Cisco Nexus Cloud Services Platform Release Notes, Release 5.2(1)SP1(7.1)

First Published: 2014-06-11
Last Updated: 2015-11-16

This document describes the features, limitations, and bugs for the Cisco Nexus Cloud Services Platform management software. Use this document in combination with documents listed in the Related Documentation, page 8.

Contents

This document includes the following information about the Cisco Nexus Cloud Services Platform:

Hardware Features

The Cisco Nexus Cloud Services Platform is a hardware shell that can host multiple virtual service blades, including the Cisco Nexus Virtual Supervisor Modules (VSMs). From a network management perspective, the hosted VSMs appear as a cluster. Each VSM and its associated VEMs make up one virtual switch.

Cisco Systems, Inc.
www.cisco.com

The Cisco Nexus Cloud Services Platform family includes the following appliances:

- Cisco Nexus 1010
- Cisco Nexus 1010-X
- Cisco Nexus 1110-S
- Cisco Nexus 1110-X

New Hardware Features

The following new hardware feature is introduced in the Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1).

Support for Cavium Nitrox Crypto Card

Beginning this release, the Cisco Nexus 1110-X enables you to use the Cavium Nitrox CNN3550-C20-NHB-2.0-G Security processor card (SSL card), to offload security processing and crypto acceleration. The SSL card is available as a field replacement unit (FRU) for the Cisco Nexus Cloud Services Platform and provides up to 30 Gbps (aggregated) of SSL offload for all virtual service blades (VSBs) on the Cisco Nexus Cloud Services Platform.

For detailed information about how to insert the SSL card on the Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*. To enable the SSL card and configure the crypto bandwidth, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.

Cisco Nexus Cloud Services Platform Features

Table 1 lists the features of the Cisco Nexus Cloud Services Platform appliances.

Table 1 Cisco Nexus Cloud Services Platform Appliance Features

Cisco Nexus Cloud Services Platform Appliance	Memory	Hard Disk	Support for VSBs
Cisco Nexus 1010	16GB	One TB SATA	Up to 6 VSBs (limited by the available RAM on the Cisco Nexus Cloud Services Platform)
Cisco Nexus 1010-X	48GB	Two 2-TB SAS drives	Up to 10 VSBs
Cisco Nexus 1110-S	32GB	Two 2-TB SATA drives	Up to 10 VSBs
Cisco Nexus 1110-X	64GB	Four 4-TB SATA drives	Up to 14 VSBs

For information about the hardware feature descriptions and specifications, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide.*

For information about the software installation and upgrade, see the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*.

Software Features

The Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1) supports the following new features:

Support for the 10 G Interface Card on the Cisco Nexus 1110-X

Starting Release 5.2(1)SP1(7.1), the Cisco Nexus Cloud Services Platform Software detects the presence and enables use of the UCS VIC 1225 10 G Dual Port NIC (10 G card) on the Cisco Nexus 1110-X. On the Cisco Nexus 1110-X, you can replace the UCS 10 G card or the Intel IG quad port NIC with a Cavium Nitrox card on the same PCI slot. After a fresh installation of the Cisco Nexus 1110-X, or an upgrade to this release, you can assign uplinks to the 10 G interface, or form a port channel with another 10 G interface.

For detailed information about how to switch the 10 G card with the Cavium SSL card or the Intel 1G quad port NIC, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

For information about enabling the10 G card and other caveats about enabling the 10 G card, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.

No Support for Static Topology

Starting Release 5.2(1)SP1(7.1), the Cisco Nexus Cloud Services Platform supports only a flexible topology as the default topology type. All previously configured static topology settings will be converted to the flexible topology upon an upgrade to the current release. For more information about the benefits of connecting to your network in a flexible topology, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.

Support for Cavium Nitrox Crypto Card

The Cavium Nitrox security processor card on the Cisco Nexus 1110-X provides a total of 30 GBps of SSL offload capacity that is shared by all the VSBs on the Cisco Nexus Cloud Services Platform. The Cisco Nexus Cloud Services Platform slices the security processor card and allocates the corresponding capacities to the VSBs based on their bandwidth requirement. However, you have to configure the VSBs to utilize the allocated slice of the security processor card.

