

Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 19.2

First Published: 2018-12-20

Last Modified: 2019-08-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface vii

Audience vii

Related Documentation vii

List of Acronyms and Abbreviations viii

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

About Cisco SD-WAN Cloud OnRamp for Colocation Solution 1

Cisco SD-WAN Cloud OnRamp for Colocation Solution Overview 1

Cisco SD-WAN Cloud OnRamp for Colocation Solution Components 2

CHAPTER 2

Prerequisites and Requirements of Cisco SD-WAN Cloud OnRamp for Colocation Solution 5

Cisco SD-WAN Cloud OnRamp for Colocation Solution Requirements 5

Hardware Requirements 5

Software Requirements 6

Wiring Requirements 7

Prerequisites for Deploying Solution 8

Ordering and Sizing of Cisco SD-WAN Cloud OnRamp for Colocation Devices 9

CHAPTER 3

Get Started with Cisco SD-WAN Cloud OnRamp for Colocation Solution 11

Cisco SD-WAN Cloud OnRamp for Colocation Solution–Deployment Workflow 11

Cluster Activation Flow 12

Cluster Deactivation Flow 12

Service Chain Deployment 12

Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP 13

Log Into CIMC User Interface 13

Activate Virtual Device 14

Map NFVIS Cloud OnRamp for Colocation Image 15
Bring Up Cloud Services Platform Devices 15
Bring Up Switch Devices 17
Bring Up Cisco Colo Manager 19
Provision and Configure CloudOnRamp for Colocation 20
Provision DHCP Server Per Colocation 20
Device Port Connectivity Details and Service Chaining 21
Validated Service Chains 24
Validated VM Packages 25
Customized Service Chains 26

CHAPTER 4 **Configure Cisco SD-WAN Cloud OnRamp for Colocation Devices from vManage** 27
Add Cloud OnRamp Colocation Devices into vManage 27
Delete Cloud OnRamp for Colocation Devices from vManage 27
Manage Clusters in vManage 28
Provision and Configure Cluster 30
Create and Activate Clusters 31
Cluster Settings 35
View Cluster from vManage 36
Edit Cluster in vManage 37
Add CSP Device to Cluster 38
Delete or RMA CSP Device from Cluster 39
Delete CSP with CCM 41
Remove PNF Devices from Cluster 42
Remove Cluster from vManage 42
Remove and Replace Switch 43
Reactivate Cluster from vManage 45
Manage Service Groups 46
VNF Placement for Service Chains in vManage 46
Create Service Chain in a Service Group 46
Create Custom Service Chain 50
Physical Network Function Workflow 51
Custom Service Chain with Shared PNF Devices 52
Configure PNF and Catalyst 9500 55

Custom Service Chain with Shared VNF Devices 55
Shared VNF Use Cases 57
View Service Groups in vManage 63
Edit Service Group in vManage 63
Attach and Detach Service Group with Cluster 64
Day-N Configuration Workflow of Cisco SD-WAN Cloud OnRamp for Colocation Solution 65

CHAPTER 5 **Software Image Management (SWIM) for Cluster Components and SWIM 67**
Manage VM Catalog and Repository 67
VNF Image Format 68
Upload VNF Images in vManage Repository 68
Create Customized VNF Image 69
View VNF Images in vManage Repository 74
Delete VNF Images from vManage Repository 74
Upgrade NFVIS Software Through vManage 75
Upload NFVIS Upgrade Image 75
Upgrade CSP Device with NFVIS Upgrade Image 76

CHAPTER 6 **Monitor Cisco SD-WAN Cloud OnRamp for Colocation Devices 79**
Monitor Operational Status of Cloud OnRamp for Colocation Devices from vManage 79
View Information About VNFs from vManage 81
View Cisco Colo Manager Health from vManage 81
Monitor Cloud OnRamp Colocation Clusters from vManage 84
Cisco Colo Manager States for Switch Configuration 87
Cisco Colo Manager States and Transitions from Host 87
Cisco Colo Manager Notifications 88
VM Alarms 90
Cloud Services Platform Real-Time Commands 91

CHAPTER 7 **High Availability 93**
Redundancy 93
Redundancy of Network Fabric 94
Redundancy of x86 Compute Hardware 94
Redundancy of Physical NIC or Interface 94

Redundancy of NFVIS, Virtualization Infrastructure 94
Redundancy of Service Chain or VNF 94
Recovery of Cisco Colo Manager 95
Handle Various Failure Scenarios 95

CHAPTER 8 **Troubleshoot Cisco SD-WAN Cloud OnRamp for Colocation Solution** 97
Troubleshoot Catalyst 9500 Issues 97
Troubleshoot Cloud Services Platform Issues 102
DHCP IP Address Assignment 107
Troubleshoot Cisco Colo Manager Issues 108
Troubleshoot Service Chain Issues 108
Troubleshoot Physical Network Function Management Issues 110
Log Collection from CSP 110
Troubleshoot vManage Issues 111

CHAPTER 9 **Custom Packaging Details for Shared VNF** 113
vEdge Variable List 113
CSR Variable List 117
ASAv Variable List 121



Preface

This guide provides information about how to configure and deploy Cisco SD-WAN Cloud OnRamp for Colocation solution on a supported Cisco hardware device. The guide also provides details on virtual machine deployments, configuration of software features.

This guide assumes that readers have a broad understanding of networking terminologies and principles. It also assumes prior exposure to current trends in multi-cloud offerings.

- Audience, on page vii
- Related Documentation, on page vii
- List of Acronyms and Abbreviations, on page viii
- Obtaining Documentation and Submitting a Service Request, on page ix

Audience

This guide is intended for network administrators and operators who are familiar with basic Linux installation and configuration requirements.

Related Documentation

- Configuration Guide for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Configuration Guide for Cisco Catalyst 9500 Switches
- Cisco Cloud Services Platform 5000 Hardware Installation Guide
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM

List of Acronyms and Abbreviations

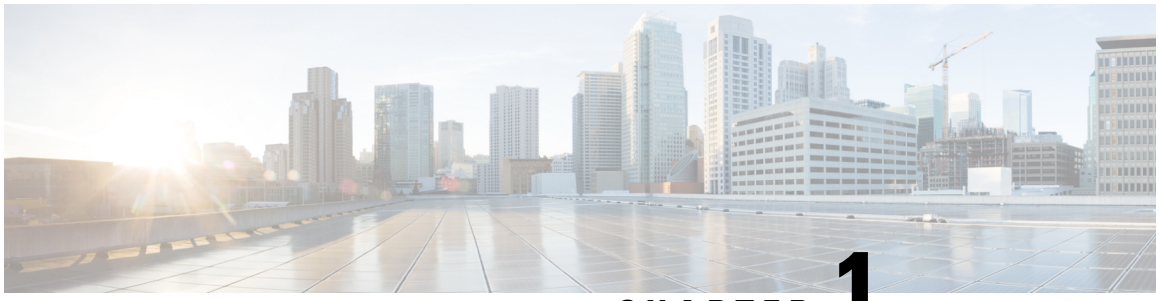
Table 1: List of Acronyms and Abbreviations

Acronym or Abbreviation	Expansion
CSP	Cloud Services Platform
CIMC	Cisco Integrated Management Controller
Cisco SD-WAN Cloud OnRamp for Colocation	Name of the solution
DHCP	Dynamic Host Configuration Protocol
DNA	Digital Network Architecture
DMZ	Demilitarized Zone
NAT	Network Address Translation
NSO	Network Services Orchestrator
FP	Function Pack (NSO)
NIC	Network Interface Controller
NFVIS	Network Function Virtualization Infrastructure Software
OVS	Open Virtual Switch
SD-WAN	Software-defined Wide Area Networking
SR-IOV	Single Root IO Virtualization
STUN	Session Traversal Utilities for NAT
SWIM	Software Image management
VEPA	Virtual Ethernet Port Aggregator
VM	Virtual Machine
VNF	Virtual Network Function
PNF	Physical Network Function
vNIC	Virtual Network Interface Controller

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

About Cisco SD-WAN Cloud OnRamp for Colocation Solution

- Cisco SD-WAN Cloud OnRamp for Colocation Solution Overview, on page 1
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Components, on page 2

Cisco SD-WAN Cloud OnRamp for Colocation Solution Overview

Digitization is placing high demands on IT to increase their speed of services and products that are delivered to customers, partners, and employees, while maintaining a high level of security. The interconnectivity between users and applications is becoming complex digital business architecture. This means network must be fast and flexible to meet the expanding changes and demand. At the same time, users want to increase the speed and reduce complexity of deployment without compromising the security.

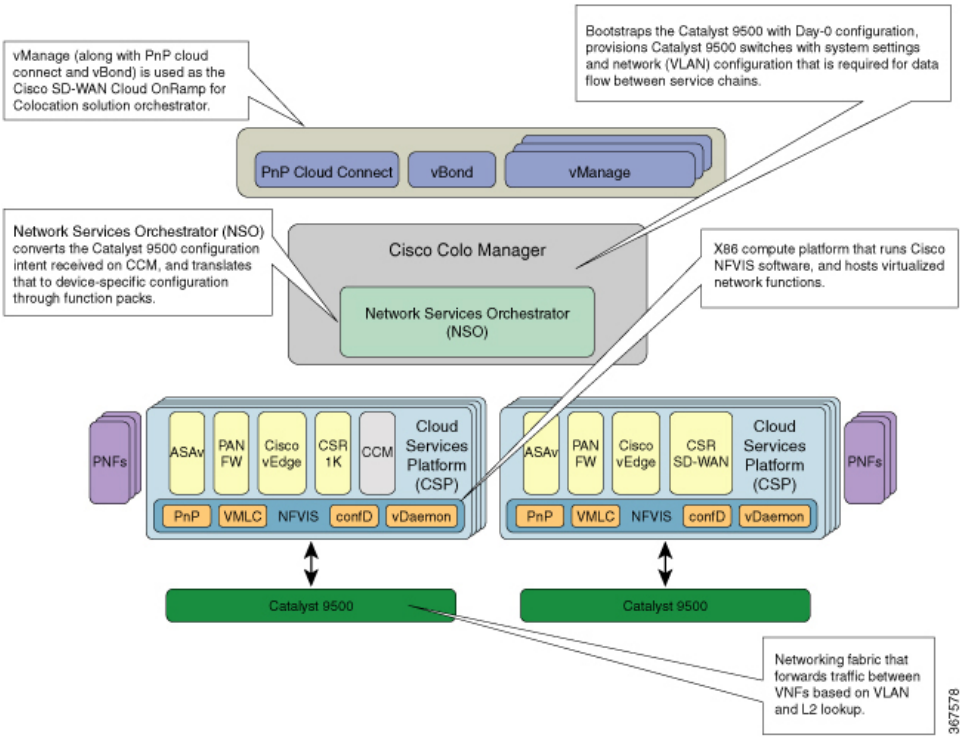
A Cloud OnRamp for Colocation is a campus, large branch, or a colocation, where the traffic gets aggregated. Cisco SD-WAN Cloud OnRamp for Colocation solution is a flexible architecture that securely connects to enterprise applications that are hosted in the enterprise data center, public cloud, private or hybrid cloud to its endpoints such as, employees, devices, customers, or partners. This functionality is achieved by using Cloud Services Platform 5000 (CSP 5444) as the base Network Function Virtualization (NFV) platform that securely connects endpoints of an enterprise to applications. By deploying Cisco SD-WAN Cloud OnRamp for Colocation solution in colocation centers, customers can virtualize network services and other applications, and consolidate them into a single platform. The primary goal of the Cisco SD-WAN Cloud OnRamp for Colocation solution is to facilitate secure multicloud connectivity for Enterprise customers.

The Cisco SD-WAN Cloud OnRamp for Colocation solution offers the following benefits:

- Performance—Enterprises can optimize application performance by strategically placing the Cisco SD-WAN Cloud OnRamp for Colocation solution in colocation centers that are closest to the SaaS and public IaaS cloud providers.
- Agility—By virtualizing network services, enterprises can simplify their operations. Scaling up and down, and adding new services can now be done remotely. The Cisco Network Function Virtualization Infrastructure Software (NFVIS) on CSP 5444 negates the need to order, cable, rack, and stack dedicated hardware appliances when capacity must be increased or changes are required.
- Security—The centralization of communication patterns between employees, customers, partners, and applications allows for better and more consistent implementation of security policies.

- Cost savings—By having a central location to connect to various clouds (including private clouds), enterprises can optimize the cost of circuits to connect their users to applications. The circuit costs for a colocation facility are less than in a private data center.

Figure 1: Cisco SD-WAN Cloud OnRamp for Colocation Solution Architectural Overview



The Cisco SD-WAN Cloud OnRamp for Colocation solution can be deployed in multiple colocations. A colocation is a stack of compute and networking fabric that brings up multiple virtual networking functions and multiple service chains on them. This stack connects branch users, endpoints to a hybrid cloud or data center. vManage is used as the orchestrator to provision the devices in a colocation. Each colocation does not have visibility of other colocations in the same site or across sites.

Cisco SD-WAN Cloud OnRamp for Colocation Solution Components

The various components of Cisco SD-WAN Cloud OnRamp for Colocation solution are:

- **Cisco Cloud Services Platform 5444** —Cloud Services Platform (CSP) is an x86 Linux hardware platform that runs NFVIS software. It is used as the compute platform for hosting the virtual network functions in the Cisco SD-WAN Cloud OnRamp for Colocation solution. Multiple CSP 5444 systems can be used in a Cisco SD-WAN Cloud OnRamp for Colocation deployment.

  Cisco Network Function Virtualization Infrastructure Software —The Cisco Network Function Virtualization Infrastructure Software (NFVIS) software is used as the base virtualization infrastructure software running on the x86 compute platform. The Cisco NFVIS software provides VM lifecycle management, VM service chaining, VM image management, platform management, PNP for bootstrapping

a device, AAA features, syslog, and SNMP server. The NFVIS software provides programmable REST and netconf APIs for all the mentioned functionalities. See the NFVIS Functionality Changes for SD-WAN Cloud OnRamp for Colocation in NFVIS documentation.

- **Virtual Network Functions** —The Cisco SD-WAN Cloud OnRamp for Colocation solution supports both Cisco-developed and third-party virtual network functions (VNFs). The following table includes the validated VNFs and their versions:

Table 2: Validated Virtual Network Functions

Virtual Network Functions	Version
Cisco CSR1000v	16.9.1, 16.10.1, 16.11.1, 16.12.1
Cisco ASAv	9.9.2, 9.10.1, 9.12.2
Cisco FTDv	6.2.3, 6.3, 6.4.0.1
Cisco vEdge Cloud	18.4, 19.1, 19.2
Cisco IOS XE SD-WAN	16.12.1
Palo Alto Firewall (PAFW)	8.0.5, 8.1.3, 9.0.0
Fortinet Firewall	6.0.2
AVI Load Balancer	18.2.1, 18.1.3

To validate third-party VNFs on the Cisco SD-WAN Cloud OnRamp for Colocation solution, you can avail the Cisco certification program. See https://developer.cisco.com/site/nfv/#the-ecosystem-program for more information about validating third-party VNFs.

- **Physical Network Functions** —A Physical Network Function (PNF) is a physical device that is dedicated to provide a specific network function as part of a colocation service chain such as a router, firewall. The following are the validated PNFs and their versions:

Table 3: Validated Physical Network Functions

Physical Network Functions	Version
Cisco FTD	6.4.0.1
Cisco ASR 1000 Series	16.12.1

- **Network Fabric** —Forwards traffic between the VNFs in a service chain by using a L2 and VLAN-based lookup. The last VNF can forward traffic to the network fabric either through L2 or L3 forwarding. The Catalyst 9500-40X switch that supports 40 10G ports and two 40G ports is used as network fabric.
- **Mangament Network** —A separate management network connects the NFVIS software running on the CSP systems, the virtual network functions, and the switches in fabric. This management network is also used for transferring files and images into and out of the systems. The Out of Band management switch configures the management network. The IP addresses assigned to the CSP devices and Catalyst 9500 switches is acquired by the management network pool through DHCP configuration. The orchestrator manages VNF management IP addresses and assigns through the VNF Day-0 configuration file.
- **Virtual Network Function Network Connectivity** — A VNF can be connected to the physical network by using either Single Root IO Virtualization (SR-IOV) or through a software virtual switch. A VNF

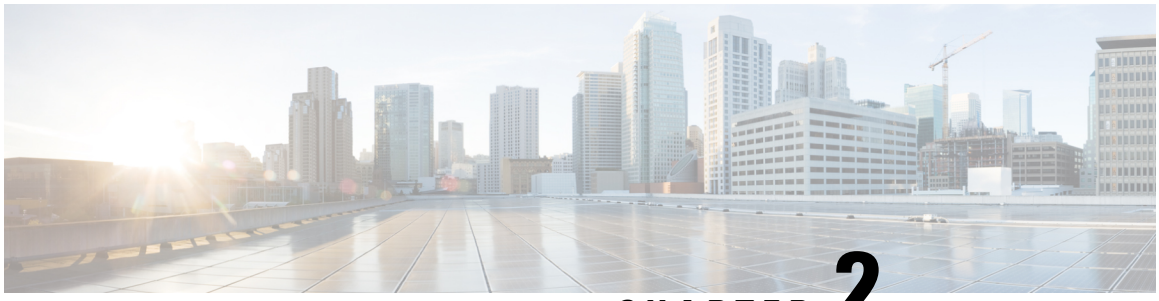
can have one or more virtual network interfaces (VNICs), which can be directly or indirectly connected to the physical network interfaces. A physical network interface can be connected to a software virtual switch and one or more VNFs can share the virtual switch. The Cisco SD-WAN Cloud OnRamp for Colocation solution manages the creation of virtual switch instances and the virtual NIC membership to create connectivity. By default, all the physical interfaces and the management interface in the CSP system are available for use by VNFs.

In Cisco SD-WAN Cloud OnRamp for Colocation deployments, SR-IOV interfaces are configured in Virtual Ethernet Port Aggregator (VEPA) mode. In this mode, the NIC sends all the traffic that is received from the VNFs to the external Catalyst 9500 switch. The Catalyst 9500 switches the traffic that is based on the L2 MAC address and VLAN. It can send the traffic back to the CSP or to an external connected network. The Catalyst 9500 switch ports that are connected to the CSP interfaces are configured in VEPA mode. When a VLAN is configured on a VNF VNIC, the VLAN must be configured on the connected port on Catalyst 9500.

A VNF using an SR-IOV interface and a VNF using the software switch can be service chained through the external switch fabric.

- **Physical Network Function Network Connectivity** — A PNF can be connected to the Catalyst 9500 switches ports, which are the free data ports available from the right side.
- **Service Chains** —In Cisco SD-WAN Cloud OnRamp for Colocation solution deployment, the traffic between the VNFs is service chained externally through Catalyst 9500. The service chaining requirement provides service chaining functionality to the traffic across VNFs running either on a single CSP or across multiple CSP systems in a cluster. The service chaining is based on the source and destination endpoints in the service chain and is not based on the provider application. In Cisco SD-WAN Cloud OnRamp for Colocation solution, L2 (VLAN, destination MAC address) based service chaining has been used. See Device Port Connectivity Details and Service Chaining for more information.
- **Cisco Colocation Manager** —The Cisco Colo Manager component is a software stack that manages switches. In this solution, Cisco Colo Manager is hosted on NFVIS software in a docker container. The CSP devices host Cisco Colo Manager along with PNFs and VNFs as shown in the solution architectural overview.

  A single Cisco Colo Manager instance per cluster is brought up in one of the CSP devices after activating a cluster. The Cisco Colo Manager software accepts the Catalyst 9500 configuration and monitors them. See Configure Cisco SD-WAN Cloud OnRamp for Colocation Devices from vManage for more information.
- **Orchestration through vManage** —The Cisco vManage is used for orchestrating the Cisco SD-WAN Cloud OnRamp for Colocation solution. The orchestrator provides the following functionalities:
  - **vBond** —The vBond orchestrator provides vManage information to the network elements that may be running behind Network Address Translation (NAT). It performs initial authentication and authorizes the network elements to provide the Session Traversal Utilities for NAT (STUN) server functionality.
  - **vManage** —vManage is an SDN controller that provides centralized configuration management, monitoring, and troubleshooting of the Cloud OnRamp for Colocation.
  - **vOrchestrator**—An orchestration layer that automates provisioning of the vBond and vManage controllers for a specific tenant.



CHAPTER 2

Prerequisites and Requirements of Cisco SD-WAN Cloud OnRamp for Colocation Solution

- Cisco SD-WAN Cloud OnRamp for Colocation Solution Requirements, on page 5
- Prerequisites for Deploying Solution, on page 8
- Ordering and Sizing of Cisco SD-WAN Cloud OnRamp for Colocation Devices, on page 9

Cisco SD-WAN Cloud OnRamp for Colocation Solution Requirements

The following are the hardware, software, Cloud OnRamp for Colocation cluster, and cabling requirements for deploying Cisco SD-WAN Cloud OnRamp for Colocation solution.

Hardware Requirements

The following table lists the hardware requirements:

Table 4: Hardware Requirements

Components	Hardware Requirements
Compute platform	Cloud Services Platform (CSP) 5444
Physical form factor	Cisco UCS C240 M5SX (2RU)
Processor cores	44 physical cores **Note** To get predictable VNF performance, disable hyper threading (HT) on the processor cores.
PCIe NIC slots	6
Disk	8 * 1.2 TB = 9.6 TB
Disk slots	26 (24 useable)

Components	Hardware Requirements
Memory	192 GB of RAM
RAID	12-Gbps SAS HW controller, 4 GB flash-backed write cache (FBWC), RAID 10.
Base Networking	4x1PCIE card in M5 6x1GE Intel i350 ports, 2x1GE LoM **Note** 2-GigE interfaces in a port channel configuration are required for the NFVIS and VM management traffic.
Network Interface Cards (NIC)	2xIntel X520 2-port 10G (Niantic) and Intel XL710 4-port 10G SFP+ (Fortville) **Note** Two Fortville 10G interfaces in port-channel configuration and connected to a virtual switch. This connectivity is required for production traffic to or from the VMs, which support only virtio interface. **Note** Two Fortville 10G interfaces in port-channel configuration and connected to a virtual switch. This configuration is required for VNF HA state synchronization between VNFs hosted on two different CSP systems. **Note** Four Niantic 10G interfaces in SR-IOV mode. The VMs that need high performance and low latency network connectivity to bypass the hypervisor or virtual switch require these interfaces. The VMs that can support SR-IOV must be connected to the SR-IOV virtual function (VFs). Link redundancy is not available in this mode. **Note** Ensure that the Fortville NIC (X710) is placed in riser 1, slot-2 and Niantic cards (X520) in riser1, slot 1; and riser 2, slot 4.
Processors (2)	2xIntel Xeon Gold 6152 Series
Power Supplies	Dual power
Network fabric	**Catalyst 9500-40X** Supports 40 10G ports and two 40G ports
Management network	Any switch with sufficient number of 1G ports and port channel feature can be used as the management switch. Two switches are recommended to support hardware and link redundancy.

Software Requirements

The following table lists the software requirements:

Table 5: Software Requirements

Components	Software Requirements
Virtualization infrastructure software	Cisco NFVIS Cloud OnRamp for Colocation See Release Notes for Cisco SD-WAN Cloud OnRamp for Colocation Solution.
Orchestration	Cisco vManage See • Cisco SD-WAN Product Documentation for more information. • Cisco SD-WAN Release Notes for more information about the latest vManage features.

All CSP devices and switches must run same version of software in a Cloud OnRamp for Colocation. Any new software version for all devices in a colocation is hosted on vManage, upon availability.

Supported Platforms and Firmware

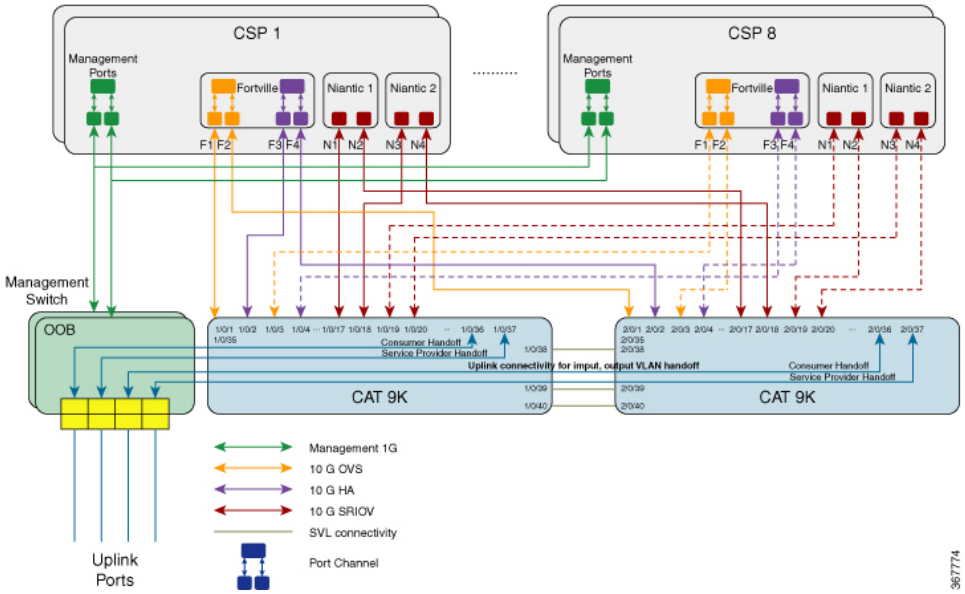
The following table lists the supported platform and firmware versions for Cisco NFVIS:

Platform	Firmware	Version
CSP-5444	BIOS	C240M5.4.0.1g.0.0912180338
	CIMC	4.0.1(c)

Wiring Requirements

The following figure shows the high-level design of the physical connectivity in a cloud onramp for colocation.

Figure 2: Cisco SD-WAN Cloud OnRamp for Colocation Physical Connectivity



In the preceding topology, each CSP has two management ports that are connected to two 1-GB ports on the Management switch. Each of the Catalyst 9500 switch is connected to the 1-GB port. This connectivity requires two ports on the Management switch per cloud onramp for colocation. The service provider handoff is connected to 10-GB ports on this switch. All service providers ports are trunked in to the Catalyst 9500 switch. All the VLANs are configured on all ports of Catalyst 9500. To achieve redundancy for this Management switch, connect another Management switch and use it for redundancy in a cloud onramp for colocation.

Note Management switches are not orchestrated and must be manually provisioned. Although OOB switches are not orchestrated, ensure that all management switches and devices are connected as per the defined topology.

Note Ensure that you provide initial configuration including VLAN POOL, IP address POOL, syslog server information per cloud onramp for colocation.

If vManage cannot reach CSP devices and Cisco Colo Manager cannot reach switches, the devices are shown as down. The serviceability dashboard within vManage shows the port status of CSP devices and switches after Cisco Colo Manager is brought up.

Prerequisites for Deploying Solution

The following are prerequisites for deploying the Cisco SD-WAN Cloud OnRamp for Colocation solution:

- A minimum of two CSP 5444 SD-WAN NH PID (two Niantics and one Fortville) required. You can order more CSP devices as per the number of service chains that are required per cluster (including HA instances). Also, consider the throughput requirement or number of sessions terminating the cloud onramp for colocation when ordering the number of CSP devices.

- A smart account that is required to propagate the ordered devices to the PNP cloud and vOrchestrator.
- Two Catalyst 9500-40X and OOB switches and a DHCP server per cluster are required.
- Port channel copper, RJ45, and data SFP along with cables for connectivity are required.
- Cisco ASR 1000 series or a router for WAN termination are required.
- Terminal server for configuring switches and CIMC is required.
- Split management IP pool per cluster into two parts. Configure one part on a DHCP server by considering number of physical devices in a cluster and IP addresses required for broadcast and gateway. Configure the other part of management IP pool on the vManage for VNFs and Cisco Colo Manager. The first IP address in the vManage management pool is used for Cisco Colo Manager. Ensure that you configure this IP address and PNP server for the switch.
- OOB management switch is required to terminate the traffic.

Ordering and Sizing of Cisco SD-WAN Cloud OnRamp for Colocation Devices

The cloud onramp for colocation cluster requirements can be categorized into small, medium, large, and extra large clusters that is based on throughput and compute demands.

Consider the following criteria to determine the various cloud onramp for colocation size categories:



Note The cloud onramp for colocation size must be determined before orchestration when ordering the devices such as, CSP devices and Catalyst 9500 switches.

- Depending on the number of connections that are required for public clouds and the number of customers trying to reach these clouds, decide the number of required service chains.
- Depending on the policies that must be enforced, decide the number of VMs required in each service chain.
- From the preceding two criteria, you can determine on an average the throughput that is required per service chain.

In a single Cisco SD-WAN Cloud OnRamp for Colocation deployment, you can deploy between two to eight CSP systems in a cluster. The following table provides information about the cloud onramp for colocation size requirements:

Table 6: Cisco SD-WAN Cloud OnRamp for Colocation Size Requirements

User Configurable				Cisco SD-WAN Cloud OnRamp for Colocation Generated Information			
Cloud OnRamp for Colocation Size	Number of Service Chain	Average VMs per Service Chain	Throughput per Service Chain (MBPS)	Number of CSP Devices	Cores per Site	Throughput Consumed (GBPS)	Throughput per CSP (GBPS)
X-Large	20	4	2	8	240-320	320	50
Large	15	4	2	6	160-240	240	50
Medium	10	4	2	4	60-160	160	50
Small	5	4	2	2	80	80	50

To determine the throughput per CSP and throughput that is consumed, you can calculate it as follows for a medium-sized cloud onramp for colocation.

