CISCO SD-WAN Cloud Ramp Colocation Solution User Guide

CISCO SD-WAN Cloud Ramp Colocation Solution User Guide

Contents

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 Cisco 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.
    - Complete wiring the CSPdevices (set up CIMC for initial CSPaccess) and Cisco Catalyst 9500-40X or

Cisco Catalyst 9500-48Y4C switches (set up console server) along with OOB or management switches. Power on all devices.

    - Set up and configure DHCP server. See Provision DHCP Server Per Colocation, on page 12 .

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 2 .
3. Set up or provision a cluster. A cluster constitutes of all the physical devices including CSP devices, and Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Get Started with Cisco SD-WAN Cloud onRamp for Colocation Solution, on page 1.
    - Bring up CSP devices. See Onboard CSP Devices Using Plug-and-Play Process , on page 5.
    - Bring up Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Bring up Switch Devices, on page 9.
    - Provision and configure a cluster. See Provision and Configure Cluster. Configure a cluster through cluster settings. See Cluster Configuration
4. Activate a cluster. See Create and Activate Clusters.
5. Design service group or service chain. See Manage Service Groups

   Note

   You can design a service chain and create a service group anytime before creating clusters or activating clusters after all VMs are uploaded to the repository.
6. Attach or Detach service group and service chains to a cluster. See Attach or Detach a Service Group in a Cluster.

   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 or Detach a Service Group in a Cluster.
    - Add and delete CSP devices from a cluster. See Add Cloud OnRamp Colocation Devices Using Cisco vManage and Delete Cloud OnRamp for Colocation Devices from Cisco vManage.
    - Deactivate a cluster. See Remove Cluster from Cisco vManage.
    - Reactivate a cluster. See Reactivate Cluster from Cisco vManage.
    - Design more service group or service chain. See Create Service Chain in a Service Group

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 Co location 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.

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 adminasthe username andpasswordasthe 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 NFVISfrom 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. 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.

Note

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.

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.
A JNLP file will be downloaded to your system. You must open the file immediately after it is downloaded to avoid the session timeout.
Note
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 On Ramp for Co location Image

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 Cisco Cloud Services Platform Devices

Table 1: Feature History

Feature Name	Release Information	Description
Onboarding CSP Device withDay-0 Configuration Using USBDrive	Cisco SD-WAN Release 20.4.1	This feature enables you to onboard CSP devices by loading the Day-0 configuration file to a USB drive. Use this onboarding option when you can't access the Internet to reach the Plug-and-Play Connect server.

To bring up the Cisco Cloud Services Platform (CSP) devices, you can use the following options:

- **Automated deployment:** Securely onboards and deploys CSPdevices with factory settings into the Cisco SD-WAN network during the Day-0 configuration. The deployment dynamically discoversthe IPaddress of Cisco vBond Orchestrator using the Plug-and-Play (PnP) process for Cisco CSP devices.
- **Bootstrap deployment:** Requires you to share the configuration files with the CSPdevices. You can either create a configuration file and copy it to a bootable USB, or add the configuration file to the USB. The bootable USB is connected and available on the devices at the time of bootup.

Onboard CSP Devices Using Plug-and-Play Process

This topic describes how the bringing up of Cisco CSP devices are automated using the PnP proces

Before you begin

- Ensure that you connect the CSP devices as per the prescribed topology, and power them on.
- Connect the Plug-and-Play (PnP) supported interface to the WAN transport (typically Internet).

Power on a Cisco CSP device. The following process occurs:

Step 1 When the device boots up, it obtains the IP address, default gateway, and DNS information through the DHCP process on the supported PnP interface of the device.
Step 2 The device connects with the Cisco cloud hosted PnP Connect server and shares its chassis or serial number with the PnP server to be authenticated by it.
Step 3 After authentication, the PnP Connect portal provides the device with information about the Cisco vBond Orchestra-tor, organization name, and root certificates.
For deployments that use enterprise root-ca certificate, information about Cisco vBond Orchestrat or IP address or DNS, organization-name, and enterprise root-ca certificate are downloaded on the device from the PnP Connect portal using the HTTPS protocol. The device uses this information to initiate control connections with the Cisco vBond Orchestra tor.
You can view the availability of the device and association with the Cisco vBond Orchestra tor on the PnP interface through the PnP Connect portal.
Step 4 The PnP Connect portal then displays a Redirect Successful status when the device is redirected through PnP to the Cisco vBond Orchestrator.
Step 5 After authentication with the Cisco vBond Orchestrator, the device is provided with Cisco vManage and Cisco vSmart Controller information to register and establish a secure connection.
Step 6 The device attempts to establish a secure control connection with the Cisco vManage server.
Step 7 After authentication with the Cisco vBond Orchestrator, the Cisco vManage server respondsto the device with the system
IP of the device and reauthenticates the device using the shared system-ip information.
Step 8 To join the Cisco SD-WAN overlay network, the device reinitiates control connections to all the SD-WAN controllers using the configured system-ip IP address.

