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

First Published: 2018-12-20

Last Modified: 2019-08-15

Cisco SD-WAN Cloud OnRamp for Colocation Solution

Find all the information you need about this release—new features, known behavior, resolved and open bugs, and related information.

Note Explore Content Hub, the all new portal that offers an enhanced product documentation experience. Content Hub offers the following features to personalize your content experience.

- Faceted Search to help you find content that is most relevant

- Customized PDFs

- Contextual Recommendations

About Cisco SD-WAN Cloud OnRamp for Colocation Solution

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 an enterprise's endpoints such as, employees, devices, customers, or partners. This functionality is achieved by using Cloud Services Platform 5000 series(CSP 5444) as the base Network Function Virtualization (NFV) platform that securely connects enterprise's endpoints 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 components of Cisco SD-WAN Cloud OnRamp for Colocation solution are :

- **Cisco Cloud Services Platform (CSP) 5444**—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.The whole solution can scale horizontally. You can have up to eight CSP devices. Depending on the load requirement, you can have anywhere from two to eight compute platforms in a cluster.

- **Cisco Network Function Virtualization Infrastructure Software (NFVIS)**—The Cisco NFVIS software is used as the base virtualization infrastructure software running on the x86 compute platform.

- **Virtual Network Functions (VNFs)**—The Cisco SD-WAN Cloud OnRamp for Colocationb solution supports both Cisco-developed and third-party virtual network functions.

- **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 router, firewall.

- **Network Fabric**—Forwards traffic between the VNFs in a service chain by using a L2 and VLAN-based lookup.

- **Mangament Network**—A separate management network connects the NFVIS software running on the CSP systems, the virtual network functions, and the switches in the fabric. This management network is also used for transferring files and images into and out of the systems. The Out of Band (OOB) management switch configures the management network.

- **VNF 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.

- **Physical Network Function Network Connectivity**—A PNF can be connected to the Catlyst 9500 switches port, which are kept free towards backend.

- **Service Chains**—In Cisco SD-WAN Cloud OnRamp for Colocation solution deployment, the traffic between the VNFs (with SR-IOV) running on the CSP 5444 systems is service chained externally through Catalyst 9500.

- **Cisco Colo Manager (CCM)**—This component is a software stack that manages a colocation. In this solution, CCM is hosted on NFVIS software in a docker container. A single CCM instance per cluster is brought up in one of the CSPs after activating a cluster.

- **Orchestration through vManage**—The Cisco vManage is used for orchestrating the Cisco SD-WAN Cloud OnRamp for Colocation solution.

Essentially, you can purchase the devices, add them in colocation centers, power them, cable them and devices automatically boot up, bootstrap themselves and get managed by vManage. You can go ahead with designing service chains, building security policies and application policies, thereby influencing the network traffic.

Software Requirements Matrix

Software Matrix

The following are the NFVIS, vManage, vBond, vSmart, vEdge, Catalyst 9500 versions.

Software	Version
vManage	19.2
NFVIS	3.12.1
vBond	19.2
vSmart	19.2
vEdge	19.2
Catalyst 9500	IOS-XE16.12.1

Note For Cisco SD-WAN Cloud OnRamp for Colocation solution deployment, ensure that you use the vEdge version, 19.1 or later. The vManage version can be greater than or equal to the vBond version, and the vBond version can be greater than or equal to the vSmart version.

New Features

- Supported VNFs: The following are the supported Cisco and third-party VNFs for this release.

  Note You must procure license for the required VNFs. Optionally, you can choose to bring in your own Day-0 configuration and repackage the VNFs, if required.

Table 1: Validated Cisco VNFs

VNF	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, 6.3.0, 6.4.0.1
Cisco vEdge Cloud	18.4, 19.1, 19.2
Cisco IOS XE SD-WAN	16.12.1

Table 2: Validated Third-party VNFs

VNF	Version
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

- Supported PNFs: The following are the supported Cisco PNFs for this release.

Table 3: Validated Cisco PNFs

PNF	Version
Cisco FTD	6.4.0.1
Cisco ASR 1000 Series	16.12.1

- Physical Network Function Management: A service chain can now have a mix of Virtual Network function (VNF) and Physical Network Function (PNF) devices. You can add PNF devices to service chains and

share them across service chains, service groups, and across a single cluster. The PNF devices can overcome the performance and scaling issues caused by using only VNF devices in a service chain.

Note Due to higher cost and maintenance of PNF devices, it is recommended to have a single PNF device that is shared across multiple service chains.

- Custom Service Chain with Shared VNF: You now have the flexibility to share Virtual Network Function (VNF) devices across service chains to improve the resource utilisation and reduce resource fragmentation.