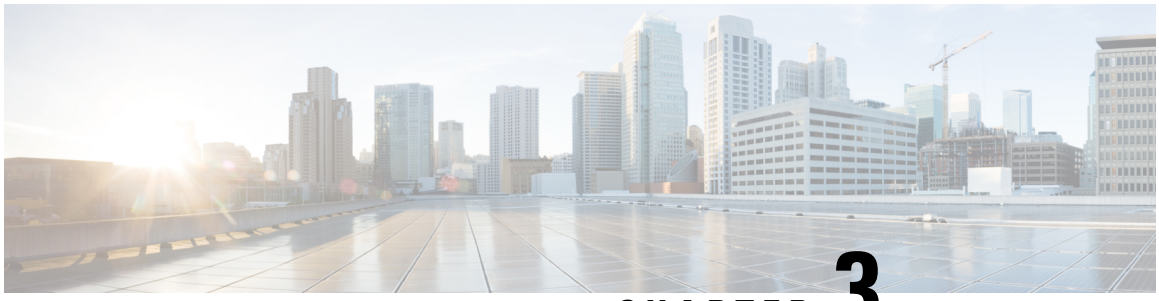
- Throughput per CSP—Each CSP device has four 10-GB SR-IOV ports, one port channel (two-10GB vNICs) for data and one port channel (two-10GB vNICs) for HA. Hence, the throughput per CSP node is:

  4*10+2*5+0=50GBPS

- Compute or Throughput consumed—For a medium-sized cloud onramp for colocation, assumptions are that each VM requires 4vCPU, each site requires ten service chains, throughput per service chain is two, and number of VMs in a service chain is two. Hence, the compute values is:

  4 CPU per Service Chain*10Service Chain*Throughput per service chain*number of VMs=160 cores per site

The maximum bidirectional throughput for a cluster is 20 GBPS.



CHAPTER 3

Get Started with Cisco SD-WAN Cloud OnRamp for Colocation Solution

- Cisco SD-WAN Cloud OnRamp for Colocation Solution–Deployment Workflow, on page 11
- Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP , on page 13
- Bring Up Cloud Services Platform Devices, on page 15
- Bring Up Switch Devices, on page 17
- Bring Up Cisco Colo Manager , on page 19
- Provision and Configure CloudOnRamp for Colocation, on page 20

Cisco SD-WAN Cloud OnRamp for Colocation Solution–Deployment Workflow

This topic outlines the sequence of how to get started with the colo devices and build clusters on vManage. Once a cluster is created and configured, you can follow the steps that are required to activate the cluster. Understand how to design service groups or service chains and attach them to an activated cluster. The supported Day-N operations are also listed in this topic.

1. Complete the solution prerequisites and requirements. See Prerequisites and Requirements of Cisco SD-WAN Cloud OnRamp for Colocation Solution, on page 5.
    - Complete wiring the CSP devices (set up CIMC for initial CSP access) and Catalyst 9500 switches (set up console server) along with OOB or management switches. Power on all devices. See Wiring Requirements, on page 7.
    - Set up and configure DHCP server. See Provision DHCP Server Per Colocation, on page 20.
2. Verify the installed version of Cisco NFVIS and install NFVIS, if necessary. See Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP , on page 13.
3. Set up or provision a cluster. A cluster constitutes of all the physical devices including CSP devices and Catalyst 9500 switches. See Get Started with Cisco SD-WAN Cloud OnRamp for Colocation Solution, on page 11.
    - Bring up CSP devices. See Bring Up Cloud Services Platform Devices, on page 15.
    - Bring up Catalyst 9500 switches. See Bring Up Switch Devices, on page 17.

- Provision and configure a cluster. See Provision and Configure Cluster, on page 30.

  Configure a cluster through cluster settings. See Cluster Settings, on page 35.

4. Activate a cluster. See Create and Activate Clusters, on page 31.
5. Design service group or service chain. See Manage Service Groups, on page 46.

Note You can design a service chain and create a service group any time before creating clusters or activating clusters if all VMs are uploaded to repository.

6. Attach or Detach service group and service chains to a cluster. See Attach and Detach Service Group with Cluster, on page 64.

Note Service chains can be attached to a cluster after the cluster is active.

7. (Optional) Perform all Day-N operations.
   - Detach a service group to detach service chains. See Attach and Detach Service Group with Cluster, on page 64.
   - Add and delete CSP devices from a cluster. See Add Cloud OnRamp Colocation Devices into vManage, on page 27 and Delete Cloud OnRamp for Colocation Devices from vManage, on page 27.
   - Deactivate a cluster. See Remove Cluster from vManage , on page 42.
   - Reactivate a cluster. See Reactivate Cluster from vManage , on page 45.
   - Design more service group or service chain. See Create Service Chain in a Service Group, on page 46.

Cluster Activation Flow

To know more about cluster activation workflow, click Cluster Activation Flow.

Cluster Deactivation Flow

To know more about cluster deactivation workflow, click Cluster Deactivation Flow.

Service Chain Deployment

To know more about service chain deployment flow, click Service Chain Deployment.

Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP

This section provides information about a series of tasks you need to perform to install NFVIS Cloud OnRamp for Colocation on a Cisco CSP device.

Log Into CIMC User Interface

Before you begin

- Ensure that you have configured the IP address to access CIMC.
- If not installed, install Adobe Flash Player 10 or later on your local system.

For details on how to configure an IP address for CIMC, see the *Set up CIMC for UCS C-Series Server* guide on cisco.com.

For information about upgrading CIMC, see the CIMC Firmware Update Utility guide on cisco.com.

Procedure

Step 1 In your web browser, enter the IP address that you configured to access CIMC during initial setup.

Step 2 If a security dialog box displays, do the following:

a) **Optional**: Select the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

Step 3 In the log in window, enter your username and password.

When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.

Step 4 Click **Log In**.

The **Change Password** dialog box only appears the first time you log into CIMC.

Step 5 Change the password as appropriate and save.

The CIMC home page is displayed.

Step 6 From the **CIMC Server** tab, select **Summary**, and click **Launch KVM Console**.

The KVM Console opens in a separate window.

Step 7 From the **Virtual Media** menu on the KVM Console, select **Activate Virtual Devices**.

If prompted with an unencrypted virtual media session message, select **Accept this session**, and click **Apply**. The virtual devices are activated now.

Step 8 From the **Virtual Media** menu on the KVM Console, select **Map CD/DVD**.

Step 9 Browse for the installation file (ISO) on your local system, and select it.

Step 10 Click **Map Device**.

The ISO image file is now mapped to the CD/DVD.

Step 11 From the **CIMC Server** tab, select **BIOS**.

For more information about upgrading BIOS, see the BIOS Upgrade guide on cisco.com.

Step 12 From the **BIOS Actions** area, select **Configure Boot Order**.

The Configure Boot Order dialog box appears.

Step 13 From the **Device Types** area, select **CD/DVD Linux Virtual CD/DVD**, and then click **Add**.

Step 14 Select **HDD**, and then click **Add**.

Step 15 Set the boot order sequence using the **Up** and **Down** options. The **CD/DVD Linux Virtual CD/DVD** boot order option must be the first choice.

Step 16 To complete the boot order setup, Click **Apply**.

Step 17 Reboot the server by selecting the **Power Off Server** option from the Server Summary page in CIMC.

Step 18 After the server is down, select the **Power On Server** option in CIMC.

When the server reboots, the KVM console will automatically install Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.

Step 19 After the installation is complete, the system is automatically rebooted from the hard drive. Log into the system when the command prompt changes from "localhost" to "nfvis" after the reboot.

Wait for some time for the system to automatically change the command prompt. If it does not change automatically, press **Enter** to manually change the command prompt from "localhost" to "nfvis". Use **admin** as the login name and **Admin123#** as the default password.

Note
The system prompts you to change the default password at the first login. You must set a strong password as per the on-screen instructions to proceed with the application. You cannot run API commands or proceed with any tasks unless you change the default password at the first login. API will return 401 unauthorized error if the default password is not reset.

Step 20 You can verify the installation using the System API or by viewing the system information from the Cisco Enterprise NFVIS portal.

Note Ensure that the RAID configuration is 4.8 TB RAID-10. To configure RAID through CIMC, see the Cisco UCS Servers RAID Guide on cisco.com.

Activate Virtual Device

You will have to launch the KVM Console to activate virtual devices.

Before you begin

Ensure that you have the Java 1.6.0_14 or a higher version installed on your local system.

Procedure

Step 1 Download the Cisco Enterprise NFVIS image from a prescribed location to your local system.

Step 2 From CIMC, select the **Server** tab, and click **Launch KVM Console**.

Note
A JNLP file will be downloaded to your system. You must open the file immediately after it is downloaded to avoid the session timeout.

Step 3 Open the renamed *.jnlp* file. When it prompts you to download Cisco Virtual KVM Console, click **Yes**. Ignore all security warnings and continue with the launch.

The KVM Console is displayed.

Step 4 From the **Virtual Media** menu on the KVM Console, select **Activate Virtual Devices**.

If prompted with an unencrypted virtual media session message, select **Accept this session**, and click **Apply**. The virtual devices are activated now.

Map NFVIS Cloud OnRamp for Colocation Image

Procedure

Step 1 From the **Virtual Media** menu on the KVM Console, select **Map CD/DVD...**.

Step 2 Browse for the installation file (ISO) on your local system, and select it .

Step 3 Click **Map Device**.
The ISO image file is now mapped to the CD/DVD.

Step 4 From the KVM console, power cycle (warm reboot) and system installation process starts and NFVIS is installed.

Bring Up Cloud Services Platform Devices

This topic describes about bringing up the CSP devices through the Day-0 configuration. Before cloud onramp for colocation configuration and provisioning, ensure that CSP devices and the compute devices are connected as per the prescribed topology, and powered on. After devices are connected and powered on, the following process occurs:

Note The CSP devices already received the IP addresses from the DHCP server in a cloud onramp for colocation management subnet.

Procedure

Step 1 PNP agent in CSP reaches "Plug and Play" (PNP) Connect (Cisco cloud based PNP connect) through secure HTTPS. As part of the Cisco device order placement, the smart account information such as, Serial Number is populated in PNP connect.

Step 2 The CSP device performs PNP call home to reach a PNP server. The CSP device reaches PNP connect through secure https.

Step 3 PNP Connect sends the vBond IP address to the CSP device by using HTTPS and XMPP.

The PNP Server sends the organization name and Service Provider (SP) organization name along with the vBond IP to the CSP device.

Step 4 The CSP device establishes Datagram Transport Layer Security (DTLS) tunnel with vBond.

What to do next

1. Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.
2. Click **Configuration** > **Devices** from the side panel.

   You can view a list of all devices and its information in a tabular format. The CSP devices that have the serial number that is associated with the word token are not yet brought up. These devices must be brought up by configuring OTP.
3. To access CSP devices and set up control connection with vManage, configure the IP address to access Cisco Integrated Management Controller (CIMC) IP address and connect to CIMC.
4. Connect to the host by logging into NFVIS by using **admin** as the login name and **Admin123#** as the default password.

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

5. Validate the installed certificate. See Failures with Certificate installation, on page 102. Also, verify if root CA has been installed. See CSP has not established connectivity with vManage, on page 104.
6. To bring up a CSP device, use the **request activate chassis-number** *chassis-serial-number* **token** *token-number* command:

   For example,

   request activate chassis-number *CSP-5444-serial-number* **token** *70d43cfbd0b3b426da63dba2dd4f4c49*

During cluster activation process, the control connection to vManage happens by using the OTP that has been generated. Then, certificates get installed on CSP from vManage automatically and the control connection switches to certificate-based from OTP-based. The CSP device establishes DTLS tunnel with vManage. The DTLS tunnel manages the configuration of the CSP devices and retrieves the operational status of CSP devices, which reflects in vManage. To verify whether CSP device establishes DTLS connection with vManage, verify from the vManage interface:

From vManage, click **Configuration** > **Devices** from the side panel. You can view the CSP device with all details, as shown.



To bring up remaining CSP devices, repeat all the mentioned steps in parallel or serially for each of the CSP devices.

Bring Up Switch Devices

This section describes about how Catalyst 9500 switch devices are brought up through the Day-0 configuration.

Before you begin

Ensure that the following are considered before bringing up the switch devices:

- Catalyst 9500 devices have both Network-Advantage and DNA-Advantage licenses. To verify the available licenses on the switch devices, use the following command:

  ```
  Device# show license status
  ```

  To know more about the license usage information, see the **`show license usage`** command in the Catalyst 9500 Command Reference.

- Either PNP redirect setup or manual PNP profile being set on the switch devices is required. For a PNP redirect setup, add switches SN and Cisco Colo Manager IP address to PNP, and add entries of devicehelper.cisco.com to OOB router of the network if the DHCP server is on OOB router. For example,

  ```
  #conf t
  #ip host devicehelper.cisco.com <OOB router of the network>
  ```

- Ensure both switches are connected as per the SVL mode configuration.

Procedure

Step 1 Clean the switch configuration if they have been previously used.

a) Renumber switch, which is required for SVL stack mode.

Note
Ensure that the switches are not touched during SVL mode. Also, do not perform any action such as, pressing enter or space, which can cause switches to complete SVL.

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

b) To erase the switch startup configuration and return it to its initial state, use the **write erase** command.

c) To reload the switch with a new configuration, use the following commands in privileged EXEC mode and enter **no** for not saving the modified configuration:

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

Note

You do not need to save the configuration.

d) Perform steps b and c on the secondary switch device after the switch stack reloading has been completed. This action ensures that the secondary switch device is reloaded twice.

Step 2 After Catalyst 9500 boots up, it gets an IP address from the local DHCP server and initiates PNP discovery.

Step 3 The DHCP server with option 43 enables Catalyst 9500 to reach the PNP server in Cisco Colo Manager.

The Cisco Colo Manager IP address is the PNP server IP address of a cluster on vManage. Ensure that DHCP server with option 43 always point to the port, 9191.

Example:

The following is an example of local PNP server for switches:

```
ip dhcp pool Cat9k
network 10.114.11.39 255.255.255.0
dns-server 172.31.232.182
default-router 172.31.232.182
option 43 ascii "5A;B2;K4;I10.114.11.40;J9191”
```

Where, 10.114.11.40 is the local PNP server or Cisco Colo Manager IP address.

The output after setting DHCP server with option 43 to port, 9191 is:

```
ip dhcp excluded-address 172.31.232.182 172.31.232.185
ip dhcp excluded-address 172.31.233.182
ip dhcp excluded-address 172.31.232.254
ip dhcp excluded-address 172.31.23.10 172.31.23.49
ip dhcp excluded-address 172.31.23.52 172.31.23.100
ip dhcp excluded-address 172.31.23.252
ip dhcp excluded-address 172.31.23.253
ip dhcp excluded-address 172.31.23.230 172.31.23.250
!
```

Step 4 After the switches reach the PNP server on Cisco Colo Manager, it pushes the Day-0 configuration. The Day-0 configuration push happens if a cluster is activated on vManage. If a cluster is not activated, the Catalyst 9500 switches reach the PNP server on Cisco Colo Manager every minute and stays in backoff mode.

After the switch devices are brought up, the SSH connection and NETCONF sessions on the switch devices are enabled for Cisco Colo Manager to push Day-N configuration and ongoing switch management is continued.

Example

About Uplink Ports 36 and 37

As per prescriptive topology, ports 36 (input VLAN handoff) and 37 (output VLAN handoff) are reserved for uplink ports.

Note The 1/0/36, 1/0/37 and 2/0/36, 2/0/37 switch ports are configured in "active" mode. If a user is not using port channel and not connected to ports 36 and 37, the OOB switch ports that are connected to Catalyst 9500 on ports 36 or 37 must be configured as "passive" mode.

For example,

- **interface Port-channel1 switchport trunk allowed VLAN 100-106**

```
example VLANs
 switchport mode trunk
!
```

- **interface TenGigabitEthernet1/0/1**

```
port connected to cat9k 1/0/36 or 1/0/37
 switchport mode trunk
 channel-group 1 mode passive
 spanning-tree portfast
!
```

- **interface TenGigabitEthernet1/0/2**

```
interface TenGigabitEthernet1/0/2
 switchport mode trunk
 channel-group 1 mode passive
 spanning-tree portfast
!
```

What to do next

To bring up another switch, repeat all the mentioned steps in sequence for the next switch.

Bring Up Cisco Colo Manager

This section describes about how Cisco Colo Manager is brought up. The Cisco Colo Manager acts as a PNP agent for the Catalyst 9K switches in a cluster. It takes care of the Day-0 configuration push to the Catalyst 9K switches and also relays the configuration from vManage to Catalyst 9K.

Note During cluster activation process, Cisco Colo Manager is automatically brought up.

Procedure

Step 1 All CSP devices in the cloud onramp for colocation establish a DTLS tunnel with vManage.

Step 2 vManage selects one CSP device by sending a NETCONF action API to bring up Cisco Colo Manager on that CSP device.

Step 3 Cisco Colo Manager is in "Starting" state when it is brought up. Cisco Colo Manager can then move to "Healthy" or "Unhealthy" state depending on the health check status.

What to do next

After switch configuration and once colo manager is up, both switches reach the colo manager. Ensure that you check the PNP list on Cisco Colo Manager to verify that both the switch devices have called home. See Switch devices are not calling home to PNP or Cisco Colo Manager, on page 97.

Note For activation to continue, both switches must call home.

Provision and Configure CloudOnRamp for Colocation

To order Cisco SD-WAN Cloud OnRamp for Colocation PID, choose Cisco SD-WAN Cloud OnRamp for Colocation on Cisco Commerce Workspace (CCW).

Customer-specific order details such as, Smart Account name, Virtual Account name must be provided while ordering.

To provision and configure a cloud onramp for colocation, perform the following:

1. Ensure that Cloud Service Platform (CSP) devices and Cisco Catalyst 9500 switches are connected as per the prescribed topology, and powered on. See Wiring Requirements, on page 7 for more information.
2. The Smart Account synchronizes customer-specific device order details with PNP Connect and vOrchestrator.

Ensure that you provide initial configuration information including VLAN pool, IP address pool, and syslog.

Provision DHCP Server Per Colocation

To manage IP addresses of the physical devices such as switches, VNFs, and CSP devices, you must configure a DHCP server per colocation. The Cisco Colo Manager IP address can be configured in DHCP option 43 for Catalyst 9500 to reach Cisco Colo Manager.

vManage fixes and assigns Cisco Colo Manager IP addresses for a colocation. It manages and assigns IP addresses of all VNFs through Day-0 configuration.

Note The subnet for both physical (CSP devices, switches) and virtual appliances (Cisco Colo Manager, VNF) must be same.

You can pick an appropriate subnet for a colocation and limit the pool for IP addresses depending on the number of CSP devices and switches in a colocation. vManage picks the first IP address entered in the VNF management IP pool in the vManage interface and configures it as the (Switch PNP Server IP) Cisco Colo Manager IP address. The second and third IP addresses form the management pool are used for switch management IP addresses. The **Switch PNP Server IP** field can be edited to provide an alternative IP address

if a different IP address is configured in the DHCP server for PNP of switches. The remaining IP addresses from the vManage pool are assigned to the remaining VNFs in the colocation.

Note Ensure that you set up a DNS server in each colocation.

Device Port Connectivity Details and Service Chaining

In Cisco SD-WAN Cloud OnRamp for Colocation deployments, the Catalyst 9500 connected to CSP systems perform service chaining. If VMs support SR-IOV, Catalyst 9500 performs service chaining, whereas VMs without SR-IOV support, service chaining is done by Open Virtual Switch (OVS).

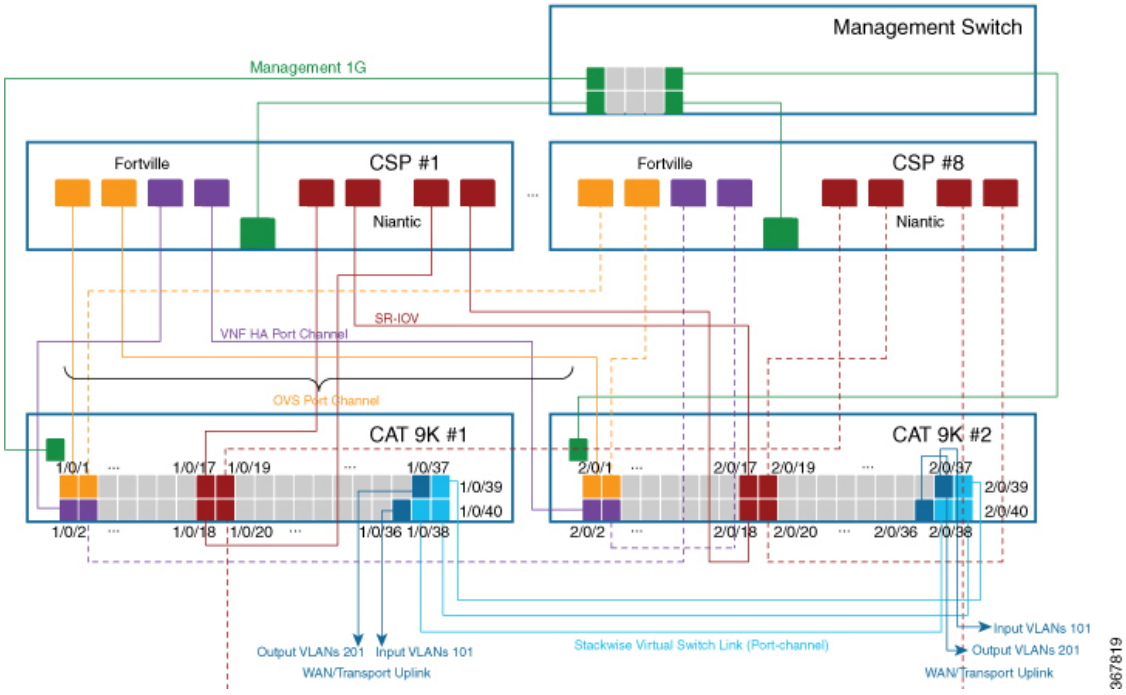
Virtual switch-based service chains are used for High Availability traffic and control traffic.

VLAN-based L2 service chaining from Catalyst 9500 is used for Cisco SD-WAN Cloud OnRamp for Colocation solution. In this service chaining, each virtual NIC interface of a VM in a service chain is configured on the same access VLAN on a CSP virtual switch. The switch pushes the VLAN tag of the packets entering and leaving the vNIC interface. The VNF can remain unaware of the next service in the service chain. To forward traffic between the VNFs hosted either on the same CSP or across different CSP devices in a cluster, the physical switch with the matching VLAN gets configured.

In Cisco SD-WAN Cloud OnRamp for Colocation deployments, the deja-vu check is disabled on the switch ports that are connected to the CSP system for unicast traffic.

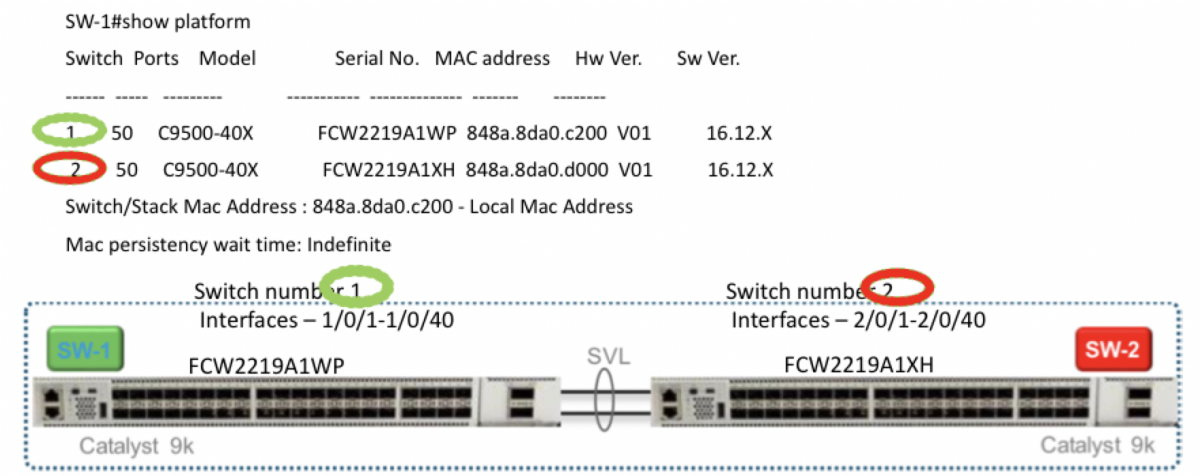
The following topology displays connectivity of the CSP ports to Catalyst 9500 switches and OOB switch.

Figure 3: Service Chain Connectivity with OVS, VEPA Enabled Switch Ports



The following is the location of an interface in switches:

Note The location of an interface is applicable once switches are in SVL mode after successful cluster activation.



The following ports are VEPA disabled and configured with port channels:

- 1/0/1-1/0/16
- 2/0/1-2/0/16

The following ports are VEPA enabled and port channels configuration is disabled:

- 1/0/17-1/0/32
- 2/0/17-2/0/32

Note VEPA ports are only applicable to SRIOV interfaces.

The following ports are the WAN connectivity ports:

- 1/0/36, 2/0/36—Connect port 1/0/36 to receive outside traffic from branch/VPN connections (via an OOB switch).
- 1/0/37, 2/0/37—Connect port 1/0/37 to forward service chain traffic to specific VLANs that is mapped to provider networks on an OOB switch.

You can connect the ports as follows:

- Data ports—Connect ports 1/0/1-1/0/35 to CSP devices. To achieve redundancy and HA across switches, you can connect two ports to one CSP and the other two can be connected to next CSP. For example, ports 1/0/1 and 2/0/1 is used for data and HA respectively can be connected to the first CSP, CSP #1. Next, 1/0/2 and 2/0/2 is another port channel that is connected to the next CSP, CSP #2, and so on. Hence, the OVS ports consume all eight CSP devices.
- WAN connectivity ports—Connect port 1/0/36 on configured VLAN/s to receive outside traffic (Input VLAN handoff). Connect port 1/0/37 to forward service chain traffic to specific VLANs that is mapped

to provider networks (Output VLAN handoff). External input or output VLAN traffic can come from branch or VPN connections and provider networks terminate at the Cloud OnRamp for Colocation through the OOB switch. For each service chain configured in the cluster and input or output VLAN configured for each service chain, the configuration on the ports, 36 and 37 occurs during service chain deployment.

If ports 36 or 37 are connected to the OOB switch and not using port channels, ensure that all VLAN handoffs are configured either on input or output VLAN handoffs correspondingly. For example, if port 36 is connected, configure all VLAN handoff on input VLAN handoff for a service chain. If port 37 is s connected, configure all VLAN handoff on output VLAN handoff for a service chain.

- Connect ports 1/0/38-1/0/40 in Stackwise Virtual Switch Link (SVL) configuration.
- Ports for PNF—The following table provides the ports available for PNF:

Table 7: Ports on Catalyst 9500 for PNF

Number of CSP Devices	Number of PNFs	Ports available on Switch Consoles (SVL mode)	Ports available on First Switch (physical connectivity)	Ports available on Second Switch (physical connectivity)
7	1	1/0/15-1/0/16, 2/0/15-2/0/16, 1/0/31-1/0/32, 2/0/31-2/0/32	1/0/15-1/0/16, 1/0/31-1/0/32	2/0/15-2/0/16, 2/0/31-2/0/32
6	2	1/0/13-1/0/16, 2/0/13-2/0/16, 1/0/29-1/0/32, 2/0/29-2/0/32	1/0/13-1/0/16, 1/0/29-1/0/32	2/0/13-2/0/16, 2/0/29-2/0/32
4	4	1/0/11-1/0/16, 2/0/11-2/0/16, 1/0/27-1/0/32, 2/0/27-2/0/3	1/0/11-1/0/16, 1/0/27-1/0/32	2/0/11-2/0/16, 2/0/27-2/0/32

To remove CSP devices and shuffle ports, perform the following steps:

1. If all eight CSP devices are connected to switches and if you want to connect a PNF device to the switches:
   a. Deactivate or remove the eighth CSP (CSP connected to the right most data ports on switch) from the cluster by using the RMA workflow on vManage. See Delete Cloud OnRamp for Colocation Devices from vManage, on page 27.
   b. Disconnect the CSP physical connections on Catalyst 9500.
   c. Connect the PNF device in place of the disconnected CSP.
2. If one of the first seven CSP devices must be removed to make additional ports available for PNF, perform the following steps:

a. Perform the steps mentioned in 1.

b. Move the right most connected CSP that is the eighth CSP to the ports that are made available by the removed CSP.

   For example, if the first CSP is removed, move the eighth CSP to the position of the first CSP and connect the PNF in place of the eighth CSP.

For this phase of Cisco SD-WAN Cloud OnRamp for Colocation solution deployment, full chain VNF configuration is supported. In a full chain configuration, all the VNFs for the producer and consumer chains are part of a single service chain. The VNFs are not shared across different types of producers and consumers. A separate instance of a service chain supports each combination of consumer and producer type. For a full chain configuration, all the VNFs in a chain are L2 service chained.