Onboard CSP Devices Using USB Bootstrapping Process

If you’re unable to use the automated discovery option, use this deployment option to configure the factory-shipped device, which comes without any configuration.

We recommend this deployment option when:

- The device is connected to a private WAN transport (MPLS) that can’t provide a dynamic IP address.
- Internet access isn’t available to reach the Plug-and-Play Connect server.

Points to Consider

- The USB drive can have multiple Day-0 configuration files, which are identified by the serial number of the device in the file name. This naming convention enables you to use the same USB drive for bootstrapping multiple devices.
  - The supported Day-0 configurations included in the configuration file are:
  - Static IP configuration of the device
  - Cisco vBond Orchestrator IP address and the port configuration
  - DNS server and domain name configuration
- The bootstrap configuration can be uploaded to a USB key and inserted into a device at the install sit

Before you begin

- The device must be in factory default state with no added configuration.
- The device must be installed with a fresh image of Cisco NFVIS.
- The USB drive must be Virtual File Allocation Table (VFAT) formatted to recognize and automount the drive. Insert the USB drive into a laptop or desktop to format it.
- The device should be able to reach the Cisco vBond Orchestrator.

Step 1 Create a configuration file on the root folder of the USB drive. Ensure that the configuration file name is, nfvis_config_SERIAL.xml, where SERIAL represents the serial number of the CSP device. For example, nfvis_config_ WZP232903K6.xml

Step 2 Copy the following to the configuration file.

Note

It's mandatory to copy the above-mentioned static IP configuration of the device to the configuration file. The static IP configuration of the device is represented by the following Day-0 configurations:

Step 3 *Insert the USB drive into the Cisco CSP device and power on the device.*

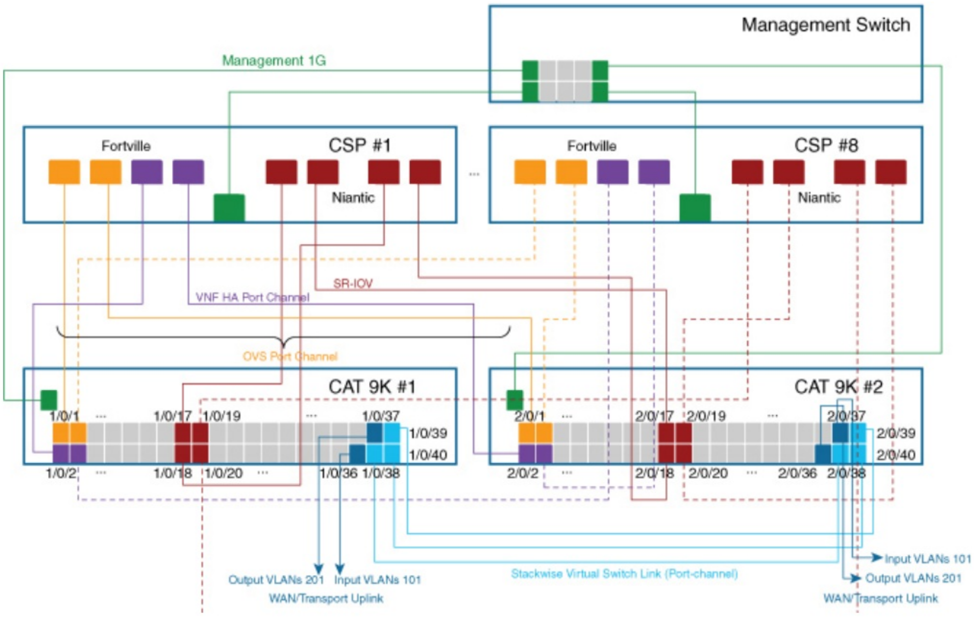
When the device boots up, the device searches for the configuration file in the bootable USB drive. After the file is located, the device suspends the PnP process and loads the bootstrap configuration file.

Step 4 Remove the USB drive.
If you don't unmount the USB drive and reboot the device after the configuration has been applied, the USB drive configuration isn't reapplied. The CSP device isn't in Factory Data Reset (FDR) state or restored to its original system state.

