Cisco Nexus 3600 NX-OS Software Upgrade and Downgrade Guide, Release 7.x

First Published: 2018-06-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation for Cisco Nexus 3600 Platform Switches

The entire Cisco Nexus 3600 platform switch documentation set is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

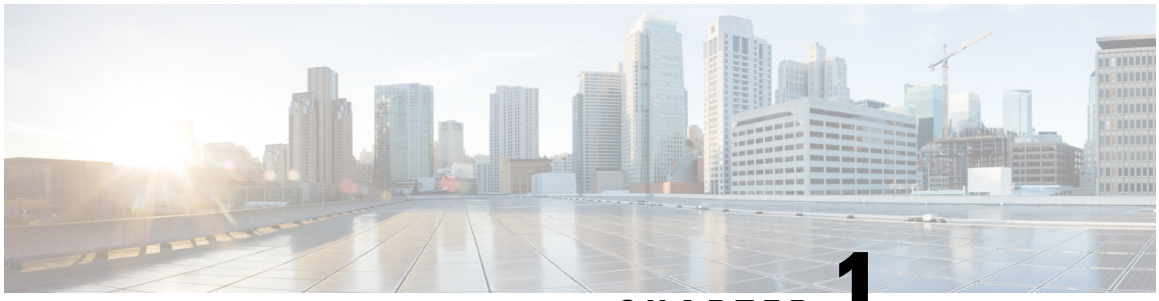
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Preface



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3600 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

• New and Changed Information, on page 1

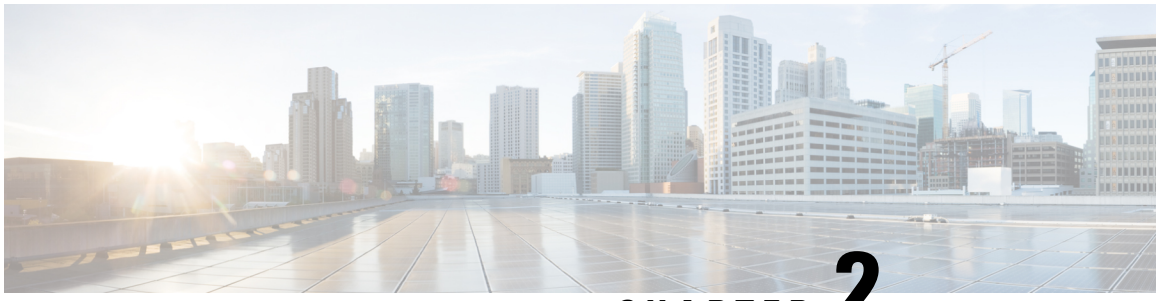
New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 3600 NX-OS Software Upgrade and Downgrade Guide, Release 7.x* and tells you where they are documented.

Table 1: New and Changed Features for Cisco NX-OS Release 7.x

Feature	Description	Changed in Release	Where Documented
No updates	Not applicable	7.0(3)F3(4)	Not applicable
No updates	Not applicable	7.0(3)F3(3a)	Not applicable
No updates	Not applicable	7.0(3)F3(3)	Not applicable
No updates	Not applicable	7.0(3)F3(2)	Not applicable

New and Changed Information



CHAPTER 2

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

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

About the Software Image

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of one NXOS software image. The image filename begins with "n3600" or "nxos," beginning with Cisco NX-OS Release 7.0(3)F3(4)] (for example, nxos.7.0.3.F3.4.bin).

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

Note Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename (for example, n9000-dk9.7.0.3.F3.4.**CSCab00001**.gbin). For more information on SMUs, see the Cisco Nexus 3600 NX-OS System Management Configuration Guide.

Recommendations for Upgrading the Cisco NX-OS Software

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

Prerequisites for Upgrading the Cisco NX-OS Software

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

- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device.

  On a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module during the Cisco NX-OS software upgrade if you have an active configuration session.
- Ensure that the device has a route to the remote server. The device and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets. To verify connectivity to the remote server, use the **ping** command.

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

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

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

Cisco NX-OS Software Upgrade Guidelines

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

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

- Schedule the upgrade when your network is stable and steady.

- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- Perform the installation on the active supervisor module, not the standby supervisor module.
- To upgrade from any release prior to Cisco NX-OS Release 7.0(3)F3(4), you must perform a write erase and reload the device. To upgrade from Cisco NX-OS Release 7.0(3)F3(4) to any later release, we recommend that you use the **install all** command, although we also support changing the boot variables and reloading the device.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the Cisco Nexus 3600 Series NX-OS Security Configuration Guide.
- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles [beginning with Cisco NX-OS Release 7.0(3)F3(1)], you have the option to move some of the running-configuration commands to a switch profile. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a nondisruptive upgrade.