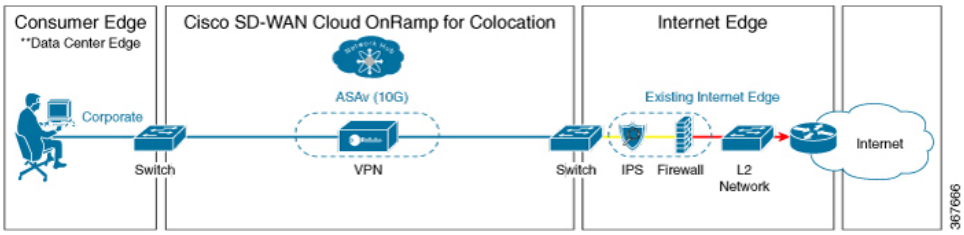
The vManage orchestrator manages the Cisco SD-WAN Cloud OnRamp for Colocation solution service chain configuration. vManage assigns the VLANs from the VLAN pool that is provided for the colocation to the individual VM vNICs and configures the switch with appropriate VLANs. The VNFs can remain unaware about the service chain. Apart from the Day-0 VNF configuration, vManage does not configure the individual VNFs that take part in the service chain. See Configure Cisco SD-WAN Cloud OnRamp for Colocation Devices from vManage, on page 27 for detailed steps of managing service chain through vManage.

Validated Service Chains

In Cisco SD-WAN Cloud OnRamp for Colocation solution deployments, the following are the four validated service chains that you can deploy within a cluster from vManage. For all the validated service chains, each VM can be instantiated in HA or standalone modes.

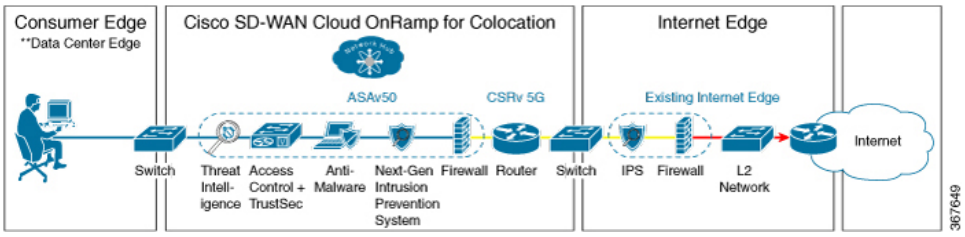
- Employee Remote VPN Access—In this service chain, there is a firewall, which can be in L3 VPN HA or L3 VPN non-HA modes. The firewall VNFs can be ASAv, Palo Alto Networks Firewall, Firepower_Threat_Defense_Virtual (FTDv). Here, ASAv is in routed mode, no Day-0 configuration support for the VPN connect, no BGP on consumer chain, and no VLANs.

  Figure 4: Employee Remote VPN Access Service Chain



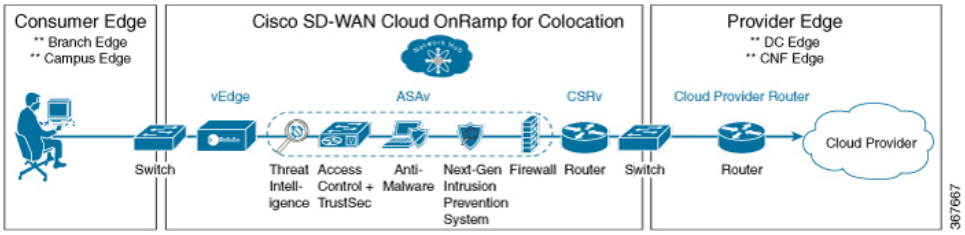
- Internet Edge (Outbound Internet, eCommerce, SaaS)—In this service chain, a firewall is followed with a router. The firewall modes can be L3-VLAN HA and L3-VLAN non-HA. The routers can be in L3 HA and L3 non-HA modes. The firewall VNFs are ASAv, Palo Alto Networks Firewall, FDTv; and router VNF is Cisco CSR. Here, ASAv is always in routed mode. One VLAN handoff is required and inbound subinterfaces can be up to four. The termination can be in routed mode or in a trunk mode with subinterfaces up to four. You can choose the hypervisor tagged VLANs versus VNF to do the VLAN tagging. In VNF VLAN tagging, you can terminate to a minimum of 1 VLAN and maximum of 4 VLANs. In hypervisor tagged VLANs, all VLANs are tagged in the same inbound VNF interface.

Figure 5: Internet Edge Service Chain



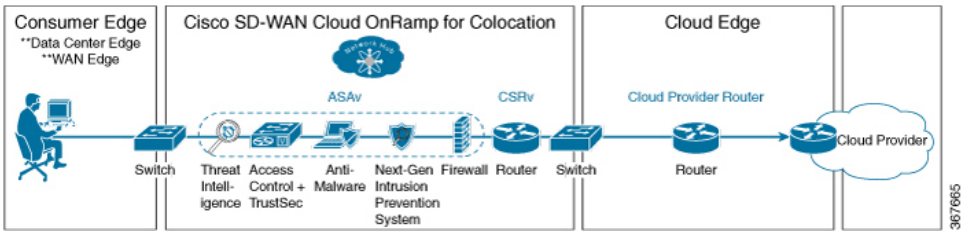
- SD-WAN Access—In this service chain, vEdge is followed by a firewall, which is followed by a router. The firewall modes can be L2 HA, L2 non-HA, L3 HA and L3 non-HA. The routers can be in L3 HA and L3 non-HA modes. The firewall VNFs can be any supported VNFs and router VNF is Cisco CSR.

Figure 6: SD-WAN Access Service Chain



- Cloud Edge (Public Cloud Access)—In this service chain, firewall is followed by a router, where the firewall is in routed mode. The firewall modes can be, L3 HA and L3 non-HA. The routers can be in L3 HA and L3 non-HA modes. The firewall VNFs can be any supported VNFs and router VNF is Cisco CSR. This service chain is Internet Edge (Outbound Internet, eCommerce, SaaS) with firewall mode being L3.

Figure 7: Cloud Edge (Public Cloud Access) Service Chain



See Create Service Chain in a Service Group, on page 46 topic about how you can choose the validated service chains through vManage.

Validated VM Packages

VM packages are created as per use cases. These packages have recommended Day-0 configuration for each supported use case. Any user can bring the required custom Day-0 configuration and package the VM as per their requirement. In the validated packages, various Day-0 configurations are bundled into a single VM package. For example, if a VM is a firewall VM, it can be used in transparent or routed mode if it is in the middle of a service chain. If a VM is the first or last VM in a service chain, it can be a terminating tunnel to a branch or provider, or routed traffic, or can terminate multiple branches, or a provider. Each use case is set up as a special tag in image metadata for a user to make a selection at deployment or while provisioning a

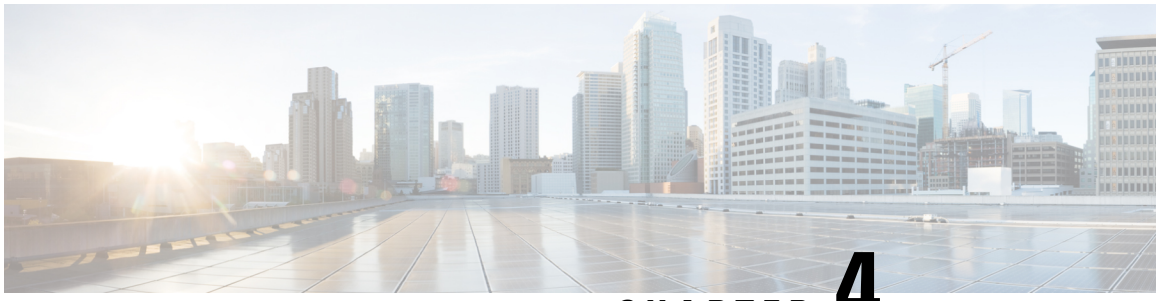
service chain. If a VM is in the center of a service chain, vManage can automate the IP addresses and VLANs for those segments. If VM is terminating to a branch or provider, user must configure the IP addresses, peer addresses, autonomous system numbers, and others.

Customized Service Chains

Service chains are a named list of service-functions and associated endpoint-group through which packets flow. You can customize service chains and create service chain templates. A service chain template is a chain of VMs serving the intent of connecting the ingress traffic to the cloud. Service chain templates can have predefined service chains containing validated VMs that have been mentioned in the Cisco SD-WAN Cloud OnRamp for Colocation Solution Components, on page 2 topic.

The first VNF and the last VNF in a customized service chain can be a router (or firewall). In SD-WAN case, the first VM is a vEdge, which is orchestrated. In non-SD-WAN case, the first VM can be modeled as a gateway router, which is not orchestrated.

You can choose a service chain template and modify the template by inserting one or more VMs and delete one or more VMs. For each VM in the service chain, you can select the VM image that has been brought up from the VM catalog. For example, if the first VM in the service chain is a ROUTER, you can select either Cisco 1000v, or choose from VM repository, or any third-party router. See Chapter, Configure Cisco SD-WAN Cloud OnRamp for Colocation Devices from vManage, on page 27 for information about how to customize service chains.



CHAPTER 4

Configure Cisco SD-WAN Cloud OnRamp for Colocation Devices from vManage

- Add Cloud OnRamp Colocation Devices into vManage, on page 27
- Delete Cloud OnRamp for Colocation Devices from vManage, on page 27
- Manage Clusters in vManage , on page 28
- Manage Service Groups, on page 46
- Attach and Detach Service Group with Cluster, on page 64
- Day-N Configuration Workflow of Cisco SD-WAN Cloud OnRamp for Colocation Solution, on page 65

Add Cloud OnRamp Colocation Devices into vManage

You can add CSP devices, switch devices, and VNFs through vManage.

Before you begin

Ensure that you have the following setup details such as:

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

When you order the Cisco SD-WAN Cloud OnRamp for Colocation solution PID, all cloud onramp for colocation device information is received though smart account that can be accessed by vManage.

Delete Cloud OnRamp for Colocation Devices from vManage

To delete the CSP devices from 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 being deleted, detach service groups. See Attach and Detach Service Group with Cluster, on page 64.
- If a CSP device that is being deleted is hosting Cisco Colo Manager, see Recovery of Cisco Colo Manager, on page 95.

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.
Step 2 In Cisco vManage, in the **Configuration** > **Certificates** screen, locate the device, click **More Actions**, and click **Invalid**.
Step 3 In the **Configuration** > **Certificates** screen, click **Send to Controller**.
Step 4 In the **Configuration** > **Devices** screen, in the **WAN Edge List** tab, select the device.
Step 5 Click the **More Actions** icon to the right of the row and click **Delete WAN Edge**.
Step 6 Click **OK** to confirm deletion of the device.

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

Manage Clusters in vManage

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

The three steps to configure Cloud OnRamp for Colocation devices are:

- Create a cluster. See Create and Activate Clusters, on page 31.
- Create a service group. See Create Service Chain in a Service Group, on page 46.
- Attach a cluster with a service group. See Attach and Detach Service Group with Cluster, on page 64.

A Cloud OnRamp for Colocation cluster is a collection of two to eight CSP devices and two switches. The supported cluster templates are:

- Small cluster—2 Catalyst 9500+2 CSP
- Medium Cluster—2 Catalyst 9500+4 CSP
- Large Cluster—2 Catalyst 9500+6 CSP
- X-Large Cluster—2 Catalyst 9500+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.

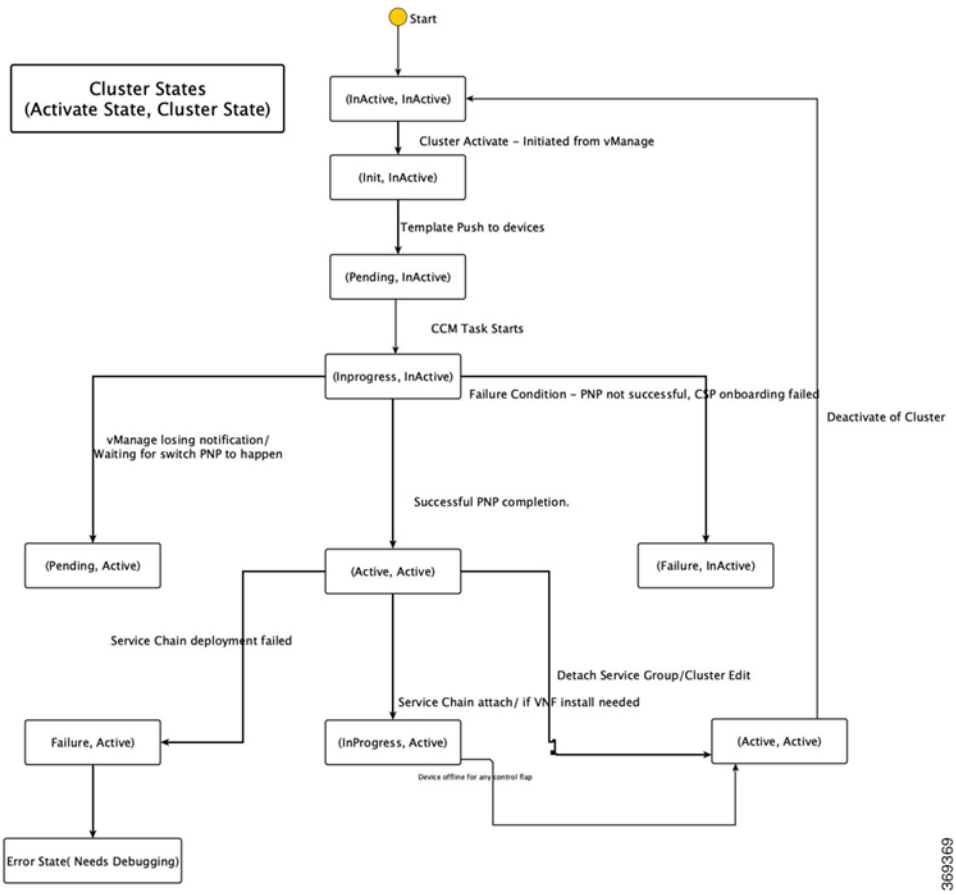
Ensure that all devices that you bring into a cluster have the same software version.

Following are the cluster states:

- Incomplete—When a cluster is created from the 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 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 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, on page 97 for more information about cleaning switch configuration that has been used previously.

Provision and Configure Cluster

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

To provision and configure a cluster, perform the following:

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

   CSP devices can be added to a cluster and configured through 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 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 throughput is in MBPS, and you can assign as high as 10 GB, and as low as 10 MB. The default service chain bandwidth is 10 MBPS. See the Device Port Connectivity Details and Service Chaining, on page 21 and Ordering and Sizing of Cisco SD-WAN Cloud OnRamp for Colocation Devices topics.

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 filled by the 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 has been completed.

   You can watch the cluster status change from in progress to active or error.

To edit a cluster, perform the following:

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. They can be attached with a cluster after the cluster is active.

Create and Activate Clusters

This topic provide the steps about how a cluster can be formed with CSP devices, Catalyst 9500 switches as single unit, and provision the cluster with cluster-specific configuration.

Before you begin

Ensure that the clock on Cisco vManage and CSP devices are synchronized.

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage , choose **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLOCATION screen, perform the following tasks:

a) In the **Cluster** tab, click the **Configure & Provision Cluster** button.

A graphical representation of the default cluster, which consists of two switches each connected to two Cloud Services Platform (CSP) devices is displayed in the design view window.

b) Provide cluster name, description, site id, and location information.

Table 8: Cluster Information

Field	Description
Cluster Name	The cluster name can be up to 128 characters and can contain only alphanumeric characters.
Description	The description can be up to 2048 characters and can contain only alphanumeric characters.
Site ID	Specifies overlay network site identifier. This entry can be a value from 1 through 4294967295 (2^{32}– 1).
Location	The location can be up to 128 characters and can contain only alphanumeric characters.

c) From the graphical representation, to configure a switch, click a switch icon, the **Edit Switch** dialog box is displayed. Provide a name and choose the switch serial number. Click **Save**.

The switch name can be up to 128 characters and can contain only alphanumeric characters.

When you order Cisco SD-WAN Cloud OnRamp for Colocation solution PID on CCW and buy the Catalyst 9500 switches, a serial number is assigned for the switches. These serial numbers are integrated with vManage through PNP.

Note

You can keep the serial number field blank, design your cluster, and edit the cluster later to include the serial number after you have bought the switches.

d) To configure another switch, repeat the previous step.

e) From the graphical representation, to configure CSP, click a CSP icon in the CSP box. The **Edit CSP** dialog box is displayed. Provide a hostname and choose the CSP serial number. Click **Save**.

The hostname can be up to 128 characters and can contain only alphanumeric characters.

Note
You can keep the serial number field blank, design your cluster, and edit the cluster later to include the serial number after you have bought CSP devices. However, you cannot activate a cluster, where the serial number of CSP devices are not being included.

Note
Ensure that you configure the OTP for the CSP devices to bring them up. See Bring Up Cloud Services Platform Devices, on page 15.

f) To add remaining CSP devices, repeat step e.
After you design a cluster, an ellipsis that is enclosed in a yellow circle next to the device appears if a serial number has not been assigned for a device.

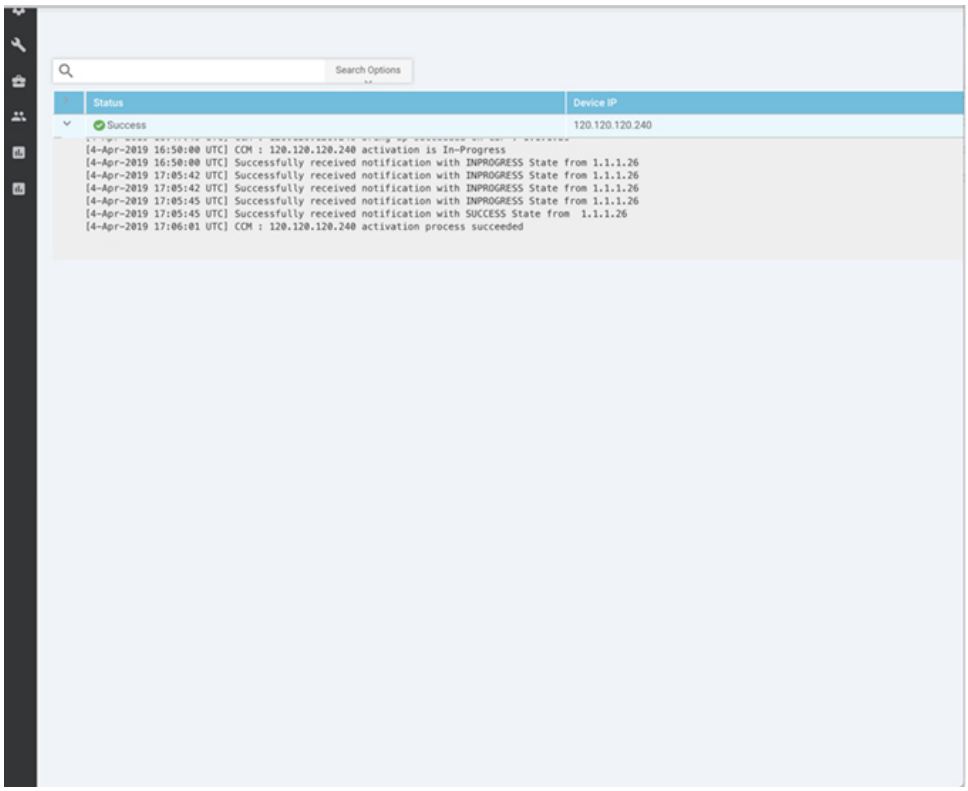
g) To edit a CSP device configuration, click a CSP from the graphical representation, and follow the process that is mentioned in substep e.

h) For mandatory and optional global parameters to be set for a cluster, click and choose from **Cluster Settings** drop-down. The dialog boxes for each of the global parameters are displayed. Enter values for the cluster settings parameters and click **Save**. See Cluster Settings, on page 35.

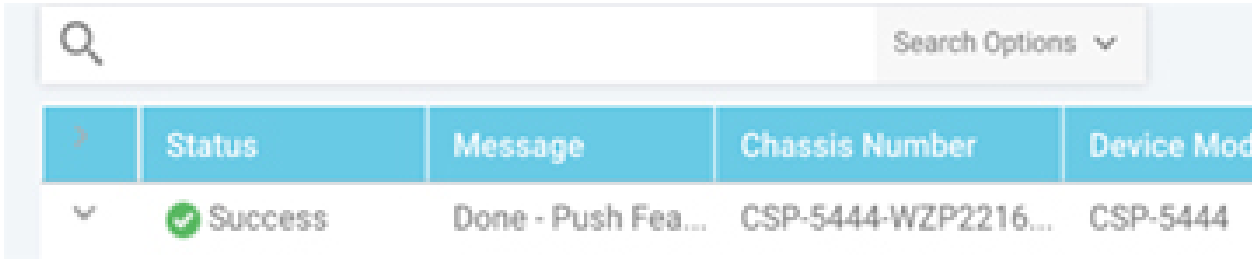
i) Click the **Save Cluster** button.

Step 3 In the **Cluster** tab, to activate a cluster, click a cluster, click the **More Actions** icon to the right of its row, click **Activate** against the cluster.

When you click Activate, vManage establishes a DTLS tunnel with CSP devices in the cluster where it connects with the switches through Cisco Colo Manager. After the DTLS connection is running, a CSP device in the cluster is chosen to host the Cisco Colo Manager. Cisco Colo Manager is brought up and vManage sends global parameter configurations to the CSP devices and switches. To verify if a cluster has been activated, you can view the task progress as shown.



To verify if cluster has been activated from the CSP end, you can view the task progress as shown.



If the Cisco Colo Manager status does not go to "HEALTHY" after "STARTING", see Troubleshoot Cisco Colo Manager Issues, on page 108 .

If the status of Cisco Colo Manager goes 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, on page 97 .

If the status of the tasks running on a CSP device does not show success for more than five minutes after the activation through OTP, see Troubleshoot Cloud Services Platform Issues, on page 102 .

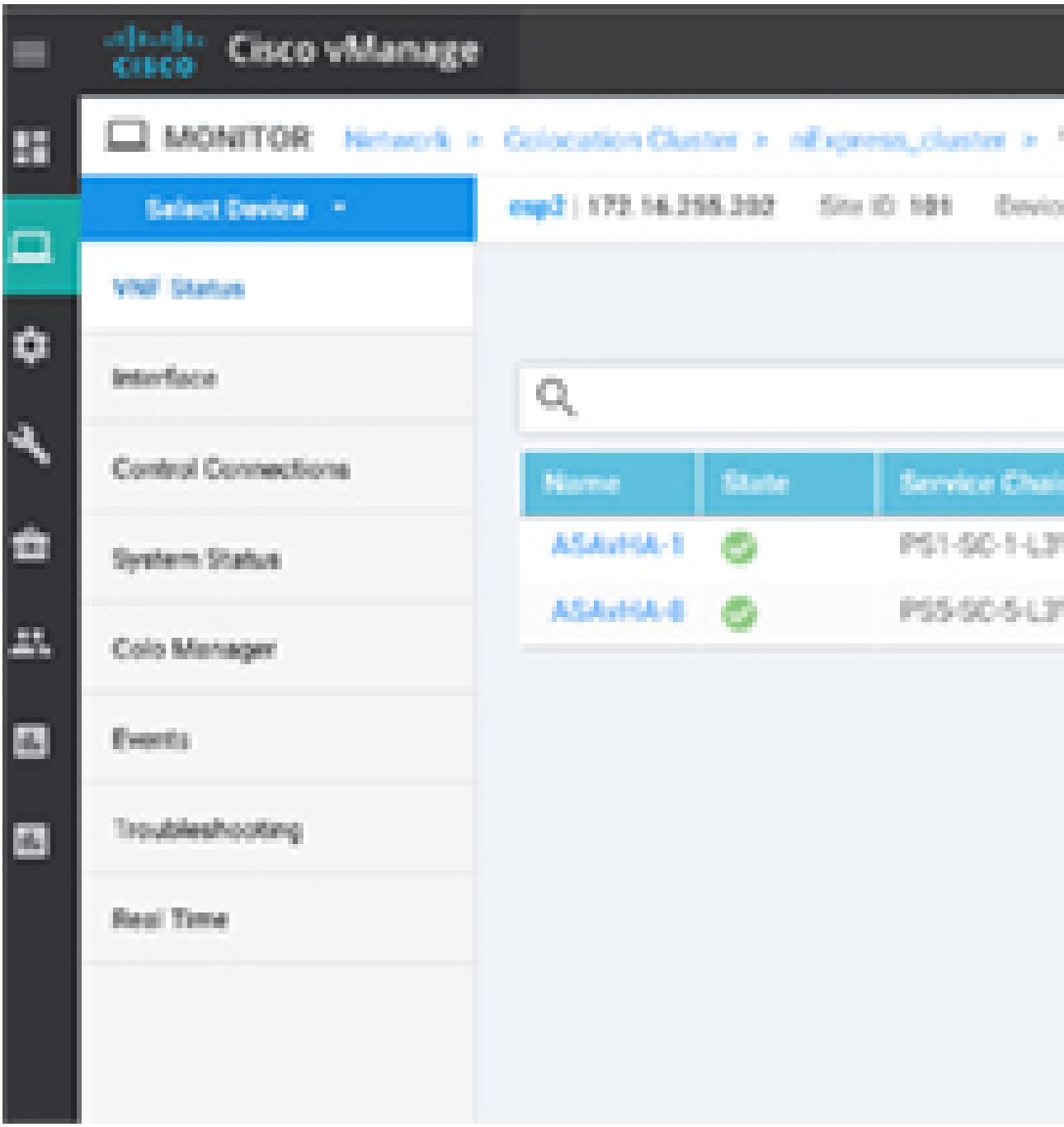
Note If a cluster goes into a "PENDING" state, click the **More Actions** icon to the right of its row, and then click the **Sync** button. This action moves a cluster back to an "ACTIVE" state.

To view if a cluster moves back to an "ACTIVE" state, you can view the successful activation as shown.



To determine the service groups present on CSP devices, navigate to **Monitor** > **Network** > **Colocation Cluster**.

Choose a cluster and then choose a CSP device as shown in the following image. You can choose and view other CSP devices.



Cluster Settings

The cluster settings parameters are:

- Configure login credentials for the cluster:

  1. In the Cluster Settings drop-down, click **Credentials**. The Credentials dialog box is displayed. Enter the values for the following fields:

     (Mandatory) Template Name: The template name can be up to 128 characters and can contain only alphanumeric characters.

     (Optional) Description: The description can be up to 2048 characters and can contain only alphanumeric characters.

  2. Click **New User**.

     Provide name, password, and role of a user.

- Configure the Resource pool for the cluster:

  1. In the Cluster Settings drop-down, click **Resource Pool**. The Resource Pool dialog box is displayed. Enter the values for the following fields:

     (Mandatory) Name: Name of the IP address pool. The name can be up to 128 characters and can contain only alphanumeric characters.

     (Optional) Description: IP address pool description. The description can be up to 2048 characters and can contain only alphanumeric characters.

     (Mandatory) DTLS Tunnel IP: 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).

     (Mandatory) Service Chain VLAN Pool: Numbers of the VLAN 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).



Note A VLAN range brings up VNFs, so that each circuit has VLAN configured when it comes up. The VLAN pool can only start from 1021 as switch reserves the VLANs until 1021. We recommend you to enter VLAN pools between 1021-2021.

     (Mandatory) VNF Data Plane IP Pool: 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).

     (Mandatory) VNF Management IP Pool: IP addresses to be used for theVNF. 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.

(Mandatory) Management Subnet Gateway: IP address of the gateway to the management network. It enables DNS to exit the cluster.

(Mandatory) Management Mask: Mask value for the failover cluster. For example, /24 and not 255.255.255.0

(Mandatory) Switch PNP Server IP: IP address of the switch device.

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

- Optionally, configure NTP servers for the cluster:

1. In the Cluster Settings drop-down, select NTP. The NTP configuration box is displayed. Enter the values for the following fields:

   Template Name: Name of the NTP template. The name can be up to 128 characters and can contain only alphanumeric characters.

   Description: The description can be up to 2048 characters and can contain only alphanumeric characters.

   Preferred server: IP address of the primary NTP server.

   Backup server: IP address of the secondary NTP server.

- Optionally, configure syslog parameters for the cluster:

1. In the Cluster Settings drop-down, select Syslog. The System Log configuration box is displayed. Enter the values for the following fields:

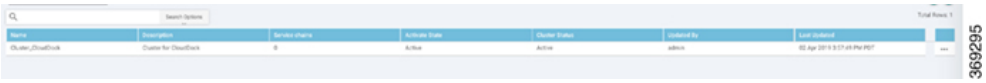
   Template Name: Name of the System Log template. The name can be up to 128 characters and can contain only alphanumeric characters.

   Description: The description can be up to 2048 characters and can contain only alphanumeric characters.

   Severity drop-down: Select the severity of syslog messages to be logged.

2. To configure a syslog server, click **New Server**.
3. Type the IP address of a syslog server.

If all global parameters are set through cluster settings, you can verify if the cluster has been activated successfully, as shown.



View Cluster from vManage

To view a cluster configuration, perform the following steps:

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, choose **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted.

Step 3 In the **Cluster** tab, click a cluster, click the **More Actions** icon to the right of its row, and click **View** against the cluster.

The Cluster window opens, displaying the switches and CSP devices in the cluster and showing which cluster settings have been configured.

Step 4 You can only view the global parameters being set, configuration of switches and CSP devices.

Step 5 Click the **Cancel** button to return to the CLOUD ONRAMP FOR COLOCATION Cluster screen.

Edit Cluster in vManage

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, select **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted.

Step 3 In the **Cluster** tab, click a cluster, click the **More Actions** icon to the right of its row, and click **Edit** against the cluster.

The Cluster window opens, displaying the switches and CSP devices in the cluster and showing which cluster settings have been configured.

