Upgrading the Cisco VSG and the Cisco Prime NSC

This chapter contains the following sections:

Complete Upgrade Procedure

Table 1: Refer to the Section in Table Based on your Pre-upgrade Product Release

You are Upgrading From	Follow The Sequential Steps in the Following Section:
Cisco VSG Release 5.2(1)VSG1(4.1) to Release 5.2(1)VSG2(1.1a) and Cisco VNMC Release 2.1 to Cisco Prime NSC Release 3.2	Upgrade Procedures for Cisco VSG Release 5.2(1)VSG1(4.1) to Release 5.2(1)VSG2(1.1a) and Cisco VNMC 2.1 to Cisco Prime NSC Release 3.2. This includes upgrade procedures for Cisco Nexus 1000V Release 5.2(1)SM1(5.1) to Release 5.2(1)SM1(5.2).

To upgrade the Cisco Prime NSC, Cisco VSG, and Cisco Nexus 1000V, follow the steps sequentially:

1. Stage 1: Upgrading Cisco Prime NSC
2. Stage 2: Upgrading a Cisco VSG Pair
3. Stage 3: Upgrading the VSM pair and the VEMs

Note We highly recommend that you upgrade the Cisco VSG and the Cisco Prime NSC in the sequence listed. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco Prime NSC must be upgraded with the corresponding policy agent (PA).

Information About Cisco Prime NSC Upgrades

When you upgrade the Cisco Prime NSC software, all current (command-line interface) CLI and (graphical user interface) GUI sessions are interrupted, which means that you must restart any CLI or GUI sessions.

Information About Cisco VSG Upgrades

The upgrade procedure for a standalone Cisco VSG is hitful, which means that you must manually reload the Cisco VSG for the new image to become effective. In HA mode, the upgrade is hitless, which means that the standby Cisco VSG is upgraded first and then after a switchover, the previously active Cisco VSG is upgraded.

Because license information is not stored with the Cisco VSG but is maintained between the Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM), if packets are received at the Cisco VSG, that means that the license is valid and the packets are processed.

An upgrade affects two bin files: the kickstart file and the system file.

An upgrade does not erase any of the existing information, when the Cisco VSG comes online. Because the Cisco VSG is stateless, it gets all this information from the Cisco Prime NSC at bootup.

Upgrade Guidelines and Limitations

Before upgrading the Cisco Prime NSC, Cisco VSG, and Cisco Nexus 1000V, read the following:

- We highly recommend that you upgrade the Cisco VSG and the Cisco Prime NSC in the order provided. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco Prime NSC must be upgraded with the corresponding policy agent (PA).
- Before upgrading to a new VSG version with VSG Universal License (UL), make sure that you change VSM mode to advanced and save the configuration. Installing VSG with UL without changing the VSM mode to advanced may cause VSG service failure.
- We recommend that you take a snapshot or backup (clone) of the original Cisco Prime NSC and VSM prior to the upgrade process and then perform an ISSU upgrade process on both the VSM and the Cisco VSG. We do not recommend that you perform a manual upgrade.
- For a full In-service Software Upgrade (ISSU) upgrade on both the Cisco VSG and VSM, follow these rules:
  - Install the Cisco Prime NSC before installing the Cisco VSG and VSM. The ISSU upgrade installs a new PA.
  - A new PA with an old Cisco Prime NSC is not supported and there should never be an interim stage in this state.
  - A copy run start is not required after the VSM upgrade.

- Upgrade instructions include the following information:
  - Different stages of complete upgrade procedures and operations which are supported at different stages.
  - Different component versions after each stage.
  - Different operations supported after each stage.

Upgrade Procedure for Cisco VSG Release 5.2(1)VSG1(4.1) to Release 5.2(1)VSG2(1.1a), Cisco VNMC Release 2.1 to Cisco Prime NSC Release 3.2 and Cisco Nexus 1000V Release 5.2(1)SM1(5.1) to Release 5.2(1)SM1(5.2)

Cisco VSG Release 5.2(1)VSG1(4.1) to 5.2(1)VSG2(1.1a) and Cisco VNMC 2.1 to Cisco Prime NSC 3.0.2 to Cisco Prime NSC 3.2 Staged Upgrade

