Upgrading or Downgrading the Cisco Nexus 3600 Series NX-OS Software

This chapter describes how to upgrade or downgrade the Cisco NX-OS software. It contains the following sections:

About the Software Image

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of one NXOS software image. The image filename begins with "nxos".

Only this image is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 3600 Series switches.

Note Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename. For more information on SMUs, see the Cisco Nexus 3600 System Management Configuration Guide.

Note Cisco also provides electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. The EPLD image upgrades are independent from the Cisco NX-OS software upgrades.

Recommendations for Upgrading the Cisco NX-OS Software

Cisco recommends performing a Nexus Health and Configuration Check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices and Security Vulnerabilities, missing recommended configurations and so on. For more information about the procedure, see Perform Nexus Health and Configuration Check.

Cisco NX-OS Software Upgrade Guidelines

Note The Cisco Nexus 3600 Series NX-OS Release Notes contain specific upgrade guidelines for each release. See the Release Notes before starting the upgrade.

The following upgrade paths are supported for upgrading from an earlier release to a Cisco NX-OS 9.2(x) release:

- Cisco NX-OS Release 7.0(3)F3(3)/(3c) to Cisco NX-OS Release 7.0(3)F3(4) to Cisco NX-OS Release 9.2(x)
- Cisco NX-OS Release 7.0(3)F3(5) to Cisco NX-OS Release 9.2(x)
- Cisco NX-OS Release 9.2(x) to Cisco NX-OS Release 9.2(x)

Note For information on upgrading in a vPC environment, see vPC Upgrade and Downgrade Procedure for Nexus 9000 -R series switches.

iCAM must be disabled before upgrading from Cisco NX-OS Release 7.0(3)I7(1) to Cisco NX-OS Release 9.2(x) or 9.3(x). Only upgrading from Cisco NX-OS Release 9.2(4) to Cisco NX-OS Release 9.3(1) can be performed if iCAM is enabled.

To upgrade from any release prior to Cisco NX-OS Release 7.0(3)F3(3c), you must backup the switch configuration, perform a write erase, and reload the device. To upgrade from Cisco NX-OS Release 7.0(3)F3(4) to any later release, we recommend that you use the **install all** command.

Note Upgrading from Cisco NX-OS Release 7.0(3)F3(4) to 9.2(x) or later releases may take a longer time to boot due to the ASCII configuration being replayed. Please perform a **copy running-config startup-config** after upgrading to 9.2(x) or higher releases to avoid long boot times during future reloads.

Beginning with Cisco NX-OS Release 9.2(1), a simplified NX-OS numbering format is used for the platforms that are supported in the release. In order to support a software upgrade from previous releases that have the old release format, an installer feature supplies an I9(x) label as a suffix to the actual release during the upgrade operation. This label is printed as part of the image during the upgrade operation from any prior release to a Cisco NX-OS 9.2(x) release, and it can be ignored.

Before attempting to upgrade to any software image, follow these guidelines:

- Schedule the upgrade when your network is stable and steady.
- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software upgrade. See the Hardware Installation Guide for your specific chassis.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the Cisco Nexus 3600 Series NX-OS Security Configuration Guide.
- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles, you have the option to move some of the running-configuration commands to a switch profile. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.
- By default, the software upgrade process is disruptive.
- For a Cisco Nexus 36180YC-R switch with configured egress RACLs, prior to upgrading from a 7.x release to a 9.x release, follow these steps to ensure the RACLs are maintained and the upgrade is completed without issue:

  1. Add TCAM entries for egress RACL using the **hardware access-list tcam region e-racl** command.
  2. Save the configuration and reload.
  3. Upgrade to a 9.x release.

  For more information about configuring TCAM regions, see the *Cisco Nexus 3600 NX-OS Security Configuration Guide*.

Prerequisites for Upgrading the Cisco NX-OS Software

Upgrading the Cisco NX-OS software has the following prerequisites:

- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device.
- Ensure that the device has a route to the remote server. The device and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets. To verify connectivity to the remote server, use the **ping** command.

```
switch# ping 172.18.217.1 vrf management
PING 172.18.217.1 (172.18.217.1): 56 data bytes
64 bytes from 172.18.217.1: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 172.18.217.1: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 172.18.217.1: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 172.18.217.1: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 172.18.217.1: icmp_seq=4 ttl=239 time=76.5 ms
```

```
--- 172.18.217.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 76.5/83.645/106.647 ms
```

For more information on configuration sessions, see the *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade from a Cisco NX-OS 9.2(x) release to a later 9.2(x) release or from Cisco NX-OS Release 7.0(3)F3(4) to a Cisco NX-OS 9.2(x) release.