- Service chain health monitoring: The service chain health is now monitored by running periodic checks on the service chain data path and reporting the overall status.
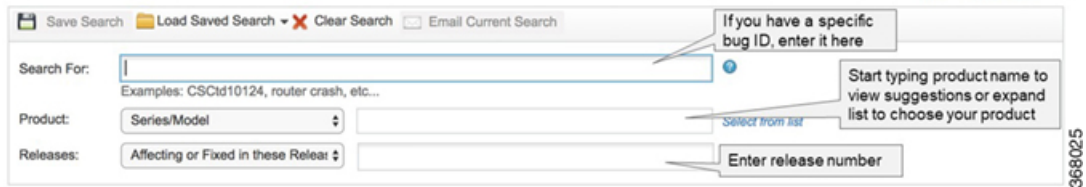
Note For service chain health monitoring to be enabled on all CSP devices in a cluster, ensure that you install the NFVIS version 3.12.1 or later.
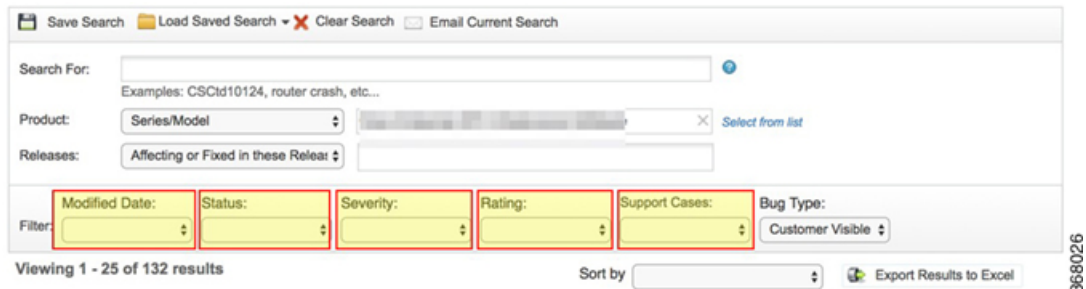
Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Open vManage Bugs

All open vManage bugs for this release are available in the Cisco Bug Search Tool through the Open Bug Search.

Bug ID	Description
CSCvp26351	Monitoring and service chain Health graphs show old data of the VNF
CSCvp94264	Template push fails to devices after vManage upgrade–Failed to publish the task on message bus.
CSCvq67077	vManage assigns same BGP number to ASR and FTD PNF.
CSCvq70732	VLAN allocation failed, even after detaching all the service groups due a leak.
CSCvq75400	Any error with service group attach or detach is not displayed on the GUI.
CSCvn25349	The detach cluster option is updated to Attach cluster option even though you do not click on "Configure".
CSCvp58736	The CSP devices and switches should be excluded from vSmart functionality dependencies.
CSCvq01420	The CSP unreachable but VNF devices are shown as active on the Service page.
CSCvq30141	The edit and update of description does not get saved.
CSCvq36133	vManage Service chain health monitoring–No details found for undetermined status in the GUI.
CSCvq45972	CSP name is different from system ip in the **Monitor** > **Network** > **Colocation Clusters**.
CSCvq50405	The monitor page should show PNF type as PNF instead of VNF.
CSCvq56847	Edit of a HA service group to StandAlone service group throws an error and deletes all service chain.
CSCvq58527	The OUTSIDE AS is not assigned for L2 chains when the first and last VNF is shared.
CSCvq68729	The device opitons are not working in **Monitor** > **Network** > **Colocation Cluster**.
CSCvq68814	In Detach/Attach SG, the CCM displays, "Device needs to install some apps"
CSCvq69020	While attaching service group, CCM task failed with 'Authentication failed', error.
CSCvq70928	Attaching a servie group from the cluster page does not throw error if packaging is wrong
CSCvq74676	The cEdge serial numbers are not shown when cEdge package is used for VNF.
CSCvq77416	The shared vEdge does NOT substitute neighbor IP with L2 FW in between
CSCvq77500	When using shared vEdge multiple VNFs incorrectly, it shows as DOWN
CSCvq77501	SC Monitoring payload is incorrect with FTDvL2 in vEdge(shared), ftdvL2, csr(nonshared)
CSCvo19765	The custom service chain should have the ability to remove the VNF while editing.

Bug ID	Description
CSCvp07407	PAFW UUID is missing in Day-0.
CSCvq04126	The packaging tool does not allow bootup_time -1 prompt.
CSCvq86158	After deleting a service chain from service group and saving causes java NullPointerException.
CSCvq86546	Attachment of a service group with cluster fails due to discontiguous VLANs.

Open Device Bugs

All open device bugs for this release are available in the Cisco Bug Search Tool through the Open Bug Search.

Bug ID	Description
CSCvo66687	Attaching or detaching of service groups fails due to configuration database being locked by session.
CSCvq23082	vdaemon is not fine due to nfvis-confd failure after factory default reset.
CSCvq28505	Drop rate is high when traffic is distributed across 10 VMs.
CSCvq32744	Traffic drop is high when one of the VNF is cross pinned.
CSCvq32759	The drop rate is at 1% with 7G traffic–3.5G each direction
CSCvq50747	CCM application times out and then the on sync database is locked by econfd.
CSCvq80322	Error while attaching device to DPDK on an OVS bridge
CSCvo83560	vManage reports failure for the outstanding changes in database
CSCvp35946	vEdge fails to come up with Day-0 configuration and interface comes up as DHCP–seen intermittently.
CSCvq61948	Application times out when using the **factory default reset all** command.
CSCvq78654	The CLI error, "Clear installed-certificates" is displayed for Cisco NFVIS software.
CSCvq35040	During vdaemon commits, "the configuration database is locked by session <id> system tcp git/vdaemon/vdaemon_misc.c is displayed.

Related Documentation

- Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software

- Release Notes for Cisco SD-WAN Product Documentation

- Solution User Guides for Cisco SD-WAN Cloud OnRamp for Colocation

- Hardware Guides for Cisco Catalyst 9500 Series Switches

- Hardware Guide for Cisco Cloud Services Platform 5000

- Configuration Guides for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Configuration Guides for Cisco Catalyst 9500 Switches
- Configuration Guides for Cisco Network Plug and Play Application
- Command Reference Guides for Cisco Enterprise Network Function Virtualization Infrastructure Software