Upgrade or Downgrade the Nexus 9000 Series NX-OS Software

Software image

The NX-OS software image is an image that

- consolidates the necessary system components into one image,
- includes a bundled EPLD image beginning with Release 10.5(3)F, and
- uses a 64-bit format with different prefixes for supported Nexus platforms.

Each Nexus switch is shipped with the NX-OS software preinstalled. The NX-OS software consists of one NX-OS software image, and this image is required to load the NX-OS operating system.

Note Beginning with Release 10.5(3)F, NX-OS no longer provides a separate EPLD image. The EPLD image is bundled with all NX-OS images, increasing image sizes. For more information, refer to Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.

NX-OS Release 10.6(x) supports only 64-bit images, which include:

- The 64-bit NX-OS image file name with `nxos64-cs` as the prefix (for example, `nxos64-cs.10.5.3.F.bin`) is supported on all Nexus 9000 series switches except Nexus 9500 -R and -R2 switches and line cards, Nexus 9800 switches, and N9364E-SG2 switches.
- The 64-bit NX-OS image file name with `nxos64-msll` as the prefix (for example, `nxos64-msll.10.5.3.F.bin`) is supported only on Nexus 9500 Series -R and -R2 modular switches.
- The64-bit NX-OS image file name with `nxos64-s1` as the prefix (for example, `nxos64-s1.10.5.3.bin`) is mandatory on Nexus 9800 and N9364E-SG2 switches. This image is supported from NX-OS Release 10.5(1)F on Nexus 9800 switches and from 10.5(3)F on N9364E-SG2 switches.
- The 64-bit NX-OS image file name with `nxos64-s1-dpu` as the prefix (for example, `nxos64-s1-dpu.10.6.2.F.bin`) is mandatory on N9324C-SE1U and N9348Y2C6D-SE1U Smart switches. This image is supported from NX-OS Release 10.6(2)F. Currently, these switches work in networking mode only.

Note

- Only disruptive upgrade is supported on the Smart switches.
- Service-acceleration feature is not supported in 10.6(2)F.

The Nexus 9000 Series switches support disruptive software upgrades and downgrades by default.

For information about the supported upgrade paths, see the CiscoNexus 9000 and 3000 Upgrade and ISSU Matrix.

Note

- Until NX-OS Release 10.5(2)F, we provided separate electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. For more information on the EPLD image and the upgrade process, see the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.
- 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 and generally include the ID number of the resolved defect in the filename (for example, n9000-dk10.1.1.**CSCab00001**.gbin). For more information on SMUs, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

EPLD image

The Nexus 9000 Series NX-OS mode switches contain several programmable logical devices (PLDs) that provide hardware functions in all modules. PLDs include electronic programmable logic devices (EPLDs), field programmable gate arrays (FPGAs), and complex programmable logic devices (CPLDs), but not ASICs. In this document, the term EPLD is used for FPGA and CPLDs. EPLD upgrades improve hardware functions and resolve known issues.

- For more information about EPLD, refer to Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.

- Until NX-OS Release 10.5(2)F, ISSU supports EPLD upgrades using the **install all nxos**<*nxos-image*>**epld**<*epld-image*> command during disruptive system (NX-OS) upgrade.
- While upgrading from pre-10.5(3)F releases to 10.5(3)F and later, first upgrade to 10.5(3) NX-OS using the **install all**<*nxos-image*> command. Then, after the NX-OS upgrade is complete, upgrade EPLD using the **install epld** command.
- Beginning with NX-OS Release 10.5(3)F, EPLD upgrade takes place during an ISSU system upgrade. To avoid EPLD upgrade, use the **skip-epld** option. Do not use the **epld**<*epld-image*> option as the EPLD image is bundled with the NX-OS images and a separate EPLD image is no longer provided.

Prerequisites for NX-OS software upgrade

The prerequisites that you must meet before upgrading the NX-OS software are:

- Verify the recommended upgrade paths between releases are specified in the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.
- Ensure that no user—who has access to the device or the network—is configuring the device or the network during the upgrade. You cannot configure a device during an upgrade. To verify that you have no active configuration sessions, use the **show configuration session summary** command.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the NX-OS software image on your device. While upgrading NX-OS software on a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module if there is an active configuration session.
- To transfer NX-OS software images to the Nexus switch through a file transfer protocol such as TFTP, FTP, SFTP, and SCP, verify that the Nexus switch can connect to the remote file server where the NX-OS software images are stored. If you do not have a router to route traffic between sub nets, ensure that the Nexus switch and the remote file server are on the same sub network. To verify connectivity to the remote server, transfer a test file using a file transfer protocol of your choice or use the ping command if the remote file server is configured to respond to ICMP Echo Request packets. Here is an example of using the **ping** command to verify connectivity to a remote file server `192.0.2.100`.

```
switch# ping 192.0.2.100 vrf management
PING 192.0.2.100 (192.0.2.100): 56 data bytes
64 bytes from 192.0.2.100: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 192.0.2.100: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 192.0.2.100: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 192.0.2.100: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 192.0.2.100: icmp_seq=4 ttl=239 time=76.5 ms

--- 192.0.2.100 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 non-disruptive ISSU in spanning tree topology, before running the **show spanning-tree issu-impact** command, the criteria that you must verify include
  - no topology change must be active in any STP instance
  - Bridge Assurance (BA) should not be active on any port (except MCT and vPC peer link)
  - there should be no Non-Edge Designated Forwarding port (except MCT and vPC peer link), and

- ISSU criteria must be met on the vPC peer switch.

Note For more information about configuration sessions, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide specific to your release.

Nexus health and configuration checks

A Nexus health and configuration check is an automated diagnostic service that

- analyzes Nexus switch logs to identify issues and provides recommendations
- checks critical configurations such as virtual Port Channel (vPC), multicast, and Layer 3 uplinks, and
- ensures best practices and detects inconsistencies in complex environments.

We recommend performing a Nexus health and configuration check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices, security vulnerabilities, and missing recommended configurations. For more information about the procedure, see Perform Nexus Health and Configuration Check.

NX-OS Software upgrade guidelines

Before attempting to upgrade to any software image, follow the guidelines and limitations listed under these sub sections to ensure compatibility, minimize disruptions, and maintain operational stability.

Note For ISSU compatibility for all releases, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

- Generic
- Software image and SMU
- EPLD
- Release specific
- Switch specific
- Disruptive and non-disruptive ISSU
- Enhanced mode
- Feature specific
- FEX
- FC/FCoE NPV
- VXLAN with TRM

- Unsupported PIDs

Generic

The guidelines that apply to all upgrades irrespective of the releases are

- A pre-upgrade generic checklist includes:
  - 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. For more information about your specific chassis, see the relevant Hardware Installation Guide.
  - Perform the installation on the active supervisor module, not the standby supervisor module.
- When you use **install all** with **no-reload** option, the saved configuration cannot be used before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with new version of NX-OS.
- During upgrade, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, upgrade with binary restore retains the primary key after the reboot.
- ISSU is blocked if **boot poap enable** is configured.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a non-disruptive upgrade.

Note vPC peering between an enhanced ISSU mode (boot mode lxc) configured switch and a non-enhanced ISSU mode switch is not supported.

- During an ISSU, the software reload process on the first vPC device locks its vPC peer device by using CFS messaging over the vPC communications channel. Only one device at a time is upgraded. When the first device completes its upgrade, it unlocks its peer device. The second device then performs the upgrade process, locking the first device as it does so. During the upgrade, the two vPC devices temporarily run different releases of NX-OS; however, the system functions correctly because of its backward compatibility support.
- ISSU is not supported when onePK is enabled. You can run the **show feature | include onep** command to verify that this feature is disabled before performing an ISSU or enhanced ISSU.
- Occasionally, while the switch is operationally up and running, the Device not found logs are displayed on the console. This issue is observed because the switch attempts to find an older ASIC version and the error messages for the PCI probe failure are enabled in the code. There is no functionality impact or traffic loss due to this issue.

- For secure POAP, ensure that DHCP snooping is enabled and set firewall rules to block unintended or malicious DHCP servers. For more information on POAP, see the Cisco Nexus 9000 Series Fundamentals Configuration Guide.
- When you upgrade from an earlier release to a 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 on configuration, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
- Guest Shell is disabled during an ISSU and reactivated after the upgrade. All applications running in the Guest Shell are affected.
- While performing an ISSU, VRRP and VRRPv3 display these messages:
  - If VRRPv3 is enabled:

```
2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
"vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can
change
vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all
 Vrrp
Peers to avoid Vrrp State transitions. - sysmgr
```

  - If VRRP is enabled:

