Release Notes for Cisco SD-WAN Cloud OnRamp for Colocation Solution, Release 20.1.1

First Published: 2018-12-20

Last Modified: 2020-05-04

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 CoLocation 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.

- **Mangement 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 Catalyst 9500-40X switches port, which is 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**— 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. Then, 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 Cisco Enterprise NFV Infrastructure Software, Cisco vManage, Cisco vBond Orchestrator, Cisco vSmart Controller, Cisco vEdge Device, Catalyst 9500-40X versions.

Software	Version
Cisco vManage	Cisco SD-WAN Release 20.1.1.1
Cisco vBond Orchestrator	Cisco SD-WAN Release 20.1.1
Cisco vSmart Controller	Cisco SD-WAN Release 20.1.1
Cisco vEdge Device	Cisco SD-WAN Release 20.1.1
Cisco Enterprise NFV Infrastructure Software (NFVIS)	Release 4.1.1

Software	Version
Catalyst 9500-40X	IOS-XE 16.12.1

All release-specific information for Cisco vSmart Controllers, Cisco vBond Orchestrators, Cisco vManage is included in Cisco SD-WAN Release Notes.

New Features

- Supported VNFs and PNFs on Cisco SD-WAN Cloud onRamp for CoLocation Solution: This release supports the updated versions of the following VNFs and PNFs on Cisco SD-WAN Cloud onRamp for CoLocation solution.

> **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	17.1
Cisco CSR SD-WAN	16.12.1, 16.12.2r
Cisco ASAv	9.12.2, 9.13.1
CheckPoint	R80.30
Cisco FTDv/NGFW	6.4.0.1, 6.5.0-115
Cisco vEdge Cloud router	19.2, 20.1

Table 2: Validated Third-party VNFs

VNF	Version
Palo Alto Firewall (PAFW)	9.0
Fortinet Firewall	6.0.2

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

Table 3: Validated Cisco PNFs

PNF	Version
Cisco FTD Model: FPR-9300	6.4.0.1, 6.5
Cisco ASR 1000 Series	16.12.1, 17.1

- **Monitor Cluster Activation Progress**: This feature allows you to monitor the progress of activating a cluster at each step and view any failures that may occur during the process. The process of activating a cluster approximately takes 30 minutes or longer, and you can monitor the progress using the vManage task view window and events from Monitoring page.

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

- **VNF States and Color Codes**: This feature allows you to determine the state of a deployed VM using color codes, which you can view on the **Monitor** > **Network** page.

- **Network Utilization Charts for SR-IOV Enabled NICs and OVS Switch**: This feature allows you to view network utilization charts of VM VNICs connected to both SR-IOV enabled NICs and OVS switch.

Important Notes

- Deactivate cluster workflow is not supported: The workflow to deactivate a cluster and then subsequently activate the cluster is not supported through vManage. Therefore, it is recommended to delete and recreate the cluster, instead.

- Fortinet Firewall L2 in HA mode is not supported: A service chain deployed with Fortinet VNF in L2 HA mode is not supported in Cisco SD-WAN Cloud onRamp for CoLocation solution.
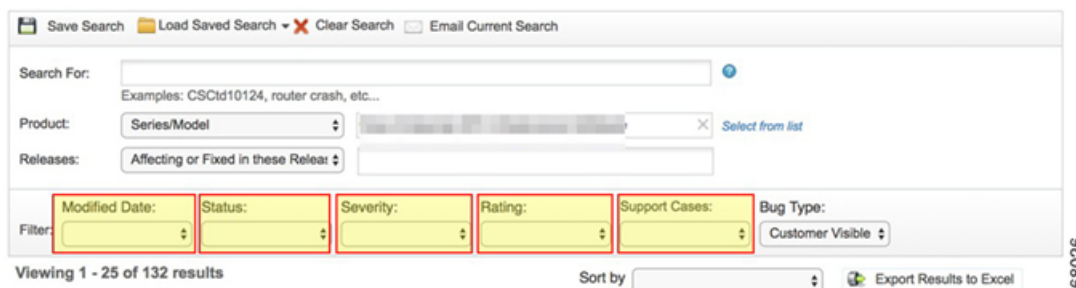
Open Bugs