Virtual Appliance	Original State	Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade	Stage 3: VSM/VEM Upgrade
Cisco Prime NSC	Old Cisco VNMC 2.1	New Cisco Prime NSC 3.0.2	New Cisco Prime NSC 3.0.2	New Cisco Prime NSC 3.0.2
	New Cisco Prime NSC 3.0.2	New Cisco Prime NSC 3.2	New Cisco Prime NSC 3.2	New Cisco Prime NSC 3.2
Cisco VSG	Old 5.2(1)VSG1(4.1)	Old 5.2(1)VSG1(4.1)	New 5.2(1)VSG2(1.1a)	New 5.2(1)VSG2(1.1a)
VSG PA	Old 2.0	Old 2.0	New 2.1	New 2.1
VSM	Old 5.2(1)SM1(5.1)	Old 5.2(1)SM1(5.1)	Old 5.2(1)SM1(5.1)	New 5.2(1)SM1(5.2)
VEM	Old 4.2(1)SV1(5.2b)	Old 4.2(1)SV1(5.2b)	Old 4.2(1)SV1(5.2b)	New 4.2(1)SV2(2.1)
VSM PA	Old 2.0	Old 2.0	Old 2.0	New 3.2

Virtual Appliance	Original State	Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade	Stage 3: VSM/VEM Upgrade
Supported operations after upgrading to each stage	All operations supported	• Existing data sessions (offloaded). • New data sessions. • Allows Cisco Nexus 1000V switch (non-vservice) operations including non-vservice port profiles.	• Short disruption in new data session establishment during the Cisco VSG upgrade. • Other operations are fully supported. • Full Layer 3 VSG and VM VLAN support.	• All operations are supported if all the upgrades including VEMs are successful. • Restricted operations (below) apply only if all VEMs are not upgraded • Disruption of data traffic during VEM upgrades. • Layer 3 VSG and VM VLAN support.

Virtual Appliance	Original State	Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade	Stage 3: VSM/VEM Upgrade
Restricted operations after upgrading to each stage	None	• No Cisco Prime NSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No Vmotion of vservice firewalled VMs on N1k • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco Prime NSC to VSG control operations are restricted).	• No Cisco Prime NSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No Vmotion of vservice firewalled VMs on N1k. • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco Prime NSC to VSG control operations are restricted).	**The following restricted operations apply only if all VEMs are not upgraded:** • No Cisco Prime NSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No boot strap of devices (VNMC, VSM,VSG). • No Vmotion of vservice VMs on N1k. • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • No N1k switch (non vservice) operations, including non-vservice PPs (VSM+VEM ugraded) (All VSM to Cisco Prime NSC to VSG control operations are restricted).

Note ISSU upgrade is not supported for VSG and VSM that involves installing a new PA. However, on both , you should install the Cisco Prime NSC first. The new PA may not support the old VNMC.

Upgrading VNMC Release 2.1 to Cisco Prime NSC 3.0.2

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco Prime NSC Release 3.0.2 downloaded.
- You have added two hard disks to the VNMC VM. For more information on Cisco Prime NSC requirements, see System Requirements.

SUMMARY STEPS

1. nsc# **connect local-mgmt**
2. (Optional) nsc (local-mgmt)# **show version**
3. (Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/***filename*
6. (Optional) nsc (local-mgmt)# **service status**
7. (Optional) nsc (local-mgmt)# **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	nsc# **connect local-mgmt**	Places you in local management mode.
Step 2	nsc (local-mgmt)# **show version**	(Optional) Displays the version information for the Cisco Prime NSC software.
Step 3	nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	(Optional) Copies the Cisco Prime NSC software file to the VM.
Step 4	nsc (local-mgmt)# **dir bootflash:/**	Verifies that the desired file is copied in the directory.
Step 5	nsc (local-mgmt)# **update bootflash:/***filename*	Begins the update of the Cisco Prime NSC software.

	Command or Action	Purpose
Step 6	nsc (local-mgmt)# **service status**	(Optional) Allows you to verify that the server is operating as desired.
Step 7	nsc (local-mgmt)# **show version**	(Optional) Allows you to verify that the Cisco Prime NSC software version is updated. **Note** After you upgrade to Cisco Prime NSC Release 3.0.2, you might see the previous version of Cisco VNMC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco VNMC:

```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
----                -------             -------        ----
core                Base System         2.1            2.1
service-reg         Service Registry    2.1            2.1
policy-mgr          Policy Manager      2.1            2.1
resource-mgr        Resource Manager    2.1            2.1
vm-mgr              VM manager          2.1            none
```

The following example shows how to copy the Cisco Prime NSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.0.2e.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

The following example shows how to see the directory information for Cisco Prime NSC:

```
nsc(local-mgmt)# dir bootflash:/

    1.1G Oct 14 00:57 nsc.3.0.2e.bin

Usage for bootflash://

             6359716 KB used
            10889320 KB free
            18187836 KB total
```

