Upgrading the Cisco Nexus 1000V

This chapter contains the following sections:

Information About the Software Upgrade

Upgrade Software Sources

Note An interactive upgrade tool has been provided to assist you in determining the correct upgrade steps based on your current environment and the one to which you want to upgrade.

You can obtain your upgrade-related software from the following sources listed in this table:

Table 1: Obtaining the Upgrade Software

Source	Description
Cisco	Download the current release of the Cisco Nexus 1000V software from http://www.cisco.com/en/US/products/ps9902/index.html.
VMware	Download the VMware software from the VMware website. The current Cisco Nexus 1000V software release image for VMware Release 5.1 is at the VMware web site: • Online portal for VMware Update Manager (VUM): http://hostupdate.vmware.com/software/VUM/PRODUCTION/csco-main/esx/csco/csco-index.xml • Offline patch portal: http://www.vmware.com/patchmgr/download.portal

For information about your software and platform compatibility, see the *Cisco Nexus 1000V and VMware Compatibility Information* document.

Information about NetFlow Upgrade

With Distributed NetFlow, the switch sends NetFlow export packets directly from the VEMs to the collectors.

During the upgrade process, the switch migrates from the old centralized model to the new distributed model. As part of this migration, unsupported commands are removed and/or converted as part of the VSM upgrade. The new and changed commands are available as soon as all of the VEMs are upgraded and the feature level is updated. Additionally, the following new requirements are imposed on the network reachability:

- The collectors must be Layer 3 reachable from at least one vmknic on each VEM host.
- Strict Reverse Path Forwarding (RPF) might need to be disabled on the routers between the VEM hosts and the collectors.

These are the removed, converted, and new commands:

Command	Change
cache size	Removed. The cache size is no longer user configurable.

Command	Change
timeout active **timeout inactive**	Converted. The configured **timeout active** and **timeout inactive** values are consolidated and converted to be the **flow timeout active** and **flow timeout inactive** values. The new consolidated timeouts are set to the maximum of the old individual timeouts. **Note** After conversion, subsequent changes to the timeouts do not apply to the existing interface configurations on non-upgraded VEMs.
source mgmt	Converted. The configured **source mgmt** values are converted to be the **source lc-exp** values. The NetFlow export packets are no longer sent from the VSM's mgmt0 interface.
netflow layer2-switched input	New. The **netflow layer2-switched input** command configures the Layer 2 default record.
match datalink	New. The **match datalink** command configures the Layer 2 record fields.

Prerequisites for the Upgrade

Before You Begin

The Virtual Service Domain (VSD) feature is no longer supported and must be removed before upgrading to Release 5.2(1)SV3(1.3).

The Upgrade Application cannot be used for the direct upgrade of the Virtual Supervisor Module(VSMs) from Releases 4.2(1)SV1(4), 4.2(1)SV1(5.1), 4.2(1)SV1(5.2), 5.2(1)SV3(1.1), and 5.2(1)SV3(1.2) to the current release.

A pair of VSMs in a high availability (HA) pair is required in order to support a nondisruptive upgrade.

A system with a single VSM can only be upgraded in a disruptive manner.

The network and server administrators must coordinate the upgrade procedure with each other.

The upgrade process is irrevocable. After the software is upgraded, you can downgrade by removing the current installation and reinstalling the software. For more information, see the "Recreating the Installation" section of the *Cisco Nexus 1000V Troubleshooting Guide*.

A combined upgrade of ESX and the Virtual Ethernet Module (VEM) in a single maintenance mode is supported in this release. A combined upgrade requires at least vCenter 5.0 Update 1 whether you upgrade manually or are using the VMware Update Manager.

You can manually upgrade the ESX and VEM in one maintenance mode as follows:

1. Place the host in maintenance mode.
2. Upgrade ESX to 5.0 or 5.1 as needed.
3. Install the VEM vSphere Installation Bundle (VIB) while the host is still in maintenance mode.
4. Remove the host from maintenance mode.

The steps for the manual combined upgrade procedure do not apply for VMware Update Manager (VUM)-based upgrades.

You can abort the upgrade procedure by pressing Ctrl-C.

Prerequisites for Upgrading VSMs

Upgrading VSMs has the following prerequisites:

- Close any active configuration sessions before upgrading the Cisco Nexus 1000V software.
- Save all changes in the running configuration to the startup configuration.
- Save a backup copy of the running configuration in external storage.
- Perform a VSM backup. For more information, see the "Configuring VSM Backup and Recovery" chapter in the *Cisco Nexus 1000V System Management Configuration Guide*.
- Use the VSM management IP address to log into VSM and perform management tasks.