Note ISSU is not supported on Cisco Nexus 3600 platform switches.

- The fast reload feature is not supported on Cisco Nexus 3600 platform switches.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade from a Cisco NX-OS 7.x release to a later 7.x release.

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

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

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

```
switch# dir bootflash:
 4096    May 21 14:49:07 2018  .rpmstore/
 4096    Aug 01 06:32:42 2017  .swtam/
 843257856    Feb 24 14:15:54 2018  nxos.7.0.3.F3.3.bin
```

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

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

```
switch# delete bootflash:nxos.7.0.3.F3.2.bin
```

Step 5 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 6 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.7.0.3.F3.4.bin
bootflash:nxos.7.0.3.F3.4.bin
```

Step 7 Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

```
switch# show file bootflash://sup-1/nxos.7.0.3.F3.4.bin sha256sum
5214d563b7985ddad67d52658af573d6c64e5a9792b35c458f5296f954bc53be
```

Step 8 Upgrade the Cisco NX-OS software using the **boot nxos bootflash:***filename* command.

```
switch# boot nxos bootflash:nxos.7.0.3.F3.4.bin
```

Step 9 Save the running configuration to the startup configuration.

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

Step 10 Erase the startup configuration file.

```
switch# write erase
```

Step 11 Reload the switch.

```
switch# reload
```

Step 12 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 13 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Prerequisites for Downgrading the Cisco NX-OS Software

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

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

Cisco NX-OS Software Downgrade Guidelines

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

- Software downgrades must be performed by doing a write erase and reloading the device.
-
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.
- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice, remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.

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

Downgrading to an Earlier Software Release

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

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

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

```
switch# dir bootflash:
4096    May 21 14:49:07 2018  .rpmstore/
4096    Aug 01 06:32:42 2017  .swtam/
843257856    Feb 24 14:15:54 2018  nxos.7.0.3.F3.4.bin
```

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

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

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

```
switch# copy scp://user@scpserver.cisco.com//download/bootflash:nxos.7.0.3.F3.3.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:nxos.7.0.3.F3.3.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

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

Step 8 Power off any unsupported modules.

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

Step 9 Downgrade the Cisco NX-OS software.

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

Step 10 Save the running configuration to the startup configuration.

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

Step 11 Erase the startup configuration file.

```
switch# write erase
```

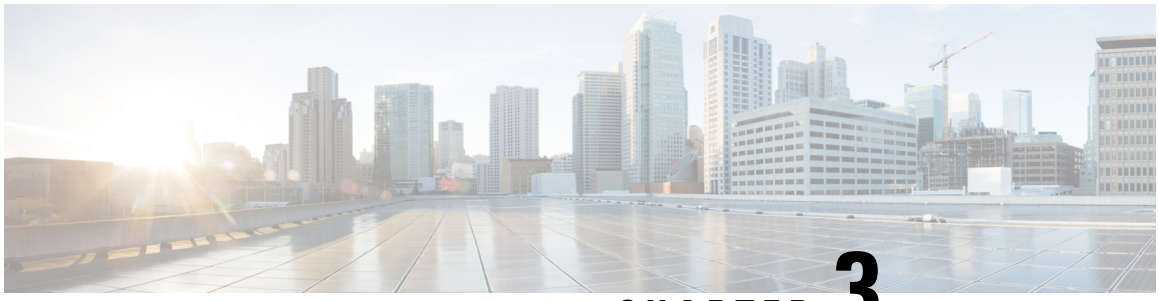
Step 12 Reload the switch.

Example:

```
switch# reload
```

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

```
switch# show version
```



CHAPTER 3

Migrating Switches in a vPC Topology

This chapter describes how to migrate from one pair of switches to another in a vPC topology. It contains the following sections:

vPC Forklift Upgrade

In a vPC topology, you can migrate from a pair of Cisco Nexus 3500 platform switches to a different pair of Cisco Nexus 3500 platform switches. For more information, see the *vPC Forklift Upgrade Scenario* section in the *Cisco Nexus 3500 Series NX-OS Interfaces Configuration Guide* on Cisco.com.

vPC Upgrade and Downgrade Process

The following list summarizes the upgrade and downgrade process in a vPC topology.

Note In vPC topologies, the two peer switches must be upgraded individually. An upgrade on one peer switch does not automatically update the vPC peer switch.