```
2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
 "vrrp-
eng" has sent the following message: Feature vrrp is configured. User can change
vrrp
timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp
Peers to
avoid Vrrp State transitions. - sysmgr
```

- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.

Software image and SMU

- Beginning with NX-OS Release 10.5(1)F, s1 image is introduced specifically for Nexus 9800 switches.

  Upgrade of Nexus 9800 switches from earlier releases that have cs image format to the s1 image format in NX-OS Release 10.5(1)F and later is supported.

- Beginning with NX-OS Release 10.4(2)F, for Nexus 9300-R platforms, to upgrade bios to the latest version you should first upgrade to nxos image. This release onwards, the install all nxos command only upgrades the nxos sw to the latest version but the bios image will be upgraded to the last bios released prior to 10.4(2)F version.

  To upgrade to bios released with 10.4(2)F or higher version, first upgrade the nxos image and then use bios-force option to upgrade the bios. For example,

  1. Install all nxos bootflash:nxos64-msll.10.4.2.F.bin.

     The system reloads and boots up with 10.4(2)F image.

  2. Install all nxos bios-force.

Note The switch reloads twice, once for nxos upgrade and then again for bios upgrade.

- For platforms that need to be upgraded from any release to nxos64-cs.10.3(1)F or higher release, use nxos.9.3.10.bin or nxos64-cs.10.2(3)F or higher release as an interim hop. This restriction is applicable to both disruptive and non-disruptive upgrades. The nxos64-msll.10.3(1)F does not have this restriction.
- Loading an unsupported image on Nexus 9800 platform switches cause the switch to be stuck. Only a power cycle can reset it.
- Beginning with NX-OS Release 10.2(2)F, Nexus 9504 and 9508 platform switches, and Nexus 9508-R, R2, and RX line cards support NX-OS 64-bit images. Disruptive upgrade from earlier releases to 10.2(2)F 64-bit NX-OS image is supported. NX-OS 32-bit image is not supported on these platform switches anymore.
- Beginning with NX-OS Release 10.1(x), when an existing SMU is active, if you install a bundle that contains the existing active SMU, the installer installs only the non-existing SMUs.
- The **install all** command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore is not recommended.

Note For Nexus 9500 platform switches with -R line cards, you must save the configuration and reload the device to upgrade from NX-OS Release 7.0(3)F3(5) to 9.3(1). To upgrade from NX-OS Release 9.2(2) or 9.2(3), we recommend that you use the **install all** command.

- You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on the *Software Download* website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on the *Software Download* website.
- The **install all** command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore it is not recommended.

EPLD

- From NX-OS Release 10.6(1)F, while installing nx-os using the **install all nx-os** command on switches affected by secure boot vulnerability, if the IO FPGA version of the device is lower than the Fixed IO FPGA version, EPLD upgrade does not take place. To upgrade the FPGA, use the **install epld** command. For more information about switches affected by secure boot vulnerability and Fixed IO FPGA version, refer to *Table 1* in the FPGA/EPLD Upgrade Procedure to Address Secure Boot Vulnerability document.
- From NX-OS Release 10.5(3)F, while installing nx-os using the **install all nx-os** command on switches affected by secure boot vulnerability, EPLD upgrade does not take place. To upgrade the FPGA, use the **install epld** command. For more information about switches affected by secure boot vulnerability, refer to *Table 1* in the FPGA/EPLD Upgrade Procedure to Address Secure Boot Vulnerability document.

- Beginning with NX-OS Release 10.5(3)F, all NX-OS images are bundled with EPLD image and EPLD upgrade is triggered automatically as part of **install all nxos** command. However, you have the option to skip EPLD image upgrade.
- ISSU supports EPLD image upgrades using **install all nxos** <*nxos-image*> **epld** <*epld-image*> command, during disruptive system (NX-OS) upgrade. Beginning with NX-OS Release 10.5(3)F, do not use the **epld** <*epld_image*> option as the EPLD image is bundled with the NXOS images and a separate EPLD image is no longer provided.
- ISSU is not supported if EPLD is not at NX-OS Release 7.0(3)I3(1) or later.

Release specific

- Beginning with NX-OS Release 10.4(2)F, SR ISSU is not supported with underlay ISIS.
- When upgrading from earlier release to NX-OS Release 10.3(3)F and later, if the **hardware rate-limiter span-egress** command is configured then it must be removed and reapplied after the upgrade/ISSU is complete.
- Beginning with NX-OS Release 10.3(2)F, 2xSFP Eth10/1-2 are not supported on N9K-C9400-SW-GX2A. However, from NX-OS Release 10.4(2)F onwards, N9K-C9400-SW-GX2A Sup card ports 2xSFP Eth10/1-2 are supported.
- ASIC SFP+ ports Eth10/1-2 are not supported in NX-OS Releases 10.3(2)F, 10.3(3)F, and 10.4(1)F. Beginning with NX-OS Release 10.4(2)F, these ports are supported. However, note that after reloading the system, these ASIC SFP+ Eth10/1-2 ports can take up to 3 minutes to link up.
- While performing an ISSU on the L2 switch in a vPC complex or a LAN scenario, the IGMP group timeout must be configured with higher value as the L2 switch will not be able to forward the reports/queries during the control plane down time. The L2 snooping querier interval must also be matched to the L3 querier interval.
- While performing an ISSU from NX-OS Release 9.3(5), 9.3(6), 9.3(7), 10.1(1), or 10.1(2) to NX-OS Release 10.2(1) or higher release, ISSU is blocked.
- ISSU is blocked when the delay configuration is present in track list Boolean/weight.
- If the IPv6 ND timeouts during ISSU, then the IPv6 BFD session may flap after the ISSU.
- When upgrading directly to NX-OS Release 10.1(x) from any release prior to 7.0(x), the upgrade is disruptive. For a non-disruptive upgrade, an intermediate upgrade to NX-OS Release 9.x is required. We recommend upgrading to the latest release of NX-OS Release 9.3(x) as an intermediate hop for the upgrade. For information about the supported upgrade paths, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.
- When upgrading from NX-OS Release 7.0(3)I6(1) or 7.0(3)I7(1) to NX-OS Release 10.1(x), if the Nexus 9000 Series switches are running vPC and they are connected to an IOS-based switch via Layer 2 vPC, there is a likelihood that the Layer 2 port channel on the IOS side will become error disabled. The workaround is to disable the spanning-tree etherchannel guard misconfig command on the IOS switch before starting the upgrade process.

  Once both the Nexus 9000 Series switches are upgraded, you can re-enable the command.
- If you are upgrading from NX-OS Release 7.0(3)I5(2) to NX-OS Release 10.1(x) by using the **install all** command, BIOS will not be upgraded due to CSCve24965. When the upgrade to NX-OS Release 10.1(x) is complete, use the **install all** command again to complete the BIOS upgrade, if applicable.

- When upgrading from NX-OS Release 9.2(4) or earlier releases to NX-OS Release 9.3(4) or later, running configuration contains extra TCAM configuration lines. You can ignore these extra lines as they do not have an effect on the upgrade and configuration.
- When performing an ISSU from NX-OS Release 9.3(1) or 9.3(2) to NX-OS Release 9.3(3) or later, ensure that the features with user-defined ports, such as **<ssh port>**, are within the prescribed port range. If the port range is incorrect, follow the syslog message recommendation. For more information about the port range, see Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide.
- For any prior release version upgrading to NX-OS Release 9.3(5) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
  - **logging level evmc** *value*
  - **logging level mvsh** *value*
  - **logging level fs-daemon** *value*
- For any prior release version upgrading to NX-OS Release 9.3(6) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
  - **logging level evmc** *value*
  - **logging level mvsh** *value*

Switch specific

- During an ISSU on a Nexus 9300 Series switch, all First-Hop Redundancy Protocols (FHRPs) will cause the other peer to become active if the node undergoing the ISSU is active.
- Beginning with NX-OS Release 10.6(2)F, Nexus 9300-GX2, H2R, and H1 series switches support non-disruptive ISSU on switches that have MACsec-enabled interfaces.
- While performing non-disruptive ISSU from NX-OS Release 10.4(6)M to 10.6(1)F and later releases, on Nexus 9300-FX switches and line cards, IGMP traffic is forwarded on vPC legs towards the vPC pair. When there are multiple FEX devices on the vPC peer undergoing ISSU, multicast traffic loss can occur during the upgrade of the FEX devices. To resolve this, configure the **ip igmp group-timeout 450** command on all VLANs that carry IGMP traffic across the vPC peer link.
- Beginning with NX-OS Release 10.4(3)F, non-disruptive ISSU is not supported on Nexus 92348GC-X.
- Beginning with NX-OS Release 10.4(1)F, only the LXC mode is supported on Nexus 9300-FX and 9300-FX2 switches, in addition to Nexus 9300-FX3 and 9300-GX switches. This allows you to perform enhanced non-disruptive ISSU with minimal downtime. However, on the rest of the Nexus 9000 switches, you have an option to perform a non-disruptive ISSU in the enhanced LXC mode with minimal downtime.
- Beginning with NX-OS Release 10.4(1)F, only the enhanced LXC mode is supported on Nexus N9K-C9332D-H2R, N9K-C9348GC-FX3, and N9K-C9348GC-FX3PH switches by default.
- Non-disruptive ISSU is not supported on interfaces with 2.5G or 5G speed on N9K-C93108TC-FX3P platform. For more information, see CSCwq38959.
- After disruptive upgrade from NX-OS Release 10.3(x) to 10.5(x) and later releases, Nexus 9300-FX switches lose FC ports configuration and the FC ports turn into Ethernet ports. However, if `port x - y mode fc` exists under `slot z` in the running configuration, though such ports are changed to Ethernet ports, after a switch reload, they change back to FC ports.

- Beginning with NX-OS Release 10.2(2)F, FCoE/FC NPV is supported on N9K-C9336C-FX2-E platform switches.

  ISSU with with FCoE (Fiber Channel over Ethernet)/FC (Fiber Channel) NPV (N-port Virtualization) is supported on some Nexus 9000 switches. An ISSU allows you to upgrade the device software while the switch continues to forward traffic. You can perform an in-service software upgrade (ISSU), also known as a nondisruptive upgrade, for some Nexus 9000 switches. The default upgrade process is disruptive. Using the nondisruptive option helps ensure a nondisruptive upgrade.