For information about installing the Cavium Nitrox Security Processor card on the Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*. For information about enabling the SSL card and configuring the bandwidth requirement, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.

Automatic Copy of Changed VSB Configuration into Running Configuration

Beginning this release of the Cisco Nexus Cloud Services Platform, you do not have to execute the **copy running-config startup-config** command to save your VSB and network configuration settings during a reload or a power failure. The **copy running-config startup-config** command is automatically executed every five minutes to persistently save your configuration settings, and copy them into the startup configuration. For a complete list of the commands that trigger the auto-save feature, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.

Note

- Even though the copy running-config startup-config command is automatically triggered at five minute intervals, it is a recommended best practice to immediately save your critical configuration settings manually.
- The auto-save of the configuration settings is triggered only if a VSB-related configuration is affected. Therefore, if you have critical configuration settings not involving a VSB, you must manually save your settings.

Support for Cisco Nexus 1000V for KVM

Cisco Nexus 1000V for KVM is a virtual distributed switch that works with the Linux Kernel-based virtual machine (KVM) open source hypervisor. The Linux KVM hypervisor is ideally suited for OpenStack environments. Using the Cisco Nexus 1000V for KVM VSM, you can create policy profiles (called port profiles on the VSM), which define port classification information, such as security settings (ACLs and so on).

When a VM is deployed, a port profile is dynamically created on the Cisco Nexus 1000V for KVM for each unique combination of policy port profile and network segment. All other VMs deployed with the same policy to this network reuse this dynamic port profile. You can use the Cisco Nexus 1000V for KVM as a virtual service blade on the Cisco Nexus Cloud Services Platform. For more information about the Cisco Nexus 1000V for KVM, see *Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*.

Notes About Upgrading to the Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1)

- When you upgrade from an earlier release to the Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1), your previously configured static network topology will be converted to a flexible topology. For more information about flexible topology, see the *Cisco Nexus Cloud Services Platform Software Configuration Guide*.
- Before you upgrade to the Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1), you must upgrade to the following Cisco Integrated Management Controller (CIMC) software:
  - Version 1.5(4e) for the Cisco Nexus 1110 product family
  - Version 1.4(3s) for the Cisco Nexus 1010 product family
- You must reconfigure the SNMP user accounts after you upgrade to Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1). For detailed information about how to reconfigure the SNMP user accounts, see SNMP User Accounts Must Be Reconfigured After an Upgrade.

Software Compatibility

The Cisco Nexus Cloud Services Platform controls the virtual services and blades running on the Cisco Nexus 1010 and Cisco Nexus 1110 appliances.

For details on Software Compatibility with the Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Software Compatibility Information Guide.*

Configuration Limits

For detailed information on the weighting matrix and the supported configuration of VSBs on the Cisco Nexus Cloud Services Platform, see the weighting matrix in the *Cisco Nexus Cloud Services Platform Compatibility Information Guide*.

Restrictions

The Cisco Nexus Cloud Services Platform has the following restrictions:

SNMP User Accounts Must Be Reconfigured After an Upgrade

During an upgrade, the SNMP engine ID changes internally to a unique engine ID. You must reconfigure all SNMP user accounts to work with the new engine ID. Until the SNMP user accounts are reconfigured, all SNMPv3 queries fail. This restriction is associated with the defect CSCuo12696.

After an upgrade, the engine ID is shown as 128:0:0:9:3:2:0:12:0:0:0, as follows:

```
switch# show snmp user
_____________________________________________________________
                   SNMP USERS
_____________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  _____________ ______
_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________

User                          Auth  Priv
____                          ____  ____
admin                         md5   des
(EngineID 128:0:0:9:3:2:0:12:0:0:0)
```

Complete the following steps to delete and recreate the username. Note that *paswd123* is an example that represents the SNMP user password.