Important If you connect to a VSM using the VSA serial port or the connect host from the Cisco Integrated Management Control (CIMC), do not initiate commands that are CPU intensive, such as copying image from the TFTP server to bootflash or generating a lot of screen output or updates. Use the VSA serial connections, including CIMC, only for operations such as debugging or basic configuration of the VSA.

Prerequisites for Upgrading VEMs

Caution If VMware vCenter Server is hosted on the same ESX/ESXi host as a Cisco Nexus 1000V VEM, a VUM-assisted upgrade on the host fails. You should manually VMotion the vCenter Server VM to another host before you perform an upgrade.

Note When you perform any VUM operation on hosts that are a part of a cluster, ensure that VMware HA, VMware fault tolerance (FT), and VMware Distributed Power Management (DPM) features are disabled for the entire cluster. Otherwise, VUM will fail to install the hosts in the cluster.

- If you have VXLAN Gateway installed in your deployment, we recommend that you upgrade the VXLAN gateway service module after upgrading the VSM and *before* upgrading the VEM. This recommendation applies to upgrades to Release 5.2(1)SV3(1.1) and later only.
- You are logged in to the VSM command-line interface (CLI) in EXEC mode.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VEM software file from one of the sources listed in VEM Software. For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information* document.
- If you need to migrate a vSphere host from ESX to ESXi, do it before the Cisco Nexus 1000V upgrade.
- You have placed the VEM software file in `/tmp` on the vSphere host. Placing it in the root (/) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space by entering the **vdf** command.
- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series switches with the Cisco IOS software, enter the **portfast trunk** command or the **portfast edge trunk** command.
  - On Cisco Nexus 5000 Series switches with the Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:
  - **spanning-tree bpdu filter**
  - **spanning-tree bpdu guard**
- The collectors must be L3 reachable from at least one vmknic on each VEM host.
- Strict Reverse Path Forwarding (RPF) may require disabling on the routers between the VEMs and the collectors.
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

Prerequisite to Upgrading a VSM to a 3-GB Hard Disk Drive

Cisco Nexus 1000V for VMware Release 5.2(1)SV3(1.x) and higher requires a minimum of 3-GB of hard disk drive (HDD) space. If you are upgrading from a previous release to Release 5.2(1)SV3(1.x) and you have a 2-GB HDD, you must upgrade to a 3-GB HDD.

Upgrading Hard Disk Drive Space from 2 GB to 3 GB on a VSM as a VM

We recommend that you upgrade the hard disk drive (HDD) space from 2 GB to 3 GB on a VSM VM before upgrading VSM to Release 5.2(1)SV3(1.1) or later.

Before You Begin

Make sure that the Cisco Nexus 1000V VSMs are running Release 4.2(1)SV2(1.1) or 4.2(1)SV2(2.1).

Make sure that the existing Cisco Nexus 1000V VSMs are an HA pair with 2 GB HDD.

Procedure

Step 1 Remove the existing standby VSM.

a) Right-click on the VSM VM and power off the VM.
b) Remove it from the Virtual Center inventory.

Step 2 Bring up the new standby VSM VM (with 3-GB HDD) with the same release as the active VSM using ISO. For example, if the active VSM is running Release 4.2(1)SV2(1.1), bring up the new standby VSM with Release 4.2(1)SV2(1.1).

a) Confirm that the same port profiles are used as the primary VSM for 3 network interfaces.
b) Provision a 3-GB HDD with a minimum of 2 GB of RAM reserved and allocated, and has a minimum CPU speed of 1600 MHz.

See Installing the Software from the ISO Image for more information.

Step 3 Power on the standby VSM.

a) Confirm the HA role is set as Secondary.
b) Configure the Domain ID is the same as the Primary VSM.

Step 4 After the HA pair is formed, perform a system switchover to make the standby VSM become the active VSM.

Step 5 Remove the current standby VSM.

a) Right-click on the VSM VM and power off the VM.
b) Remove it from the Virtual Center inventory.

Step 6 Change the Active VSM system redundancy role to Primary system by entering **system redundancy role primary**.

Step 7 Copy the config to start-up and perform a reload.

