



Cisco Nexus Cloud Services Platform Release Notes, Release 5.2(1)SP1(7.3)

First Published: 2015-06-05

Last Updated: 2015-11-06

This document describes the features and caveats for the Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3).

Contents

This document includes the following sections:

- [New Changes](#)
- [Installing the Cisco Nexus Cloud Services Platform Release 5.2\(1\)SP1\(7.3\)](#)
- [Upgrading to the Cisco Nexus Cloud Services Platform Release 5.2\(1\)SP1\(7.3\)](#)
- [Open Bugs](#)
- [Resolved Bugs](#)
- [Obtaining Documentation and Submitting a Service Request](#)

New Changes

The Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3) supports the following changes:

- Fix for the following OpenSSL vulnerabilities: CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-0209, and CVE-2015-0288.
- Fix for the Leap Second issue.
- Added support for IPV6 CLI configuration under the mgmt0 interface.



Installing the Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3)

The procedure to install the Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3) is the same as 5.2(1)SP1(7.1).

For installation instructions, see the [Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide, Release 5.2\(1\)SP1\(7.1\)](#).

Upgrading to the Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3)

Upgrading from Release 5.2(1)SP1(7.2) or 4.2(1)SP1(6.2)

The procedure to upgrade from Release 5.2(1)SP1(7.2) or 4.2(1)SP1(6.2) is the same as described in [Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide, Release 5.2\(1\)SP1\(7.1\)](#).

Upgrading from Release 5.2(1)SP1(7.1)

To upgrade from Release 5.2(1)SP1(7.1), a manual upgrade procedure is required. Complete the following steps.

Prerequisites

-
- Step 1** Copy the new image to the `bootflash:repository/` directory.
 - Step 2** Note the name of the image to use during the upgrade.
 - Step 3** Use the command **show system redundancy status** to note the redundancy role of the active module on which the upgrade is being performed. The role should be *primary* or *secondary*.
-

Manual Upgrade

To perform the manual upgrade:

-
- Step 1** Enter the following command to update to the new image:

```
update nexus1010 bootflash:repository/image.iso
```



Note The command and the image name do not auto complete and must be typed in completely.

```
switch# update nexus1010 bootflash:repository/nexus-1010.5.2.1.SP1.7.3.iso
coppa_mgr debug: Using URI: bootflash:/repository/nexus-1010.5.2.1.SP1.7.3.iso
Installing bootflash:/nexus-1010.5.2.1.SP1.7.3.iso
```

```

.....
Installation complete.
Save configuration and restart for changes to take effect

```

Step 2 Copy the running configuration to the startup configuration:

```

switch# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
switch#

```



Note It takes up to 10 seconds to copy the running configuration to the startup configuration. Therefore, you must wait for 10 seconds before proceeding to Step 3.

Step 3 Enter the **reload module** *module* command to reload the standby supervisor module and allow it to come back online:

```

switch# reload module ?
<1-2> Please enter the module number

```

- If the primary module is the active module:

```

switch# reload module 2
This command will reboot standby supervisor module. (y/n)? [n] y
about to reset standby sup
2014 Oct 2 09:15:23 switch %PLATFORM-2-PFM_MODULE_RESET: Manual restart of Module 2
from Command Line Interface
2014 Oct 2 09:15:46 switch %PLATFORM-2-MOD_REMOVE: Module 2 removed (Serial number
T023D7CC381)
2014 Oct 2 09:22:50 switch %PLATFORM-2-MOD_DETECT: Module 2 detected (Serial number
:unavailable) Module-Type Cisco Virtual Services Appliance Model :unavailable

```

- If the secondary module is the active module:

```

switch# reload module 1
This command will reboot standby supervisor module. (y/n)? [n] y
about to reset standby sup
switch# 2014 Oct 2 09:15:23 switch %PLATFORM-2-PFM_MODULE_RESET: Manual restart of
Module 1 from Command Line Interface
2014 Oct 2 09:15:46 switch %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial number
T023D7CC382)

```

Step 4 When the standby supervisor module is back online, verify the high availability (HA) synchronization is complete with the active module:

```

switch# show system redundancy status
Redundancy role
-----
administrative: primary
operational: primary
Redundancy mode
-----
administrative: HA
operational: HA
This supervisor (sup-1)
-----
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
Other supervisor (sup-2)
-----
Redundancy state: Standby

```

```
Supervisor state: HA standby
Internal state: HA standby
```

Step 5 After the HA synchronization is complete, switch over to the other module:

```
switch# system switchover
switch#
Broadcast message from root (console) (Thu Oct 2 09:28:33 2014):
The system is going down for reboot NOW!
```

Step 6 On the new active supervisor module, wait for the other supervisor module to come back online:

```
2014 Oct 2 09:28:33 switch %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming
active (pre-start phase).
2014 Oct 2 09:28:33 switch %SYSMGR-2-HASWITCHOVER_START: Supervisor 2 is becoming active.
2014 Oct 2 09:28:33 switch Oct 2 09:28:33 %KERN-1-SYSTEM_MSG: Failed to send MTS message.
error:-1 - kernel
2014 Oct 2 09:28:34 switch %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2014 Oct 2 09:28:58 switch %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial number )
switch# 2014 Oct 2 09:36:09 switch %PLATFORM-2-MOD_DETECT: Module 1 detected (Serial
number :unavailable) Module-Type Cisco Virtual Services Appliance Model :unavailable
```

Step 7 Verify that the module is online. When HA is complete, verify that the upgrade procedure is complete:

```
switch# show system redundancy status
Redundancy role
-----
administrative: secondary
operational: secondary
Redundancy mode
-----
administrative: HA
operational: HA
This supervisor (sup-2)
-----
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
Other supervisor (sup-1)
-----
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

Open Bugs

The following are descriptions of the open bugs in Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3). The IDs are linked to the Cisco Bug Search tool.

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	A configuration change does not automatically get copied to the startup configuration for the following commands: <ul style="list-style-type: none"> (config-if)# channel-group (config-svs-domain)# control uplink uplink int (config-svs-domain)# management uplink uplink int
CSCur20537	The install nexus1010 command returns an “Image not supported” message on 5.2(1)SP1(7.1).
CSCuw45229	After upgrading the Cisco Nexus Cloud Services Platform VSA image from Release 5.2(1)SP1(7.1) to 5.2(1)SP1(7.3), the RADIUS daemon service crashes, causing VSA reboot and failover.

Resolved Bugs

The following are descriptions of the resolved bugs in Cisco Nexus Cloud Services Platform Release 5.2(1)SP1(7.3). The IDs are linked to the Cisco Bug Search tool.

Bug ID	Headline
CSCtz32293	%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond.
CSCur30082	IPv6 CLI configuration is missing under the mgmt0 interface.
CSCus52394	The Cisco Nexus 1110 crashes when the show tech-support details command is executed. To collect Cisco Nexus 1110 platform logs, use the show tech-support nexus1010 command instead of the show tech-support details command. The command syntax to use: <pre>cpa-upgrade# show tech-support nexus1010 ? brief Gather critical information in brief commands Show the list of commands</pre>
CSCus86363	Reload or switchover might occur on the Cisco Nexus Cloud Services Platform because of the Leap Second update.

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* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.