Step 4 In the cluster design window, you can modify some of the global parameters. Based on whether a cluster is in active or inactive state, following are the restrictions for editing a cluster:

a. Inactive state.

- Edit all global parameters, and the Resource pool parameter.
- Add more CSP devices (up to eight).
- Cannot 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. Activate state.

- Edit all global parameters, except the Resource pool parameter.

Note
The Resource pool parameter cannot be changed when the cluster is activated. However, the only way to change the Resource pool parameter is to delete the cluster and recreate it again with the correct Resource pool parameter.

- Cannot 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.
- Cannot delete a cluster in active state.

Step 5 Click the **Save Cluster** button.

Add CSP Device to Cluster

You can add and configure the CSP devices through vManage.

Before you begin

Ensure that the NFVIS version that you use is same as the other CSP in the cluster.

Procedure

Step 1 In vManage , choose **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION screen appears, and the **Configure & Provision Cluster** button is highlighted.

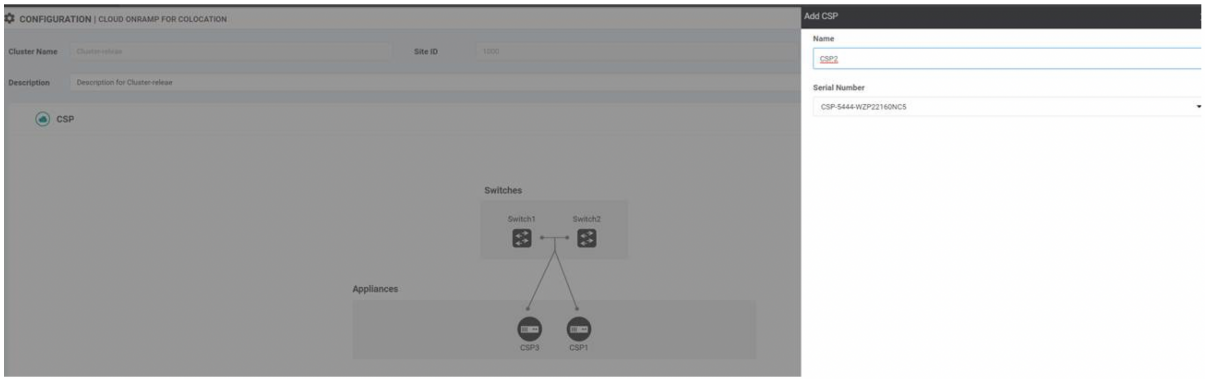
Step 2 In the **Cluster** tab, select a cluster from the table, click the **More Actions** icon to the right of its row, and choose **Add/Delete CSP**.

Step 3 To configure a CSP device, click the CSP icon in the CSP box. The **Add/Delete CSP** dialog box appears. Provide a hostname and choose the CSP serial number. Click **Save**.

The hostname can be up to 128 characters and can contain only alphanumeric characters.

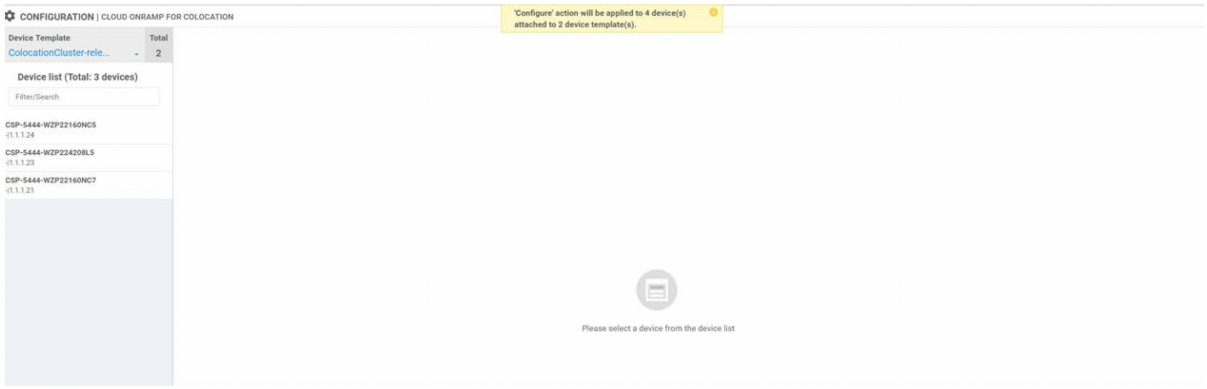
Note
Ensure that you configure the OTP for the CSP devices to bring them up. See Bring Up Cloud Services Platform Devices, on page 15.

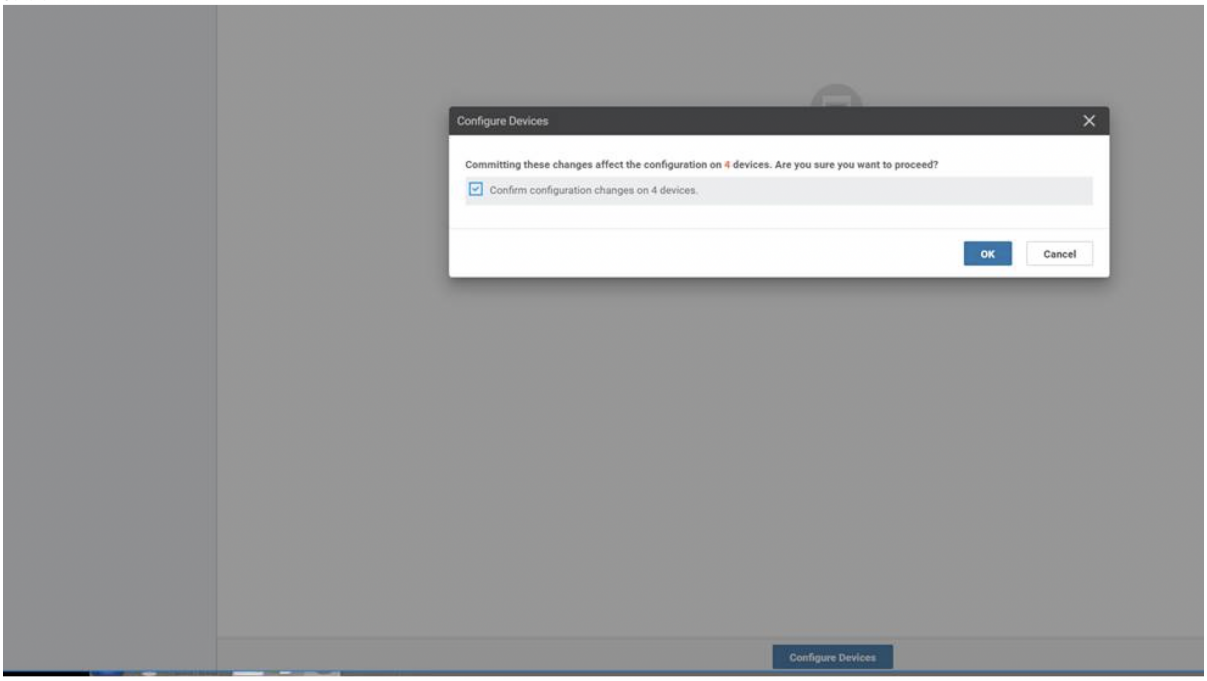
Figure 8: Add CSP



Step 4 Click **Save**.

Step 5 After saving, perform the onscreen configuration instructions as shown in the following images:





Step 6 To check the status of CSP devices, use the task view page that displays a list of all running tasks.

You can go to the Cluster or Network page, and verify if the CSP device has been added.

Delete or RMA CSP Device from Cluster

You can delete or RMA CSP devices through vManage.

Procedure

Step 1 In vManage , choose **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION screen appears, and the **Configure & Provision Cluster** button is highlighted.

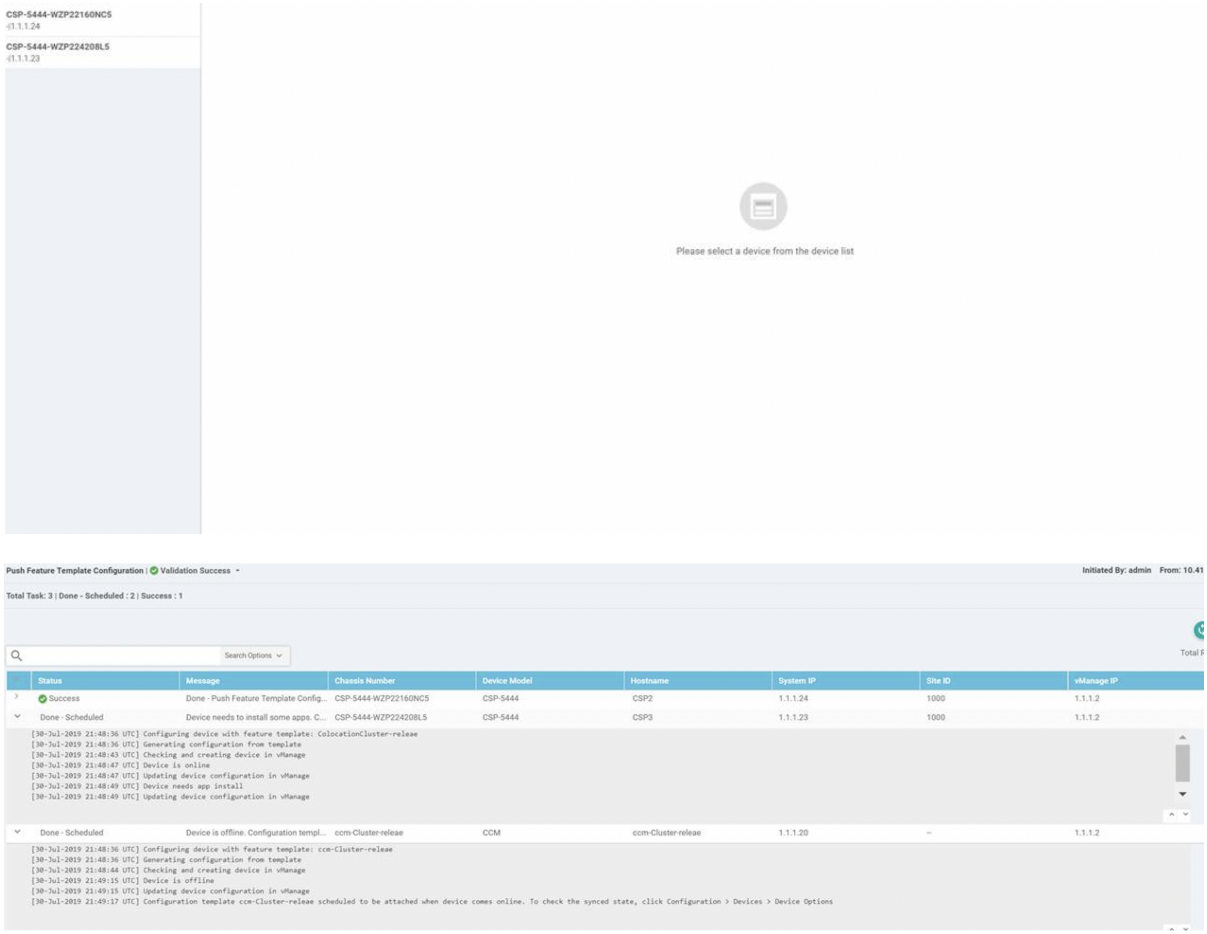
Step 2 In the **Cluster** tab, select a cluster from the table, click the **More Actions** icon to thje right of its row, and choose **Add/Delete CSP**.

Step 3 Edit CSP by clicking the CSP icon to be deleted.

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 devices to the factory default. See Factory reset of CSP device, on page 104.

Step 8 To decommission invalid CSP devices in vManage, click **Configuration** > **Devices**.

Step 9 Locate the CSP devices that are in the deactivated cluster, click the **Add/Delete CSP**, and click **Decommission WAN Edge**.

This action provides new tokens to the devices.

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

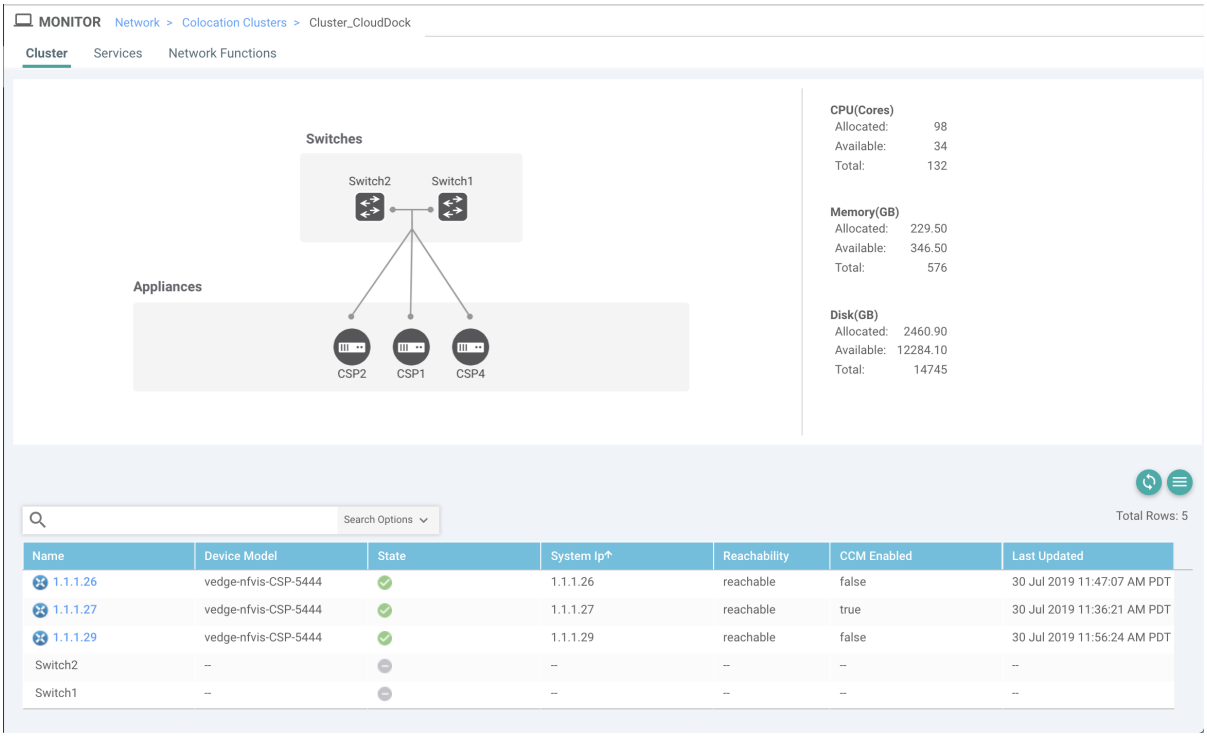
Delete CSP with CCM

Procedure

Step 1 Determine the CSP that hosts the CCM.

Step 2 If **CCM Enabled** is true on a CSP and you choose to delete the corresponding CSP, click the **More Actions** icon to thje right of its row, and choose **Add/Delete CSP**. In the following image from the Montior screen, you can view the CCM enabled state from the Detail part.

Figure 9: CSP Device with CCM



When the CSP that runs the service chain mornitoring service and CCM is removed from a cluster, ensure that you click the **Sync** button of the cluster. Clicking the sync button starts the service chain health monitoring service on a different CSP to continue monitoring the existing service chain health.

Ensure that vManage has control connections to all CSP devices so that vManage can bring up CCM instance on another CSP.

After you delete a CSP device with CCM, when a service chain is configured and attached to this cluster, the CCM instance is brought up on one of the CSP devices on this cluster. The service chain monitoring is disabled until the CCM instance is not brought up in any of the remaining CSP devices.

Remove PNF Devices from Cluster

Procedure

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 a vManaged ASR router, invalidate and decommission the device from the **Device** page.

Step 3 Remove the cables that connect the PNF with the Catalyst 9500 and manually remove the VLAN configuration from Catalyst 9500 corresponding interfaces.

Remove Cluster from vManage

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In Cisco vManage, in the **Configuration** > **Certificates** screen, locate and verify status of devices to be deleted, and click **Invalid** against the devices.

Step 3 In the **Configuration**|**Ceritificates** screen, click **Send to Controllers**.

Step 4 In vManage, click **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted.

Step 5 In the **Cluster** tab, locate the cluster that has invalid devices, click the **More Actions** icon to the right of its row, and click **Deactivate** against the cluster.

If the cluster is attached to one or more service groups, you are prompted with a message that service chains hosting the VMs are running on this device and whether you can continue with the cluster deletion. However, although you confirm deletion of a cluster, you are not allowed to remove the cluster without detaching the service groups that are hosted on this device. If the cluster is not attached to any service group, you are prompted with a message to confirm the cluster deletion.

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

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

Step 7 Click the **Cancel** button to return to the CLOUD ONRAMP FOR COLOCATION Cluster screen without deleting the cluster.

Step 8 To decommission invalid devices, in vManage, click **Configuration** > **Devices**.

Step 9 Locate the devices that are in the deactivated cluster, click the **More Actions** icon to the right of the device row, and click **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 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, on page 101 .

Remove and Replace Switch

The Catalyst 9500 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). As per the wiring requirements, these are the front side ports; 38,39 as SVL links and 40 as 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:

Procedure

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

```
1.Switch#sh switch
2.Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
3.Mac persistency wait time: Indefinite
4.                                             H/W   Current
5.Switch#   Role    Mac Address     Priority Version  State
6.-------------------------------------------------------------------------------
7.*1       Active   c4b3.6a71.0b00     1      V01     Ready
8. 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.

```
1.Switch#sh switch
2.Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
3.Mac persistency wait time: Indefinite
4.                                             H/W   Current
5.Switch#   Role    Mac Address     Priority Version  State
6.-------------------------------------------------------------------------------
7.*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 by using the following commands:

```
1.Switch#sh switch
2.Switch/Stack Mac Address : 5486.bc78.c900 - Local Mac Address
3.Mac persistency wait time: Indefinite
4.                                             H/W   Current
5.Switch#   Role    Mac Address     Priority Version  State
6.------------------------------------------------------------------------------------
7.*2       Active   5486.bc78.c900     1      V01     Ready
8.
9.
10.Switch#switch 2 renumber 1
11.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]:
12.Switch#reload
13.
14.System configuration has been modified. Save? [yes/no]: no
15.Reload command is being issued on Active unit, this will reload the whole stack
16.Proceed with reload? [confirm]
17.
18.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 switch to the second switch.

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

```
1.Switch(config)#
2.stackwise-virtual
3. domain 10
4.!
5.interface TenGigabitEthernet1/0/38
6. stackwise-virtual link 1
7.!
8.interface TenGigabitEthernet1/0/39
9. stackwise-virtual link 1
10.!
11.interface TenGigabitEthernet1/0/40
12. stackwise-virtual dual-active-detection
```

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

```
1.Switch#switch 1 renumber 2
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
3.Switch# reload
```

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

```
1.Switch#sh switch
2.Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
3.Mac persistency wait time: Indefinite
4.                                             H/W   Current
5.Switch#   Role    Mac Address     Priority Version  State
6.------------------------------------------------------------------------------------
7.*1       Active   c4b3.6a71.0b00     1      V01     Ready
8. 2       Member   5486.bc78.c900     1      V01     Ready
9.
10.
```