Step 5 *To access a CSP device, SSH to a static IP address provided in Step 2 such as, 192.168.30.6.*
Step 6 *Change the default password at the first login when the system prompts you to change.*
Ensure that you set a strong password based on the on-screen instructions. You can't run API commands or proceed with any tasks unless you change the default password at the first login.

Device Port Connectivity Details and Service Chaining for Prescriptive Connection

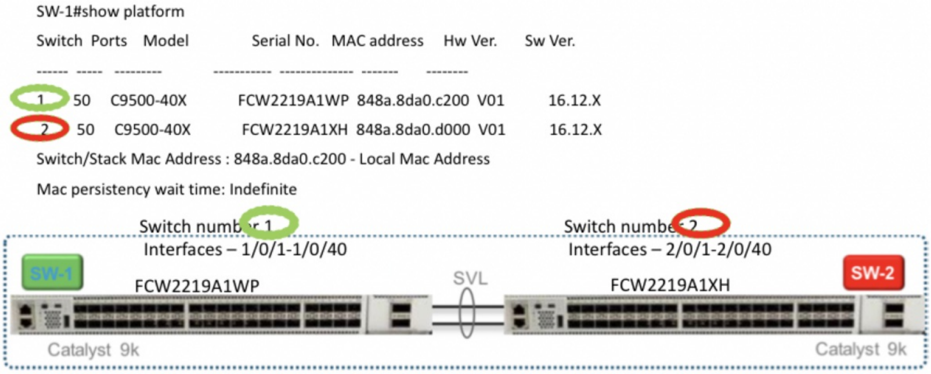
In CiscoSD-WAN Cloud onRamp for Colocation solution deployments, the Cisco Catalyst 9500-40X switches connected to CSP systems perform service chaining. If VMs support SR-IOV, Cisco Catalyst 9500-40X switches perform service chaining, whereas VMs without SR-IOV support, service chaining is done by Open Virtual Switch (OVS). Virtual switch-based service chains are used for High Availability traffic and control traffic. VLAN-based L2 service chaining from Cisco Catalyst 9500-40X switch 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 solution deployments, the deja-vu check is disabled on the switch ports that are connected to the CSP devices for unicast traffic.
The following topology displays connectivity of the CSP ports to Cisco Catalyst 9500-40X switches and the OOB switch.
Figure 1: 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.



```
SW-1#show platform

Switch  Ports   Model          Serial No.   MAC address    Hw Ver.    Sw Ver.

------  -----   ---------      -----------  -------------- -------    --------

 1      50      C9500-40X      FCW2219A1WP  848a.8da0.c200  V01       16.12.X
 2      50      C9500-40X      FCW2219A1XH  848a.8da0.d000  V01       16.12.X
Switch/Stack Mac Address : 848a.8da0.c200 - Local Mac Address

Mac persistency wait time: Indefinite
```

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).

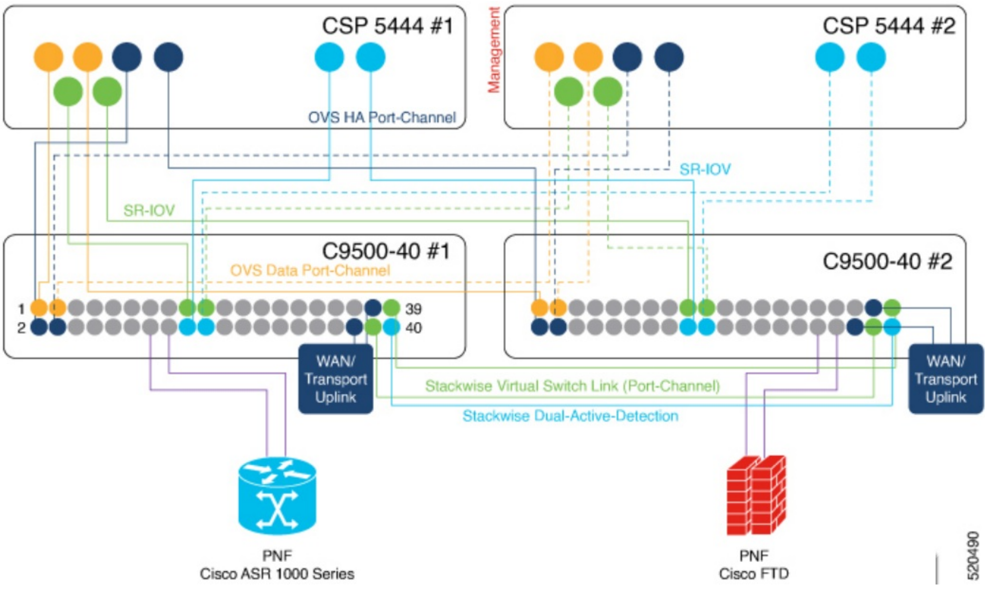
- 1/0/37, 2/0/37—Connect port 1/0/37 to forward service chain traffic to specific VLANs that is mapped to provider networks on an OOB switch.

