



Cisco Cloud Services Platform 2100 Release Notes, Release 2.3.0

First Published: 2018-07-31

Last Modified: 2018-07-31

Cisco Cloud Services Platform 2100 Release Notes

This document describes the features and limitations for the Cisco Cloud Services Platform 2100, Release 2.3.0.

Information About Cisco Cloud Services Platform 2100

Cisco Cloud Services Platform 2100 (Cisco CSP 2100) 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 2100 provides REST APIs, a web interface, and a CLI for creating and managing the virtual machine (VM) lifecycle.

Supported Cisco Networking Services

Cisco CSP 2100 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)

New Features and Enhancements

Cisco CSP 2100 Release 2.3.0 includes the following features and enhancements along with security and bug fixes:

Feature	Description
OVS DPDK	Supports OVS DPDK on all virtio ports on Niantic and Fortville NICs. VNFs can have a mix of DPDK, SRIOV, and regular virtio ports. DPDK is not supported on host and service management ports, or 1GB ports.
Converged SNMP Agents	Supports access to all MIBs through a single SNMP agent running at UDP port 161. Note Access to a subset of MIBs previously available through a secondary SNMP agent running at UDP port 1610 is retained for backward compatibility.
Adding or replacing NICs without clean install	Supports adding a NIC or replacing a NIC with the same NIC type in the same slot without requiring a clean install. Power off the server before adding or replacing a NIC, and then power it back. For earlier releases, to avoid clean install, add or replace the NIC with the same NIC type and in the same slot by following the same steps, and upgrade to release 2.3.0.
Multiple Day0 configuration files	Supports up to 8 Day0 or Day0-destination configuration files for each VNF.
Encrypted VNF VNC password	Supports masking of VNF VNC credentials by providing encrypted passwords for VNF VNC.
VNF health monitoring	Supports VNF health monitoring and recovery actions for VNFs.
Live export of services	Supports exporting a service without requiring explicit power down of the service. Service is paused during the export process.
VNF user groups	Supports new user group type, vnf-group . Users in each vnf-group can only access VNFs that are associated with that VNF group. They cannot create new VNFs.
VNF console operator role	Supports a new vnf-operator-group user role that allows operator users access VM VNC consoles.
Description for PNICs, services, and resource csp-2100	Supports adding descriptions for PNICs, services, and resource csp-2100.
New SNMP UI and MIB write support	Supports new SNMP CLI (snmp-server) that is compliant with Cisco IOS snmp-server CLI. Note Writable MIB objects are now supported.

Feature	Description
Creating Day0 configuration files locally	Supports creating a text file such as, the Day0 configuration locally.
GUI enhancements	Enhances the GUI and user experience for the services page.



Note The **Delete Cluster** button on toolbar enables deleting cluster configuration along with all members of a cluster.

Configuration Limits

Use the following configuration limits for Cisco CSP 2100.

Component	Supported Limits
Number of services in a node with hyperthreading disabled	<ul style="list-style-type: none"> For Cisco CSP 2100 with 8 or less than 8 cores, you can deploy the following number of VM cores: <i>Number of Cores – 1</i> For example, for Cisco CSP 2100 with 8 cores, you can deploy 7 VM cores. For Cisco CSP 2100 with greater than 8 and less than or equal to 16 cores, you can deploy the following number of VM cores: <i>Number of Cores – 2</i> For example, for Cisco CSP 2100 with 16 cores, you can deploy 14 VM cores. For Cisco CSP 2100 with greater than 16 cores, you can deploy the following number of VM cores: <i>Number of Cores – 4</i> For example, for Cisco CSP 2100 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

The following topics provide important notes and restrictions for Cisco CSP 2100.

Hyper-Threading Technology Support

Cisco CSP 2100 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 2100 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 2100 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.

Running 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 2100 features, you must log out and then log in to the Cisco CSP 2100.

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: 5.3.3
- 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 2100 software. For firmware update, update the CIMC version to 3.0(4a). 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_Release_Notes_3_0_4.html.

Restrictions

Cisco CSP 2100 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 2100 nodes in a cluster. This functionality is not available for the TACACS+ or RADIUS admin users.

- Only local users can log in to the Cisco CSP 2100 using CIMC console. Remote TACACS+ users cannot log in to the Cisco CSP 2100 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:
- In the Product field, choose **Series/Model** from the drop-down list and then enter **Cisco Cloud Services Platform 2100** in the text field.
 - In the Releases field, choose a criteria from the drop-down list and then enter a release number in the text field.
 - 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 2100

This section lists the documents used with the Cisco Cloud Services Platform 2100 and available on Cisco.com at the following URL:

<https://www.cisco.com/c/en/us/support/switches/cloud-services-platform-2100/tsd-products-support-series-home.html>

General Information

Cisco Cloud Services Platform 2100 Release Notes

Install and Upgrade

Cisco Cloud Services Platform 2100 Quick Start Guide

Cisco Cloud Services Platform 2100 Hardware Installation Guide

Regulatory Compliance and Safety Information for Cisco Cloud Services Platform 2100

Configuration Guide

Cisco Cloud Services Platform 2100 Configuration Guide

Reference Guides

Cisco Cloud Services Platform 2100 Command Reference Guide

Cisco Cloud Services Platform 2100 REST API Guide

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 . RSS feeds are a free service.