```
11.
12.Switch#
13.*Jun 17 21:00:57.696: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
14.*Jun 17 21:00:57.694: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2
has been elected STANDBY.
15.*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
16.
17.*Jun 17 21:01:02.651: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
18.
19.*Jun 17 21:01:53.686: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
20.*Jun 17 21:01:54.688: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
21.Switch#
22.Switch#
23.Switch#
24.Switch#
25.Switch#
26.Switch#
27.Switch#
28.Switch#sh switch
29.Switch/Stack Mac Address : c4b3.6a70.f480 - Foreign Mac Address
30.Mac persistency wait time: Indefinite
31.                                           H/W   Current
32.Switch#   Role    Mac Address     Priority Version  State
33.-------------------------------------------------------------------------------------
34.*1       Active   c4b3.6a71.0b00     1      V01     Ready
35. 2       Standby  5486.bc78.c900     1      V01     Ready
```

Reactivate Cluster from vManage

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In Cisco vManage, in the **Configuration** > **Devices** screen, locate the devices that are in the deactivated cluster.

Step 3 Get new token from vManage for the devices.

Step 4 Log into NFVIS by 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 From vManage, configure the system configuration and then activate the cluster. See Create and Activate Clusters, on page 31.

If the cluster has been deleted, recreate and then activate it.

Step 7 In Cisco vManage, in the **Configuration** > **Certificates** screen, locate, and verify status of devices.

Step 8 To validate the devices, click **Valid** if it is invalid.

Step 9 In the **Configuration|Ceritificates** screen, click **Send to Controllers**.

Manage Service Groups

A service group consists of one or more service chains. You can configure a service group through 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 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 are not met. You are notified about the resources not being available and service chains are not deployed.

Create Service Chain in a Service Group

A service group consists of one or more service chains.

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab, and then click the **Create Service Group** button. Provide the service group name and description.

The service group name can be up to 128 characters and can contain only alphanumeric characters.

The service group description can be up to 2048 characters and can contain only alphanumeric characters.

b) Click **Add Service Chain**.

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

Table 9: Add Service Chain Information

Field	Description
Name	The service chain name can be up to 128 characters and can contain only alphanumeric characters.
Description	The service chain description can be up to 2048 characters and can contain only alphanumeric characters.
Bandwidth	The service chain bandwidth is in MBPS, and you can assign as high as 10 GB, and as low as 10 MB. The default bandwidth is 10 MB.
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 through 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 subinterface VLAN list. The service chain monitoring reports status based on end-to-end connectivity. Hence, ensure that you take care of the routing and return traffic path, especially with SD-WAN chains for better results. **Note** • Ensure that you provide input and output monitoring IP addresses from input and output handoff subnets respectively. However, if the first and last VNF devices are VPN terminated, you do not need to provide an input and output monitoring IP addresses. For example, if the network function is not 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, those service chains cannot be monitored.
Service Chain	Choose a topology from the service chain drop-down. For a service chain topology, you can choose any of the four validated service chains such as, Router - Firewall - Router, Firewall, Firewall - Router. See Validated Service Chains, on page 24 You can also create a customized service chain. See Create Custom Service Chain, on page 50 .

d) In the Add Service Chain definition box, click **Add**.
Based on the service chain configuration information, a graphical representation of the service group with all the service chains and its VNFs automatically appear in the design view window. A VNF appears with a "V" or "P" around its circumference specifying that it is a virtual network function. It shows all the configured service chains within each service group. A check against the service chain indicates that all configuration information for the service chain has been completed.

After a cluster is activated, attached with the service group, and monitoring service is enabled for the service chain, when the CSP device is brought up where CCM is running, 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 from vManage , on page 84.

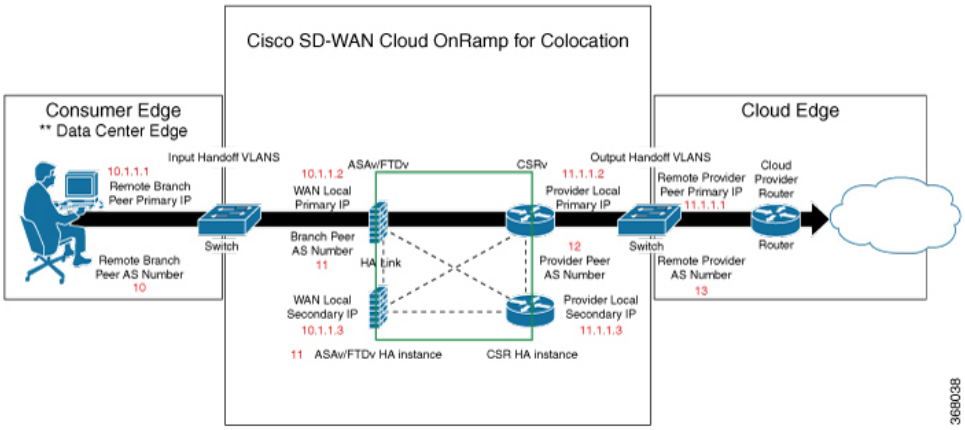
e) In the design view window, to configure a VNF, click a VNF in the service chain.
The Configure VNF dialog box appears.

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

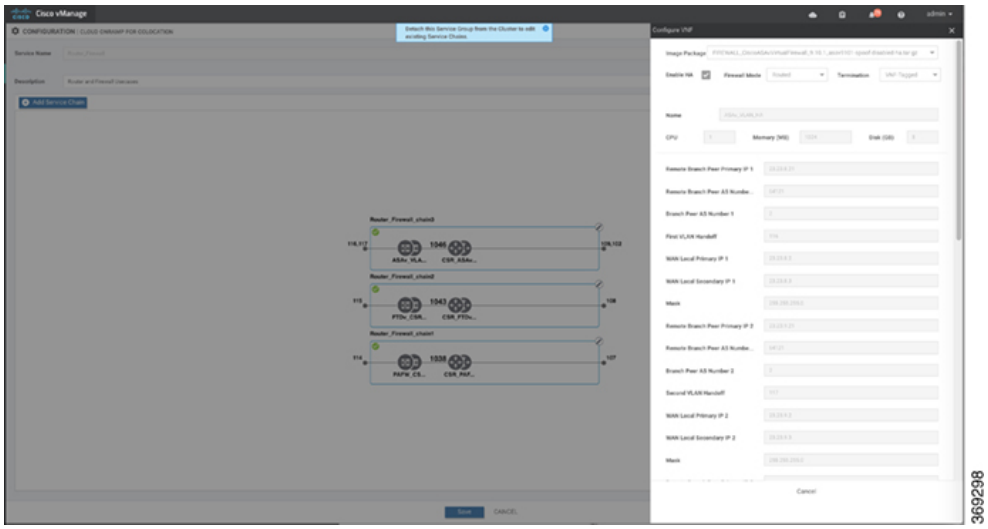
Table 10: VNF Properties of Router and Firewall

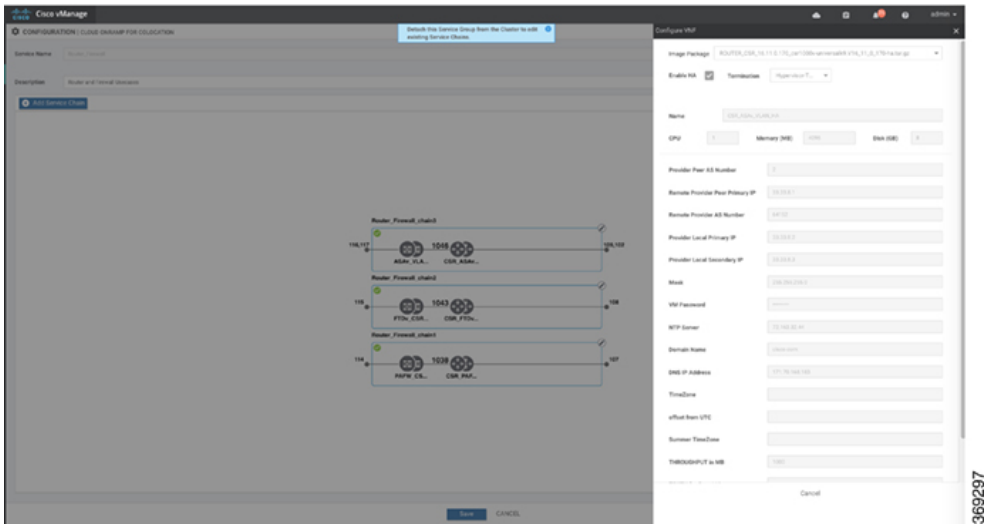
Field	Mandatory or Optional	Description
Image Package	Mandatory	Choose a router or firewall package.
Click **Fetch VNF Properties**. The available information for the image package is displayed in the Configure VNF dialog box.		
Name	Mandatory	VNF image name
CPU	Optional If you do not enter, the default value is considered, which is 1 vCpu.	Specifies the number of virtual CPUs that are required for a VNF.
Memory	Optional If you do not enter, the default value is considered, which is 1024 MB.	Specifies the maximum primary memory in MB that the VNF can use.
Disk	Optional If you do not enter, the default value is considered, which is 8 GB.	Specifies disk in GB required for the VM.
You are prompted with any custom tokenized variables from Day-0 that requires your input. Provide the values.		

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



The following images provide an example of the configuration for VNF IP addresses and autonomous system numbers in vManage.





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

Table 11: 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 only for firewall VMs and not other VMs.
Enable HA	Optional	HA enabled or not for VNF.

Field	Mandatory or Optional	Description
Termination mode	Mandatory	Specifies the following modes: • L3 mode selection with subinterfaces that are trunked. **<type>selection</type> <val help="L3 Mode With Sub-interfaces(Trunked)" display="VNF-Tagged">vlan</val>** • L3 mode with IPSEC termination from a consumer and routed to a 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 (nontrunked). **<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 from step b.
i) Click **Save**.

The new service group is listed in a table on the **Service Group** tab. To view the status of the service chains that are monitored, use the task view page that displays a list of all running tasks along with the total number of successes and failures. To determine if the service chain health monitoring is enabled SSH into CSP hosting CCM/Service chain Health monitor, use the **show cluster-master** command. If the return value is "True," service chain health monitoring is enabled on the CSP. On the CSP where service chain health monotioring is enabled, to determine the service chain health status, use the **show system:system status** command.

Create Custom Service Chain

You can customize service chains,

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

Procedure

Step 1 Create a service group and service chains within the service group. See #unique_61.

Step 2 In the **Add Service Chain** dialog box, provide 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 on the left panel, 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 **Image Package** drop-down.
b) Click **Fetch VNF Properties**.
c) Enter a name of the VNF in the **Name** field.
d) Enter the number of virtual CPUs required for the VNF in the **CPU** field.
e) Enter the amount of memory in megabytes to be allocated for the VNF in the **Memory** field.
f) Enter the amount of memory for storage in gigabytes to be allocated for the VNF in the **Disk** field.
g) Enter VNF-specific parameters, as required.

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

h) Click **Configure**.
i) 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.

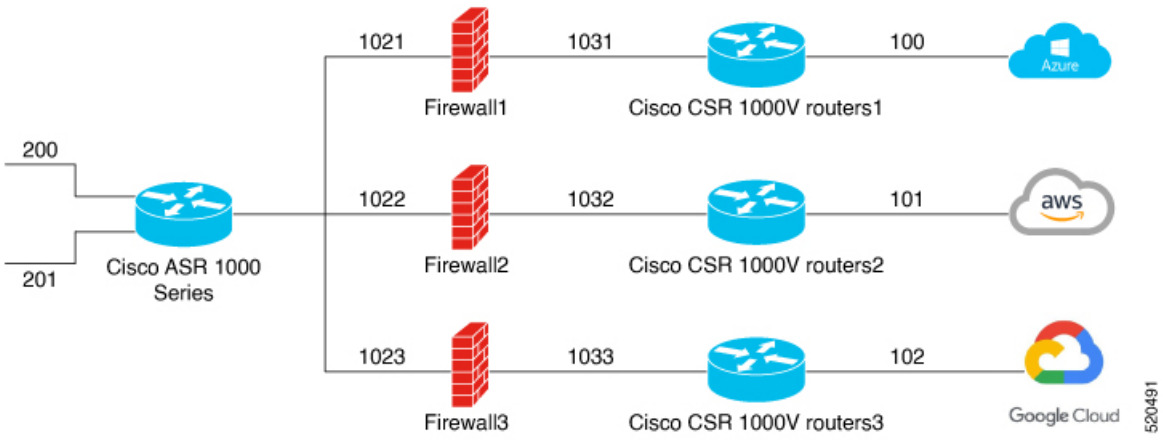
1. Connect the PNF devices to Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switch devices.
2. To make Cisco ASR 1000 Series router managed by Cisco vManage, upload WAN edge router authorized serial numbers from the Cisco Smart Account. See the "Upload WAN Edge Router Serial Numbers from Cisco 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 52.
4. Attach the service group to a cluster and check the configuration parameters that are generated. See Attach and Detach Service Group with Cluster, on page 64.
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 Catalyst 9500, on page 55.

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 10: PNF Shared with Multiple Service Chains



Custom Service Chain with Shared PNF Devices

You can customize service chains by including supported PNF devices.

Caution Ensure that you do not share PNF devices across 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.

Before you begin

For more information on validated physical network functions, refer Cisco SD-WAN Cloud OnRamp for Colocation Solution Components section.

To create a customized service chain by adding a router or firewall to an existing service chain, perform the following steps:

- If a PNF device needs to be managed by vManage, ensure that the serial number is already available in the 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.
- You can add PNF devices across service chains and service groups.
- You can share PNF devices across service groups. They can be shared across service groups by entering the same serial numbers.

- You can share PNF devices across a single cluster and cannot share across multiple clusters.

Procedure

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 46.

Step 2 In the **Add Service Chain** dialog box, provide 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. In the left panel, the set of VNF devices and PNF devices that you can add into the service chain appears. The 'V' in the circumference of VNF devicess 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 on the left panel, and drag the icon to its 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 include the HA serial number in **HA Serial**.

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

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

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

1. Check **vManaged** if the device is managed by vManage.
2. Click **Fetch Properties**.
3. Enter a name of the PNF in the **Name** field.
4. Enter the serial number of the PNF device in the **PNF Serial** field.

d) Click **Configure**.

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

Step 5 Edit an existing PNF configuration by clicking it.

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

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

rim appears on it. 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 11: Single PNF in a Service Chain

Here a service chain consists of a single PNF, Ftd_Pnf (not shared with other service chains).



Figure 12: Two PNF Devices in Service Chains

Here service chains consist of two PNFs, FTdv_PNF shared across SC1 and SC2 and ASR_PNF (non shred).

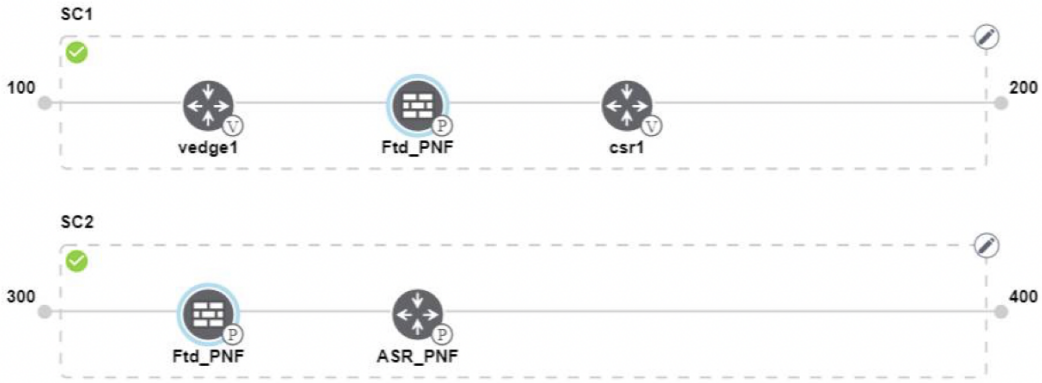
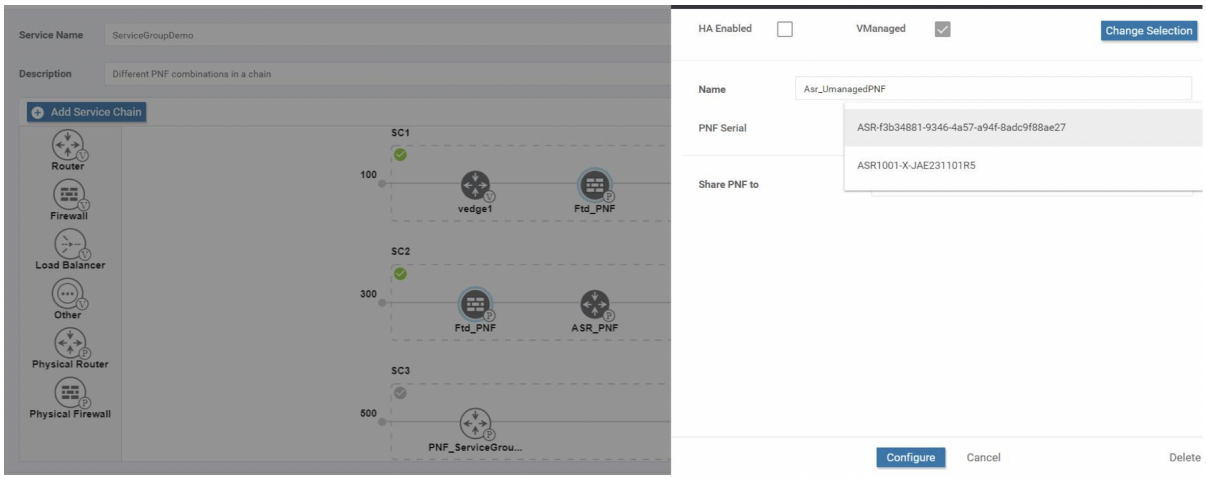


Figure 13: Three PNF Devices in Service Chains

Here service chains consist of three PNF devices in two different positions along with the vManage configuration.



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

You must attach the service groups to a cluster. After attaching service groups containing PNF devices with a cluster, the PNF configuration is not automatically pushed to the device unlike VNF devices. Instead, you must manually configure the PNF device by noting configuration that is generated on the Monitor Cloud OnRamp Colocation Clusters from vManage screen. The VLANs must be also configured on the Catalyst 9500 interfaces. 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 Catalyst 9500

Procedure

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 Device Port Connectivity Details and Service Chaining, on page 21 .

Step 2 Connect with Catalyst 9500 by using either the terminal server of any of the Catalyst 9500 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 Catalyst 9500 with interfaces that are connected the PNF. See the Monitor Cloud OnRamp Colocation Clusters from vManage screen for the generated VLAN configuration.

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

Custom Service Chain with Shared VNF Devices

You can customize service chains by including supported VNF devices.

Before you begin

Esure 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

Procedure

Step 1 Create a service group and service chains within the service group. See Create Service Chain in a Service Group, on page 46.

Step 2 In the **Add Service Chain** dialog box, provide 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. In the left panel, the 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 on the left panel, and drag the icon to its 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) Choose the software image to load from the **Image Package** drop-down.

To create a customized VNF package from vManage, see Create Customized VNF Image, on page 69.

c) Click **Fetch VNF Properties**.
d) Enter a name of the VNF in the **Name** field.
e) Enter the number of virtual CPUs required for the VNF in the **CPU** field.
f) Enter the amount of memory in megabytes to be allocated for the VNF in the **Memory** field.
g) Enter the amount of memory for storage in gigabytes to be allocated for the VNF in the **Disk** field.
h) Enter VNF-specific parameters, as required. See Create Service Chain in a Service Group, on page 46 for more information about VNF-specific properties.

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

For a complete information about the list of user and system variables for different VNF types such as vEdge, ASAv, CSR1000v when located at various positions, see Shared VNF Use Cases, on page 57 and Custom Packaging Details for Shared VNF, on page 113 .

Note
Ensure that you provide the values of the user variables if they are defined as mandatory, and for the system variables, vManage automatically sets the values for them.

i) Click **Configure**.

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

Step 5 Edit an existing VNF configuration by clicking it.

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

After a VNF is shared, if you hover on a VNF, the respective shared VNF devices are highlighted in blue color. After you choose a 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 images depict some of the shared VNF use cases and their predefined variable list:

Figure 14: Shared First vEdge VNF

The vEdge 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. To view and use the variable list that is associated for this scenario and various other scenarios, see vEdge Variable List .

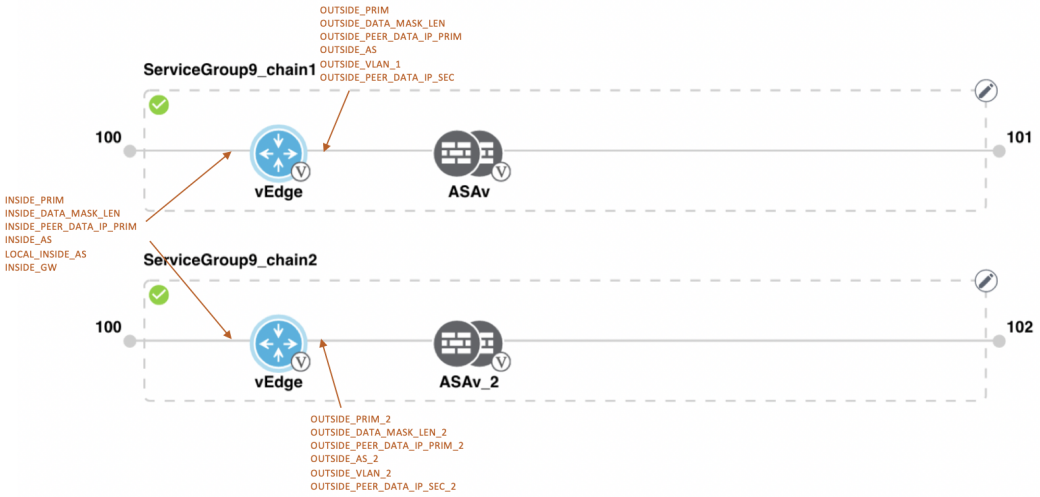


Figure 15: Shared First vEdge VNF

The vEdge 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. To view and use the variable list that is associated for this scenario and various other scenarios, see vEdge Variable List .

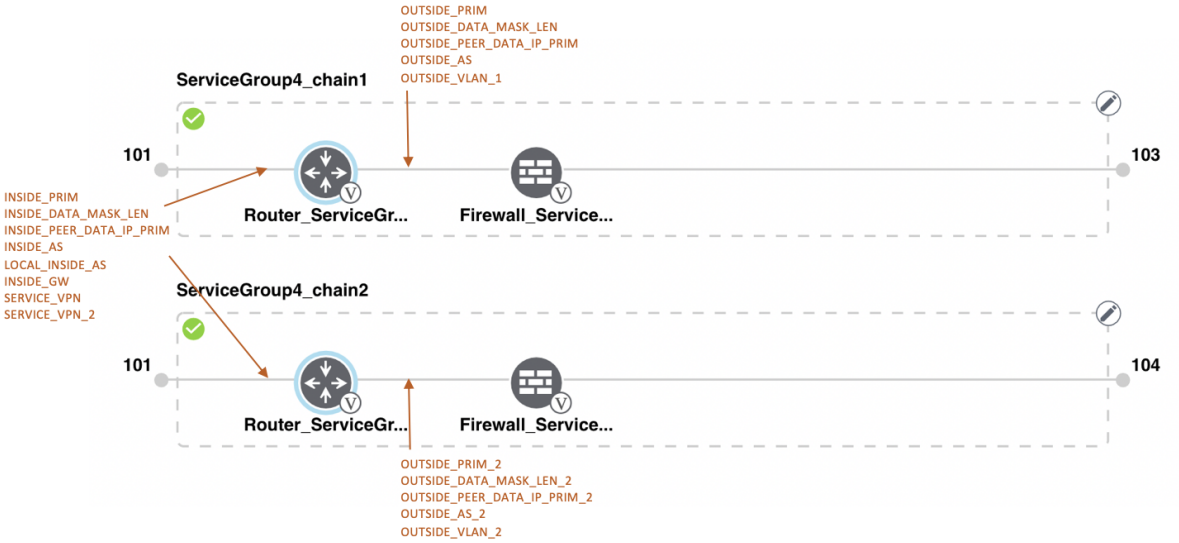


Figure 16: Shared First vEdge VNF

The vEdge 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. To view and use the variable list that is associated for this scenario and various other scenarios, see vEdge Variable List .

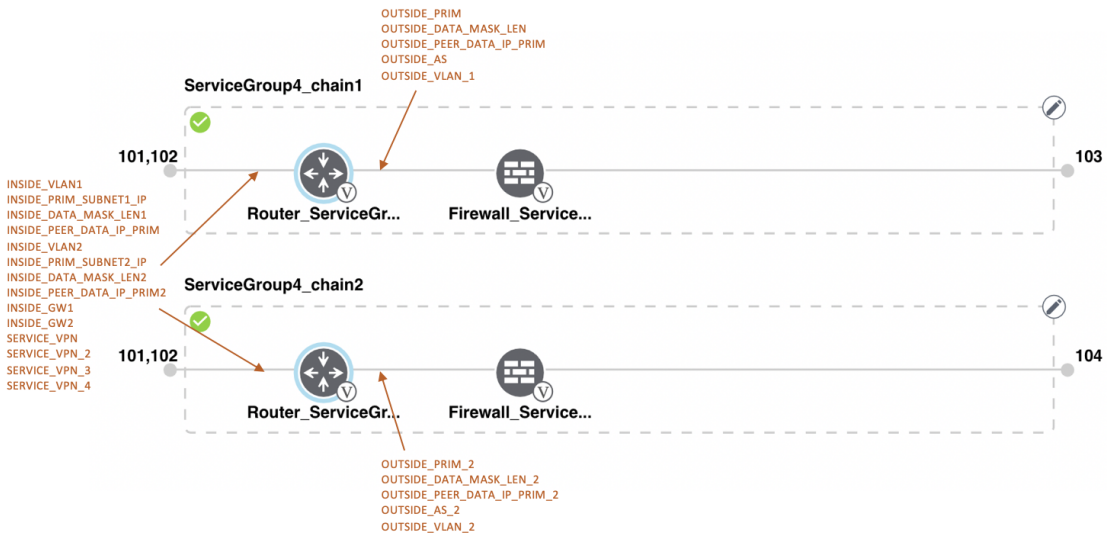


Figure 17: Shared First vEdge VNF

The vEdge 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. To view and use the variable list that is associated for this scenario and various other scenarios, see vEdge Variable List .

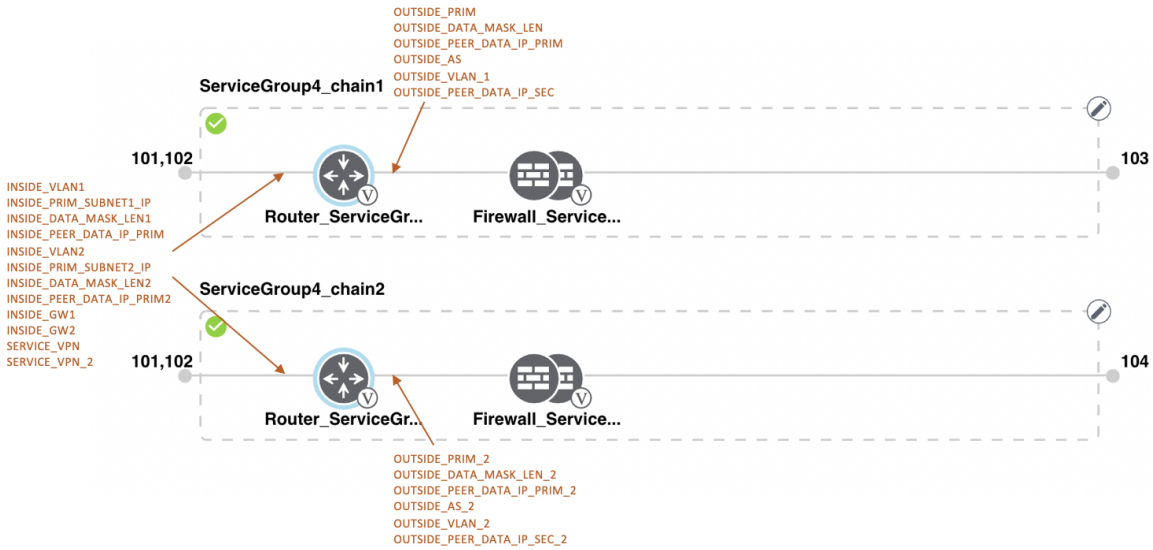


Figure 18: Shared Last CSR VNF

The CSR 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. To view and use the variable list that is associated for this scenario and various other scenarios, see CSR Variable List, on page 117 .

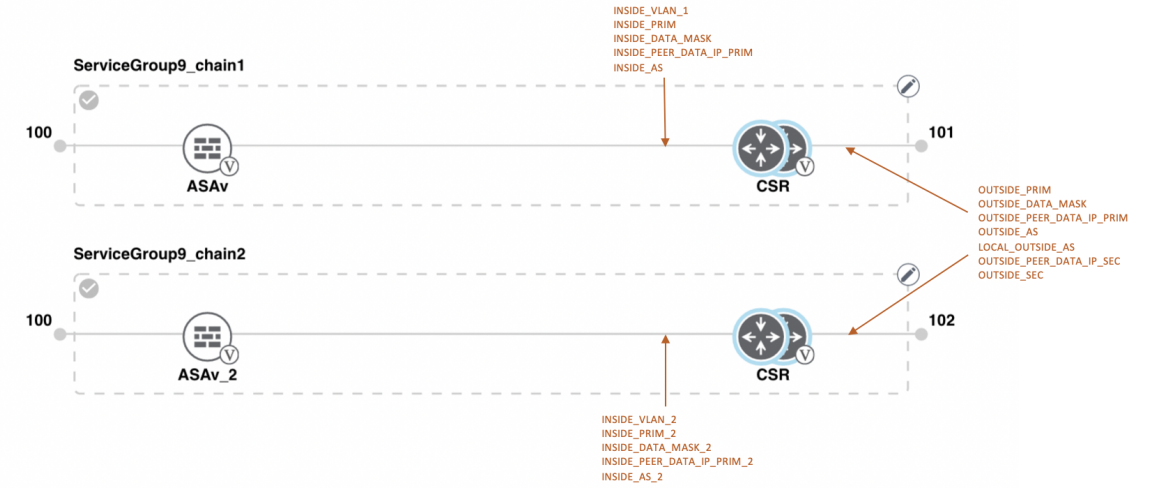


Figure 19: Shared Last CSR VNF

The CSR 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. To view and use the variable list that is associated for this scenario and various other scenarios, see CSR Variable List .

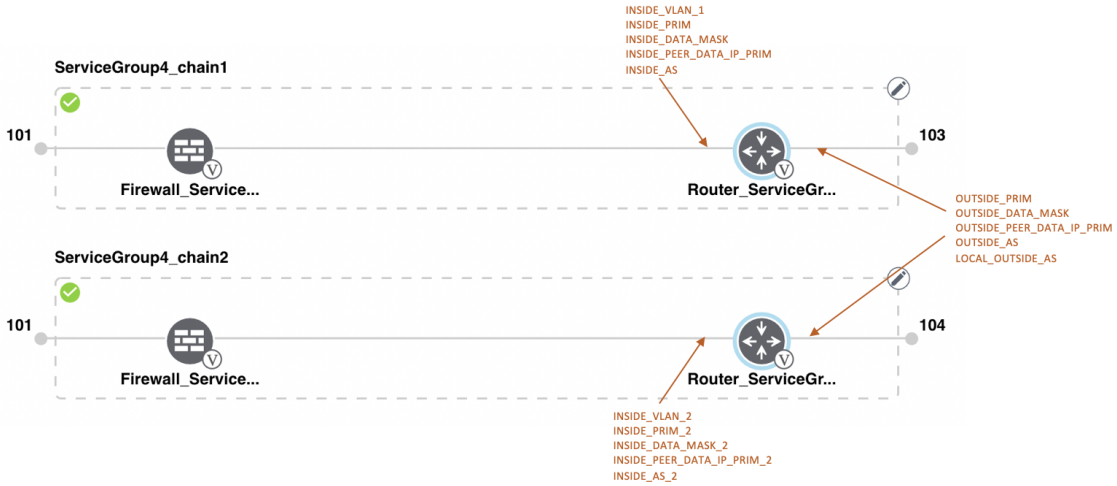


Figure 20: Shared Last CSR VNF

The CSR 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. To view and use the variable list that is associated for this scenario and various other scenarios, see CSR Variable List .

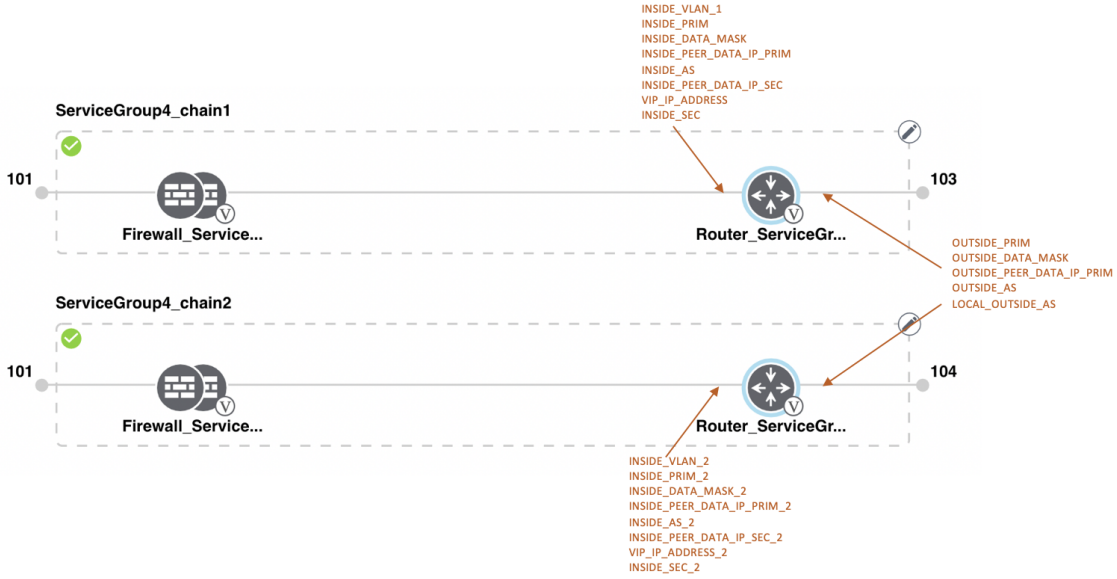


Figure 21: Shared Last CSR VNF

The CSR 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. To view and use the variable list that is associated for this scenario and various other scenarios, see CSR Variable List .

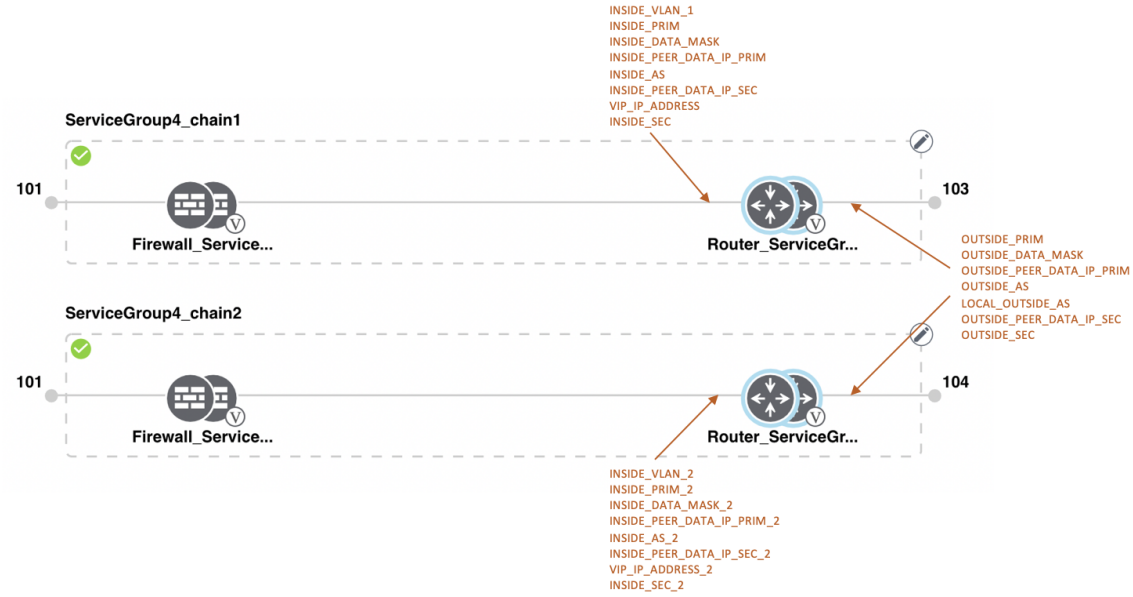


Figure 22: Shared First ASAv VNF

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 (CSR) is in redundant mode. To view and use the variable list that is associated for this scenario and various other scenarios, see ASAv Variable List, on page 121 .

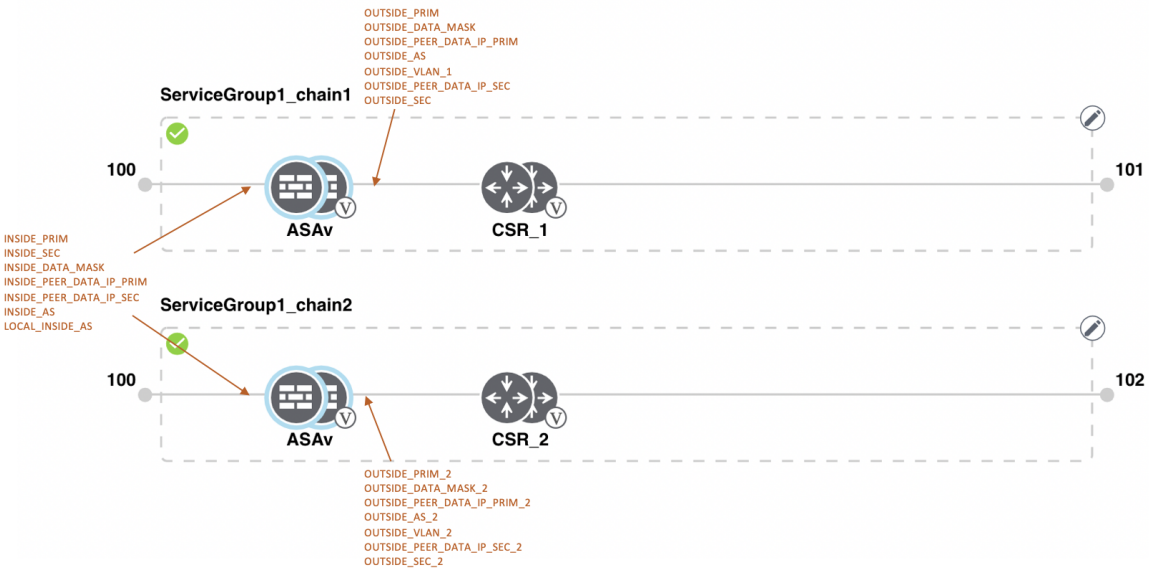


Figure 23: Shared First ASAv VNF

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. To view and use the variable list that is associated for this scenario and various other scenarios, see ASAv Variable List .

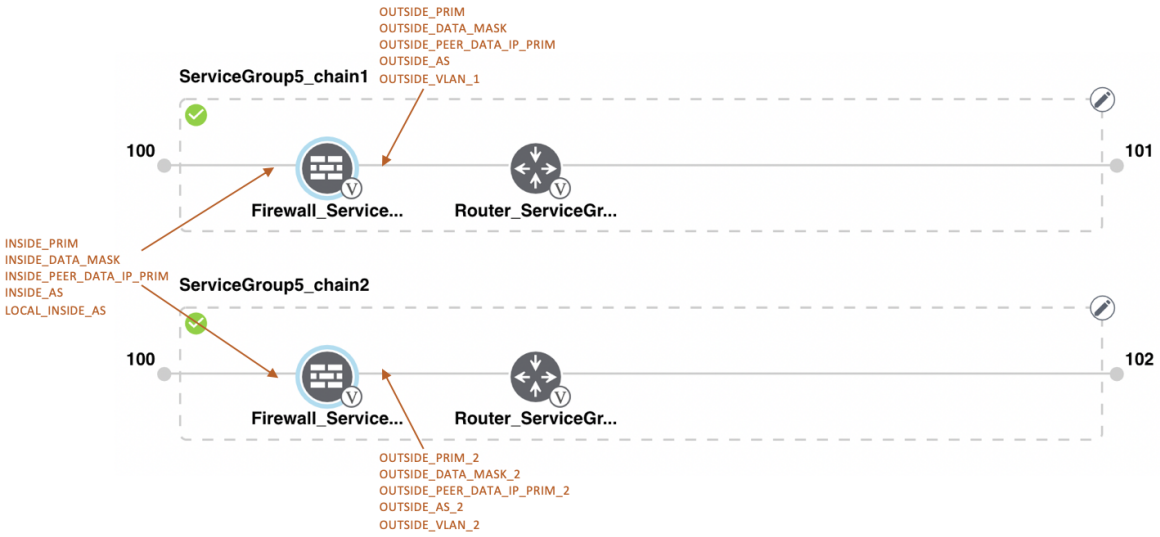


Figure 24: Shared First ASAv VNF

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. To view and use the variable list that is associated for this scenario and various other scenarios, see ASAv Variable List .

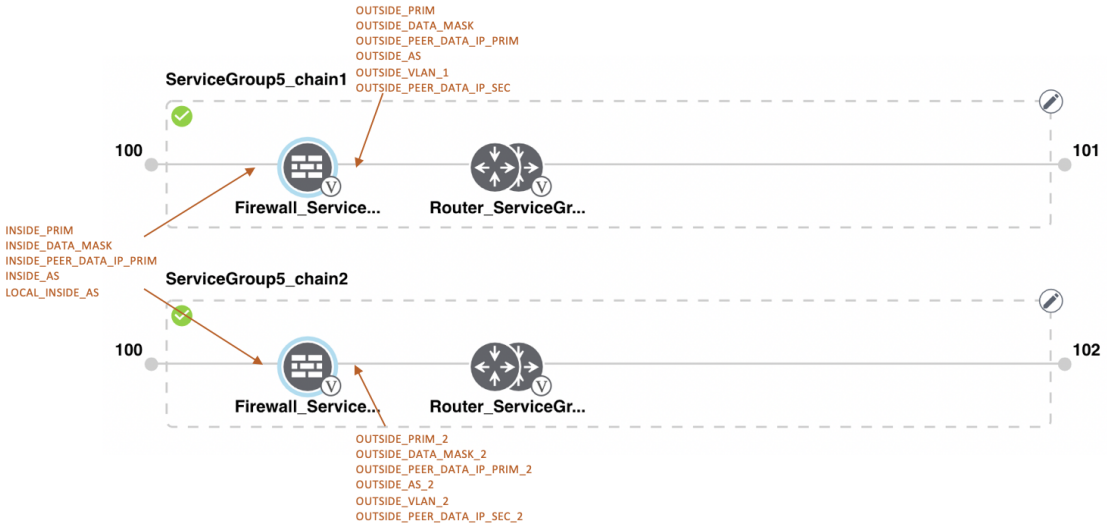
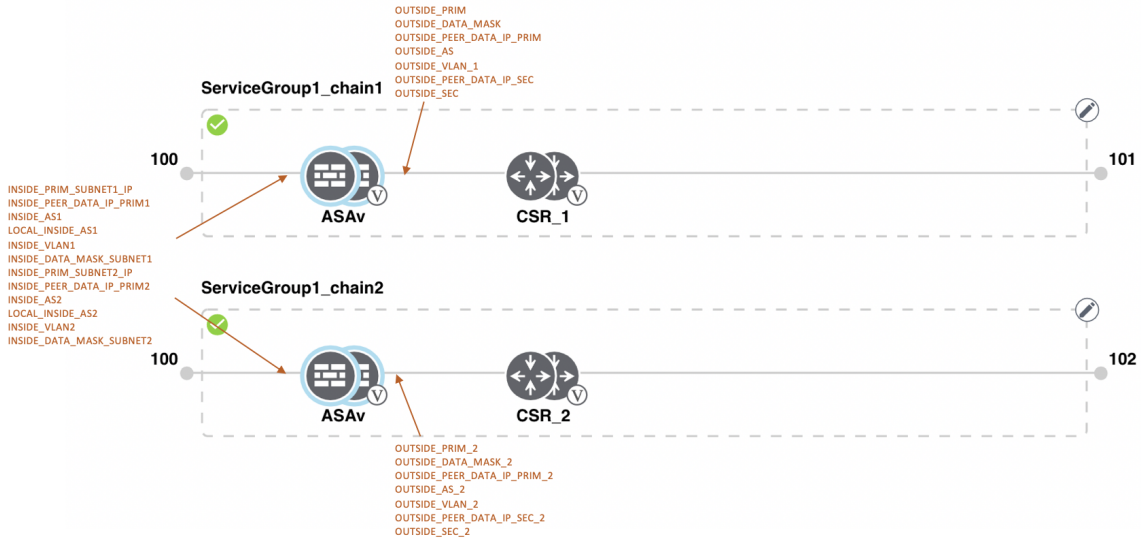


Figure 25: Shared First ASAv VNF

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 (CSR) is in redundant mode. To view and use the variable list that is associated for this scenario and various other scenarios, see ASAv Variable List .



View Service Groups in vManage

To view service groups, perform the following steps:

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLOCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab.

b) To view the service chains in the design view window, click a service chain box.

Edit Service Group in vManage

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:

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLOCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab.

b) To modify either service chain configuration or modify a VNF configuration, click a router or firewall VNF icon.

c) To add new service chains, click a service chain button.

Attach and Detach Service Group with 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 from a cluster, perform the following steps:

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Configuration** > **Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. To attach a service group with a cluster, perform the following steps:

a) In the **Cluster** tab, click a cluster from the table, click the **More Actions** icon to the right of its row, and click **Attach Service Groups**.

Step 3 In the **Attach Service Groups** dialog box, select a service group from the available service groups.

Step 4 Click the right arrow to move the chosen service groups to the selected box.

Step 5 Click **Attach**.

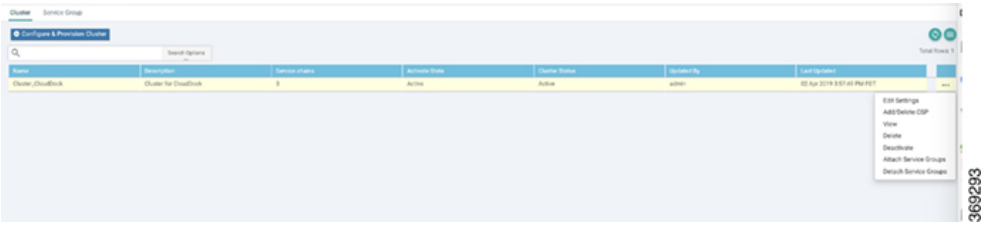
Step 6 To detach a service group from a cluster, perform the following action:

a) In the **Cluster** tab, click a cluster from the table, click the **More Actions** icon to the right of its row.

b) Click **Detach Service Groups**.

You cannot attach or detach an individual service chain within a group.

Step 7 To verify if service groups have been attached and detached, you can view from the following vManage screen:

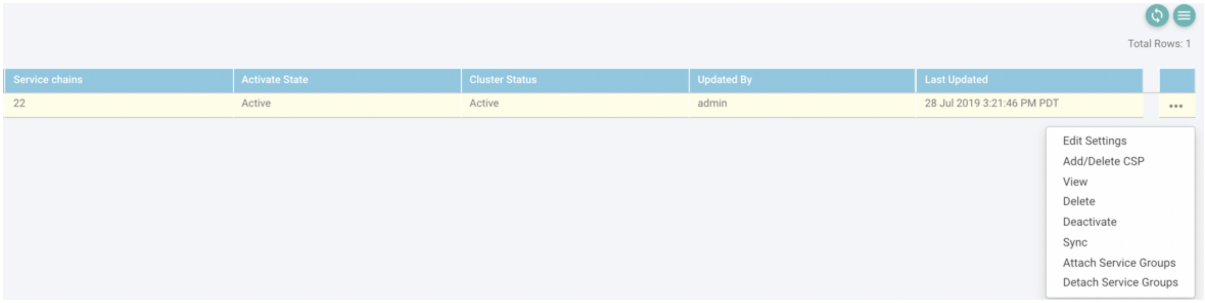


If the statuses of the tasks are "FAILURE" or in "PENDING" state for long duration, see Troubleshoot Service Chain Issues, on page 108 the topic, "Troubleshoot Service Chain Issues" in the Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide .

If a Cisco Colo Manager task fails, see Troubleshoot Cisco Colo Manager Issues, on page 108.

Note If a cluster goes into a "PENDING" state, click the **More Actions** icon to the right of its row and then click the **Sync** button. This action moves the cluster back to an "ACTIVE" state. The sync button keeps the vManage synched with the devices and is visible when a cluster is active.

Figure 26: Sync Button for a Cluster



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

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

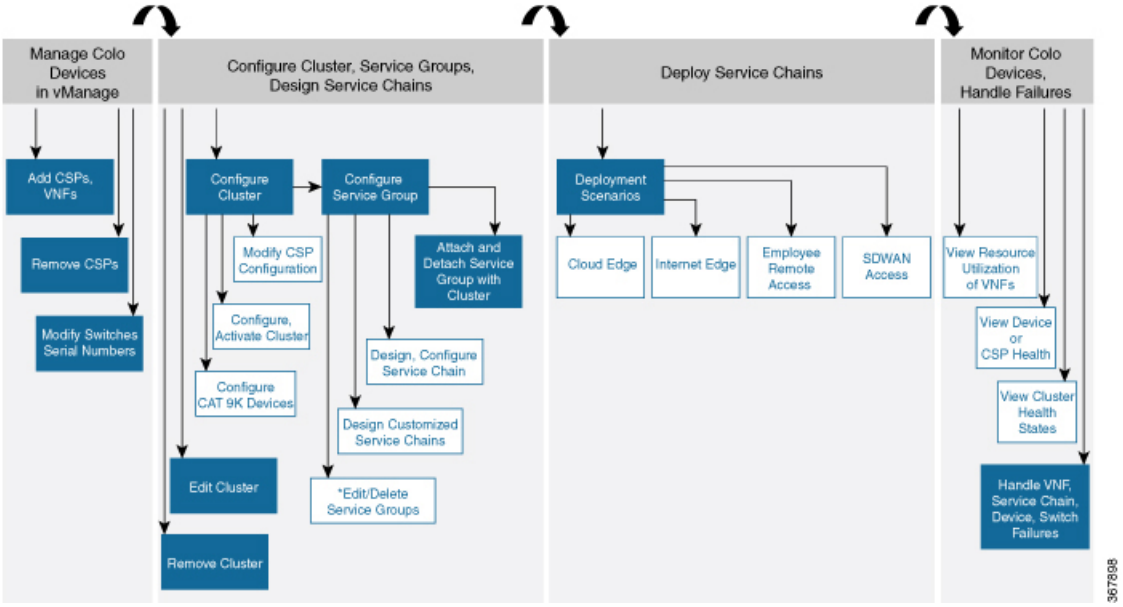
- All Day-N configuration from vManage requires clusters to be in-sync (devices have to be in synchronization with vManage) state.
- During attaching a service group, vManage runs the Placement logic to determine which VMs are placed on which CSP device.
- Switch-related Day-N configuration from vManage requires Cisco Colo Manager to be in a Healthy state.
- vManage pushes all switch-related service chain, cluster, switch configuration to Cisco Colo Manager.