You can connect the ports as follows:

- **Data ports—**Connect ports 1/0/1-1/0/35 to CSPdevices. To achieve redundancy and HA acrossswitches, 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 networksterminate 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.

The following cabling image shows how the physical network functions are connected to the Cisco Catalyst 9500-40X switches.

Figure 2: PNF Cabling Image



The following table provides the ports available for PNF:

Table 2: Ports on Cisco Catalyst 9500-40X Switches for PNF

Number of CSP Devices	Number of PNFs	Switch Ports available for PNFs on First Switch	Switch Ports available for PNFs on Second Switch
7	1	1/0/15-1/0/16,	2/0/15-2/0/16,
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
4	4	1/0/11-1/0/16,	2/0/11-2/0/16,

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 aPNFdevice 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 Cisco vManage.
   b. Disconnect the CSP physical connections on Cisco Catalyst 9500-40X switches.
   c. Connect the PNF device in place of the disconnected CSP.
2. **If one of the firstseven CSPdevices must be removed to make additional ports available forPNF, 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 the intial 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.

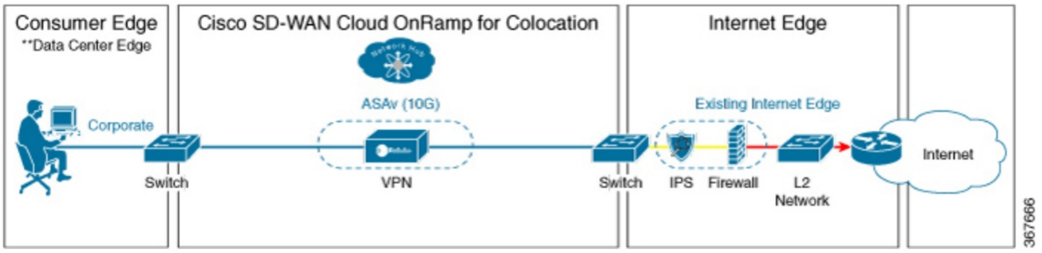
Cisco vManage manages the Cisco SD-WAN Cloud onRamp for Colocation solution service chain configuration. Cisco vManage assigns the VLANs from the VLAN pool that is provided for the colocation to the individual VM VNICs and configures the switch with appropriate VLANs. The VNFs can remain unaware about the service chain. Apart from the Day-0 VNFconfiguration, Cisco vManage does not configure the individual VNFs that are part of the service chain. .

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 Cisco vManage. For all the validated service chains, each VM can be instantiated in HA or standalone modes.

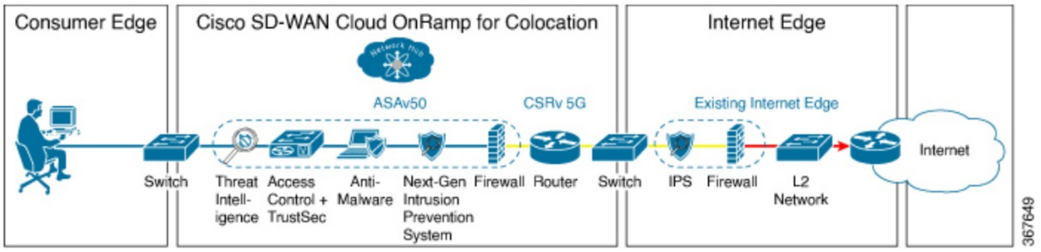
- Employee Remote VPN Access—In this service chain, there is a firewall, which can be in L3 VPN HA or L3 VPN non-HA modes. The firewall VNFs can be ASAv, Palo Alto Networks Firewall, Firepower_Threat_Defense_Virtual (FTDv). Here, ASAv is in routed mode, no Day-0 configuration support for the VPN connect,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