  Fibre Channel N-port Virtualization (NPV) can co-exist with VXLAN on different fabric uplinks but on same or different front panel ports on the Nexus 93180YC-FX, N9K-C9336C-FX2-E, and N9k-C93360YC-FX2 switches.

- Before enabling the FHS on the interface, we recommend that you carve the ifacl TCAM region on Nexus 9300 and 9500 platform switches. If you carved the ifacl TCAM region in a previous release, you must reload the system after upgrading to NX-OS Release 10.1(x). Uploading the system creates the required match qualifiers for the FHS TCAM region, ifacl.

- Before enabling the FHS, we recommend that you carve the ing-redirect TCAM region on Nexus 9200 and 9300-EX platform switches. If you carved the ing-redirect TCAM region in a previous release, you must reload the system after upgrading to NX-OS Release 10.1(x). Uploading the system creates the required match qualifiers for the FHS TCAM region, ing-redirect.

- When upgrading from Nexus 94xx, 95xx, and 96xx line cards to Nexus 9732C-EX line cards and their fabric modules, upgrade the NX-OS software before inserting the line cards and fabric modules. Failure to do so can cause a diagnostic failure on the line card and no TCAM space to be allocated. You must use the **write_erase** command followed by the **reload** command.

Disruptive and non-disruptive ISSU

- When upgrading Nexus 9300-FX2 switch from NX-OS Release 10.5(3)F to any later releases, only disruptive upgrade is supported, and ND ISSU is not supported when the system is enabled with routing template security group. However, ND ISSU is supported from NX-OS Release 10.6(1)F.

- While performing ND ISSU, if a router is configured with BGP prefix peers, prefix-peer-timeout (default value - 30s) should be greater than GR timer (default value - 120s), to allow the prefix peers to resume the connection after ISSU.

- While performing multi-hop ND ISSU upgrade to higher releases, use 10.3(5)M or higher release as an intermediate hop.

  - If the switch has been previously upgraded using multi-hop ND ISSU and experiences unexpected CoPP drops, open a TAC case to determine if remediation is required.

- Beginning with NX-OS Release 10.2(3)F, non-disruptive ISSU is supported for VPC fabric peering on all Nexus 9300-X TORs. Both standard and enhanced non-disruptive upgrades are supported. Note that ISSU should be started or triggered when there is no failure. An example for failure would be one of the VPC legs is down.

- The recommended routing protocol graceful restart timer is 600 seconds and nve source-interface hold-down-time is 400 seconds.

- It is recommended to set **disable-fka** on VFC interfaces in E or F mode, when invoking ND native ISSU on switch mode testbed. If not, it can be disruptive.

- Disruptive upgrade from any version before 9.3(10) or 10.2(3)F may fail due to CSCwb63451. You must upgrade to 9.3(10) or 10.2(3)F first, before upgrading to 10.3(1)F or later.
- Beginning from NX-OS Release 10.2(8)M onwards, Nexus 9300-FX3 supports non-disruptive upgrade.
- Beginning with NX-OS Release 10.2(3)F, for switches that are in LXC mode and for non-desruptive upgrade, a new option **skip-kernel-upgrade** is added to **install** command.
- MPLS strip, GRE strip, and any underlying ACL configuration is not ISSU compatible when you perform ND ISSU to NX-OS Release 10.2(2)F from a previous release.

  After ND ISSU to NX-OS Release 10.2(2)F or 10.2(3)F from a previous release, post GRE strip dot1q tunnel VLAN_tag might be missing. Workaround for this issue is to remove and add port ACL from L2 interfaces for GRE strip enabled interface.
- For a device that is running on NX-OS Release 10.1(2), 10.2(1)F, and 10.2(2)F, ND-ISSU is not supported if Layer 2 sub-interfaces are configured.
- When performing ND ISSU using BGP non-default hold timers, ensure that the BGP graceful-restart timer is reasonably long enough, for example, 180 seconds.
- If there is a VRF scale, for a non-disruptive ISSU under each VRF, you must configure graceful restart timer to 300 seconds.
- OpenFlow and LACP fast timer rate configurations are not supported for Non-Disruptive ISSU.
- Beginning with NX-OS Release 9.3(5), standard, nondisruptive ISSU, on switches that are configured with uRPF, is supported on:
  - Nexus 9300-EX platform switches
  - Nexus 9300-FX/FX2 platform switches, and
  - Nexus 9300-GX platform switches

Note Prior to NX-OS Release 9.3(5), if any of the above switches were configured with uRPF, standard, non-disruptive ISSU was not supported.

Enhanced mode

- Beginning with NX-OS Release 10.3(3)F, only the LXC mode is supported on Nexus 9300-FX3 and 9300-GX switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime.
- ND ISSU can be performed in LXC mode in two methods:
  - ND ISSU in LXC mode - Switchover-based ISSU that is similar to EOR. Second SUP is brought up in new container and switchover is done. The second SUP now becomes the new active. There is no change to the kernel.
  - Fallback ND LXC ISSU - This is only done when the above switchover-based ISSU cannot be done (SRG Kernel incompatible or less memory). The kernel is upgraded.
  - skip-kernel-upgrade option will force ND ISSU in LXC mode - Switchover-based ISSU (even in case when running) and target kernels are incompatible.

- For switches that are in LXC boot mode, the enhanced LXC upgrade will fall back to standard ND ISSU as the target image kernels are likely be different than the current image.

Feature specific

- From NX-OS Release 10.6(1)F, on Nexus modular switches, if the Backplane diagnostic test fails and a BACKPLANE_AUTHENTICATION_FAIL syslog appears, do not perform an upgrade or a system reload.
- While upgrading from an earlier release to 10.5(3)F or later releases, as a part of sFlow ISSU Consistency Checker, pre and post configuration files are created in the booflash. To remove the snapshot files, use the **clear system internal sflow consistency pss-snapshot** command. However, if the snapshot files are removed, the **show system internal sflow consistency issu-pss** command does not provide the expected output. For more information, refer to Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
- When the PTP feature is configured on Nexus 9300-H2R and C93400LD-H1 switches, performing an ND ISSU upgrade from version 10.4(1)F to 10.5(2)F triggers a kernel panic, resulting in an additional switch reload and causing a traffic outage. For more information, refer to CSCwh34732.
- While upgrading from NX-OS releases prior to 10.4(3) to 10.4(3) or later releases with **mode tap-aggregation** command enabled on the Layer 2 interface, make sure to enable the global **hardware acl tap-agg** command and reload.
- Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay on Nexus 9300 and 92348GC-X platform switches; and on 9300-HX platform switches from NX-OS Release 10.4(3)F. However, the following features are not supported on nondisruptive ISSU:
  - SR L2EVPN
  - ISIS and OSPF underlay
  - vPC configuration with segment-routing
  - Egress Peer engineering
  - Segment routing and GRE co existence
- While upgrading from NX-OS releases prior to 10.2(2)F to 10.2(2)F or later releases, configure the **mode tap-aggregation** command before attaching TapAgg ACLs on Layer 2 interface.
- If you upgrade from a NX-OS release that supports the CoPP feature to a 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 of configuring control plane policing, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.
- Beginning with NX-OS Release 10.1(2), CoPP is supported on N9K-X9624D-R2 and N9K-C9508-FM-R2 platform switches.
- Beginning with NX-OS Release 10.1(2), RACL is supported on N9K-X9624D-R2 and N9K-C9508-FM-R2 platform switches.
- Beginning with NX-OS Release 10.1(1), during the disruptive upgrade to the 64-bit image or a downgrade from 64-bit to 32-bit image, if feature ITD is enabled, refer to *Guidelines and Limitations for ITD* in the

Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 10.1(x), if the upgrade or downgrade proceeds with an ASIC reload.

- Beginning with NX-OS Release 10.1(1), **Fs_daemon** does not support **snmpwalk** on devices with more than 5000 files. When performing snmpwalk on a device with more than 5000 files, the error `resourceUnavailable (This is likely a out-of-memory failure within the agent)` is an expected behavior.
- When you upgrade a Nexus 9000 device to NX-OS Release 10.1(x), if a QSFP port is configured with the manual breakout command and is using a QSA, the configuration of the interface Ethernet 1/50/1 is no longer supported and must be removed. To restore the configuration, you must manually configure the interface Ethernet 1/50 on the device.
- When upgrading from NX-OS Release 9.3(3) to NX-OS Release 9.3(6) or later, if you do not retain configurations of the TRM enabled VRFs from NX-OS Release 9.3(3), or if you create new VRFs after the upgrade, the auto-generation of **ip multicast multipath s-g-hash next-hop-based** command, when feature **ngmvpn** is enabled, will not happen. You must enable the command manually for each TRM enabled VRF. For the configuration instructions, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide.
- Upgrading from NX-OS Release 9.3(1), 9.3(2) or 9.3(3) to a higher release, with Embedded Event Manager (EEM) configurations that are saved to the running configuration, may cause a DME error to be presented. The error is in the output of the **show consistency-checker dme running-config enhanced** command, specifically, the event manager commands. If this error occurs, delete all EEM applet configurations after completing the ISSU, then reapply the EEM configurations.
- When redistributing static routes, NX-OS requires the **default-information originate** command to successfully redistribute the default static route starting in 7.0(3)I7(6).

FEX

- When upgrading from NX-OS Release 9.3x to NX-OS Release 10.4x using the **install all** command, ensure that storm control is disabled on all attached Fabric Extenders (FEXs). If you do not disable storm control, the switch fails to boot up after the upgrade. (See CSCws43646.)
- Beginning with NX-OS Release 10.2(2)F, ND ISSU is supported for FEX and you need to re-adjust the BGP **graceful-restart restart time** command for the upgrade to work non-disruptively. This must be done for each FEX upgrade one-by-one.

  The following example shows the time taken to re-adjust bgp-graceful restart-time for each non-disruptive FEX upgrade.