- Cisco Colo Manager moves to In-progress state for any configuration that is received.
- 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 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 vManage about the VM file download status.

- After all VMs are downloaded, vManage sends the bulk configuration to spin all VMs.
- CSP devices send notifications to vManage about VM being brought up and its states.
- If any switches return error, vManage reports error with a detailed information and the cluster moves to a FAILURE state.

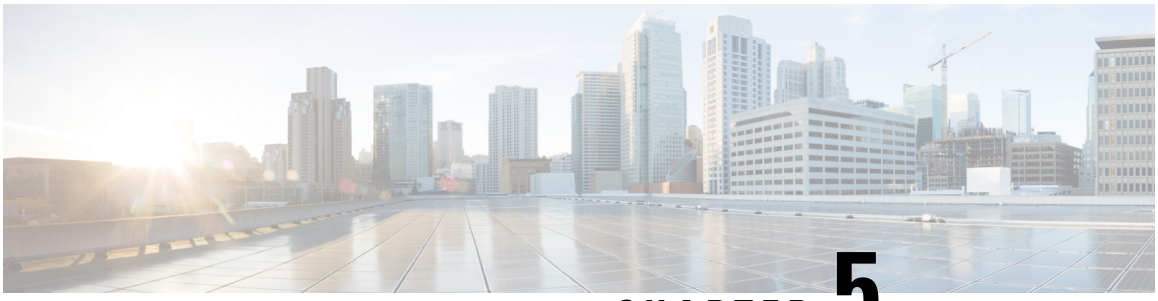
Ensure that you fix errors that are based on notifications and error messages, and then activate the Cloud OnRamp for Colocation again.

Note During the Day-N configuration, you can modify Serial Number of switches for a maximum of two switches that are allowed.

Figure 27: Day-N Workflow



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



CHAPTER 5

Software Image Management (SWIM) for Cluster Components and SWIM

- Manage VM Catalog and Repository, on page 67
- Upgrade NFVIS Software Through vManage, on page 75

Manage VM Catalog and Repository

vManage supports uploading a prepackaged Cisco VM image, tar.gz in this phase. Alternatively, you can package the VM image by providing a root disk image in any of the supported formats (qcow2). Use the linux command-line NFVIS VM packaging tool, **nfvpt.py** to package the qcow2 or alternatively create a customized VM image from vManage. See Create Customized VNF Image, on page 69.

If VM is SR-IOV capable, which means sriov_supported is set to true in image_properties.xml in the vm package *.tar.gz. Also, the service chain network is automatically connected to SR-IOV network. If sriov_supported is set to false, OVS network is created on the data port channel. It is attached to VM VNICs for service chaining, which is done by using the OVS network. For the Cisco SD-WAN Cloud OnRamp for Colocation solution, service chaining a VM uses homogeneous type of network. This type of network means it is either OVS or SR-IOV, and not a combination of SR-IOV and OVS.

Only two data VNICs are attached to any VM–one for inbound traffic and the other for outbound traffic. If more than two data interfaces are required, use subinterfaces configuration within the VM. The VM packages are stored in the VM catalog.

Note Each VM type such as firewall can have multiple VM images that are uploaded to vManage from same or different vendors being added to the catalog. Also, different versions that are based on the release of the same VM can be added to the catalog. However, ensure that the VM name is unique.

The Cisco VM image format can be bundled as *.tar.gz and can include:

- Root disk images to boot the VM.
- Package manifest for checksum validation of the file listing in the package.
- Image properties file in XML format that lists the VM meta data.
- (Optional) Day-0 configuration, other files that are required to bootstrap the VM.

- (Optional) HA Day-0 configuration if VM supports stateful HA.
- System generated properties file in XML format that lists the VM system properties

VM images can be hosted on both HTTP server local repository that vManage hosts or the remote server.

If VM is in NFVIS supported VM package format such as, tar.gz, vManage performs all the processing and you can provide variable key and values during VNF provisioning.



Note vManage only manages the Cisco VNFs, whereas Day-1 and Day-N configurations within VNF are not supported for other VNFs. See the NFVIS Configuration Guide, VM Image Packaging for more information about VM package format and content, and samples on image_properties.xml and manifest (package.mf).

To upload multiple packages for the same VM, same version, Communication Manager (CM) type, ensure that one of the three values (name, version, VNF type) are different. Then, you can repackage the VM *.tar.gz to be uploaded.

VNF Image Format

The service orchestrator does not distinguish between Cisco VNFs and third-party VNFs. All VNFs are categorized based on the services that are provided by the VNF such as router, firewall, load balancer, and others. The package metadata has VM_specific attributes. Based on HA NICs and management NICs specified in the package metadata file, orchestrator attaches management NIC and HA NIC. By default, management NIC is zero and HA NIC is one. The number of HA NICs that is specified is attached during VNF provisioning.

Upload VNF Images in vManage Repository

The VNF images are stored in vManage software respository. These VNF images are referenced during service chain deployment, and then they are pushed to NFVIS during service chain attachment.

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

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

b) Choose the location to store the virtual image.

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

  1. Drag and drop the virtual image file to the dialog box or click **Browse** to choose the virtual image from the local vManage server. For example, CSR.tar.gz, ASAv.tar.gz.
  2. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

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

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

c) Click **Submit**.

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

Create Customized VNF Image

Before you begin

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

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In the **Maintenance** > **Software Repository** screen, click the **Add Custom VNF Package** button from the **Virtual Images** tab.

Step 3 Configure the VNF with the following VNF package properties and click **Save**.

Table 12: VNF Package Properties

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

Step 4 To package a VM qcow2 image, click **File Upload** under **Image**, and browse to choose a qcow2 image file.

Step 5 To choose a bootstrap configuration file for VNF, if any, click the **Bootstrap Files** button under **Day 0 Configuration**, click **File Upload**, and then browse to choose a bootstrap file.

Include the following Day-0 configuration properties:

Table 13: Day-0 Configuration

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

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

Step 6 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize

variables of a Day-0 configuration file, click **View Configuration File** against the configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note
The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see Custom Packaging Details for Shared VNF, on page 113 for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down, and click **Done**. The highlighted property is replaced by the system variable name.
c) To add a custom variable, in the **CLI configuration** dialog box, select and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter custom variable name and choose a type from **Type** drop-down.
e) To set the custom variable attribute, do the following:

- To ensure that the custom variable is mandatory when creating a service chain, check the **Type** check box against **Mandatory**.
- To ensure that a VNF includes both primary and secondary Day-0 files, check the **Type** check box against **Common**.

f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 7 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an additional qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

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

Step 8 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 14: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	Specifies the disk size that is required for the VM operation. The maximum disk size can be 256 if the size unit is GiB.
Size Unit	Mandatory	Choose size unit. Supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. Default is a disk.
Location	Optional	Specifies location of the disk or CD-ROM. By default, it is local.

Field	Mandatory or Optional	Description
Format	Optional	Choose a disk image format. Supported formats are: qcow2, raw, and vmdk. Buy default, it is raw.
Bus	Optional	Choose a value from the drop-down. Supported values for a bus are: virtio, scsi, and ide. By default, it is virtio.

Step 9 To add VNF image properties, expand **Image Properties** and provide the following image information.

Table 15: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Specifies enabling or disabling SR-IOV support. By default, it is enabled.
Monitored	Mandatory	VM health monitoring for those VMs that can be bootstrapped. Options are: enable or disable. By default, it is enabled.
Bootup Time	Mandatory	Specifies monitoring timeout period for a monitored VM. By default, it is 600 seconds.
Serial Console	Optional	Specifies serial console that is supported or not. Options are: enable or disable. By default, it is disabled.
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. Options are: enable or disable. By default, it is disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. Options are: enable or disable. By default, it is enabled.

Step 10 To add VM resource requirements, expand **Resource Requirements** and provide the following information.

Table 16: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	Specifies CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	Specifies RAM supported by a VM. The RAM can range from 2–32.
Disk Size	Mandatory	Specifies disk size in GB supported by a VM. The disk size can range from 4–256.
Max number of VNICs	Optional	Specifies maximum number of VNICs allowed for the VM. The number of VNICs can range from 8–32 and the default value is 8.
Management VNIC ID	Mandatory	Specifies the management VNIC ID corresponding to the management interface. Valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	Specifies number of VNICs.
High Availability VNIC ID	Mandatory	Specifies VNIC IDs where high availability is enabled. Valid range is from 0–maximum number of VNICs. It should not conflict with management VNIC Id. The default value is 1.
Number of High Availability VNICs ID	Mandatory	Specifies maximum number of VNIC IDs where high availability is enabled. Valid range is 0–(maximum number of VNICs-number of management VNICs-2) and default value is 1.

Step 11 To add Day-0 configuration drive options, expand **Day0 Configuration Drive options** and provide the following information.

Table 17: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	Displays the volume label of the Day-0 configuration drive. Options are: V1 or V2. By default, it is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.

Field	Mandatory or Optional	Description
Init Drive	Optional	Mounts the Day-0 configuration file as a disk. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. Supported values for a bus are: virtio, scsi, and ide. By default, it is ide.

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

View VNF Images in vManage Repository

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To view VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

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

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

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

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

The Version Type Name column provides the type of firewall.

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

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

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

Delete VNF Images from vManage Repository

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Maintenance** > **Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VM images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

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

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



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

Upgrade NFVIS Software Through vManage

To upload and upgrade NFVIS, the upgrade image must be available as an archive file that can be uploaded to vManage repository through vManage. After you upload the NFVIS image, the upgraded image can be applied to a CSP device by using the Software Upgrade screen in vManage. You can perform the following tasks during upgrading NFVIS software through vManage:

- Upload NFVIS upgrade image. See Upload NFVIS Upgrade Image, on page 75.
- Upgrade a CSP device with the uploaded image. See Upgrade CSP Device with NFVIS Upgrade Image, on page 76.
- View the upgrade status in the CSP device. See the "View Log of Software Upgrade Activities" in the Cisco SD-WAN Configuration Guide.

Upload NFVIS Upgrade Image

Procedure

Step 1 Download the NFVIS upgrade image from a prescribed location to your local system. You can also download the software image to an FTP server in your network.

Step 2 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 3 In the **Maintenance** > **Software Repository** screen, click the **Add New Software** > **Remote Server/Remote Server - vManage** button.

You can either store the software image on a remote file server, on a remote vManage server, or on a vManage server.

Note
The vManage server is available in the current version.

vManage server–saves software images on a local vManage server.

Remote server–saves the URL pointing to the location of the software image and can be accessed through an FTP or HTTP URL.

Remote vManage server–saves software images on a remote vManager server and location of the remote vManage server is stored in the local vManage server.

Step 4 To add the image to the software repository, browse and choose the NFVIS upgrade image that you had downloaded in step1.

Step 5 Click **Add|Upload**.

The Software Repository table displays the added NFVIS upgrade image, and it is available for installing on the CSP devices. See the "Software Repository" topic in the Cisco SD-WAN Configuraion Guides.

Upgrade CSP Device with NFVIS Upgrade Image

Before you begin

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In the **Maintenance** > **Software Upgrade** > **WAN Edge** screen, view the list of all CSP devices along with their current and available versions.

Step 3 Select one or more devices, and click **Upgrade**.

Step 4 Choose a CSP device on which to upgrade the NFVIS software image.

Step 5 Click the **Upgrade** button. The **Software Upgrade** dialog box appears.

Step 6 Choose the NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

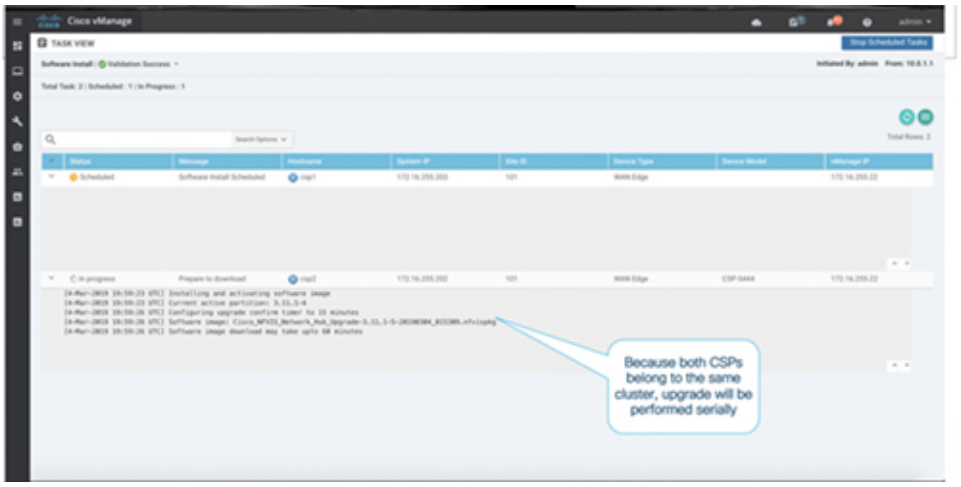
Step 7 To automatically upgrade and activate with the new NFVIS software version and reboot the CSP device, check the **Activate and Reboot** checkbox.

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

Step 8 Click **Upgrade**.

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

Note
If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happen in a sequence.



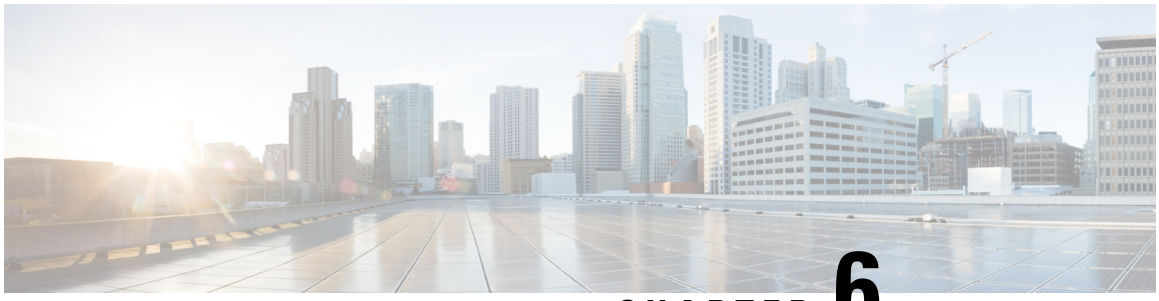
Note
The **Set the Default Software Version** option is not available for NFVIS images.

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

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



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



CHAPTER 6

Monitor Cisco SD-WAN Cloud OnRamp for Colocation Devices

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

The historical and real time operational statistics such as CPU, memory, disk and VNIC utilization charts are available for each VM and CSP. The VNF view can be navigated from a device under the cluster view or from services view. See Monitor Operational Status of Cloud OnRamp for Colocation Devices from vManage, on page 79.

- Monitor Operational Status of Cloud OnRamp for Colocation Devices from vManage, on page 79
- Cisco Colo Manager States for Switch Configuration, on page 87
- Cisco Colo Manager States and Transitions from Host, on page 87
- Cisco Colo Manager Notifications, on page 88
- VM Alarms, on page 90
- Cloud Services Platform Real-Time Commands, on page 91

Monitor Operational Status of Cloud OnRamp for Colocation Devices from vManage

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

All notifications are sent to the vManage notification stream. To view the notification stream, see Cisco SD-WAN Command Reference.

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 To view a list of all devices, click **Monitor** > **Network**.

A table lists information about all devices.

Step 3 To monitor a device, in the **WAN Edge** tab, click a CSP device or Cisco Colo Manager from the list by clicking its hostname.

By default, the System Status screen or Application screen appears. A horizontal bar at the top of the screen with the device drop-down, device name, device IP address, device site location, device model, and more information drop-down is displayed.

Step 4 If necessary, select a different device that you want to monitor.

Step 5 From the **Select Device** bar, click the **More Info** drop-down located to the right of the bar. vManage NMS opens a drop box with a summary information about the device.

In the left pane, the following are the categories of information about the device that you can view:

- VNF Status—view performance specifications, required resources, and component network functions for each VNF. See View Information About VNFs from vManage , on page 81.
- Interface—view Interface status and statistics. See the "View Interfaces" topic in the Cisco SD-WAN Configurtaion Guides.

  Note
  Interface status and statistics are only available for the OVS interfaces (non-SR-IOV).

- Control Connections—view status and statistics for control connections. See the "View Control Connections" topic in the Cisco SD-WAN Configurtaion Guides.
- System Status—view reboot and crash information, hardware component status, and CPU and memory usage. See the "View Control Connections" topic in the Cisco SD-WAN Configurtaion Guides.
- Colo Manager—view Cisco Colo Manager health status. See View Cisco Colo Manager Health from vManage , on page 81.
- Events—view latest syslog events. See the "View Events" topic in the Cisco SD-WAN Configurtaion Guides.
- Troubleshooting—view information about pings and traceroute traffic connectivity tools. See the "Troubleshoot a Device" topic in the Cisco SD-WAN Configurtaion Guides.
- Real Time—view real-time device information for feature-specific operational commands. See the "View Real-Time Data" topic in the Cisco SD-WAN Configurtaion Guides.

Step 6 To monitor clusters, click the **Colocation Clusters** tab from the Monitor|Network screen.

All clusters with relevant information are displayed in a tabular format. Click a cluster. See #unique_89 for more information.

View Information About VNFs from vManage

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Monitor** > **Network**.

The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

Step 3 Click a CSP device from the table.

Step 4 From the left pane, click **VNF Status**.

Step 5 In the table, click the VNF name. The right pane displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, disk utilization to monitor the resources utilization of a VNF.

The primary part of the right pane contains:

- Chart Options bar that includes the following options:
  - Chart Options drop-down—Click Chart Options to select the type of data to display.
  - Time periods—Click either a predefined time period, or a custom time period for which to display data.
- VNF information in graphical format.
- VNF graph legend—Select a VNF to display information for just that VNF.

The detail part of the right pane contains:

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

View Cisco Colo Manager Health from vManage

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

Procedure

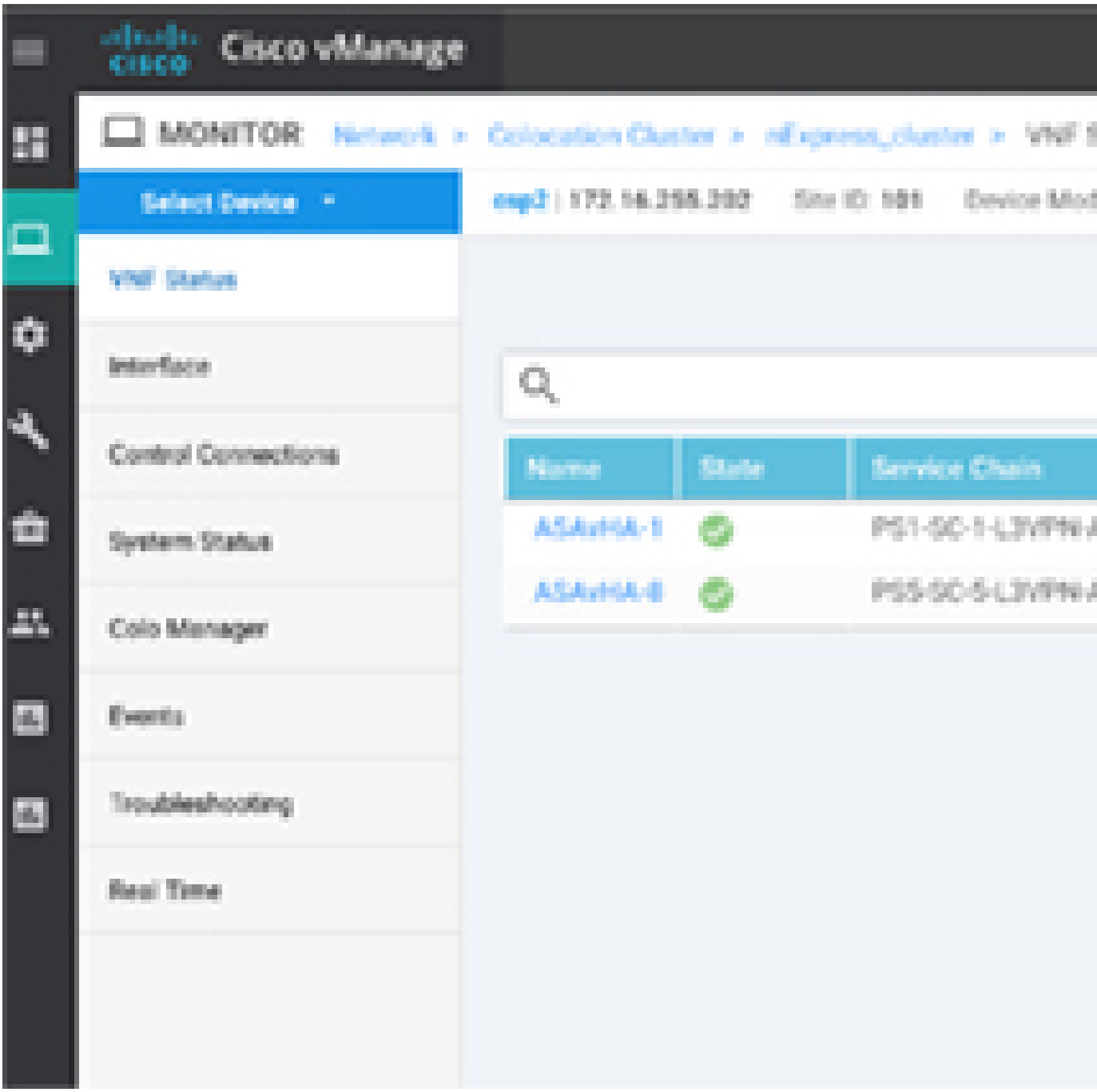
Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Monitor** > **Network**.

The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

Step 3 Click a CSP device from the table.

Step 4 From the left pane, click **Colo Manager**.



The right pane displays information about the memory usage, CPU usage, uptime, and so on, of the colo manager.

Monitor Cloud OnRamp Colocation Clusters from vManage

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

Procedure

Step 1 Log into Cisco vManage, at the URL HTTPS: //vManage-ip-address/, as a user with "admin" credentials.

Step 2 In vManage, click **Monitor** > **Network**.

Step 3 To monitor clusters, click the **Colocation Clusters** tab.

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

In the primary part of the left pane, you can view the PNF devices in a service group that are attached to a cluster along with the switches. In the right pane, you can view the cluster information such as the available and total CPU resources, available and allocated memory, and so on, based on Cloud OnRamp for Colocation size. You can see the Ordering and Sizing of Cisco SD-WAN Cloud OnRamp for Colocation Devices, on page 9 for more information.

The detail part of the left pane contains:

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

  Click a CSP cluster. VNF information is displayed in tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, and other core parameters that define performance of network service. See View Information About VNFs from vManage , on page 81.

Step 4 Click the **Services** tab.

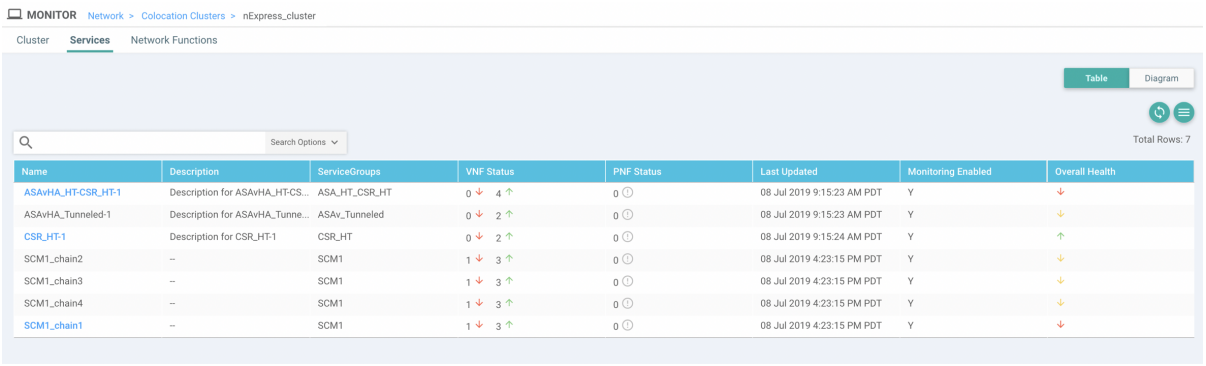
In this tab, you can view:

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

    If a service chain consists of a single PNF and PNF is orchestrated outside of vManage, then it cannot be monitored. If a service chain consists of a single network function, firewall that has VPN termination on both sides which cannot be monitored, then it is reported as Undetermined.