Figure 3: Employee Remote VPN Access Service Chain



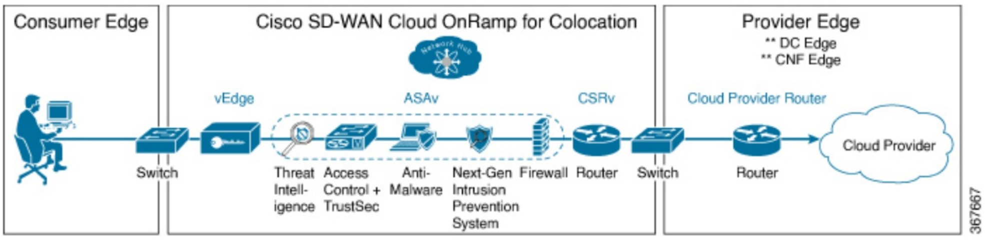
- Internet Edge (Outbound Internet, eCommerce, SaaS)—In this service chain, a firewall is followed with a router. The firewall modes can be L3-VLAN HA and L3-VLAN non-HA. The routers can be in L3 HA and L3 non-HA modes. Here, ASAv is always in routed mode. One VLAN handoff is required and inbound subinterfaces 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 4: Internet Edge Service Chain



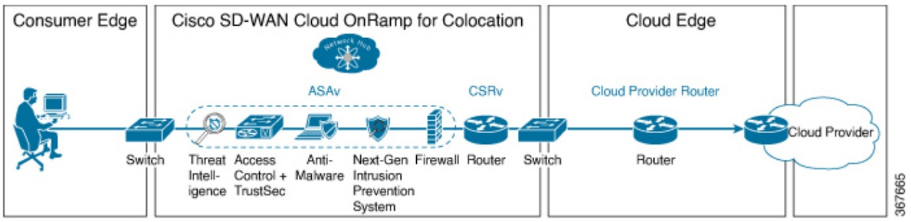
- **SD-WAN Access**—In this service chain, vEdge is followed by a firewall, which is followed by a router. The firewall modes can be L2 HA, L2 non-HA, L3 HA and L3 non-HA. The routers can be in L3 HA and L3 non-HA modes.

Figure 5: 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. This service chain is Internet Edge (Outbound Internet, eCommerce, SaaS) with firewall mode being L3.

Figure 6: Cloud Edge (Public Cloud Access) Service Chain



See **Create Service Chain in a Service Group** topic about how you can choose the validated service chains through Cisco 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, Cisco vManage can automate the IP addresses and VLANsfor those segments. If VM isterminating to a branch or provider, user must configure the IPaddresses, peer addresses, autonomous system numbers, and others.

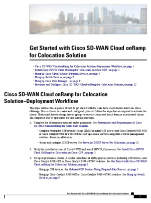
Customized Service Chains

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 .

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.

Documents / Resources



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

- Cisco SD-WAN Cloud onRamp for Colocation Solution–Deployment Workflow, on page 1
- Install Cisco NFVIS Cloud OnRamp for Colocation on Cisco CSP , on page 2
- Bring up Cisco Cloud Services Platform Devices, on page 5
- Bring up Switch Devices, on page 9
- Bring up Cisco Colo Manager , on page 11
- Provision and Configure Cisco SD-WAN Cloud onRamp for Colocation Solution, on page 12

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 Cisco 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.
   - Complete wiring the CSP devices (set up CIMC for initial CSP access) and Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches (set up console server) along with OOB or management switches. Power on all devices.
   - Set up and configure DHCP server. See Provision DHCP Server For Colocation, on page 12 .
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 2 .
3. Set up or provision a cluster. A cluster constitutes of all the physical devices including CSP devices, and Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Get Started with Cisco SD-WAN Cloud onRamp for Colocation Solution, on page 1 .
   - Bring up CSP devices. See Onboard CSP Devices Using Plug-and-Play Process , on page 5.
   - Bring up Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. See Bring up Switch Devices, on page 9.

Get Started with Cisco SD-WAN Cloud onRamp for Colocation Solution 1

CISCO SD-WAN Cloud Ramp Colocation Solution [pdf] User Guide
SD-WAN Cloud Ramp Colocation Solution, SD-WAN, Cloud Ramp Colocation Solution, Ramp Colocation Solution, Colocation Solution, Solution

References

- Configure or Change CIMC IP address on UCS C200 series servers - Cisco Community
- Cisco Catalyst SD-WAN Command Reference - Operational Commands [Cisco SD-WAN] - Cisco
- Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide - Cisco
- Cisco CIMC Firmware Update Utility User Guide - Using the CIMC Firmware Update Utility [Cisco UCS C-Series Rack Servers] - Cisco
- User Manual