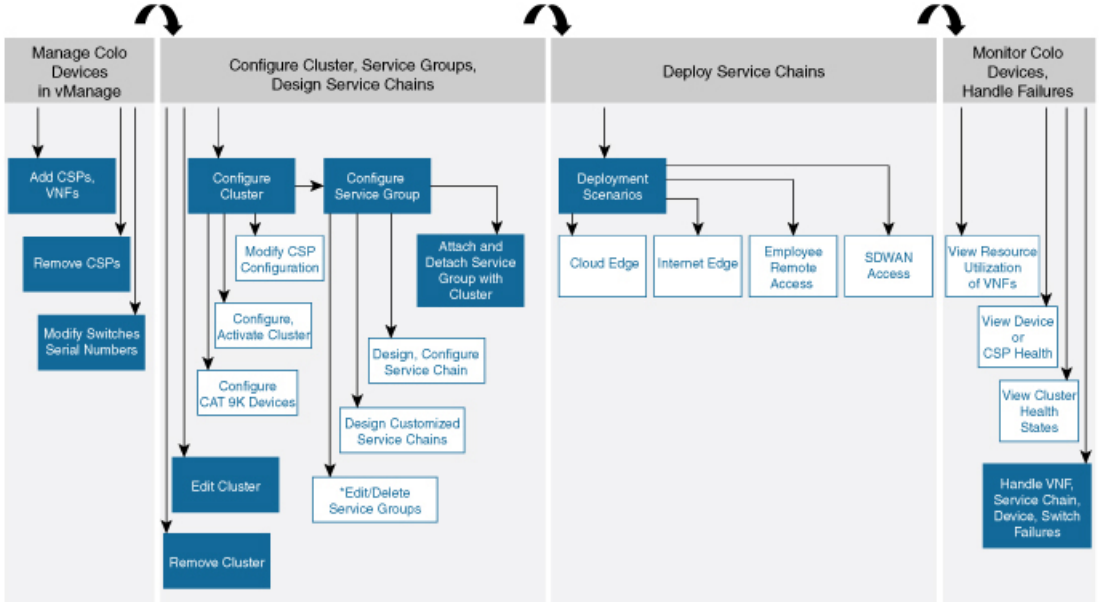
- All Day-N configuration from Cisco vManage requires clusters to be in-sync (devices have to be in synchronization with Cisco vManage) state.
- When attaching a service group with a cluster, Cisco vManage runs the Placement logic to determine which VMs are placed on specific CSP devices.
- Switch-related Day-N configuration from Cisco vManage requires Cisco Colo Manager to be in a Healthy state.
- Cisco vManage saves all switch-related service chain, cluster, switch configuration to Cisco Colo Manager.
- Cisco Colo Manager moves to In-progress state for any configuration that it receives from Cisco vManage.

- Cisco Colo Manager translates all global and service chain configuration of Cisco Colo Manager into the device-specific configuration.
- Cisco Colo Manager reports the states to Cisco vManage whether a configuration push is a success or failure.
- All the Day-N service chain or VM configuration is sent to CSP devices.
- CSP devices send notification to Cisco vManage about the VM file download status.
- After all VMs are downloaded, Cisco vManage sends the bulk configuration to bring up all VMs.
- CSP devices send notifications to Cisco vManage about VM that are brought up and the states.
- If any switch devices return error, Cisco vManage reports error with a detailed information and the cluster moves to a FAILURE state.

Ensure that you fix errors that are based on notifications and error messages, and then activate the Cloud OnRamp for Colocation cluster again.

Note During the Day-N configuration, you can modify Serial Number of switches for both the switches devices.

Figure 22: Day-N Workflow



Note *You can only edit service groups after they are detached from a cluster.