The following example shows how to start the update for the Cisco Prime NSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.0.2e.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.0(2e)        3.0(2e)
service-reg         Service Registry    3.0(2e)        3.0(2e)
policy-mgr          Policy Manager      3.0(2e)        3.0(2e)
resource-mgr        Resource Manager    3.0(2e)        3.0(2e)
vm-mgr              VM manager          3.0(2e)        none
cloudprovider-mgr   Cloud Provider Mgr  3.0(2e)        none
```

Upgrading Cisco Prime NSC 3.0.2 to Cisco Prime NSC 3.2

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco Prime NSC Release 3.2 downloaded.
- You have added two hard disks to the Cisco Prime NSC VM. For more information on Cisco Prime NSC requirements, see System Requirements.

SUMMARY STEPS

1. nsc# **connect local-mgmt**
2. (Optional) nsc (local-mgmt)# **show version**
3. (Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/***filename*
6. (Optional) nsc (local-mgmt)# **service status**
7. (Optional) nsc (local-mgmt)# **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	nsc# **connect local-mgmt**	Places you in local management mode.
Step 2	nsc (local-mgmt)# **show version**	(Optional) Displays the version information for the Cisco Prime NSC software.

	Command or Action	Purpose
Step 3	nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	(Optional) Copies the Cisco Prime NSC software file to the VM.
Step 4	nsc (local-mgmt)# **dir bootflash:/**	Verifies that the desired file is copied in the directory.
Step 5	nsc (local-mgmt)# **update bootflash:/***filename*	Begins the update of the Cisco Prime NSC software.
Step 6	nsc (local-mgmt)# **service status**	(Optional) Allows you to verify that the server is operating as desired.
Step 7	nsc (local-mgmt)# **show version**	(Optional) Allows you to verify that the Cisco Prime NSC software version is updated. **Note** After you upgrade to Cisco Prime NSC Release 3.2, you might see the previous version of Cisco Prime NSC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version

Name                 Package             Version        GUI
---- ------- ------- ----
core                 Base System         3.0(2e)        3.0(2e)
service-reg          Service Registry    3.0(2e)        3.0(2e)
policy-mgr           Policy Manager      3.0(2e)        3.0(2e)
resource-mgr         Resource Manager    3.0(2e)        3.0(2e)
vm-mgr               VM manager          3.0(2e)        none
cloudprovider-mgr    Cloud Provider Mgr  3.0(2e)        none
```

The following example shows how to copy the Cisco Prime NSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.2.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

The following example shows how to see the directory information for Cisco Prime NSC:

```
nsc(local-mgmt)# dir bootflash:/

    1.1G Oct 14 00:57 nsc.3.2.bin

Usage for bootflash://

             6359716 KB used
            10889320 KB free
            18187836 KB total
```

The following example shows how to start the update for the Cisco Prime NSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.2.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version

Name                 Package              Version        GUI
---- ------- ------- ----
core                 Base System          3.2        3.2
service-reg          Service Registry     3.2        3.2
policy-mgr           Policy Manager       3.2        3.2
resource-mgr         Resource Manager     3.2        3.2
vm-mgr               VM manager           3.2        none
cloudprovider-mgr    Cloud Provider Mgr   3.2        none
```

Upgrading Cisco VSG from Release 5.2(1)VSG1(4.1) to 5.2(1)VSG2(1.1a)

This section includes the following topics:

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have closed all the active VSG configuration sessions before upgrading the Cisco VSG software.
- You have copied the kickstart and system images from the remote server to the Cisco Nexus 1000V.

Cisco VSG Software Upgrade Guidelines

Follow these VSG upgrade guidelines while upgrading the VSG:

- Schedule the upgrade when the network is stable. Ensure that nobody is configuring the switch during the upgrade.
- Ensure that sufficient space is available for copying the upgrade images. A minimum of 200 MB of free bootflash space is required on both the active and standby VSGs.
- Avoid power interruptions to the hosts running the VSG VMs during any installation procedure.
- Ensure that the management (mgmt0) interface of the VSG is working and accessible.

- Ensure that the specified system and kickstart images are compatible with each other.
- Verify connectivity to the remote server by using the ping command.

Upgrade a VSG Pair in HA Mode

You can upgrade VSG pair in the High Availability (HA) mode.

SUMMARY STEPS

1. Log in to the active VSG.
2. Display the current boot variables.
3. Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.
4. Verify that required space is available on the standby VSG. Delete unnecessary files if required to create more space available for copying the new VSG image.
5. Copy the Cisco Nexus 1000V kickstart and system software files to a server.
6. Remove current boot variables.
7. Display the current boot variables.
8. Load the new boot variables and copy the running configuration to the startup configuration.
9. Display the current boot variables.
10. Manually reboot the system.
11. After the installation operation completes, log in and verify that the switch is running the upgraded software version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Display the current boot variables.

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
```

```
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

Step 3 Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

Step 4 Verify that required space is available on the standby VSG. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir bootflash://sup-standby/
.
.
.
Usage for bootflash://sup-standby
  577372160 bytes used
 5826600960 bytes free
 6403973120 bytes total
```