```
In the Non-disruptive upgrade with FEX, each FEX will upgrade taking about 90 secondss

(1.5 minutess) sequentially (one-by-one and not a parallel upgrade).
  Total non-disruptive upgrade time for all FEX = No. of fex * time taken per fex
                                      For 10 FEX = 10 * 90
                                                 = 900 seconds or 15 minutes
```

- When you upgrade a Nexus 9000 switch from NX-OS Release 7.x with an attached FEX in straight-through mode to 9.x and then to 10.x, the FEX Layer 2 Host Interface (HIF) configuration can be lost after upgrading to a 10.x Release. This occurs due to a design change in handling Layer 2 FEX HIF ports at boot time from Release 9.x to 10.x.

Note The issue occurs only for FEX connected in a straight-through mode and not for dual-homed (A-A) mode.

To resolve this, run the following non-intrusive commands before upgrading the switch from 9.x to 10.x:

1. Apply **no switchport** only on all Layer 3 (L3) physical and Layer 3 (L3) port-channel interfaces. For example,

```
switch(config)# interface e1/1
switch(config-if)# no switchport
```

2. Configure **system default switchport** globally and save the configuration. For example,

```
switch(config)# system default switchport
switch(config)# copy r s
```

Note The issue does not occur if:

- the switch was originally booted in 9.x with an attached FEX and then upgraded to 10.x.
- the switch was upgraded from 7.x to 9.x without an attached FEX, and the FEX was added later in 9.x before upgrading to 10.x.

- An upgrade that is performed via the **install all** command for NX-OS Release 7.0(3)I2(2b) to Release 10.1(x) might result in the VLANs being unable to be added to the existing FEX HIF trunk ports. To recover from this, the following steps should be performed after all FEXs have come online and the HIFs are operationally up:

  1. Enter the copy run bootflash:fex_config_restore.cfg command at the prompt.
  2. Enter the copy bootflash:fex_config_restore.cfg running-config echo-commands command at the prompt.

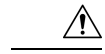
- In NX-OS Release 7.0(3)I6(1) and earlier, performing an ASCII replay or running the copy file run command on a FEX HIF configuration requires manually reapplying the FEX configuration after the FEX comes back up.

FC/FCoE NPV

- Beginning with NX-OS Release 10.1(1), ISSU is supported on FC/FCoE switch mode on Nexus 93360YC-FX2. For more information about the FC/FCoE switch mode and supported hardware, see the Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide.
- Beginning with NX-OS Release 10.1(1), enhanced ISSU is supported on FC/FCoE switch mode for Nexus 93180YC-FX and 93360YC-FX2 switches. For more information about the FC/FCoE switch mode and supported hardware, see the Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide.
- Beginning with NX-OS Release 10.1(1), Enhanced ISSU is supported on FC/FCoE NPV mode for Nexus 93180YC-FX and 93360YC-FX2 switches. For more information about the FC/FCoE NPV mode and

supported hardware, see the Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE NPV Configuration Guide.

VXLAN with TRM



Caution Following changes must be done during a maintenance window.

After upgrading a NX-OS 9000 Series switches configured with VXLAN (specifically VRF-related configurations) from NX-OS Release 7.x through 9.3 to 10.3(6) or earlier, two issues arise:

- The startup-config displays both legacy and new Layer 3 VNID configuration modes
- TRM traffic's RPF changes to the new mode for S,Gs, causing multicast traffic forwarding problems.

To avoid these issues, follow these steps:

- Enable the REST configuration input using the following commands:

```
feature nxapi
            nxapi http port 80
```

- Open a browser and enter the management IP address of the switch. This will open the Sandbox page. Use the same credentials as the switch admin login to sign in.
- In the top input textbox, enter the following command for each VRF that has an issue with the VNI ID:

```
vrf context tenant-1
        no vni 50000 l3
```

- On the right side of the page, set the Method to **`NXAPI-REST(DME)`** and keep the Input Type as **`cli`**.
- Click the **Convert (with DN)** button in the middle of the page. This will generate the XML equivalent of the configuration change.
- When the XML appears in the second textbox, click **Send** to apply the changes and remove the VNI ID configuration from the switch.
- To ensure the changes are applied, run the command:

```
copy running-config startup-config
```

Unsupported PIDs

The table displays the list of unsupported PIDs from various NX-OS Releases.

Unsupported PIDs	NX-OS Release
N9332C and N9364C	10.6(1)F
N9K-C92348GC-X	10.6(1)F
9700-EX line cards **Note** N9K-X97160YC-EX line card is supported.	10.6(1)F

Unsupported PIDs	NX-OS Release
N9K-C93180YC-EX and N9K-C93108TC-EX	10.4(x)
N9K-X9732C-EXM line card	10.3(x)
N9K-C9364C-GX	9.3(16)
N9K-C93600CD-GX	9.3(16)
N9K-C9316D-GX	9.3(16)
N9K-C93180LC-EX	9.3(x)

MACsec non-disruptive ISSU

Media Access Control Security (MACsec) non-disruptive ISSU is a feature that

- allows in-service software upgrades on switches with MACsec-enabled interfaces
- ensuring continued encryption and authentication of Ethernet traffic during the upgrade process, and
- is based on IEEE 802.1X-2014 REV of the MACsec Key Agreement (MKA) protocol. This protocol makes provision for MACsec-enabled switches to support ISSU by incorporating an additional parameter set.

MACsec is a Layer 2 security feature that provides encryption and authentication for traffic traversing Ethernet links. Nexus 9300-GX2, H2R, and H1 switches supports non-disruptive ISSU on switches that have MACsec-enabled interfaces.

Note Non-Disruptive ISSU is only supported on MACsec PSK-enabled interface.

To perform a non-disruptive ISSU on MACsec-enabled interfaces, the conditions that must be met include:

- The MACsec interfaces must use XPN cipher suites; otherwise, the upgrade is aborted.
- Both peers must run supported software versions with MKA version 2 or above. If any switch runs an older software version with MKA REV1, ISSU is aborted.

Note After completing ISSU, MACsec control plane transitions from the suspended to the secured state.

During the upgrade process, the MACsec interface can enter a new state called `suspended`. When an interface is in suspended state, it continues to encrypt outgoing data packets and decrypt incoming data packets on the interface. However, control packets may not be delivered sometimes when the interface control plane has a downtime. Due to this, a suspended interface does not support:

- Rekey results from policy timer expiry or packet number exhaustion. Packet number exhaustion-based rekey should not be triggered when using XPN cipher suites. XPN cipher suites provide a much wider window in which rekeying should occur.

- MACsec configuration changes after the interface enters a suspended state.

Note Any key expiry triggered after an interface moves to suspended state is handled only when the interface exits suspension and moves back to secured state.

Two new commands are introduced at the MACsec policy level to support this feature. For more information, refer to the *Configuring a MACsec policy* section in Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

System messages for MACsec non-disruptive ISSU

A few system messages or logs are added to notify when an interface is suspended and when it exits suspension.

- `switch %CTS-5-CTS_SUSPENSION_START: MACsec control plane operation suspended for interface: Ethernet1/18`

  - This system log indicates that an interface has moved to suspended state.

- `switch %CTS-5-CTS_SUSPENSION_REQUESTED: Requesting suspension of MACsec control plane operation for interface: Ethernet1/18`

  - This system log indicates that the peer interface has requested suspension to be started.

- `switch %CTS-5-CTS_SUSPENSION_STOP: MACsec control plane operation resumed for interface: Ethernet1/18`

  - This system log indicates that the suspension has ended and the interface is back to its original state.

ISSU platform support

The tables in this section summarize which Nexus platforms support standard and enhanced ISSU, the software release when support was introduced, and any features not supported for non-disruptive upgrades.

Note Enhanced ISSU cannot be supported if there is kernel update in the target release without reloading the container. The system prompts the

