Cisco Cloud Services Platform Release Notes, Release 2.3.2

First Published: 2019-04-17

Last Modified: 2019-04-17

Cisco Cloud Services Platform Release Notes

This document describes the features and limitations for the Cisco Cloud Services Platforms 2100 and 5000, Release 2.3.2.

Information About Cisco Cloud Services Platform

Cisco Cloud Services Platform is a software and hardware platform for data center network functions virtualization. This open kernel virtual machine (KVM) platform, with Red Hat Enterprise Linux (RHEL) 7.3 as the base operating system, is designed to host networking virtual services. Cisco CSP provides REST APIs, a web interface, and a CLI for creating and managing the virtual machine (VM) lifecycle.

Supported Cisco Networking Services

Cisco CSP can host any Cisco or third-party VNF that is supported on KVM hypervisor. Some of the Cisco VNFs available include the following:

- Cisco Cloud Services Router (CSR) 1000V virtual router
- Cisco IOS® XRv 9000 Router
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower™ NGFW Virtual
- Cisco Prime® Virtual Network Analysis Module (vNAM)
- Cisco Virtual Wide Area Application Services (vWAAS)
- Cisco Web Security Virtual Appliance (WSAv)
- Cisco Virtual Security Gateway (VSG) for Cisco Nexus® 1000V Series Switch deployments
- Cisco Virtual Supervisor Module (VSM) for Cisco Nexus 1000V Series Switch deployments
- Cisco Data Center Network Manager (DCNM)

Resolved Bugs

This is a patch release. It includes the entire 2.3.1 content and the fixes for the following two bugs.

Bug Id	Description
CSCvp18597	CSP install fails on CSP 5000
CSCvp33800	CSP 2100 or CSP 5000 Intel niantic family, 2x10G NIC VF link stays down after a PF link reset.

For more information, see Cloud Services Platform 2.3.1 product documentaion.

Configuration Limits

Use the following configuration limits for Cisco CSP.

Component	Supported Limits
Number of services in a node with hyperthreading disabled	• For Cisco CSP with 8 or less than 8 cores, you can deploy the following number of VM cores: *Number of Cores* – 1 For example, for Cisco CSP with 8 cores, you can deploy 7 VM cores. • For Cisco CSP with greater than 8 and less than or equal to 16 cores, you can deploy the following number of VM cores: *Number of Cores* – 2 For example, for Cisco CSP with 16 cores, you can deploy 14 VM cores. • For Cisco CSP with greater than 16 cores, you can deploy the following number of VM cores: *Number of Cores* – 4 For example, for Cisco CSP with 36 cores, you can deploy 32 VM cores.
Total number of nodes in a cluster	10
Number of vNICs per service	24

Important Notes and Restrictions

Following are the important notes and restrictions for Cisco CSP.

Hyper-Threading Technology Support

Cisco CSP hardware supports Hyper-Threading (HTT). However by default, HTT is disabled and must be kept disabled, as it is not supported. This action avoids VNFs sharing same CPU cores, cache and memory bus that can result in stalls or latency issues, and VNF data plane performance degradation. The enablement or disablement of Hyper-Threading is done by CIMC on CSP 5000 hardware.

Changing IP Address of the Management Interface for NFS Configurations

If NFS is configured on the system, note the following:

- Changing the management IP address causes an outage of the VNC console and stats collection for 15 to 30 minutes.
- Reboot of the system can take up to 30 minutes.

As a workaround, you can unconfigure the NFS mount before performing these operations and reconfigure the NFS mount after the operation is complete. You can also reboot the system from the Cisco CSP CIMC connection.

Configuring Passthrough Interfaces

When a service has passthrough as well as non-passthrough vNICs, we recommend that you first define the non-passthrough vNICs and then define the passthrough vNICs.

Run config terminal Command After Initial Setup

The **config terminal** command fails when you run it after performing the initial setup for a new installation. This happens because the admin user is not assigned to a group at the initial login. To run this command and configure Cisco CSP features, you must log out and then log in to Cisco CSP.

Network Interface Card (NIC) Driver Compatibility

This release includes the following NICs Physical function (PF) drivers. See VNF documentations for more information about compatibility between the Virtual function (VF) driver included in VNF and the NICs PF drivers.

- Ixgbe PF driver version: 5.5.3
- I40e PF driver version: 1.6.27-k

Spectre and Meltdown Firmware Update

This release include fixes for spectre and meltdown issue in Cisco CSP software. For firmware update, update the CIMC version to 4.0(1a). See the Cisco UCS C-Series Software Release Notes for more information about CIMC version at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_RN_4_0_1.html.

Restrictions

Cisco CSP has the following restrictions:

- Management interfaces cannot be configured as passthrough interfaces.
- Only local admin users have the functionality to autocopy images in repositories across the Cisco CSP nodes in a cluster. This functionality is not available for the TACACS+ or RADIUS admin users.
- Only local users can log in to Cisco CSP using CIMC console. Remote TACACS+ users cannot log in to Cisco CSP by using CIMC console.
- Only the vNIC e1000 model is supported with Cisco VSM and Cisco VSG services.
- Only ISO image files are supported with Cisco VSM and Cisco VSG services.

Using the Bug Search Tool

Use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

Step 1 Go to the Cisco Bug Search Tool.

Step 2 In the Log In screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at https://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the **Search For** field and press **Enter**.

Step 4 To search for bugs related to a specific release, do the following:

a) In the Product field, choose **Series/Model** from the drop-down list and then enter **Cisco Cloud Services Platform 2100** or **Cisco Cloud Services Platform 5000** in the text field.

b) In the Releases field, choose a criteria from the drop-down list and then enter a release number in the text field.

c) Press **Enter**.

When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so on.

Tip To export the results to a spreadsheet, click the **Export Results to Excel** link.

Related Documentation for Cisco Cloud Services Platform

- Data Sheet for Cisco Cloud Services Platform 5000 Series
- Release Notes for Cisco Cloud Services Platform
- Quick Start Guide for Cisco Cloud Services Platform
- Hardware Installation Guide for Cisco Cloud Services Platform
- Regulatory Compliance and Safety Information for Cisco Cloud Services Plarform
- Configuration Guide for Cisco Cloud Services Platform
- Command Reference Guide for Cisco Cloud Services Platform
- REST API Guide for Cisco Cloud Services Platform

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.