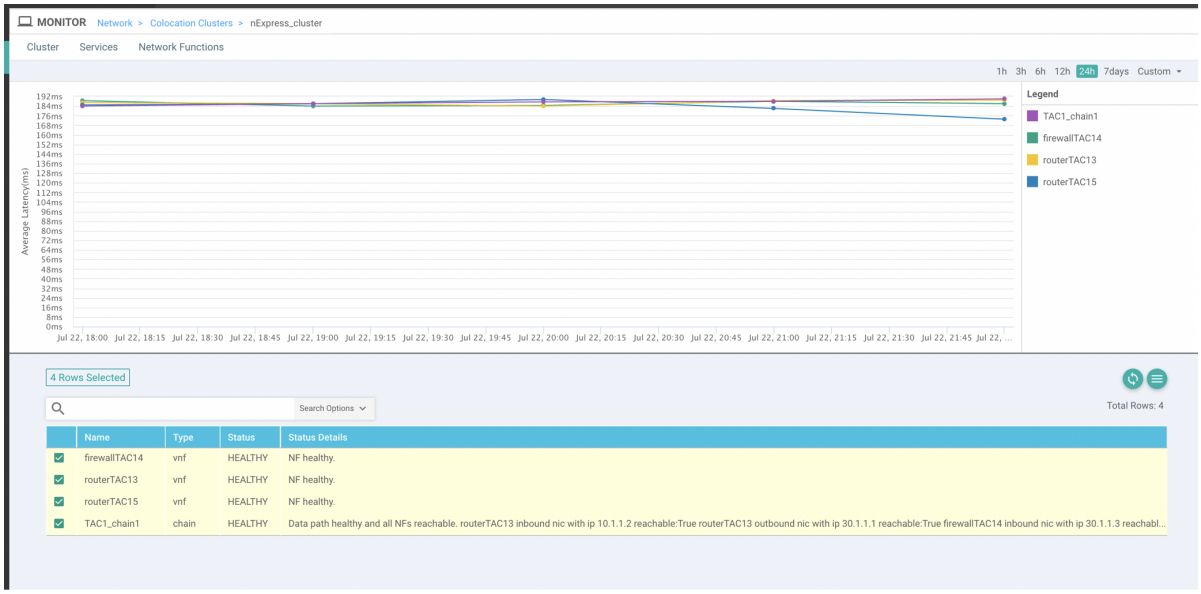
Note
If the status of a service chain is undetermined, you cannot choose the service chain to view the detailed monitoring information.

Figure 28: Service Chain Health Monitoring Results



- Click a service group that is in Healthy or Unhealthy state. The primary part of the service chain monitoring in the right pane contains the following elements:

Figure 29: Service Chain Health Monitoring Status



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

The detail part of the right pane contains:

- Filter criteria
- A table that lists information about all service chains, VNFs, PNFs, their health status, and types.
  - Check the checkbox at the left of a row to select and deselect a service chain, VNF, PNF.
  - To change the sort order of a column, click the column title.

In the following image, the status details column indicate the monitored data path and it provides the per hop analysis.

- Click the **Diagram** button and view the service group with all its service chains and VNFs in the design view window.
- Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
- Select a service group from the **Service Groups** drop-down. The design view displays the selected service group with all its service chains and VNFs.

Step 5 Click the **Network Functions** tab.

In this tab, you can view:

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

  VNF information is displayed in tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, Share NF column, and other core parameters that define performance of network service. Click a VNF to view more information about the VNF. See View Information About VNFs from vManage , on page 81.

- PNF information is displayed in tabular format. The table includes information such as the serial number and PNF type. To view and note configuration of a specific PNF, click the desired PNF serial number. Ensure that you manually note all the configuration of the PNFs and then configure the PNF devices. For example, the following are some of the PNF configuration where you position the PNF at various locations in the service chain. See Custom Service Chain with Shared PNF Devices, on page 52 to create services chains by adding PNFs. Also, see the ASR 1000 Series Aggregation Services Routers Configuration Guides and Cisco Firepower Threat Defense Configuration Guides to configure the PNFs manually.

Figure 30: PNF in the First Position with Service Chain Side Parameters

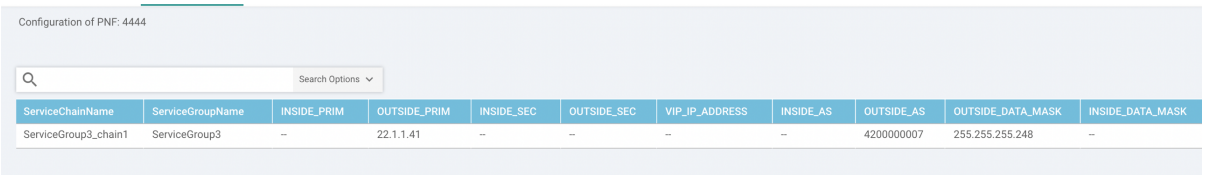


Figure 31: PNF in the First Position with Outside Neighbor Information

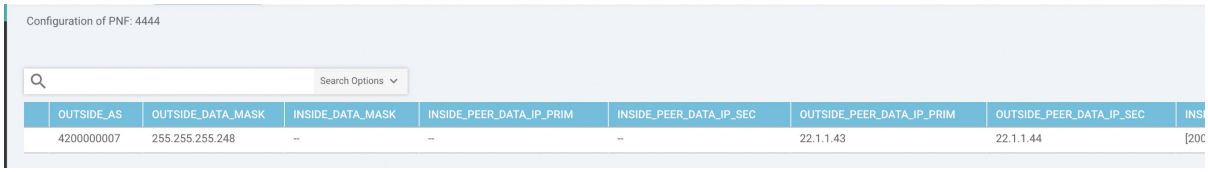


Figure 32: PNF Shared Across Two Service Chains

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

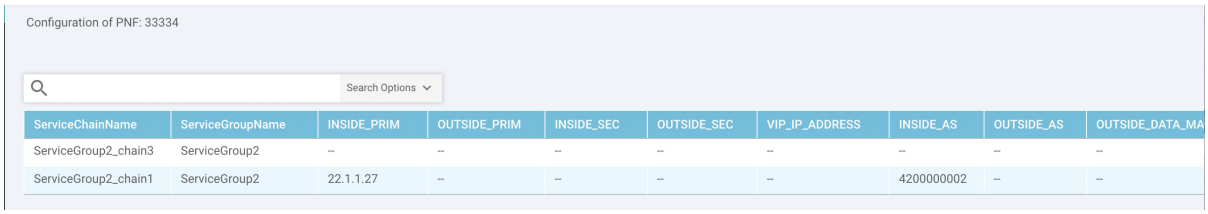


Figure 33: PNF Shared Across Two Service Chains with Outside Neighbor Information



Cisco Colo Manager States for Switch Configuration

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

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

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

Note A notification is sent when Cisco Colo Manager state changes. See Cisco Colo Manager Notifications, on page 88.

Cisco Colo Manager States and Transitions from Host

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

- Starting—when Cisco Colo Manager has been brought up and health check script has not been run. During this phase, vManage waits for CSP state to change to Healthy.

- Healthy—when the health check script has been run and it has passed the checks. This state implies that the operational model for configuration status can be queried or configuration can be pushed. During this phase, if Cisco Colo Manager is in INIT state, vManage pushes the device list. If Cisco Colo Manager is not in INIT state, Cloud OnRamp for Colocation may be in degraded state and recovery flow must happen.
- Unhealthy—when all the necessary packages in Network Services Orchestrator (NSO) are not up. This state can be due to various reasons such as, NSO did not come up, Cisco Colo Manager package did not come up, or other reasons. This state implies that the operational model for configuration status is not up and configuration cannot be pushed.

Cisco Colo Manager Notifications

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

See NFVIS Notifications in the NFVIS Integration with vManage chapter.

The various Cisco Colo Manager internal state machines are:

Table 18: ccmEvent

Cisco Colo Manager States	Notification Trigger	Notification Output Example

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

Cisco Colo Manager States	Notification Trigger	Notification Output Example
IN-PROGRESS	vManage pushes intent and Cisco Colo Manager moves to in-progress state. **Note** Cisco Colo Manager generates multiple in-progress notifications for the switches that are brought up.	notification eventTime 2019-04-08T17:37:54.536953+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message IN-PROGRESS details Received configuration from vManage event-type CCM-STATUS !
SUCCESS	During cluster activation, after Catalyst 9500 switches have been successfully onboarded, status moves to SUCCESS. For any incremental configuration push, status moves to SUCCESS only if configuration has been pushed successfully to the switches.	notification eventTime 2019-04-08T17:51:48.044286+00:00 ccmEvent severity-level minor host-name ccm user-id vmanage_admin config-change false transaction-id 0 status SUCCESS status-code 0 status-message SUCCESS details Devices done onboarding event-type CCM-STATUS ! ! admin@ncs#
FAILURE	If onboarding of switches fail duirng cluster activation failure, status moves to FAILURE. If any incremental configuration push fails, status moves to FAILURE. **Note** The failure state cannot transition to another state without end-user intervention.	notification eventTime 2019-04-08T18:01:44.943198+00:00 ccmEvent severity-level critical host-name ccm user-id vmanage_admin config-change false transaction-id 0 status FAILURE status-code 0 status-message FAILURE details SVL bringup not successful. Could not sync TenGigabitEthernet2/0/* interfaces. event-type CCM-STATUS ! ! admin@ncs#

VM Alarms

The following are VM alarms and they can be viewed from vManage, when alarms are received.

Table 19: Alarms

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

Alarm	Trigger Condition	Syslog Messages
VM_MONITOR_SET	vm monitoring set	nfvis %SYS-6-VM_MONITOR_SET: Setting VM monitoring successful: SystemAdminTena_ROUTER_0_df6733c1- 0768-4ae6-8dce-b223ecdb036c

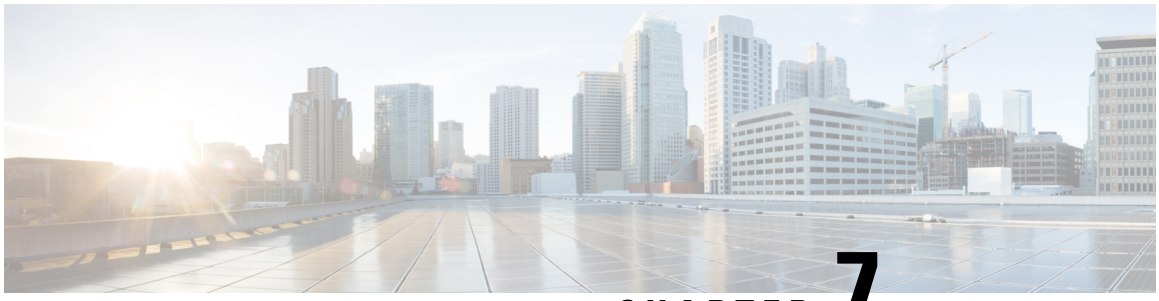
See Cisco NFVIS Configuration Guide for more information about syslog support and VM alarms.

Cloud Services Platform Real-Time Commands

Table 20: Real-Time Commands

System Information
Container status
show control connections
Control connection history
Control local properties
Control summary
Control statistics
Control valid vEdges
valid vManage ID
HW Alarms
HW Environments
PNICs
System Status
Host System Mgmt Info
Host System settings
Host System processes
Resource CPU allocation
RBAC Authentication
Resource CPU VNFs

Hardware Inventory
Hardware Temperature thresholds
Control affinity stats



CHAPTER 7

High Availability

The Cisco SD-WAN Cloud OnRamp for Colocation solution allows various consumers to access various repetitive applications securely. The Cisco SD-WAN Cloud OnRamp for Colocation High Availability (HA) is designed to handle several types of failure possible in a cluster deployment. The following types of failures can occur in a Cisco SD-WAN Cloud OnRamp for Colocation solution deployment:

- Compute failure
- Switch failure
- Service chain failure

To resolve the failures, use the following mechanisms:

- Redundancy
- Failure detection

- Redundancy, on page 93
- Handle Various Failure Scenarios, on page 95

Redundancy

The following are the components where redundancy has been added to address failure of the component:

- x86 Compute Hardware—See Redundancy of x86 Compute Hardware, on page 94.
- Network Fabric—See Redundancy of Network Fabric, on page 94.
- Physical NIC/interface—See Redundancy of Physical NIC or Interface, on page 94.
- NFVIS Virtualization Infrastructure—See Redundancy of NFVIS, Virtualization Infrastructure, on page 94.
- Service-Chain/VNF—See Redundancy of Service Chain or VNF, on page 94.
- Cisco Colo Manager—See Recovery of Cisco Colo Manager, on page 95.

Redundancy of Network Fabric

Network Fabric—The hardware switch redundancy features are used to handle network fabric failures. In a switch failure, ensure that the standby switch takes over the traffic traversing through the failed switch.

Redundancy of x86 Compute Hardware

x86 Compute Hardware—Any hardware components such as, processor, storage, and others that are used on the x86 compute hardware can fail leading to a complete CSP system failure. The SD-WAN Cloud OnRamp for Colocation orchestrator continuously monitors the health of the x86 compute platform by using ICMP ping through the management interface. In a system failure, the orchestrator shows the device status and the service chains and VMs impacted. Take desired action to bring up service chains. See Monitor Cisco SD-WAN Cloud OnRamp for Colocation Devices, on page 79. Depending on the operational status of the VNFs, the VMs must be brought up on a different CSP if enough are resources are available. This action allows the VNF to retain the Day-N configuration. If the VNF disk is using local storage, the entire service group must be respun on another CSP device with the Day-0 configuration that is stored in the orchestrator.

Redundancy of Physical NIC or Interface

Physical NIC or interface—If a physical NIC or interface or cable fails or gets disconnected, the VNFs that are using those interfaces are impacted. If a VNF is using an OVS network, the port channel configuration is used to achieve a link redundancy. If a VNF is using an OVS network, and if the VNF has an HA instance, that instance has been already brought up on a different CSP. The failover happens to this VNF on the second CSP. If there is no second VNF instance, the service chain with the failed VNF must be deleted and reinstantiated.

Redundancy of NFVIS, Virtualization Infrastructure

NFVIS Virtualization Infrastructure—Multiple types of failures in the NFVIS software layer can occur. One of the critical components of CSP can crash or the host Linux kernel can panic or one of the critical components fails to respond. In case of critical component failures, the NFVIS software generates netconf notifications. The orchestrator uses these notifications to show the failure on vManage dashboard. If the CSP or NFVIS crashes or control connection goes down, the orchestrator shows that device reachability is down. You can resolve a networking issue (if any), or reboot the CSP device. If device does not recover, you must proceed with removing the CSP device.

Redundancy of Service Chain or VNF

Service Chain or VNF—Some of the VNFs in an SD-WAN Cloud OnRamp for Colocation service chain such as, firewall may support stateful redundancy features by using a standby VNF, whereas VNFs such as CSR may not support stateful redundancy. The Cisco SD-WAN Cloud OnRamp for Colocation solution relies on the VNFs to achieve VNF high availability. Service chain level HA is not supported. If a VNF supports stateful HA, it detects the failure and performs a switchover. The assumption is that the previously active VNF goes down and reboots as a standby VNF if the CSP device hosting VNF is functional and all the NIC or interface connectivity is functional. If the VNF does not come up, HA for VNF is not functional from that time and your intervention is required.

If a VNF does not support HA, it is assumed that the VNF reboots if any critical process fails within the VNF and no HA support is available for such VNFs.

Recovery of Cisco Colo Manager

Cisco Colo Manager Recovery—Cisco Colo Manager is brought up on a CSP device in a Cloud OnRamp for Colocation. vManage selects a CSP with the DTLS tunnel to bring up Cisco Colo Manager. The Cisco Colo Manager recovery flow is required during the following scenario:

If a CSP hosting Cisco Colo Manager is considered for Return Material Authorization (RMA) process and there are at least two other CSP devices in the cluster after deleting this CSP, then a new Cisco Colo Manager is brought up automatically by vManage on one of the existing two CSP devices during a new configuration push.



Note You must power down the CSP device that has been considered for RMA process or perform a factory default reset on the CSP device. This task ensures that there is only one Cisco Colo Manager in the cluster.



Note A host with Cisco Colo Manager running can restart or reboot, and this action is not a recovery scenario as Cisco Colo Manager should come up intact with all the configuration and operational data.

If after a cluster is successfully activated and then Cisco Colo Manager becomes unhealthy, see Troubleshoot Cisco Colo Manager Issues, on page 108.

Handle Various Failure Scenarios

- VNF failure
  - If a VM in a service chain that is HA capable goes down, the standby VM takes over. This standby service chain is functional within few seconds. NFVIS software on CSP tries to bring up the failed active VM if it is a monitored VM. If the VM recovers successfully, it switches over to active and standby modes successfully. If VM did not recover successfully and you want to bring up HA capability on this VM, tear down the service chain and bring up new service chain with HA capability. Here, VM detects that the failure is based on heartbeat and there must not be any impact on traffic (except few seconds). If an active VM recovers, this VM could become active again or stay as standby and this state varies from VM to VM.
  - If a VM is not HA capable, the service chain fails and traffic is black holed. Cisco Colo Manager detects this failure and hence vManage as it receives notification that VM is down and service chain is down, vManage sends an alert. If the VM recovers successfully, the same notification is sent and the service chain is functional without any intervention. If the VM does not recover successfully, tear down the service chain and bring up a new service chain.
- Service chain failure
  - If all VMs in a service chain support HA, service chains can have active and standby service chains. If an active service chain goes down, the standby service chain takes over and is functional within few seconds. This behavior is VM level HA and VM failover behavior takes over. NFVIS software on CSP also tries to bring up the failed active VMs (for monitored VMs) and if they recover successfully, the VMs switch over to active and standby modes successfully.

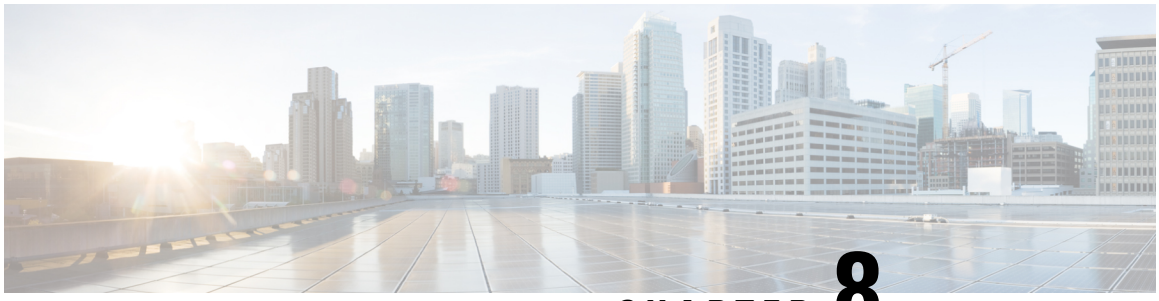
- If VMs are not HA capable, the service chain fails and traffic is black holed. NFVIS and Cisco Colo Manager send notifications that VMs are down and vManage sends an alert. Based on the notification, bring up another active service chain. If the service chain has recovered successfully, the same notification is sent and the service chain is functional without any intervention.

- Device failure

  If a CSP is down, all the service chains and VMs running on that CSP are also down. Cisco Colo Manager sends notifications to vManage that device is not reachable and vManage itself must detect DTLS connectivity loss with the CSP device. vManage sends alert about the CSP device and you must bring up the service chains on another CSP by creating the service chains and pushing the configuration to a colocation. If there is not enough compute hardware, add another CSP to a colocation and push the service chain configuration to the CSP.

- Switch link failure

  If a link from a switch is down, the other switch takes over and service chain traffic continues.



CHAPTER 8

Troubleshoot Cisco SD-WAN Cloud OnRamp for Colocation Solution

- Troubleshoot Catalyst 9500 Issues, on page 97
- Troubleshoot Cloud Services Platform Issues, on page 102
- DHCP IP Address Assignment, on page 107
- Troubleshoot Cisco Colo Manager Issues, on page 108
- Troubleshoot Service Chain Issues, on page 108
- Troubleshoot Physical Network Function Management Issues, on page 110
- Log Collection from CSP, on page 110
- Troubleshoot vManage Issues, on page 111

Troubleshoot Catalyst 9500 Issues

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

General Catalyst 9500 Issues

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

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

Devices have called home

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

Devices have not called home

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

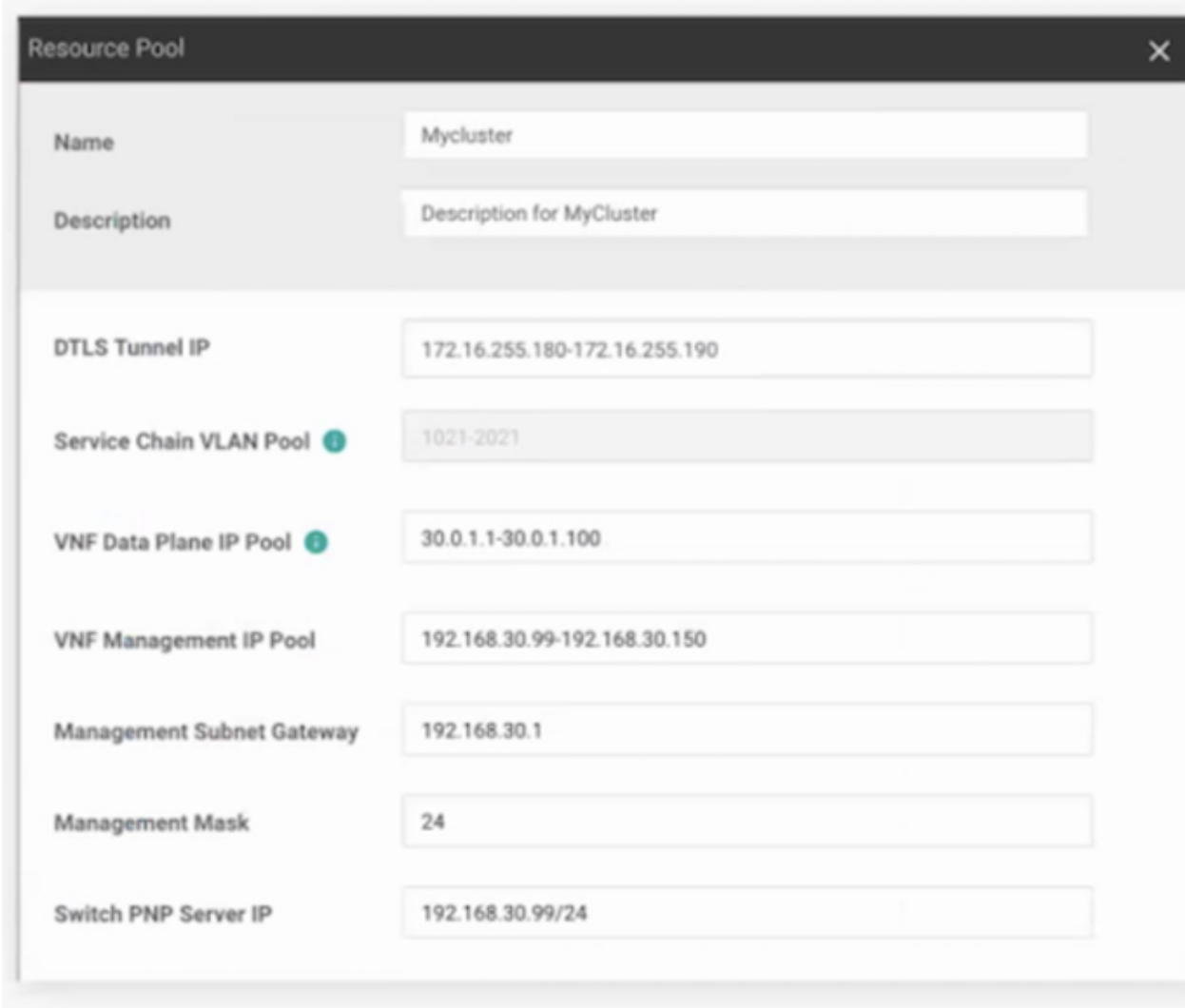
<– Empty list

Action:

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

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

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



5. Ping and determine whether both switches are reachable.

Catalyst 9500 failed to reach through DHCP option 43

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

Action:

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

Day-0 configuration push failed on both Catalyst 9500 switches

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

Action:

1. Clean the Catalyst 9K switches to INIT state.
2. Deactivate and Reactivate the cluster again from vManage to repush the Day-0 configuration.

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

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

Action:

1. Clean the secondary Catalyst 9K switch to INIT state.
2. Deactivate and Reactivate the cluster again from vManage to repush the Day-0 configuration.

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

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

Action:

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

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

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

Action:

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

Unable to log into Catalyst 9500 after PNP from vManage

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

Action:

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



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

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

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



Note Ensure that you set password as a scrypt string.

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

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

Action:

1. If a cluster activation is in still in pending state, verify if colo-config-status is in IN-PROGRESS state. If state is In-Progress, the synchronization has not been done and no new configurations can be pushed. This process can take up to 20 minutes.
   a. If Cloud OnRamp for Colocation configuration status is In-progress state for a long time, SSH into NFVIS as an admin user. Use the **ccm-console** command to log into Cisco Colo Manager. Run the **show pnp list** command. Verify if two switches are added.
   b. If only one switch is displayed, ensure that the other switch configuration is cleaned by using the **write erase** command and reloaded. The secondary switch startup configuration must be erased and returned to its initial state.
   c. Ensure switch connectivity with PNP server in Cisco Colo Manager.
     ```

2. If a cluster has been activated successfully, verify if colo-config-status is in "SUCCESS" state. If status is displayed as Success, your admin password must have been pushed to a switch. If not, on vManage, add a new credential to the switch and then push new configurations.
3. If a cluster activation fails and colo-config-status is in "FAILED" state, use the RBAC to push a new authentication from ccm-console. In the following example, the password is encryption of "Cisco-123."

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



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

Clean switches configuration and reset switches to factory defaults

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

Action:

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



Note The switch renumbering is essential for SVL stack mode.

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

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

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

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

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

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

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

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

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

4. To view the devices status in a colocation, use the **show colo-config-status** command. If status is in "In-progress," the switch devices are not yet synchronized and vManage cannot send any further configuration. See Chapter, Monitor Cisco SD-WAN Cloud OnRamp for Colocation Devices, on page 79 for more information about Cisco Colo Manager state transitions.

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

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

Troubleshoot Cloud Services Platform Issues

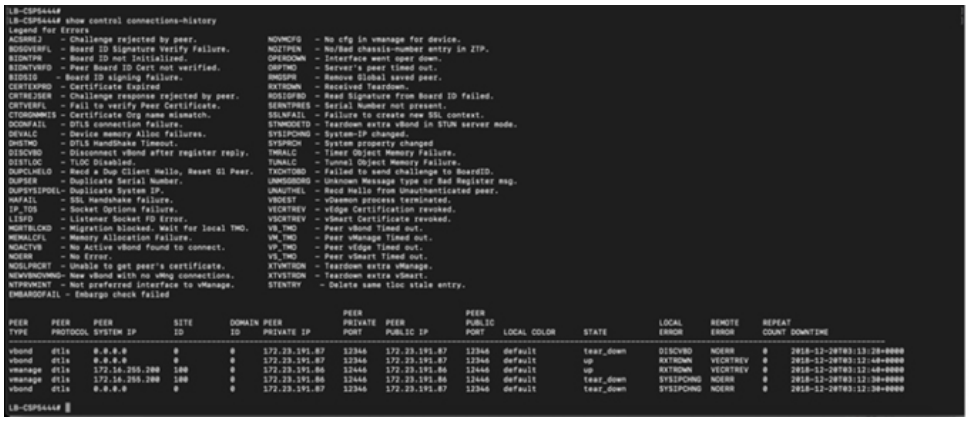
This section covers some of the common Cloud Services platform (CSP) problems and how to troubleshoot them.

General Cloud Services Platform Issues

Failures with Certificate installation

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

Figure 34: Certificate Installation Failure



Action:

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

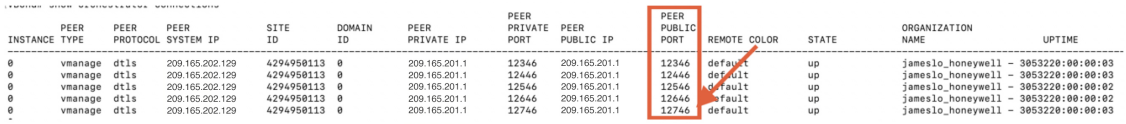