```
Host kernel is not compatible with target image. Full ISSU will be performed and control plane will be impacted.
```

message. In effect, the system performs non-disruptive ISSU instead of enhanced ISSU.

ISSU for Nexus 9200 platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with NX-OS Release 7.0(3)I6(1): Nexus 92300YC Beginning with NX-OS Release 9.3(3): Nexus 92348GC-X	Both ISSU types are disruptive for Nexus 9200 platform switches configured with features such as • Segment routing • Tetration **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 92348GC-X platform switches. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4. **Note** Beginning with NX-OS Release 10.4(3)F, non-disruptive ISSU is not supported on Nexus 92348GC-X. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4.
Enhanced	Nexus 92300YC	

ISSU for Nexus 9300 platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with NX-OS Release 9.3(3): Nexus 9332C Nexus 9364C **Note** ISSU on Nexus 9300 platform switches is supported when the switch is the spanning tree root. You can use the **show spanning-tree issu-impact** command to verify if the switch meets this criteria.	Both ISSU types are disruptive for Nexus 9300 platform switches configured with features such as • Dual-homed FEX • Segment routing • MACsec **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4.
Enhanced	Beginning with NX-OS Release 9.3(5): Nexus 9332C Nexus 9364C **Note** ISSU on Nexus 9300 platform switches is supported when the switch is the spanning tree root. You can use the **show spanning-tree issu-impact** command to verify if the switch meets this criteria.	

ISSU for Nexus 9300-X platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with NX-OS Release 10.2(3)F, VPC Fabric peering is supported on Nexus 9300-X TORs.	Beginning with NX-OS Release 10.2(3)F, the VXLAN and VPC features that are not supported during non- disruptive ISSU for VPC Fabric Peering include • TRM • VXLAN IPv6 underlay • Proportional Multipath for VNF • VXLAN Flood-and-learn • HSRP and VRRP • VXLAN Cloudsec • VXLAN to SR Handoff and all Handoff features • Multi-Site, and • MACsec **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for VXLAN to SR Handoff with BGP as underlay on Nexus 9300-X platform switches.
Enhanced	Beginning with NX-OS Release 10.2(3)F, VPC Fabric peering is supported on Nexus 9300-X TORs.	

ISSU for Nexus 9300-EX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with NX-OS Release 7.0(3)I6(1): Nexus 93108TC-EX Nexus 93180YC-EX	Both ISSU types are disruptive for Nexus 9300-EX platform switches configured with features such as • Segment routing • Tetration, and • MACsec **Note** Beginning with NX-OS Release 10.2(1), both ISSU types are non-disruptive for Nexus 9300-EX platform switches configured with Straight-Through FEX and Dual-Homed FEX.
Enhanced	Beginning with NX-OS Release 7.0(3)I7(3): Nexus 93108TC-EX Nexus 93180YC-EX	

ISSU for Nexus 9300-FX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	NX-OS Release 9.3(1) and 9.3(2): None Beginning with NX-OS Release 9.3(3): Nexus 9336C-FX2 Nexus 93240YC-FX2 Nexus 93240YC-FX2Z Nexus 9348GC-FXP Nexus 93108TC-FX Nexus 93180YC-FX Beginning with NX-OS Release 10.2(1)F: Nexus 93180YC-FX3 Nexus 93180YC-FX3S Beginning with NX-OS Release 10.4(1)F: 9348GC-FX3 9348GC-FX3PH Beginning with NX-OS Release 10.4(2)F: 93108TC-FX3	Standard ISSU is disruptive for Nexus 9300-FX platform switches configured with features such as • Segment Routing • TRM Feature, and • MACsec **Note** Beginning with NX-OS Release 10.2(1), Standard ISSU is non-disruptive for Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX. Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 93180YC-FX3 and FX3S platform switches. Beginning with NX-OS Release 10.4(1)F, standard ISSU is not supported on Nexus 9300-FX and 9300-FX2 platform switches. **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4.

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	NX-OS Release 9.3(1), 9.3(2), and 9.3(3): None Beginning with NX-OS Release 9.3(5): Nexus 9336C-FX2 Nexus 93240YC-FX2 Nexus 93216TC-FX2 Nexus 93360YC-FX2 Nexus 93240YC-FX2Z Nexus 9348GC-FXP Nexus 93108TC-FX Nexus 93180YC-FX Beginning with NX-OS Release 10.1(1), Enhanced ISSU is supported on the following platforms with FC/FCoE features: Nexus 93360YC-FX2 Nexus 93180YC-FX Beginning with NX-OS Release 10.2(1)F, Enhanced ISSU is supported on the following platforms: Nexus 93180YC-FX3 Nexus 93180YC-FX3S Beginning with NX-OS Release 10.4(1)F: 9348GC-FX3 9348GC-FX3PH Beginning with NX-OS Release 10.4(2)F: 93108TC-FX3 Beginning with NX-OS Release 10.2(2)F, Enhanced ISSU is supported on the following platform with FC/FCoE features: N9K-C9336C-FX2-E	

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
		Enhanced ISSU is disruptive for Nexus 9300-FX platform switches configured with features such as • Segment Routing • TRM Feature, and • MACsec **Note** In NX-OS Releases 9.3(x), Enhanced ISSU on Nexus 93360YC-FX2 and Nexus 93180YC-FX with FC/FCoE features will be disruptive. **Note** Beginning with NX-OS Release 10.2(1), Enhanced ISSU is non-disruptive for Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX. Beginning with NX-OS Release 10.3(3)F, only the LXC mode is supported on Nexus 9300-FX3 and 9300-FX3S switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime. Beginning with NX-OS Release 10.4(1)F, only the LXC mode is supported on Nexus 9300-FX and 9300-FX2 switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime. **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see NX-OS Software

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
		upgrade guidelines, on page 4.

ISSU for Nexus 9300-GX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with NX-OS Release 10.1(1): Nexus 9364C-GX Nexus 9316D-GX Nexus 93600CD-GX **Note** Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 9300-GX platform switches.	• TRM Feature • Segment Routing **Note** Beginning with NX-OS Release 10.3(3)F, standard ISSU is not supported on Nexus 9300-GX platform switches. **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4.
Enhanced	Beginning with NX-OS Release 10.1(1): Nexus 9364C-GX Nexus 9316D-GX Nexus 93600CD-GX Beginning with NX-OS Release 10.2(2)F, Enhanced ISSU is supported on Nexus 9300-GX2B platform switches. Beginning with NX-OS Release 10.2(3)F, Enhanced ISSU is supported on Nexus 9300-GX2A platform switches. Beginning with NX-OS Release 10.3(3)F, only the LXC mode is supported on Nexus 9300-GX switches, which allows you to perform enhanced non-disruptive ISSU with minimal downtime.	• TRM Feature • Segment Routing **Note** Beginning with NX-OS Release 10.4(2)F, non-disruptive ISSU is supported for segment routing traffic engineering (SR-TE) features with BGP as underlay only on Nexus 9300 platform switches. For more information about the features that are not supported, see NX-OS Software upgrade guidelines, on page 4.

ISSU for Nexus 9300-HX platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	Boot mode LXC ISSU is supported by default on the following Nexus C9300-HX platform switches: • N9K-C9332D-H2R - Beginning with NX-OS Release 10.4(1)F • N9K-C93400LD-H1 - Beginning with NX-OS Release 10.4(2)F • N9K-C9364C-H1 - Beginning with NX-OS Release 10.4(3)F **Note** ND-ISSU from any 10.4(x) or 10.5(x) releases to 10.5(3)F release is not supported on N9K-C9364C-H1.	• SR L2EVPN • ISIS and OSPF underlay • vPC configuration with segment-routing • Egress Peer engineering • Segment routing and GRE co-existence • MACsec

ISSU for Nexus 9400 platform switches

ISSU Type	Release and Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	Beginning with NX-OS Release 10.4(1)F, Enhanced ISSU is supported on Nexus C9408 platform switch.	• TRM Feature • Segment Routing • MACsec

Upgrade paths

For a list of specific releases from which you can perform a disruptive upgrade or a non-disruptive ISSU, see the Cisco Nexus 9000 Series NX-OS Release Notes for your particular release.

For ISSU compatibility for all releases and information about the upgrade paths, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

In general, ISSU is supported from

- a major release to any associated maintenance release
- the last two maintenance releases to the next two major releases, and
- an earlier maintenance release to the next two major releases.

Install upgrade patches

On Nexus 9500 series switches only, a software upgrade from NX-OS Release 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a) to any other NX-OS release requires installing two patches prior to upgrading using the **install all** command. These patches are available for each respective release and can be downloaded using the links below.

Caution Failing to follow this procedure could require console access in order to recover the switch after the upgrade.

Note These patches are only for upgrading. After the upgrade, the patch is automatically removed. If you decide not to upgrade after installing the patches, do not deactivate it. Deactivating the patch may cause a bios_daemon crash.

Cisco NX-OS Release 7.0(3)I1(2) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3a) Upgrade Patch

To install these patches prior to upgrading using the install all command, follow the instructions shown below. An example is demonstrated below with an NX-OS software patch and upgrade from 7.0(3)I1(2) to 7.0(3)I7(1):

Procedure

Step 1 Add both patches with the **install add bootflash:**{*patch-file.bin*} command.

Example:

```
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 16 completed successfully at Thu Mar  3 04:24:13 2016
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 17 completed successfully at Thu Mar  3 04:24:43 2016
```

Step 2 Activate both patches with the **install activate** { *patch-file.bin* } command.

Example:

```
switch(config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 18 completed successfully at Thu Mar  3 04:28:38 2016
switch (config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 19 completed successfully at Thu Mar  3 04:29:08 2016
```

Step 3 Commit both patches with the **install commit** { *patch-file.bin* } command.

Example:

```
switch(config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 20 completed successfully at Thu Mar  3 04:30:38 2016
switch (config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 21 completed successfully at Thu Mar  3 04:31:16 2016
```

Step 4 Proceed with a software upgrade to the chosen target release with the **install all** command.

Example:

```
switch (config)# install all nxos bootflash:nxos.7.0.3.I7.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /nxos.7.0.3.I7.1.bin
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I7.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
```

```
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

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

Notifying services about system upgrade.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  Incompatible image
     6       yes      disruptive         reset  Incompatible image
     8       yes      disruptive         reset  Incompatible image
     9       yes      disruptive         reset  Incompatible image
    10       yes      disruptive         reset  Incompatible image
    11       yes      disruptive         reset  Incompatible image
    14       yes      disruptive         reset  Incompatible image
    15       yes      disruptive         reset  Incompatible image
    16       yes      disruptive         reset  Incompatible image
    21       yes      disruptive         reset  Incompatible image
    22       yes      disruptive         reset  Incompatible image
    23       yes      disruptive         reset  Incompatible image
    24       yes      disruptive         reset  Incompatible image
    25       yes      disruptive         reset  Incompatible image
    26       yes      disruptive         reset  Incompatible image
    27       yes      disruptive         reset  Incompatible image
    28       yes      disruptive         reset  Incompatible image
    29       yes      disruptive         reset  Incompatible image
    30       yes      disruptive         reset  Incompatible image

Images will be upgraded according to following table:
Module  Image               Running-Version(pri:alt)         New-Version  Upg-Required
------  -----  ------------------------------------  ------------------  ------------
     1  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     1   bios                v01.42(00:v01.42(00           v01.48(00           yes
     6  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     6   bios                v01.48(00:v01.48(00           v01.48(00            no
     8  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     8   bios                v01.48(00:v01.29(00           v01.48(00            no
     9  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     9   bios                v01.48(00:v01.35(00           v01.48(00            no
    10  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    10   bios                v01.48(00:v01.42(00           v01.48(00            no
    11  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    11   bios                v01.48(00:v01.52(00           v01.48(00            no
    14  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    14   bios                v01.48(00:v01.48(00           v01.48(00            no
    15  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    15   bios                v01.48(00:v01.40(00           v01.48(00            no
    16  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    16   bios                v01.48(00:v01.42(00           v01.48(00            no
    21  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    21   bios                v01.48(00:v01.42(00           v01.48(00            no
    22  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    22   bios                v01.48(00:v01.40(00           v01.48(00            no
    23  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    23   bios                v01.48(00:v01.40(00           v01.48(00            no
    24  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
    24   bios                v01.48(00:v01.40(00           v01.48(00            no
    25  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
```

```
    25   bios                    v01.48(00:v01.40(00           v01.48(00            no
    26  lcn9k                           7.0(3)I1(2)         7.0(3)I7(1)           yes
    26   bios                    v01.48(00:v01.40(00           v01.48(00            no
    27   nxos                           7.0(3)I1(2)         7.0(3)I7(1)           yes
    27   bios  v08.06(09/10/2014):v08.18(08/11/2015)  v08.26(01/12/2016)           yes
    28   nxos                           7.0(3)I1(2)         7.0(3)I7(1)           yes
    28   bios  v08.06(09/10/2014):v08.26(01/12/2016)  v08.26(01/12/2016)           yes
    29  lcn9k                           7.0(3)I1(2)         7.0(3)I7(1)           yes
    29   bios                    v01.48(00:v01.35(00           v01.48(00            no
    30  lcn9k                           7.0(3)I1(2)         7.0(3)I7(1)           yes
    30   bios                    v01.48(00:v01.35(00           v01.48(00            no

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

Install is in progress, please wait.