Step 8 Verify the current role by entering **show system redundancy status**. Role should be set as Primary.

Step 9 Bring up the new standby VSM VM (with 3-GB HDD) using ISO following Step 2 and Step 3.

Step 10 After the HA pair is formed, verify it by entering **show system internal flash**. It should reflect the VSM with 3-GB HDD.

What to Do Next

Perform an in-service software upgrade (ISSU) to Release 5.2(1)SV3(1.1) or later.

Upgrading Hard Disk Drive Space from 2 GB to 3 GB on a VSM on a VSB

We recommend that you upgrade the VSM that is deployed on a CSP from a 2-GB hard disk drive (HDD) to a 3-GB HDD.

Procedure

Step 1 Identify the standby VSM by entering the **show virtual-service-blade summary** command.

```
N1110# show virtual-service-blade summary

Name                      HA-Role     HA-Status     Status                Location
------------------------------------------------------------------------------
switch                    PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
switch                    SECONDARY   STANDBY     VSB POWERED ON           SECONDARY

N1110#
```

The output shows that the standby VSM is running on the secondary Cisco Nexus 1010 Virtual Service Blade (VSB).

Step 2 Shut down and delete the standby VSM on the secondary VSB.

a) N1110# **configure terminal**
b) N1110#(config)**virtual-service-blade** name switch
c) N1110#(config-vsb-config)**shutdown secondary**
d) N1110#(config-vsb-config)**no enable secondary**

Step 3 Bring up the new secondary VSB with Release 4.2(1)SV2(1.1) using ISO.
See the Cisco Nexus 1100 Series Virtual Services Appliances Deployment Guide White Paper for more information.

Step 4 Change the disk size to 3 GB or more.

```
N1110(config-vsb-config)# disksize 4
```

Step 5 Enable the standby VSM on the secondary VSB.
See the Cisco Nexus 1100 Series Virtual Services Appliances Deployment Guide White Paper for more information.

```
N1110# sh virtual-service-blade summary

------------------------------------------------------------------------------
Name                      HA-Role     HA-Status   Status                  Location
------------------------------------------------------------------------------
switch                    PRIMARY     ACTIVE      VSB POWERED ON          PRIMARY
switch                    SECONDARY   NONE        VSB NOT PRESENT         SECONDARY
switch1                   PRIMARY     NONE        VSB NOT PRESENT         PRIMARY
switch1                   SECONDARY   STANDBY     VSB POWERED ON          SECONDARY

N1110#
```

Step 6 Perform a system switchover to make the active VSM on the primary VSB become the standby VSM. To do this, enter the **system switchover** command on the active VSM.

```
N1110# system switchover
N1110(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                 HA-Role     HA-Status   Status                   Location
--------------------------------------------------------------------------------
switch                   PRIMARY     STANDBY     VSB POWERED ON           PRIMARY
switch                   SECONDARY   NONE        VSB NOT PRESENT          SECONDARY
switch1                  PRIMARY     NONE        VSB NOT PRESENT          PRIMARY
switch1                  SECONDARY   ACTIVE      VSB POWERED ON           SECONDARY

N1110(config-vsb-config#
```

Step 7 After the HA pair is formed, shutdown and delete the standby VSM on the primary VSB.

```
N1110(config)# virtual-service-blade switch
N1110(config-vsb-config)# shutdown primary
N1110(config-vsb-config)# no enable primary

N1110(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                HA-Role     HA-Status   Status                   Location
--------------------------------------------------------------------------------
switch                   PRIMARY     NONE        VSB NOT PRESENT          PRIMARY
switch                   SECONDARY   NONE        VSB NOT PRESENT          SECONDARY
switch1                  PRIMARY     NONE        VSB NOT PRESENT          PRIMARY
switch1                  SECONDARY   ACTIVE      VSB POWERED ON           SECONDARY

N1110(config-vsb-config)#
```

Step 8 Bring up the new VSB with Release 4.2(2)SV2(1.1) using ISO.
See the Cisco Nexus 1100 Series Virtual Services Appliances Deployment Guide White Paper for more information.