- vbond with error SERNTPRES–This error is caused, if the serial or token on device do not match with vBond serial or token. Check vManage to ensure that the device is in "valid" state and it was decommissioned properly.
- vManage with error NOVMCFG–This error is caused if the template was not attached to the device. Activating the cluster resolves this issue.

- On vBond, verify that the **show orchestrator valid-vedges** command shows the device correctly. This means that the device is valid with the same token that you had used.
- Ensure that the clock on vManage and CSP devices are synchronized.

Failures with Control Connection

The **show control connections-history** displays DCONFAIL. Open the firewall for the ports from the command, as shown.

Figure 35: Failure with Control Connection, DCONFAIL



INSTANCE	PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	ORGANIZATION NAME	UPTIME
0	vmanage	dtls	209.165.202.129	4294950113	0	209.165.201.1	12346	209.165.201.1	12346	default	up	jameslo_honeywell - 3053220:00:00:03	
0	vmanage	dtls	209.165.202.129	4294950113	0	209.165.201.1	12446	209.165.201.1	12446	default	up	jameslo_honeywell - 3053220:00:00:03	
0	vmanage	dtls	209.165.202.129	4294950113	0	209.165.201.1	12546	209.165.201.1	12546	default	up	jameslo_honeywell - 3053220:00:00:02	
0	vmanage	dtls	209.165.202.129	4294950113	0	209.165.201.1	12646	209.165.201.1	12646	default	up	jameslo_honeywell - 3053220:00:00:02	
0	vmanage	dtls	209.165.202.129	4294950113	0	209.165.201.1	12746	209.165.201.1	12746	default	up	jameslo_honeywell - 3053220:00:00:03	

Action:

Any of the following ports can be used to negotiate for control connection. You can open all the ports as mentioned in the following table:

Core Number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

CSP does not have a DHCP IP address

The CSP device does not get displayed in vManage as a connected device.

Action:

1. Connect to a CSP through the CIMC interface.
2. Verify if the CSP has an IP address by running the `show system:system settings` command on the Cloud OnRamp for Colocation management port.
3. Verify if the DHCP server has IP addresses. To assign a static IP address and configure DHCP sticky IP, see DHCP IP Address Assignment, on page 107.
4. Verify that the PNP server is reachable by a ping.

5. From the PNP server, verify if the CSP device can be contacted and claimed, or redirection is successful. In the PNP portal, if it shows Pending Redirection for the device, verify if the serial number is same as CSP devices.
6. Use the **`show platform-details`** command on CSP to determine the serial number.
7. In the PNP portal, verify if it shows Connected.

CSP has not established connectivity with vManage

The CSP device does not get displayed in vManage as a connected device.

Action:

1. Verify if the CSP device has root CA installed from PNP by using the **`show certificate installed`** and **`show certificate root-ca-cert`** .
2. Verify if CSP can ping the vBond IP address. Then, attain the vBond IP by using the **`show running-config viptela-system:system`**
3. If ping to vBond fails, verify the network connectivity on the management interface.
4. If ping to vBond goes through, use the **`running-config vpn 0`** to view the configuration for control connection.
5. If the control connection configuration exists, verify vManage settings.
6. In vManage, verify if a cluster is activated and device OTP information has been included by using the **`show control connections`** and **`show control local-properties`** commands.
7. Verify if the CSP token number has been manually entered by using the **`request vedge-cloud activate chassi-number token-number`** command. Rerun the command with the correct OTP.

Factory reset of CSP device

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

CSPxx# factory-default-reset all

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

CSP with a bad storage disk

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

Action:

Replace the faulty disk.

CSP device has less memory or CPU

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

Action:

Upgrade the specific CSP device that matches the minimum requirements.

I/O cards on CSP device are on wrong slots

Action:

Verify the slot details from CIMC inventory.

Colo Manager is not healthy on a CSP device

Action:

1. To verify Cisco Colo Manager state:
   a. Verify the health of the container by using the **`show container ColoMgr`** command. See Troubleshoot Cisco Colo Manager Issues, on page 108.
   b. View notifications about events from the Viptela device by using the **`show notification stream viptela`** command.
2. To access Cisco Colo Manager, run the **`ccm console`** command on the CSP device where Cisco Colo Manager has been enabled.

   This action takes you to the Cisco Colo Manager CLI. Run the **show running-config cluster** *cluster name* command.
3. Get the logs from vManage by using the **`admin-tech`** command. Alternatively, you can get the logs from the device directly. See Log Collection from CSP, on page 110.

Day-0 configuration push to CSP fails

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

Action:

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

CSP does not get added to a cluster

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

Action:

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

IP connectivity with CSP cannot be retained

When CSP 5444 devices renew its DHCP IP, the IP connectivity to the CSP cannot be retained.

Action:

For DHCP IP address allocation, ensure that the DHCP server is always on the same subnet as the CSP 5444 devices.

CSP devices are not able to reach vManage

Action:

Perform the following steps:

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

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

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

   ```
   --- mgmt-bond ----
   bond_mode: balance-slb
   bond may use recirculation: no, Recirc-ID : -1
   bond-hash-basis: 0
   updelay: 0 ms
   downdelay: 0 ms
   next rebalance: 3479 ms
   lacp_status: configured
   active slave mac: 00:00:00:00:00:00(none)
   slave eth0-1: disabled
                 may_enable: false
   slave eth0-2: disabled
                 may_enable: false
   ```

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

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


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


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

Note vManage manages the CSP devices and hence OOB configuration through NETCONF or REST API or CLI causes devices to be out of synchronization with vManage. vManage deletes this configuration when the next configuration is pushed from vManage. For any troubleshooting, to configure the CSP or NFVIS, use configuration only in shared mode and/or NETCONF target candidate followed by commit. This configuration is required as the Confd database, CDB is in a candidate mode on NFVIS for Cisco SD-WAN Cloud OnRamp for Colocation solution. If the **confg t** CLI mode or NETCONF target running is used, the CDB database can be out of synchronization and cause strange behavior on CSP devices and results into an unusable cluster.

DHCP IP Address Assignment

To configure a static IP address:

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

   For example,

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

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

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

   For example,

   nfvis# **config shared**

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

Configure DHCP Sticky IP

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

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

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

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

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

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

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

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

Troubleshoot Cisco Colo Manager Issues

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

General Cisco Colo Manager Issues

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

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

Action:

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

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

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

Troubleshoot Service Chain Issues

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

General Service Chain Issues

Service chain addition or deletion in to a service group fails

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

  Action:

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

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

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

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

     b. If more information is required to debug the failure, collect logs by using the **`admin-tech`** command on CSP hosting Cisco Colo Manager. Alternatively, you can get the logs from the device directly. See Log Collection from CSP, on page 110.

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



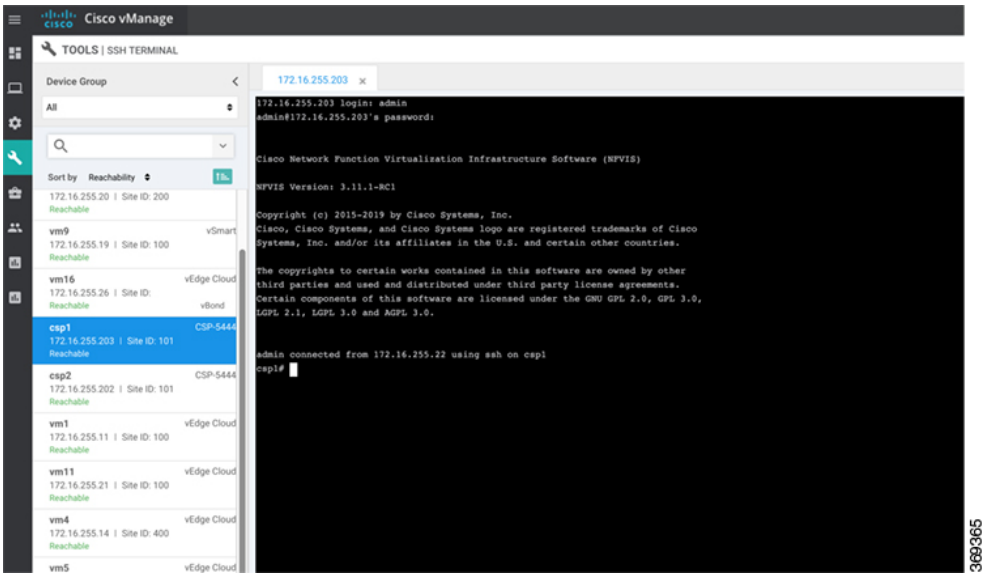
Note If service chain addition or deletion results in a failure on Cisco Colo Manager, there is an option to synchronize.

During service chain addition, VNF goes into error state

VNF is shown as down on vManage.

Action:

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



3. Run the following commands:

   nfvis# show system:system deployments

   nfvis# get the VNF ID

   For example,

   NAME ID STATE

   Firewall2_SG-3 40 running

   nfvis# support show config-drive content 40

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

Troubleshoot Physical Network Function Management Issues

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

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

Log Collection from CSP

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

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

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

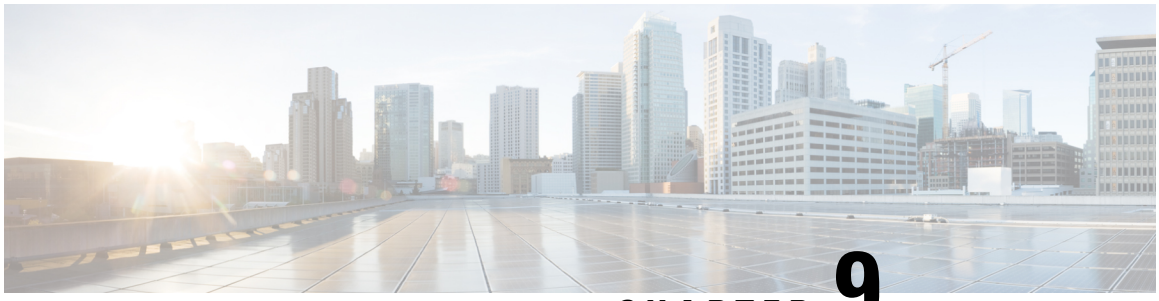
To secure copying a log file from the Cisco NFVIS to an external system or from an external system to Cisco NFVIS, the admin user can use the scp command in privileged EXEC mode. The following example shows the scp techsupport command:

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

Troubleshoot vManage Issues

Use the following location to troubleshoot vManage issues,

SD-WAN Techzone Knowledge Base



CHAPTER 9

Custom Packaging Details for Shared VNF

- vEdge Variable List, on page 113
- CSR Variable List, on page 117
- ASAv Variable List, on page 121

vEdge Variable List

In the following vEdge variable list, same variable names can be used for service chains five and six respectively with appropriate renumbering as mentioned for service chains.

vEdge Variable List

vEdge Is in StandAlone Mode and Neighbor Is in HA Mode
The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor (ASAv firewall) is in HA mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables wh Shared.**
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_PRIM	ORG_NAME	
INSIDE_DATA_MASK_LEN	BGP_NO	
INSIDE_PEER_DATA_IP_PRIM	SYSTEM_IP	
INSIDE_AS	MGMT_PRIM	
LOCAL_INSIDE_AS	MGMT_MASK_LEN	
INSIDE_GW	MGMT_GW	
SERVICE_VPN	RCC	
SERVICE_VPN_2	VM_INSTANCE_NAME	

User Variables	System Variables	
SERVICE_VPN_3	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_4	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_

vEdge Variable List

vEdge Is in StandAlone Mode and Neighbor Is in StandAlone Mode

The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables when Shared.**
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_PRIM	ORG_NAME	
INSIDE_DATA_MASK_LEN	BGP_NO	
INSIDE_PEER_DATA_IP_PRIM	SYSTEM_IP	
INSIDE_AS	MGMT_PRIM	
LOCAL_INSIDE_AS	MGMT_MASK_LEN	
INSIDE_GW	MGMT_GW	
SERVICE_VPN	RCC	
SERVICE_VPN_2	VM_INSTANCE_NAME	

User Variables	System Variables	
SERVICE_VPN_3	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_4	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MA
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DA
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MA
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DA
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

vEdge Variable List

vEdge Is in StandAlone Mode and Neighbor Is in StandAlone Mode

The input to the first VNF is in the trunk mode (VNF-tagged) and the neighbor is in StandAlone mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables wh Shared**
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_VLAN1	ORG_NAME	
INSIDE_PRIM_SUBNET1_IP	BGP_NO	
INSIDE_DATA_MASK_LEN1	SYSTEM_IP	
INSIDE_VLAN2	MGMT_PRIM	
INSIDE_PRIM_SUBNET2_IP	MGMT_MASK_LEN	
INSIDE_DATA_MASK_LEN2	MGMT_GW	
INSIDE_GW1	RCC	
INSIDE_GW2	VM_INSTANCE_NAME	
SERVICE_VPN	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_2	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MA

User Variables	System Variables	
SERVICE_VPN_3	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_
SERVICE_VPN_4	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

vEdge Variable List

vEdge Is in StandAlone Mode and Neighbor Is in HA Mode
The input to the first VNF is in the trunk mode (VNF-tagged) and the neighbor is in HA mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables when Shared.**
DNS_SERVER	OTP	
UUID	VBOND_IP	
INSIDE_VLAN1	ORG_NAME	
INSIDE_PRIM_SUBNET1_IP	BGP_NO	
INSIDE_DATA_MASK_LEN1	SYSTEM_IP	
INSIDE_VLAN2	MGMT_PRIM	
INSIDE_PRIM_SUBNET2_IP	MGMT_MASK_LEN	
INSIDE_DATA_MASK_LEN2	MGMT_GW	
INSIDE_GW1	RCC	
INSIDE_GW2	VM_INSTANCE_NAME	
SERVICE_VPN	OUTSIDE_PRIM	OUTSIDE_PRIM_3
SERVICE_VPN_2	OUTSIDE_DATA_MASK_LEN	OUTSIDE_DATA_MASK
SERVICE_VPN_3	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_
SERVICE_VPN_4	OUTSIDE_AS	OUTSIDE_AS_3

User Variables	System Variables	
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DA
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_LEN_2	OUTSIDE_DATA_MA
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DA
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DA

CSR Variable List

CSR Variable List

Last CSR VNF Is in HA Mode and Neighbor Is in StandAlone Mode
The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor (ASAv firewall) is in StandAlone mode.

User Variables	System Variables	
	Mandatory Variables	**Optional Variables**
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	MGMT_SEC	
PASS	INSIDE_VLAN_1	INSIDE_VLAN_3
OUTSIDE_PRIM	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_DATA_MASI

User Variables	System Variables	
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP
OUTSIDE_AS	INSIDE_AS	INSIDE_AS_3
LOCAL_OUTSIDE_AS	INSIDE_VLAN_2	INSIDE_VLAN_4
OUTSIDE_PEER_DATA_IP_SEC	INSIDE_PRIM_2	INSIDE_PRIM_4
OUTSIDE_SEC	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP
	INSIDE_AS_2	INSIDE_AS_4

CSR Variable List

Last CSR VNF Is in StandAlone Mode and Neighbor Is in StandAlone Mode

The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

User Variables	System Variables	
	Mandatory Variables	**Optional Variables**
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	INSIDE_VLAN_1	INSIDE_VLAN_3
PASS	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_PRIM	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3
OUTSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_AS	INSIDE_AS_3
OUTSIDE_AS	INSIDE_PEER_DATA_IP_SEC	INSIDE_PEER_DATA_IP
LOCAL_OUTSIDE_AS	VIP_IP_ADDRESS	VIP_IP_ADDRESS_3
	INSIDE_SEC	INSIDE_SEC_3

User Variables	System Variables	
	INSIDE_VLAN_2	INSIDE_VLAN_4
	INSIDE_PRIM_2	INSIDE_PRIM_4
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA
	INSIDE_AS_2	INSIDE_AS_4
	INSIDE_PEER_DATA_IP_SEC_2	INSIDE_PEER_DATA
	VIP_IP_ADDRESS_2	VIP_IP_ADDRESS_4
	INSIDE_SEC_2	INSIDE_SEC_4

CSR Variable List

Last CSR VNF Is in StandAlone Mode and Neighbor Is in HA Mode
The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor is in HA mode.

User Variables	System Variables	
	Mandatory Variables	**Optional Variables**
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	INSIDE_VLAN_1	INSIDE_VLAN_3
PASS	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_PRIM	INSIDE_DATA_MASK	INSIDE_DATA_MASK
OUTSIDE_DATA_MASK	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_AS	INSIDE_AS_3
OUTSIDE_AS	INSIDE_VLAN_2	INSIDE_VLAN_4
LOCAL_OUTSIDE_AS	INSIDE_PRIM_2	INSIDE_PRIM_4

User Variables	System Variables	
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA_IP
	INSIDE_AS_2	INSIDE_AS_4

CSR Variable List

Last CSR VNF Is in HA Mode and Neighbor Is in HA Mode
The output from the last VNF is in access mode (hypervisor-tagged) and the neighbor is in HA mode.

User Variables	System Variables	
	Mandatory Variables	**Optional Variables**
DOMAIN_NAME	VM_INSTANCE_NAME	
DNS_SERVER	TNAME	
NTP_SERVER	ORG_NAME	
TIMEZONE	BGP_NO	
OFFSET	SYSTEM_IP	
SUMMER_TIMEZONE	MGMT_PRIM	
TECH_PACKAGE	MGMT_MASK	
THROUGHPUT_IN_MB	MGMT_GW	
TOKEN_VALUE	MGMT_SEC	
PASS	INSIDE_VLAN_1	INSIDE_VLAN_3
OUTSIDE_PRIM	INSIDE_PRIM	INSIDE_PRIM_3
OUTSIDE_DATA_MASK	INSIDE_DATA_MASK	INSIDE_DATA_MASK_3
OUTSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP_PRIM	INSIDE_PEER_DATA_IP
OUTSIDE_AS	INSIDE_AS	INSIDE_AS_3
LOCAL_OUTSIDE_AS	INSIDE_PEER_DATA_IP_SEC	INSIDE_PEER_DATA_IP
OUTSIDE_PEER_DATA_IP_SEC	VIP_IP_ADDRESS	VIP_IP_ADDRESS_3
OUTSIDE_SEC	INSIDE_SEC	INSIDE_SEC_3
	INSIDE_VLAN_2	INSIDE_VLAN_4
	INSIDE_PRIM_2	INSIDE_PRIM_4
	INSIDE_DATA_MASK_2	INSIDE_DATA_MASK_4

User Variables	System Variables	
	INSIDE_PEER_DATA_IP_PRIM_2	INSIDE_PEER_DATA
	INSIDE_AS_2	INSIDE_AS_4
	INSIDE_PEER_DATA_IP_SEC_2	INSIDE_PEER_DATA
	VIP_IP_ADDRESS_2	VIP_IP_ADDRESS_4

ASAv Variable List

Note In the following ASAv variable list, same variable names can be used for service chains five and six respectively with appropriate renumbering as mentioned for service chains.

ASAv Variable List

First ASAv VNF Is in HA Mode and Neighbor Is in HA Mode
The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor (CSR) is in HA mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables wh Shared.**
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	HA_PRIM_IP	
INSIDE_PRIM	HA_SEC_IP	
INSIDE_SEC	HA_MASK	
INSIDE_DATA_MASK	MGMT_PRIM	
INSIDE_PEER_DATA_IP_PRIM	MGMT_MASK	

User Variables	System Variables	
INSIDE_PEER_DATA_IP_SEC	MGMT_GW	
INSIDE_AS	MGMT_SEC	
LOCAL_INSIDE_AS	OUTSIDE_PRIM	OUTSIDE_PRIM_3
	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_
	OUTSIDE_SEC	OUTSIDE_SEC_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_
	OUTSIDE_SEC_2	OUTSIDE_SEC_4

ASAv Variable List

First ASAv VNF Is in StandAlone Mode and Neighbor Is in StandAlone Mode

The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in StandAlone mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables when Shared.**
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	

User Variables	System Variables	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	MGMT_PRIM	
INSIDE_PRIM	MGMT_MASK	
INSIDE_DATA_MASK	MGMT_GW	
INSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_AS	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MA
LOCAL_INSIDE_AS	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DA
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MA
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DA
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4

ASAv Variable List

First ASAv VNF Is in StandAlone Mode and Neighbor Is in HA Mode
The input to the first VNF is in access mode (hypervisor-tagged) and the neighbor is in HA mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables wh Shared.**
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	
ID_TOKEN	VM_INSTANCE_NAME	

User Variables	System Variables	
PASS	TNAME	
TIMEZONE	MGMT_PRIM	
INSIDE_PRIM	MGMT_MASK	
INSIDE_DATA_MASK	MGMT_GW	
INSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_AS	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MASK
LOCAL_INSIDE_AS	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DATA_
	OUTSIDE_AS	OUTSIDE_AS_3
	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DATA_
	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MASK
	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DATA_
	OUTSIDE_AS_2	OUTSIDE_AS_4
	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DATA_

ASAv Variable List

First ASAv VNF Is in HA Mode and Neighbor Is in HA Mode

The input to the first VNF is in the trunk mode (vnf-tagged) and the neighbor is in HA mode.

User Variables	System Variables	
	Mandatory Variables when Service Chains 1 and 2 are Shared.	**Optional Variables when Shared.**
DNS_SERVER	OTP	
OFFSET	VBOND_IP	
SUMMER_TIMEZONE	ORG_NAME	
DOMAIN_NAME	BGP_NO	
NTP_SERVER_NAME	SYSTEM_IP	
LIC_LEVEL	RCC	

User Variables	System Variables	
ID_TOKEN	VM_INSTANCE_NAME	
PASS	TNAME	
TIMEZONE	HA_PRIM_IP	
INSIDE_PRIM_SUBNET1_IP	HA_SEC_IP	
INSIDE_PEER_DATA_IP_PRIM1	HA_MASK	
INSIDE_AS1	MGMT_PRIM	
LOCAL_INSIDE_AS1	MGMT_MASK	
INSIDE_VLAN1	MGMT_GW	
INSIDE_DATA_MASK_SUBNET1	MGMT_GW	
INSIDE_PRIM_SUBNET2_IP	OUTSIDE_PRIM	OUTSIDE_PRIM_3
INSIDE_PEER_DATA_IP_PRIM2	OUTSIDE_DATA_MASK	OUTSIDE_DATA_MA
INSIDE_AS2	OUTSIDE_PEER_DATA_IP_PRIM	OUTSIDE_PEER_DA
LOCAL_INSIDE_AS2	OUTSIDE_AS	OUTSIDE_AS_3
INSIDE_VLAN2	OUTSIDE_VLAN_1	OUTSIDE_VLAN_3
INSIDE_DATA_MASK_SUBNET2	OUTSIDE_PEER_DATA_IP_SEC	OUTSIDE_PEER_DA
INSIDE_PRIM_SUBNET3_IP	OUTSIDE_SEC	OUTSIDE_SEC_3
INSIDE_PEER_DATA_IP_PRIM3	OUTSIDE_PRIM_2	OUTSIDE_PRIM_4
INSIDE_AS3	OUTSIDE_DATA_MASK_2	OUTSIDE_DATA_MA
LOCAL_INSIDE_AS3	OUTSIDE_PEER_DATA_IP_PRIM_2	OUTSIDE_PEER_DA
INSIDE_VLAN3	OUTSIDE_AS_2	OUTSIDE_AS_4
INSIDE_DATA_MASK_SUBNET3	OUTSIDE_VLAN_2	OUTSIDE_VLAN_4
INSIDE_PRIM_SUBNET4_IP	OUTSIDE_PEER_DATA_IP_SEC_2	OUTSIDE_PEER_DA
INSIDE_PEER_DATA_IP_PRIM4	OUTSIDE_SEC_2	OUTSIDE_SEC_4
INSIDE_AS4		
LOCAL_INSIDE_AS4		
INSIDE_VLAN4		
INSIDE_DATA_MASK_SUBNET4		