Performing runtime checks.
[####################] 100% -- SUCCESS

Syncing image bootflash:/nxos.7.0.3.I7.1.bin to standby.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 6: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 8: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 9: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 10: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 11: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 14: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 15: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 16: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS
```

```
Module 21: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 22: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 23: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 24: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 25: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 26: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 28: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 29: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 30: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS
Finishing the upgrade, switch will reboot in 10 seconds.
switch(config)#
User Access Verification

switch login:
[ 2644.917727] [1456980048]  writing reset reason 88,

CISCO SWITCH Ver 8.26

CISCO SWITCH Ver 8.26
Memory Size (Bytes): 0x0000000080000000 + 0x0000000380000000
 Relocated to memory
Time: 6/3/2016  4:41:8
Detected CISCO IOFPGA
Booting from Primary Bios
Code Signing Results: 0x0
Using Upgrade FPGA
FPGA Revision        : 0x27
FPGA ID             : 0x1168153
FPGA Date           : 0x20160111
Reset Cause Register: 0x22
Boot Ctrl Register  : 0x60ff
EventLog  Register1 : 0x2000000
EventLog  Register2 : 0xfbe77fff
```

```
Version 2.16.1240. Copyright (C) 2013 American Megatrends, Inc.
Board type  1
IOFPGA @ 0xe8000000
SLOT_ID @ 0x1b
Standalone chassis
check_bootmode: grub: Continue grub
Trying to read config file /boot/grub/menu.lst.local from (hd0,4)
 Filesystem type is ext2fs, partition type 0x83

Booting bootflash:/nxos.7.0.3.I7.1.bin ...
Booting bootflash:/nxos.7.0.3.I7.1.bin
Trying diskboot
 Filesystem type is ext2fs, partition type 0x83
IOFPGA ID: 1168153
Image valid


Image Signature verification was Successful.

Boot Time: 3/3/2016  4:41:44
INIT: version 2.88 booting
Unsquashing rootfs ...

Loading IGB driver ...
Installing SSE module ... done
Creating the sse device node ... done
Loading I2C driver ...
Installing CCTRL driver for card_type 3 ...
CCTRL driver for card_index 21000 ...
old data: 4000004 new data: 1
Not Micron SSD...

Checking all filesystems.......
Installing default sprom values ...
 done.Configuring network ...
Installing LC netdev ...
Installing psdev ...
Installing veobc ...
Installing OBFL driver ...
mounting plog for N9k!
tune2fs 1.42.1 (17-Feb-2012)
Setting reserved blocks percentage to 0% (0 blocks)
Starting portmap daemon...
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
Loading system software
Installing local RPMS
Patch Repository Setup completed successfully
dealing with default shell..
file /proc/cmdline found, look for shell
unset shelltype, nothing to do..
user add file found..edit it
Uncompressing system image: Thu Jun 3 04:42:11 UTC 2016
blogger: nothing to do.

..done Thu Mar 3 04:42:11 UTC 2016
Creating /dev/mcelog
Starting mcelog daemon
Overwriting dme stub lib
Replaced dme stub lib
INIT: Entering runlevel: 3
```

```
Running S93thirdparty-script...

2016 Mar  3 04:42:37 switch%$ VDC-1 %$  %USER-2-SYSTEM_MSG: <<%USBHSD-2-MOUNT>> logflash: online  -
 usbhsd
2016 Mar  3 04:42:37 switch%$ VDC-1 %$ Mar  3 04:42:37 %KERN-2-SYSTEM_MSG: [   12.509615] hwport
mode=6 - kernel
2016 Mar  3 04:42:40 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Installing virtual service 'guestshell+'
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG: <<%ASCII-CFG-2-CONF_CONTROL>> Binary
restore - ascii-cfg[13904]
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG: <<%ASCII-CFG-2-CONF_CONTROL>> Restore
 DME database - ascii-cfg[13904]
2016 Mar  3 04:42:42 switch%$ VDC-1 %$ netstack: Registration with cli server complete
2016 Mar  3 04:43:00 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: ssnmgr_app_init called on ssnmgr up -
aclmgr
2016 Mar  3 04:43:09 switch%$ VDC-1 %$ %USER-0-SYSTEM_MSG: end of default policer - copp
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Install success virtual service
'guestshell+'; Activating
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual service
'guestshell+'
2016 Mar  3 04:43:13 switch%$ VDC-1 %$ %CARDCLIENT-2-FPGA_BOOT_PRIMARY: IOFPGA booted from Primary
2016 Mar  3 04:43:18 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: IPV6 Netlink thread init successful  -
icmpv6
2016 Mar  3 04:43:19 switch%$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online


User Access Verification
switchlogin:
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 1
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 6
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 8
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 9
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 10
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 11
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 14
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 15
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 16
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 21
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 22
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 23
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 24
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 25
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 26
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 28
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 29
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence of Module 30
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 1 ok (Serial number XYZ284014RR)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 2 ok (Serial number XYZ285111TC)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 3 ok (Serial number XYZ285111QQ)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 3 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 4 ok (Serial number XYZ284014TI)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 4 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 5 ok (Serial number XYZ284014TS)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 5 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 1 (Fan1(sys_fan1) fan)
 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 2 (Fan2(sys_fan2) fan)
 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 3 (Fan3(sys_fan3) fan)
 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 30 detected (Serial number
ABC1234DE56) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 30 powered up (Serial number
```

```
ABC1234DE56)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 28 detected (Serial number
:unavailable) Module-Type Supervisor Module Model :unavailable
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 29 detected (Serial number
ABC1234DEFG) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 29 powered up (Serial number
ABC1234DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 21 detected (Serial number
ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 22 detected (Serial number
ABC1211DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 21 powered up (Serial number
ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 22 powered up (Serial number
ABC1211DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 23 detected (Serial number
ABC1234D5EF) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 23 powered up (Serial number
ABC1234D5EF)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 24 detected (Serial number
ABC1211DE3F) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 24 powered up (Serial number
ABC1211DE3F)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 25 detected (Serial number
ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 25 powered up (Serial number
ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 26 detected (Serial number
ABC1211DE34) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 26 powered up (Serial number
ABC1211DE34)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 1. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 1 detected (Serial number
ABC1217DEFG) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 1 powered up (Serial number
ABC1217DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 9. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 9 detected (Serial number
ABC1236D4E5) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 9 powered up (Serial number
ABC1236D4E5)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 10. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 10 detected (Serial number
ABC1217EFGH) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 10 powered up (Serial number
ABC1217EFGH)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 11. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 11 detected (Serial number
ABC123DEF4) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 11 powered up (Serial number
ABC123DEF4)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 15. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 15 detected (Serial number
ABC1212DEFG) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 15 powered up (Serial number
ABC1212DEFG)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 16. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 16 detected (Serial number
```

```
ABCD1235DEFG) Module-Type 48x1/10G SFP+ 4x40G Ethernet Module Model N9K-X9464PX
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 16 powered up (Serial number
ABCD1235DEFG)
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 14. Ejector based shutdown enabled
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 14 detected (Serial number
ABC9876DE5F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 14 powered up (Serial number
ABC9876DE5F)
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 6. Ejector based shutdown enabled
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 6 detected (Serial number
ABC9876DE3F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 6 powered up (Serial number
ABC9876DE3F)
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All Ejectors closed
 for module 8. Ejector based shutdown enabled
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 8 detected (Serial number
ABC3456D7E8) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 8 powered up (Serial number
ABC3456D7E8)
2016 Mar  3 04:44:56 switch%$ VDC-1 %$ %USBHSD-STANDBY-2-MOUNT: logflash: online
2016 Mar  3 04:47:31 switch%$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated virtual
service 'guestshell+'
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED: The guest shell has been enabled.
 The command 'guestshell' may be used to access it, 'guestshell destroy' to remove it.

User Access Verification

switch#  show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2016, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.26
  NXOS: version 7.0(3)I7(1)
  BIOS compile time:  06/12/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I7.1.bin
  NXOS compile time:  2/8/2016 20:00:00 [02/09/2016 05:18:17]


Hardware
  cisco Nexus9000 C9516 (16 Slot) Chassis ("Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2403 0 @ 1.80GHz with 16401664 kB of memory.
  Processor Board ID SAL1745FTPW
```

```
  Device name: switch
  bootflash:   20971520 kB
Kernel uptime is 0 day(s), 0 hour(s), 8 minute(s), 13 second(s)

Last reset at 235176 usecs after  Thu Mar  3 04:40:48 2016

  Reason: Reset due to upgrade
  System version: 7.0(3)I1(2)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
switch#
```

Upgrade the NX-OS software

Use this procedure to upgrade to the latest NX-OS 10.6(x) release.

Note

- By default, the software upgrade process is disruptive.
- If an error message appears during the upgrade, the upgrade fails because of the reason indicated. For more information about possible causes and solutions, see the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide.

Before you begin

- Read the release notes for the software image file for any exceptions to this upgrade procedure. For more information about software image file, see the Cisco Nexus 9000 Series NX-OS Release Notes.

Procedure

Step 1 Log in to the device on the console port connection.

Step 2 Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
16384    Oct 30 17:05:32 2020  lost+found/
1964291584    Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-local
 4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

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

a) If you need more space on the active supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.9.2.1.bin
```

b) Verify that there is space available on the standby supervisor module.

```
switch# dir bootflash://sup-standby/
16384    Oct 30 17:05:32 2020  lost+found/
1964291584    Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-standby
4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

c) (Optional) If you need more space on the standby supervisor module, delete any unnecessary files to make space available.

```
switch# delete bootflash://sup-standby/nxos.9.2.1.bin
```

Step 3 Log in and choose the software image file for your device from the Software Download website, and download it to a file server.

Step 4 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/nxos64.10.2.1.F.bin bootflash:nxos64.10.2.1.F.bin
```

Note
The compaction feature is deprecated from NX-OS Release 10.5(2)F

For software images requiring compaction, you must use SCP, HTTP, or HTTPS as the source and bootflash or USB as the destination. This example uses SCP and bootflash:

```
switch# copy scp://user@scpserver.cisco.com//download/nxos64.10.2.1.F.bin
bootflash:nxos64.10.2.1.F.bin compact vrf management use-kstack

user1@10.65.42.196's password:
nxos64.10.2.1.F.bin 100% 1887MB 6.6MB/s 04:47
Copy complete, now saving to disk (please wait)...
Copy complete.
```

The **compact** keyword compacts the NX-OS image before copying the file to the supervisor module.

Note
Software image compaction is only supported on SCP, HTTP, or HTTPS. If you attempt compaction with any other protocol, the system returns the following error:

```
Compact option is allowed only with source as scp/http/https and destination
as bootflash or usb
```

Note
Compacted images are not supported with LXC boot mode.