Step 5 Copy the Cisco Nexus 1000V kickstart and system software files to a server.

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
 ./
vsg(config)#copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.1.1a.bin ./
```

Step 6 Remove current boot variables.

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

Step 7 Display the current boot variables.

```
vsg(config)#  show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

Step 8 Load the new boot variables and copy the running configuration to the startup configuration.

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
```

```
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
vsg(config)# copy running-config startup-config
```

Step 9 Display the current boot variables.

```
vsg(config)#  show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set
```

Step 10 Manually reboot the system.

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

If you want to continue with the reboot, press Y.
```

Note The system reboot takes approximately 10 seconds.

Step 11 After the installation operation completes, log in and verify that the switch is running the upgraded software version.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 5.2(1)VSG2(1.1a)
  system:    version 5.2(1)VSG2(1.1a)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
  system compile time:     12/6/2013 16:00:00 [12/06/2013 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
```

```
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB

Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

Upgrading a Device for Standalone VSG

SUMMARY STEPS

1. Log in to the active VSG.
2. Use the show boot command to display the current boot variables.
3. Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.
4. Copy the Cisco Nexus 1000V kickstart and system software files to a server.
5. Remove current boot variables.
6. Display the current boot variables.
7. Load the new boot variables and copy the running configuration to the startup configuration.
8. Display the current boot variables.
9. Manually reboot the system.
10. After the installation operation completes, log in and verify that the switch is running the upgraded software version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Use the show boot command to display the current boot variables.

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set

Boot Variables on next reload:
```

```
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

Step 3 Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

Step 4 Copy the Cisco Nexus 1000V kickstart and system software files to a server.

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
 ./
```

Step 5 Remove current boot variables.

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

Step 6 Display the current boot variables.

```
vsg(config)# show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

Step 7 Load the new boot variables and copy the running configuration to the startup configuration.

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
vsg(config)# copy running-config startup-config
```

Step 8 Display the current boot variables.

```
vsg(config)#  show boot
Current Boot Variables:
```

```
sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

Step 9 Manually reboot the system.

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

If you want to continue with the reboot, press Y.
```

Note The system reboot takes approximately 10 seconds.

Step 10 After the installation operation completes, log in and verify that the switch is running the upgraded software version.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 5.2(1)VSG2(1.1a)
  system:    version 5.2(1)VSG2(1.1a)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
  system compile time:     12/6/2013 16:00:00 [12/06/2013 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB
```

```
Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

Re-registering the Policy Agent with the Upgraded VSG

You need to re-register the policy agent after upgrading the Cisco VSG.

SUMMARY STEPS

1. Log in to the active VSG.
2. Check the current policy agent version.
3. Enter the configuration mode.
4. Unregister the old policy agent from VSG.
5. Register the new policy agent with the VSG.
6. Copy the current running configuration to the startup configuration.
7. Verify the updated policy agent version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Check the current policy agent version.

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsg
VSG#
```

Step 3 Enter the configuration mode.

```
vsg# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSG(config)#
```

Step 4 Unregister the old policy agent from VSG.

```
VSG(config)# nsc-policy-agent
VSG(config-nsc-policy-agent)# no policy-agent-image
```

Step 5 Register the new policy agent with the VSG.

```
VSG(config-nsc-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.2.1.1e.bin
VSG(config-nsc-policy-agent)# exit
VSG(config)#
```

Step 6 Copy the current running configuration to the startup configuration.

```
VSG(config)# copy running startup
[########################################] 100%
```

Step 7 Verify the updated policy agent version.

```
VSG(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
VSG(config)#
```

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V platform involves:

- Upgrading the VSM
- Upgrading the Cisco VSEM
- Upgrading the VEM Software

For detailed information about upgrading the Cisco Nexus 1000V for Microsoft Hyper-V, see the Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V chapter in Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide, available at: http://www.cisco.com/en/US/partner/products/ps13056/prod_installation_guides_list.html