Step 9 Enable the primary VSM.
See the Cisco Nexus 1100 Series Virtual Services Appliances Deployment Guide White Paper for more information.

```
N1110(config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                     HA-Role     HA-Status   Status                   Location
--------------------------------------------------------------------------------
switch                   PRIMARY     NONE        VSB NOT PRESENT          PRIMARY
switch                   SECONDARY   NONE        VSB NOT PRESENT          SECONDARY
switch1                  PRIMARY     STANDBY     VSB POWERED ON           PRIMARY
switch1                  SECONDARY   ACTIVE      VSB POWERED ON           SECONDARY

N1110(config-vsb-config)#
```

Step 10 Verify that the HDD size has changed. The following example shows that the HDD size is 4 GB.

```
N1110(config)# show system internal flash

Mount-on                 1K-blocks      Used   Available   Use%  Filesystem
        /                           307200     87628      219572     29   /dev/root
```

```
        /proc                          0         0         0      0   proc
        /isan                     614400    243076    371324     40   none
        /var/sysmgr               512000     18896    493104      4   none
        /var/sysmgr/ftp           204800        40    204760      1   none
        /dev/shm                  358400     30268    328132      9   none
        /volatile                  20480         0     20480      0   none
        /debug                      2048         8      2040      1   none
        /dev/mqueue                    0         0         0      0   none
        /mnt/cfg/0                326681      8360    301455      3   /dev/hda5
        /mnt/cfg/1                326681      8359    301456      3   /dev/hda6
        /var/sysmgr/startup-cfg   409600      1168    408432      1   none
        /dev/pts                       0         0         0      0   devpts
        /mnt/pss                  326671      8625    301178      3   /dev/hda3
        /bootflash               3122988    151756   2812592      6   /dev/hda4
        /bootflash_sup-remote    3122992    151760   2812592      6
127.1.1.1:/mnt/bootflash/
```

What to Do Next

Perform an in-service software upgrade (ISSU) to Release 5.2(1)SV3(1.1) or later.

Verifying that the VSM has 3-GB of Hard Disk Drive Storage

You can display the system internal flash to verify that you have a minimum of 3-GB of hard disk drive space.

Procedure

Step 1 Display the system internal flash.

```
switch# show system internal flash
Mount-on                  1K-blocks      Used   Available   Use%  Filesystem
/                            307200     77808      229392     26   /dev/root
/mnt/pss                     248895      8164      227879      4   /dev/sda3
/proc                             0         0           0      0   proc
/isan                        614400    372236      242164     61   none
/var/sysmgr                 1048576    488704      559872     47   none
/var/sysmgr/ftp              204800        52      204748      1   none
/nxos/tmp                     20480         0       20480      0   none
/dev/shm                     358400     89660      268740     26   none
/volatile                     20480         0       20480      0   none
/debug                         2048       128        1920      7   none
/dev/mqueue                       0         0           0      0   none
/mnt/cfg/0                   248895      4494      231551      2   /dev/sda5
/mnt/cfg/1                   241116      4493      224175      2   /dev/sda6
/var/sysmgr/startup-cfg      409600      5892      403708      2   none
/dev/pts                          0         0           0      0   devpts
/mnt/pss                     248895      8164      227879      4   /dev/sda3
/bootflash                  2332296   1918624      295196     87   /dev/sda4
/sys                              0         0           0      0   sysfs
```

Step 2 Make sure that the number of blocks allocated to the /mnt/cfg/0, /mnt/cfg/1, /mnt/pss, and /bootflash partitions equals at least 3 GB.

Guidelines and Limitations for Upgrading the Cisco Nexus 1000V

Before attempting to migrate to any software image version, follow these guidelines:

Caution During the upgrade process, the Cisco Nexus 1000V does not support any new additions such as modules, virtual NICs (vNICs), or VM NICs and does not support any configuration changes. VM NIC and vNIC port-profile changes might render VM NICs and vNICs in an unusable state.

Note We recommended that you use vSphere 5.0 Update 1 or later instead of vSphere 5.0.

- You are upgrading the Cisco Nexus 1000V software to the current release.
- Scheduling—Schedule the upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- Hardware—Avoid power interruptions to the hosts that run the VSM VMs during any installation procedure.
- Connectivity to remote servers — do the following:
  - Copy the kickstart and system images from the remote server to the Cisco Nexus 1000V.
  - Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.
- Software images— Do the following:
  - Make sure that the system and kickstart images are the same version.
  - Retrieve the images in one of two ways:
    - Locally—Images are locally available on the upgrade CD-ROM/ISO image.
    - Remotely—Images are in a remote location and you specify the destination using the remote server parameters and the filename to be used locally.
- Commands to use—Do the following:
  - Verify connectivity to the remote server by using the **ping** command.
  - If you are using Layer 3 mode for VSM-to-VEM connectivity, verify the IP address on the Layer 3 control interface using the **show interface** {**control0** | **mgmt0**} command. If the IP address is missing, re-apply the IP address configuration on the corresponding Layer 3 control interface.