Note
Software image compaction is only supported on Nexus 9300-series platform switches.

a) You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.

```
switch# show file bootflash:nxos.10.1.1.bin md5sum
2242a7f876f1304118fd175c66f69b34

switch# show file bootflash:nxos.10.1.1.bin sha512sum
7f25cce57ca137a79211fb3835338aae64acf9b021b75cec5d4156e873b4274ca4f98e9a74fe4c8961
f5ace99ed65f3826650599369f84ab07265d7c5d61b57f
```

b) You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on the Software Download website.

```
switch# show file bootflash:nxos64.10.2.1.F.bin md5sum
c49660952215822afd30bb7958a0765a

switch# show file bootflash:nxos64.10.2.1.F.bin sha256sum
2a64efbb381fabbb52054af74cf3efda1691772a49a70ddd35550431cadecf8e

switch# show file bootflash:nxos64.10.2.1.F.bin sha512sum
3bf6a771aa4a192a8e1383e348b26bb483356a9774d74ba39edbf7718248483b3391942d8103de8104deea8fda212266e70bd736220cff34943bd8e359432975
```

Step 5 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# # show install all impact nxos bootflash:nxos64.10.2.1.F.bin
```

During the compatibility check, the ISSU-related messages listed in this table can appear in the **Reason** field.

Reason Field Message	Description
Incompatible image for ISSU	The NX-OS image to which you are attempting to upgrade does not support ISSU.
Default upgrade is not hitless	By default, the software upgrade process is disruptive. You must configure the **non-disruptive** option to perform an ISSU.

Step 6 Save the running configuration to the startup configuration.

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

Step 7 Upgrade the NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **non-disruptive** | **non-interruptive** | **serial**| **skip-epld** | **skip-bios-upgrade** | **skip-kernel-upgrade**] command.

```
switch# install all nxos bootflash:nxos64.10.5.3.F.bin
```

Note
From NX-OS Release 10.5(3)F, EPLD upgrade can be performed with either the no-reload or the non-disruptive option.

The available options are:

- **no-reload**—Exits the software upgrade process before the device reloads.

  Note
  When you use **install all** with **no-reload** option, no additional configuration changes can be made before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with the new version of NX-OS (along with EPLD from 10.5(3)F). From Release 10.5(3)F onwards, though the EPLD and BIOS are programmed but not upgraded, a switch reload is required for them to take effect.

- **non-disruptive**—Performs an in-service software upgrade (ISSU) to prevent the disruption of data traffic. (By default, the software upgrade process is disruptive.) From Release 10.5(3)F onwards, though the EPLD and BIOS are programmed but not upgraded, a switch reload is required for them to take effect.
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.
- **serial**—Upgrades the I/O modules in Nexus 9500 Series switches one at a time. (By default, the I/O modules are upgraded in parallel, which reduces the overall upgrade time. Specifically, the I/O modules are upgraded in parallel in this order: the first half of the line cards and fabric modules, the second half of the line cards and fabric modules, the first system controller, the second system controller.)
- **skip-epld**—Installs only the nxos image, and not the epld image. This option is available from 10.5(3)F.
- **skip-bios-upgrade**—Installs only the nxos image, and skips the BIOS upgrade. This option is available from 10.5(3)F.
- **skip-kernel-upgrade**—Installs only the nxos image, and skips the kernel upgrade. This option is available from 10.5(3)F.

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 NX-OS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image, if necessary.
- Starting from 10.5(3)F, during the image upgrade, you can also apply SMUs so the SMU is installed with the new image using the **install all nxos** <*nxos image*> **package** <*smu package*> **non-disruptive non-interruptive** command.

```
install all nxos nxos64-cs.10.5.3.F.bin.upg package nxos64-cs.CSCab123456
-1.0.0-10.5.3.lib32_64_n9000.rpm non-disruptive non-interruptive
```

Step 8 (Optional) Post upgrade actions.

a) Display the entire upgrade process.

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

b) Log in and verify that the device is running the required software version.

```
switch# show version
```

c) If necessary, install the relevant licenses to ensure that the required features are available on the device. For more information about the licenses, see the Cisco NX-OS Licensing Options Guideand Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.

In-Service Software Upgrade

An in-service software upgrade (ISSU) is an upgrade that

- allows you to upgrade the device software while the switch continues to forward traffic,

  reduces or eliminates the downtime typically caused by software upgrades, and

  is also known as non-disruptive upgrade.

You can perform an ISSU or non-disruptive upgrade for some switches. (See the ISSU platform support, on page 17 for a complete list of supported platforms.)

- The default upgrade process is disruptive. Therefore, ISSU needs to be enabled using the command-line interface (CLI), as described in the configuration section of this document.
- Using the non-disruptive option helps ensure a non-disruptive upgrade. The guest shell is disabled during the ISSU process and it is later reactivated after the upgrade.
- Enhanced ISSUs are supported for some Nexus 9000 Series switches.

ISSU scenarios and platform support

The supported ISSU scenarios include

- performing standard ISSU on Top-of-Rack (ToR) switches with a single supervisor, and
- performing enhanced ISSU on Top-of-Rack (ToR) switches with a single supervisor

Details for each scenario are described below.

Performing standard ISSU on Top-of-Rack (ToR) switches with a single Supervisor

The ToR Nexus 9300 platform switches are the NX-OS switches with single supervisors. Performing ISSU on the Nexus 9000 Series switches causes the supervisor CPU to reset and to load the new software version. After the CPU loads the updated version of the NX-OS software, the system restores the control plane to the previous known configuration and the runtime state and it gets in-sync with the data plane, thereby completing the ISSU process.

The data plane traffic is not disrupted during the ISSU process. In other words, the data plane forwards the packets while the control plane is being upgraded, any servers that are connected to the Nexus 9000 Series switches do not see any traffic disruption. The control plane downtime during the ISSU process is approximately less than 120 seconds.

Performing enhanced ISSU on Top-of-Rack (ToR) switches with a single Supervisor

Note Enhanced ISSU is not supported if there are any underlying kernel differences. The system prompts the

```
Host kernel is not compatible with target image. Full ISSU will be performed and control
plane will be impacted.
```

message: In effect, the system performs non-disruptive ISSU instead of enhanced ISSU.

The NX-OS software normally runs directly on the hardware. However, configuring enhanced or container-based ISSU on single supervisor ToRs is accomplished by creating virtual instances of the supervisor modules and the line cards. With enhanced ISSU, the software runs inside a separate Linux container (LXC) for the supervisors and the line cards. A third container is created as part of the ISSU procedure, and it is brought up as a standby supervisor.

The virtual instances (or the Linux containers) communicate with each other using an emulated Ethernet connection. In the normal state, only two Linux containers are instantiated: vSup1 (a virtual SUP container in an active role) and vLC (a virtual linecard container). Enhanced ISSU requires 16G memory on the switch.

To enable booting in the enhanced ISSU (LXC) mode, use the **[no] boot mode lxc** command. This command is executed in the configuration mode. Here is a sample configuration for your reference.

```
switch(config)# boot mode lxc
Using LXC boot mode
Please save the configuration and reload system to switch into the LXC mode.
switch(config)# copy r s
[########################################] 100%
Copy complete.
```

Note Reload the switch first, when enabling enhanced ISSU for the first time.

During the software upgrade with enhanced ISSU, the supervisor control plane stays up with minimal switchover downtime disruption and the forwarding state of the network is maintained accurately during the upgrade. The supervisor is upgraded first and the line card is upgraded next.

The data plane traffic is not disrupted during the ISSU process. The control plane downtime is less than 6 seconds.

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

For information on ISSU and high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

NX-OS upgrade history

During the life of a Nexus 9000 switch, many upgrade procedures can be performed. Upgrades can occur for maintenance purposes or to update the operating system to obtain new features. Over time, switches can be updated on numerous occasions. Viewing the types of upgrades and when they occurred can help in troubleshooting issues or simply understanding the history of the switch.

Nexus 9000 switches log all upgrade activity performed over time providing a comprehensive history of these events. The stored upgrade history types are:

- Cisco NX-OS System Upgrades
- Electronic Programmable Logic Device (EPLD) Upgrades, and
- Software Maintenance Upgrade (SMU) Installations

View the NX-OS upgrade history by entering the **show upgrade history** command. The output displays any upgrade activity that previously occurred on the switch and defines the start and end times for each event. The following is an example output of the **show upgrade history** command:

```
switch# show upgrade history
     TYPE            VERSION               DATE                 STATUS
NXOS system image  10.5(3)          06 Mar 2025 03:08:17     Installation End
NXOS system image  10.5(3)          06 Mar 2025 03:01:41     Installation started
NXOS system image  10.5(3)          06 Mar 2025 02:16:25     Installation End
NXOS EPLD          epld.img         06 Mar 2025 02:11:43     EPLD Upgrade completed
NXOS EPLD          epld.img         06 Mar 2025 02:00:22     EPLD Upgrade started
NXOS system image  10.5(3)          06 Mar 2025 01:52:46     Installation started
NXOS system image  10.5(3)          06 Mar 2025 01:19:05     Installation End
NXOS EPLD          epld.img         06 Mar 2025 01:19:04     EPLD Upgrade completed
NXOS EPLD          epld.img         06 Mar 2025 01:07:42     EPLD Upgrade started
NXOS system image  10.5(3)          06 Mar 2025 01:00:48     Installation started
```

View the NX-OS upgrade history details by entering the **show upgrade history details** command. The output displays user login details (user name/session ID) under LOGIN column on the switch along with upgrade history. Here is an sample output of the **show upgrade history details** command.