1. Switch A and B are running a Cisco NX-OS release. Switch A is the primary switch and switch B is the secondary switch. Use the **copy r s** command on both the switches.

```
secondary_switch# show vpc role
vPC Role status
----------------------------------------------------
vPC role : secondary
vPC system-mac : 00:23:04:ee:be:64
vPC system-priority : 32667
vPC local system-mac : 70:df:2f:eb:1c:ab
vPC local role-priority : 100
vPC peer system-mac : 70:df:2f:eb:86:1f
vPC peer role-priority : 90
secondary_switch#

primary_switch# show vpc role
vPC Role status
```

```
-------------------------------------------------
vPC role : primary
vPC system-mac : 00:23:04:ee:be:64
vPC system-priority : 32667
vPC local system-mac : 70:df:2f:eb:86:1f
vPC local role-priority : 90
vPC peer system-mac : 70:df:2f:eb:1c:ab
vPC peer role-priority : 100
BF-Leaf-2#

secondary_switch# copy r s v
[########################################] 100%
Copy complete.

primary_switch# copy r s v
[########################################] 100%
Copy complete.
```

2. Bring down the peer link (PL) on switch A. Switch B brings down its vPC legs.

```
primary_switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
primary_switch(config)# int port-channel 100
primary_switch(config-if)# shutdown

Reload switch B with H_dev image (change bootvar /reload)

secondary_switch(config)# boot nxos nxos.9.0.42.bin
Performing image verification and compatibility check, please wait....
secondary_switch(config)#
secondary_switch(config)# copy r s v
[########################################] 100%
Copy complete.


secondary_switch# reload
This command will reboot the system. (y/n)? [n] y


After reload
---------------------
secondary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is alive
Configuration consistency status : failed
Per-vlan consistency status : success
Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : none established
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 90s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
```

```
1 Po100 down -

secondary_switch#

primary_switch(config-if)# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 20
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs and BDs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled, timer is off.(timeout = 240s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 down -
```

3. Configure vPC auto-recovery under the vPC domain on switch B. Enable **vpc upgrade** (exec command).

```
secondary_switch(config)# vpc domain 100
secondary_switch(config-vpc-domain)# auto-recovery
secondary_switch(config-vpc-domain)# end

secondary_switch# show running-config vpc
!Command: show running-config vpc
!Running configuration last done at: Wed May 16 06:34:10 2018
!Time: Wed May 16 06:34:14 2018
version 7.0(3)IHD8(1) Bios:version 01.11
feature vpc
vpc domain 100
peer-switch
role priority 100
peer-keepalive destination 10.1.31.30 source 10.1.31.29
delay restore 90
peer-gateway
auto-recovery
ipv6 nd synchronize
ip arp synchronize
interface port-channel100
vpc peer-link
interface port-channel2001
vpc 101

secondary_switch# show vpc upgrade                      >> Hidden command
vPC upgrade : FALSE
SVI Timer : 10
Delay Restore Timer : 90
Delay Orphan Port Timer : 0



secondary_switch# vpc upgrade   >> exec command

secondary_switch# show vpc upgrade
```

```
vPC upgrade : TRUE
SVI Timer : 0
Delay Restore Timer : 0
Delay Orphan Port Timer : 0
secondary_switch#
```

4. After L3 routes are learned on switch B, reload switch A with the new release image. Switch B takes over the primary role and brings up its vPC legs in approximately 5 seconds.

```
primary_switch(config)# show boot
Current Boot Variables:
sup-1
NXOS variable = bootflash:/nxos.7.0.3.F3.4.bin
No module boot variable set
Boot Variables on next reload:
sup-1
NXOS variable = bootflash:/nxos.7.0.3.F3.4.bin_new_tor_source
No module boot variable set
primary_switch(config)# end

primary_switch# show boot
Current Boot Variables:
sup-1
NXOS variable = bootflash:/nxos.7.0.3.F3.4.bin_new_tor_source
No module boot variable set
Boot Variables on next reload:
sup-1
NXOS variable = bootflash:/nxos.7.0.3.F3.4.bin_new_tor_source
No module boot variable set
primary_switch# reload
This command will reboot the system. (y/n)? [n] y

secondary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is not reachable through peer-keepalive
Configuration consistency status : failed
Per-vlan consistency status : success
Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : primary
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status : Enabled, timer is off.(timeout = 240s)
Delay-restore status : Timer is off.(timeout = 0s)
Delay-restore SVI status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 down -
vPC status
```

5. When switch A comes back up, it brings up the peer link on switch A.

```
primary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary, operational secondary
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 90s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,101-400
```

6. For downgrade, reload both the switches at the same time.

INDEX