Step 1 Delete the username:

```
switch(config)#no snmp user admin auth md5 paswd123 engineID 128:0:0:9:3:2:0:12:0:0:0
```

Step 2 Use one of the following options to recreate the username:

Option 1

```
switch(config)# snmp user admin auth md5 paswd123
```

Option 2

```
switch(config)# snmp-server user admin auth md5 paswd123 priv aes-128 paswd123
```

Step 3 Confirm that the engine ID has been updated, as follows:

Option 1

```
switch# show snmp user
_____________________________________________________________
                   SNMP USERS
_____________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  ____________  ______
admin                         md5   no            network-operator

_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________

User                          Auth  Priv
____                          ____  ____
```

Option 2

```
switch(config)# show snmp user
_____________________________________________________________
                   SNMP USERS
_____________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  ____________  ______
admin                         md5   aes-128(no)   network-operator

_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________

User                          Auth  Priv
____                          ____  ____
```

Step 4 Verify that the engine ID is unique:

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903005056A0544E
                     [Dec] 128:000:000:009:003:000:080:086:160:084:078
```

Domain ID and HA Role Cannot Be Changed

The configured domain ID and high availability (HA) role (standalone, primary, or secondary) can never be changed. To change the domain ID or the HA role, you must use the **write erase** command.

Boot Variables Cannot Be Manually Configured

The boot variables cannot be configured manually. To change the boot variables, you must enter the **install nexus CSP** command. This command installs the software from the bootflash:/repository directory and updates the boot variables with the name of the software image.

Changing the Control or Mgmt VLAN Requires a Reload

If you change the control or management VLAN, you must execute the **copy running-config startup-config** command to save your configuration and reload the software before the change takes effect.

DNS Resolution

The Cisco Nexus Cloud Services Platform cannot resolve a domain name or hostname to an IP address.

Bugs

This section includes the following topics:

Open Bugs

The following are descriptions of the open bugs in Cisco Nexus Cloud Services Platform, Release 5.2(1)SP1(7.1). The bug ID links you to the Cisco Bug Search tool.

Table 2 Open Bugs

Bug ID	Headline
CSCuj77643	Deploying or removing the Citrix NetScaler 1000V restarts the Cisco Nexus 1000V VSM, and the Cisco Virtual Security Gateway VSBs of all 4.2(x) Releases.
CSCuo98930	Change of specific configuration does not get auto-copied into the startup configuration for the following commands: 1. **(config-if)# channel-group** 2. **(config-svs-domain)# control uplink** <*uplink int*> 3. **(config-svs-domain)# management uplink** <*uplink int*>

Table 2 Open Bugs (continued)

Bug ID	Headline
CSCup06508	Cisco Nexus Cloud Services Platform does not receive fragmented IP packets over management interfaces.
CSCur20537	The **install nexus1010** command returns an “Image not supported” message on 5.2(1)SP1(7.1).
CSCur30082	The IPv6 CLI configuration is not visible under the mgmt0 interface. The Cisco Nexus Cloud Services Platform does not accept the IPv6 configuration.

Resolved Bugs

The following bugs are resolved in the Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.1). The bug ID links you to the Cisco Bug Search tool.

Table 3 Resolved Bugs

Bug ID	Caveat Headline
CSCub39408	No error message is displayed when upgrade from an earlier release fails.
CSCuo47378	The primary and secondary Cisco Nexus Cloud Services Platforms fail to form high availability (HA) due to warm standby mode.
CSCua80533	Cisco NAM login fails and the VSB summary is lost after an upgrade
CSCuj82300	Citrix NetScaler 1000V VSB cannot be deployed on the Cisco Nexus 1010.

Related Documentation

The Cisco Nexus Cloud Services Platform documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps12752/tsd_products_support_series_home.html

Cisco Nexus 1000V

Cisco Nexus 1000V for VMware vSphere:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 1000V for Microsoft Hyper-V:

https://www.cisco.com/en/US/products/ps13056/tsd_products_support_series_home.html

Cisco Virtual Security Gateway

Cisco Virtual Security Gateway

Documentation Feedback

To provide technical feedback on this document or report an error or omission, please send your comments to:

- nexus1k-docfeedback@cisco.com

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.