CHAPTER 5

Understanding In-Service Software Upgrades

This chapter describes the Cisco NX-OS in-service software upgrades (ISSU) and includes the following sections:

Information About ISSU

In a Nexus 7000 series chassis with dual supervisors, you can use the in-service software upgrade (ISSU) feature to upgrade the system software while the system continues to forward traffic. An ISSU uses the existing features of nonstop forwarding (NSF) with stateful switchover (SSO) to perform the software upgrade with no system downtime.

An ISSU is initiated through the command-line interface (CLI) by an administrator. When initiated, an ISSU updates (as needed) the following components on the system:

- Supervisor BIOS, kickstart image, and system image
- Module BIOS and image
- Connectivity Management Processor (CMP) BIOS and image

In a redundant system with two supervisors, one of the supervisors is active while the other operates in the standby mode. During an ISSU, the new software is loaded onto the standby supervisor while the active supervisor continues to operate using the old software. As part of the upgrade, a switchover occurs between the active and standby supervisors, and the standby supervisor becomes active and begins running the new software. After the switchover, the new software is loaded onto the (formerly active) standby supervisor.

Virtualization Support

An ISSU-based upgrade is a system-wide upgrade that applies the same image and versions across the entire system, including all configured virtual device contexts (VDCs). VDCs are primarily a control-plane and user-interface virtualization and cannot run independent image versions per virtualized resource.

Note For complete information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*.

Licensing Requirements

The following table shows the licensing requirements for system-level high availability features:

Product	License Requirement
Cisco NX-OS	The ISSU feature requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you.
VDC	VDC requires an Advanced Services license.

For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations

An ISSU has the following limitations and restrictions:

- Do not change any configuration settings or network connections during the upgrade. Any changes in the network settings may cause a disruptive upgrade.
- In some cases, the software upgrades may be disruptive. These exception scenarios can occur under the following conditions:
  - A single supervisor system with kickstart or system image changes.
  - A dual-supervisor system with incompatible system software images.
- Configuration mode is blocked during the ISSU to prevent any changes.
- Before you perform an ISSU from NX-OS release 5.2(x) to 6.0(x) or an ISSU / ISSD between any two NX-OS 6.0(x) releases, you must first remove QoS policies and ACLs from interfaces that are in the down state. If this is not performed, the installer process will abort the upgrade or downgrade process, and a message similar to the following will be displayed:

```
Service "ipqosmgr" : Please remove inactive policies using the command "clear
inactive-config qos" Pre-upgrade check failed. Return code 0x415E0055 (Need to clear
inactive-if-config from qos manager using the command "conf;clear inactive-config qos"
or can manually clear the config shown by the command: "show running-config ipqos
inactive-if-config").
```

Note The automatic command **clear inactive-config qos**, that clears inactive configuration, will delete the port channel policies even if one of the ports in a port channel has inactive policies. Guidelines for manual policy removal: During a manual removal, when the interface is part of a port channel, remove the policy map or access list from the port channel or remove the interface from the port channel before performing the ISSU or ISSD. For all other interface types, please remove the policy map or access list from the interface.

For more information about compatible upgrades and downgrades, see the *Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*.

How an ISSU Works

On a Nexus 7000 series with two supervisors, the ISSU process follows these steps:

1. Begins when the administrator uses the **install all** command
2. Verifies the location and integrity of the new software image files
3. Verifies the operational status and the current software versions of both supervisors and all switching modules to ensure that the system is capable of an ISSU
4. Loads the new software image to the standby supervisor and brings it up to the HA ready state
5. Forces a supervisor switchover
6. Loads the new software image to the (formerly active) standby supervisor and brings it up to the HA ready state
7. Performs a nondisruptive upgrade of each switching module, one at a time
8. Upgrades the Connectivity Management Processor (CMP)

During the upgrade process, the system presents detailed status information on the console, requesting administrator confirmation at key steps.

Configuring ISSU

For ISSU configuration details, see the *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x*.

Determining ISSU Compatibility

An ISSU may be disruptive if you have configured features that are not supported on the new software image. To determine ISSU compatibility, use the **show incompatibility system command**.

This example shows how to determine ISSU compatibility:

```
switch#  show incompatibility system bootflash:n7000-s1-dk9.4.1.4.bin
The following configurations on active are incompatible with  the system image
1) Service : vpc , Capability : CAP_FEATURE_VPC_ENABLED
Description : vPC feature is enabled
Capability requirement : STRICT
Disable command : Disable vPC using "no feature vpc"

2) Service : copp , Capability : CAP_FEATURE_COPP_DISTRIBUTED_POLICING
Description : Distributed policing for copp is enabled.
Capability requirement : STRICT
Disable command : Disable distributed policing using "no copp distributed-polici
ng enable”
```

Additional References

For additional information related to implementing ISSU, see the following sections:

Related Documents

Related Topic	Document Title
ISSU configuration	"Software Images" chapter of the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*
Virtual device context (VDC)	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*
Licensing	*Cisco NX-OS Licensing Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-SYSTEM-EXT-MIB: ciscoHaGroup, cseSwCoresTable, cseHaRestartNotify, cseShutDownNotify, cseFailSwCoreNotify, cseFailSwCoreNotifyExtended • CISCO-PROCESS-MIB • CISCO-RF-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No RFCs are supported by this feature	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html