- Use the **install all** command to upgrade your software. This command upgrades the VSMs.
- Do not enter another **install all** command while running the installation. You can run commands other than configuration commands.
- During the VSM upgrade, if you try to add a new VEM or any of the VEMs are detached due to uplink flaps, the VEM attachment is queued until the upgrade completes.
- If VEMs get removed after the VSM upgrade, use the **system switchover** command to perform a system switchover after the HA pair is established.

Note If the ESX hosts are not compatible with the software image that you install on the VSM, a traffic disruption occurs in those modules, depending on your configuration. The **install all** command output identifies these scenarios. The hosts must be at the right version before the upgrade.

Before upgrading the VEMs, note these guidelines and limitations.

Note It is your responsibility to monitor and install all the relevant patches on VMware ESX hosts.

- The VEM software can be upgraded manually using the CLI or upgraded automatically using VUM.
- During the VEM upgrade process, VEMs reattach to the VSM.
- Connectivity to the VSM can be lost during a VEM upgrade when the interfaces of a VSM VM connect to its own Distributed Virtual Switch (DVS).
- If you are upgrading a VEM using a Cisco Nexus 1000V bundle, follow the instructions in your VMware documentation. For more details about VMware bundled software, see the *Cisco Nexus 1000V and VMware Compatibility Information* document.

Caution Do not enter the **vemlog**, **vemcmd**, or **vempkt** commands during the VEM upgrade process because these commands impact the upgrade.

Note For ESXi 5.1 update 2 and later, the minimum versions are as follows:

- VMware vCenter Server 5.1, 799731
- VMware Update Manager 5.1, 782803

For ESXi 5.5 update 1 and later, the minimum versions are as follows:

- VMware vCenter Server 5.0.0, 455964
- VMware Update Manager 5.0.0 432001

If you plan to do a combined upgrade of ESX and VEM, the minimum vCenter Server/VUM version required is 623373/639867.

This procedure is different from the upgrade to Release 4.2(1)SV1(4). In this procedure, you upgrade the VSMs first by using the **install all** command and then you upgrade the VEMs.

- You can upgrade the hosts in the DVS a few at a time across multiple maintenance windows. The only exception is if you are upgrading the VEM alone using VUM with the ESX version unchanged.

Upgrade Procedures

The following table lists the upgrade steps.

Note Ensure that you have changed the VSM mode to advanced, before upgrading VSM. VSG services are not available in the essential mode.

Table 2: Upgrade Paths from Cisco Nexus 1000V Releases

If you are running this configuration	Follow these steps
Release 4.0(4)SV1(1), 4.0(4)SV1(2), 4.2(1)SV1(4), 4.2(1)SV1(5.1), and 4.2(1)SV1(5.2)	Direct upgrades from these releases are not supported.
Releases 4.0(4)SV1(3x) Series	**1** Upgrading from Releases 4.0(4)SV1(3,3a,3b,3c,3d) to release 4.2(1)SV2(1.1) or later at the following URL: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_4_b/upgrade/software/guide/n1000v_upgrade_software.html#wp465259 **2** Upgrade from Releases 4.2(1)SV2(1.1) and later releases to the current release.

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4x) Series with a vSphere release 4.0 Update 1 or later	**1** Upgrading from VMware Release 4.0 to VMwrae Release 5.0 or later. **2** Upgrading VSMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **3** Upgrading VEMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **4** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **5** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.
Release 4.2(1)SV1(4x) Series with a vSphere release 4.1 GA, patches, or updates	**1** Upgrading from VMware Release 4.1 to VMwrae Release 5.0 or later. **2** Upgrading VSMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **3** Upgrading VEMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **4** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **5** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.
Release 4.2(1)SV1(4x) with a vSphere release 5.0 GA, patches, or updates.	**1** Upgrading VSMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **2** Upgrading VEMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **3** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **4** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.

The following table lists the upgrade steps when upgrading from Release 4.2(1)SV1(5x) and later releases to the current release.