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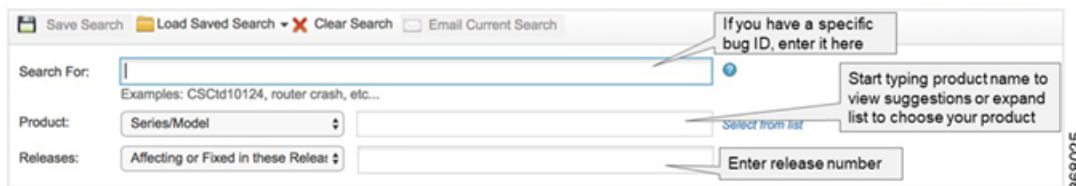
You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Open Cisco vManage Bugs

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

Bug ID	Description
CSCvt13638	vManage template attach to CSP results in application error in CSP RMA use case if CSP is hosting CCM.
CSCvt92077	Ping fails seen intermittently on Cisco ASAv inbound/outbound interfaces when Catalyst 9500-40X is rebooted.
CSCvt92184	Cisco vEdge device ping failures seen intermittently when Catalyst 9500-40X is rebooted.
CSCvn25349	When trying to detach a service chain from cluster, if all steps are not completed by clicking complete and instead you go back to the browser, the detach option changes to attach option.
CSCvq30141	Editing and updating the description field of service group does not get saved.
CSCvq56847	Modifying a High Availability (HA) enabled service group to Non-HA service group returns an error and deletes all service chains in that Service Group.
CSCvp07407	PAFW Day-0 configuration should have unique UUID and if it is changed to a variable, vManage cannot generate value for that UUID causing template attach of service chain to fail.
CSCvq58527	A service group containing shared service chain with first and last NF shared, if the middle VNFs have a combination of firewalls in transparent and routed mode, it causes template attach failure.
CSCvr59253	A non-shared service chain cannot connect to multiple providers terminating different VLANs.
CSCvr59276	Attaching a shared service chain with only one VNF in the chain causes failure.
CSCvt11875	Service chain does not get attached if service chain QoS bandwidth is greater than 5GBPS.
CSCvu02373	The deactivation and reactivation of a cluster after a failed cluster activation results in CCM task failure error.
CSCvt22455	When a service chain template is attached, the "Unable to close a netconf session" error message is seen intermittently.

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.

Bug ID	Description
CSCvt13619	Qos related classmap and policymap configuration on Catalyst 9500-40X switch remain after deleting a CSP with CCM from a 3-Node cluster.
CSCvo83560	The attaching or detaching service chain causes failure some times and vManage shows the error–Outstanding changes in database on CSP
CSCvs29599	The CSP device might show on CSP console: "ipmi_si IPI0001:00: IPMI message handler: BMC returned incorrect response".
CSCvt14589	The CSP device might show on CSP console: "segfault at 0 ip 00007fe3dd640901 error 4 in libc-2.17.so"
CSCvt96036	Fortinet VM in transparent mode with High availability instances not able to peer with each other leads to high network traffic on host management.
CSCvr81085	Service chain bandwidth policing (QoS) does not work if same VLANs are terminated on different service chains. Does not work for shared service chains also.
CSCvt55532	VLANs did not get saved to the Catalyst 9500-40X switch on service chain attach–RPC error seen on CCM
CSCvu04242	vManage monitor network colocation cluster device interface statistics are zero for some physical ports
CSCvt99475	VM monitoring state toggles between 'Deploying' and 'Alive' temporarily
CSCvt99640	Cluster activation failure due to management interface administratively down on Catalyst 9500-40X switch
CSCvu08553	VM in INERT state prior to upgrade results in all VMs marked SHUTDOWN after upgrade

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