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 3600 Series NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
```

Note We recommend that you have the image file for at least one previous release of the Cisco NX-OS software on the device to use if the new image file does not load successfully.

Step 4 If you need more space on the supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.7.0.3.F3.3.bin
```

Step 5 Verify that there is space available on the active and the standby supervisor modules.

Step 6 If you need more space on the supervisor module, delete any unnecessary files to make space available.

Step 7 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 8 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.9.2.2.bin bootflash:nxos.9.2.2.bin
```

Step 9 Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

```
switch# show file bootflash://sup-1/nxos.9.2.2.bin sha256sum
5214d563b7985ddad67d52658af573d6c64e5a9792b35c458f5296f954bc53be
```

Step 10 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# show install all impact nxos bootflash:nxos.9.2.2.bin
```

Step 11 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 12 Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **non-interruptive**] command.

```
switch# install all nxos bootflash:nxos.9.2.2.bin
```

The following options are available:

- **no-reload**—Exits the software upgrade process before the device is reloaded.
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.

Note If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 13 (Optional) Display the entire upgrade process.

```
switch# show install all status
```

Step 14 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 15 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Cisco NX-OS Software Downgrade Guidelines

Before attempting to downgrade to an earlier software release, follow these guidelines:

- Software downgrades from a Cisco NX-OS 9.2(x) release to an earlier 9.2(x) release or to Cisco NX-OS Release 7.0(3)F3(4) should be performed using the **install all** command.
- iCAM must be disabled before downgrading from Release Release 9.2(x) or Release 9.3(x) → 7.0(3)I7(1). Only Release 9.3(1) → Release 9.2(4) can be performed if iCAM is enabled.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.
- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice,

remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.

- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.

Note Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as nondisruptive downgrades, are not supported.

Prerequisites for Downgrading the Cisco NX-OS Software

Downgrading the Cisco NX-OS software has the following prerequisites:

- Before you downgrade from a Cisco NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier Cisco NX-OS release that does not support the CoPP feature, you should verify compatibility using the **show incompatibility nxos bootflash:***filename* command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.

Downgrading to an Earlier Software Release

Use this procedure to downgrade from a Cisco NX-OS 9.2(x) release to an earlier 9.2(x) release or from a Cisco NX-OS 9.2(x) release to Cisco NX-OS Release 7.0(3)F3(4).

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 3600 NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Verify that the image file for the downgrade is present on the active supervisor module bootflash:.

```
switch# dir bootflash:
```

Step 4 If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 5 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.9.2.1.bin bootflash:nxos.9.2.1.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:nxos.9.2.1.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

Step 7 Disable any features that are incompatible with the downgrade image.

Step 8 Check for any hardware incompatibilities.

```
switch# show install all impact nxos bootflash:nxos.9.2.1.bin
```

Step 9 Power off any unsupported modules.

```
switch# poweroff module module-number
```

Step 10 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 11 Downgrade the Cisco NX-OS software.

```
switch# install all nxos bootflash:nxos.9.2.1.bin
switch# install all nxos nxos.9.2.1.bin.CCO
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.2.1.bin.CCO for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.1.bin.CCO.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.1.bin.CCO.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
2018 Jul 12 09:59:20 Bifrost_L3_Snake %$ VDC-1 %$ %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured
 from vty by admin on vsh.bin.30370
[####################] 100% -- SUCCESS



Compatibility check is done:
Module bootable Impact Install-type Reason
------ -------- -------------- ------------ ------
1 yes disruptive reset Incompatible image for ISSU



Images will be upgraded according to following table:
Module Image Running-Version(pri:alt) New-Version Upg-Required
------ ---------- ---------------------------------------- -------------------- ------------
1 nxos 9.2(2) 9.2(1) yes
1 bios v01.11(08/06/2018):v01.11(08/06/2018) v01.10(05/15/2018) no
```

```
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n]
```

Note If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 12 (Optional) Display the entire downgrade process.

Example:

```
switch# show install all status
```

Step 13 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```