```
switch# show upgrade history details
   TYPE            VERSION                  DATE                   LOGIN
     STATUS
NXOS system image  10.5(3)                 06 Mar 2025 03:08:17   username/10.1.1.25
Installation End
NXOS system image  10.5(3)                 06 Mar 2025 03:01:41   username/10.1.1.25
Installation started
NXOS system image  10.5(3)                 06 Mar 2025 02:16:25   username/10.1.1.25
Installation End
NXOS EPLD          epld.img                06 Mar 2025 02:11:43
EPLD Upgrade completed
NXOS EPLD          epld.img                06 Mar 2025 02:00:22
EPLD Upgrade started
NXOS system image  10.5(3)                 06 Mar 2025 01:52:46   username/10.1.1.25
Installation started
NXOS system image  10.5(3)                 06 Mar 2025 01:19:05   username/10.1.1.25
Installation End
NXOS EPLD          epld.img                06 Mar 2025 01:19:04
EPLD Upgrade completed
NXOS EPLD          epld.img                06 Mar 2025 01:07:42
EPLD Upgrade started
NXOS system image  10.5(3)                 06 Mar 2025 01:00:48   username/10.1.1.25
Installation started
NXOS EPLD          n9000-epld.10.5.1.F.img 05 Mar 2025 23:29:18   username/10.1.1.25
EPLD Upgrade completed
NXOS EPLD          n9000-epld.10.5.1.F.img 05 Mar 2025 23:17:59   username/10.1.1.25
EPLD Upgrade started
NXOS EPLD          epld.img                05 Mar 2025 22:55:11
EPLD Upgrade completed
NXOS EPLD          epld.img                05 Mar 2025 22:37:36
EPLD Upgrade started
```

Prerequisites for NX-OS Software downgrade

The prerequisites for downgrading the NX-OS software include

- Before downgrading from a NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier release that does not support the CoPP feature, verify compatibility using the **show**

incompatibility nxos bootflash:*filename* command. If incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.

- Save, commit, or discard any active configuration sessions before downgrading the NX-OS software image on your device.

NX-OS software downgrade guidelines

Read and follow these guidelines and limitations listed in this section before downgrading your NX-OS software from the current release to an earlier release.

- The only supported method of downgrading a Nexus 9000 Series switch is to utilize the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.

  Disable the Guest Shell if you need to downgrade from NX-OS Release 9.3(x) to an earlier release.

  - Performing an ISSU downgrade from NX-OS Release 9.3(x) to Release 7.0(3)I4(1) with an FCoE (Fiber Channel over Ethernet) NPV (N-port Virtualization) configuration causes the port channel to crash with a core file:

    ```
    [################## ] 38%2016 Apr 18 20:52:35 n93-ns1 %$ VDC-1 %$ %SYSMGR-2-
                  SERVICE_CRASHED: Service "port-channel" (PID 14976) hasn't caught
    signal 11 (core will
                  be saved)
    ```

  - ISSU (non-disruptive) downgrade is not supported

- On Nexus 9500 switches with N9508-E2 Fabric module, downgrade from any 9.x or 10.x supported releases to any unsupported releases of 7.x is not supported.
- When downgrading from the NX-OS Release 9.3(x) to earlier releases, any ACL with the statistics per-entry command enabled and applied as RACL needs the statistics per-entry command removed from the running configuration before downgrading. Otherwise, the interfaces on which this ACL is applied as a RACL will be error disabled after the downgrade.
- Prior to downgrading a Nexus 9500-series switch, with -FX or -FX+EX line cards, from NX-OS Release 10.1(x) to earlier releases (9.2(x) or 7.x), the TCAM region that applies to NetFlow (ing-netflow) should be carved to zero (0) using the following command:

  hardware access-list tcam region ing-netflow 0

  The configuration change is required because the default ing-netflow TCAM region in 9.3(1) and onwards is 512 while the default in 9.2(x) and earlier is 0.
- When downgrading from the NX-OS Release 10.1(x) to a release prior to 9.3(x), make sure that the ACL TCAM usage for ingress features does exceed the allocated TCAM space in the absence of the label sharing feature. Label sharing is a new feature in NX-OS Release 9.3(x). Otherwise, interfaces with RACLs that could not fit in the TCAM will be disabled after the downgrade.
- Software downgrades should be performed using the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.
- This limitation applies to Nexus platform switches that support Trust Anchor Module (TAM):

The TACACS global key cannot be restored when downgrading from NX-OS Release 9.3(3) and higher to any earlier version. TAM was updated to version-7 in 9.3(3), but earlier NX-OS versions used TAM version-3.

- iCAM must be disabled before downgrading from 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.
- Beginning with NX-OS Release 9.3(3), new configuration commands exist for SRAPP (with sub-mode options for MPLS and SRTE). The SRAPP configuration on the switch running release 9.3(3) (or later) will not be present if the switch is downgraded to an earlier release.
- 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. For more information about your specific chassis, see the relevant Hardware Installation Guide.
- NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a 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 NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
- Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as non-disruptive downgrades, are not supported.
- While downgrading from the NX-OS Release 10.2(1)F or higher to an earlier release, the **install all** command is blocked when the delay config is present in track list Boolean/weight.
- While performing ISSD from NX-OS Release 10.2(3)F to NX-OS Release 10.2(2)F with **epbr L2** applied on interfaces, remove the policies from interfaces before performing ISSD to avoid the duplicate tracks issue.
- Beginning with NX-OS Release 10.2(3)F, if you have configured the **lldp chassis-id switch** command, then you must disable the command before performing ISSD.
- Beginning with 10.2(3)F, although application of ePBR policy to access ports is supported, downgrading with this configuration is not recommended.
- When feature ngmvpn is enabled and a disruptive downgrade is performed from NX-OS Release 10.3(2)F to NX-OS Release 10.3(1)F, although a few VRFs are missing from the show run output, this is only a display issue, and has no functional impact.
- When a switch is downgraded from NX-OS Release 10.3(3)F or 10.4(1)F to a version that supports both Native and LXC modes, the switch always goes to Native mode even if the upgrade was done from LXC mode. To keep the mode persistent after a downgrade, ensure that you perform the downgrade in the following sequence:

Note

- The following sections are applicable only to Nexus 9300-FX3 and 9300-GX platform switches.
- When system comes up in native mode on downgrade, boot mode lxc is removed from configuration.

- LXC mode upgrade/downgrade: For example,
  1. The switch is running on NX-OS Release 10.3(2)F in LXC mode.
  2. Upgrade the version to NX-OS Release 10.3(3)F (LXC mode).
  3. Downgrade the version to NX-OS Release 10.3(2)F to the Native mode.
  4. Execute the boot mode lxc configuration command, save the configuration, and reload the switch.
  5. The switch comes up in NX-OS Release 10.3(2)F LXC mode.

- Native mode upgrade/downgrade:

  Example 1

  1. The switch (9300-FX3 or 9300-GX) is running on NX-OS Release 10.3(2)F in the Native mode.
  2. Upgrade the version to NX-OS Release 10.3(3)F (LXC mode), as these (9300-FX3 or 9300-GX) switches support only LXC mode.
  3. Downgrade to any earlier NX-OS Release [for example, 10.3(2)].
  4. The switch comes up in NX-OS Release 10.3(2)F in Native mode.

  Example 2

  1. The switch (Nexus 9300-FX or 9300-FX2) is running on NX-OS Release 10.3(2)F in the Native mode.
  2. Upgrade the version to NX-OS Release 10.4(1)F (LXC mode), as these switches support only LXC mode.
  3. Downgrade to any earlier NX-OS Release [for example, 10.3(2)].
  4. The switch comes up in NX-OS Release 10.3(2)F in Native mode.

- When you downgrade from NX-OS Release 10.4(2)F to any earlier releases until 10.3(2)F (included), N9K-C9400-SW-GX2A Sup card ports 2xSFP Eth10/1-2 are not supported.
- When Nexus 9400 has feature security-group enabled, then downgrade from 10.5(1)F release to a lower release is not possible as feature security-group is not supported on 9400 in 10.4(3)F release and earlier.
- Downgrade of Nexus 9800 switches that have s1 image format from NX-OS Release 10.5(1)F to earlier releases that have cs image format is supported. However, as the s1 image is not present in earlier releases, the downgrade should be done to the cs image from the corresponding release.
- If you are on NX-OS Release 10.5(2)F, where DSVNI with IPv6 underlay feature is supported, and downgrade to a release that does not support this feature, then this leads to traffic loss for DSVNI VLANs. To avoid this, ensure that you remove the IPv6 underlay with downstream VNI configuration before downgrading.
- During downgrade, where both source and target images support Type-6 encryption, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, downgrade with binary restore retains the primary key after the reboot, provided both source and target images support Type-6 encryption.

If you downgrade the system from an image that supports Type-6 encryption to an image that does not support Type-6 encryption, compatibility check fails.

- When a switch is downgraded from NX-OS Release 10.6(1)F to any lower releases, the **allow feature-set fex** configuration gets added to the running configuration file.

Downgrade to an earlier software release

The downgrade of Nexus 9000 switches involves using the supported **install all** command to revert to an earlier NX-OS software release, ensuring compatibility by checking for software and hardware incompatibilities, disabling unsupported features, and following a structured procedure including saving configurations and reloading the switch.

Note Downgrade from 10.5(1)F, 10.5(2)F and 10.5(3)F releases is not supported to release 10.4(6)F and can result in the configuration loss or its corruption. If a downgrade from these releases to 10.4(6)F is necessary, downgrade first to 10.4(5)F and then upgrade to 10.4(6)F release or upgrade first to 10.5(4)F release and then downgrade to 10.4(6)F release. See CSCwr21007 in the *Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.4(7)M*.

Note If an error message appears during the downgrade, the downgrade fails due to the indicated reason. See the appropriate version of the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide for a list of possible causes and solutions.

Before you begin

Read the release notes for the software image file for any exceptions to this downgrade procedure. For information about software image file, see the appropriate version of the Cisco Nexus 9000 Series NX-OS Release Notes.

Procedure

Step 1 Log in to the device on the console port connection.

Step 2 Verify the software image file and copy it to the active supervisor module.

a) Verify that the image file for the downgrade is present on the active supervisor module bootflash.

Example:

```
switch# dir bootflash:
```

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

Note
If you need more space on the active or standby supervisor module bootflash, use the **delete** command to remove unnecessary files.

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

Example:

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

Step 3 Check for any incompatibilities.

a) Check for any software incompatibilities.

Example:

```
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.

b) Check for any hardware incompatibilities.

Example:

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

Step 4 Mitigate incompatibilities.

a) Disable any features that are incompatible with the downgrade image.

b) Power off any unsupported modules.

Example:

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

Step 5 Save the running configuration to the startup configuration.

Example:

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

Step 6 Downgrade the NX-OS software using the **install all nxos bootflash** <*nxos_image_to_downgrade*> command.

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 7 (Optional) Display the entire downgrade process.

Example:

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

Step 8 (Optional) Log in and verify that the device is running the required software version.

Example:

```
switch# show version
```