Table 3: Upgrade Paths from Releases 4.2(1)SV1(5x) and Later Releases

If you are running this configuration	Follow these steps
With vSphere 4.1 GA, patches, or updates.	**1** Upgrading from VMware Release 4.1 to VMware Release 5.0 or later. **2** Upgrading VSMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **3** Upgrading VEMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **4** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **5** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.
With vSphere 5.0 GA, patches, or updates.	**1** Upgrading VSMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **2** Upgrading VEMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **3** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **4** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.
With ESX version upgrade.	Installing and Upgrading VMware

Upgrade Types

Upgrades can be one of three types:

- Upgrade of the Cisco Nexus 1000V version only, with vSphere version intact. See Upgrading the Cisco Nexus 1000V Only.
- Upgrade of both vSphere and Cisco Nexus 1000V versions together. See Combined Upgrade of vSphere and Cisco Nexus 1000V.
- Upgrade of vSphere version only, with the Cisco Nexus 1000V version intact. See the Installing and Upgrading VMware appendix.

Upgrading the Cisco Nexus 1000V Only

You must complete the following procedures to upgrade the Cisco Nexus 1000V only.

1. Upgrade the VSM. See VSM Upgrade Procedures.
2. Upgrade the VEM.
   - For Stateless ESXi, see Installing the VEM Software on a Stateless ESXi Host.
   - For a VUM-based upgrade of a Stateful ESX or ESXi, use a host upgrade baseline with the VEM depot. See Upgrading the ESXi Hosts to Release 5.x.
   - For a stateful manual upgrade using the **esxupdate** or **esxcli** commands, see Installing ESXi 5.1 Host Software Using the CLI.

Combined Upgrade of vSphere and Cisco Nexus 1000V

You can perform a combined upgrade of vSphere and Cisco Nexus 1000V.

If any of the hosts are running ESX 4.0 when the VSM is upgraded, the **installer** command displays that some VEMs are incompatible. You can proceed if you are planning a combined upgrade of the Cisco Nexus 1000V 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV2(2.1), and ESX 4.0/4.1 to current release with ESX 5.0/5.1/5.5.

Note Starting with the 4.2(1)SV2(2.1) release, during an VSM upgrade, if you have incompatible hosts attached to the VSM you will be allowed to upgrade from the current release of Cisco Nexus 1000V software to the later releases. You will see a warning message on incompatible host when you upgrade. Ignore the warning message and continue with the upgrade and the VSM will be upgraded to the latest version. You can perform a combined upgrade on the incompatible hosts.

Note A combined upgrade is supported only for vCenter Server 5.0 Update 1 or later.

The following procedures are necessary to perform a combined upgrade.

1. Upgrading the vCenter Server
2. Upgrading the vCenter Update Manager to Release 5.5
3. Upgrading VSMs from Releases 4.2(1)SV2(1.1x), 4.2(1)SV2(2.1x), to 5.2(1)SV3(1.x)
4. Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image
5. Upgrading the ESXi Hosts to Release 5.x
6. Verifying the Build Number and Upgrade

Reserving the Memory and CPU on the Virtual Supervisor Module Virtual Machine

From the current release of Cisco Nexus 1000V software, the VSM requires 4-GB RAM and two 2048-MHz vCPUs reservation to accommodate the new scalability limits.

Note When you install the Cisco Nexus 1000V software VSM through the OVA files for the first time, the RAM and CPU reservations are automatically reflected.

To upgrade to the current release of Cisco Nexus 1000V software and update the CPU and RAM reservations, use the following procedure:

Procedure

Step 1 Upgrade from the previous release of Cisco Nexus 1000V software to the current release of Cisco Nexus 1000V software.

Step 2 Once the upgrade is complete, power off the secondary VSM.

Step 3 Change the RAM size from 2 or 3 GB to 4 GB and change the RAM reservation from 2 or 3 GB to 4 GB.

Step 4 Under CPU settings, change the number of vCPUs to 2 and change the CPU reservation from 1.5 GHz to 2048 MHz.

Step 5 Power on the secondary VSM.

Step 6 Perform a system switch over to get the secondary VSM as Active.

Step 7 Power off the primary VSM and repeat steps 3 to 6.

Step 8 After the primary and secondary VSM have the correct CPU and RAM reservations, the VSM is able to accommodate the scale numbers that are supported on Release 5.2(1)SV3(1.1) or later.

Note You do not have to change the CPU and RAM reservations to continue to support for the scale numbers supported in releases before Release 5.2(1)SV3(1.1).

Reserving the Memory and CPU for the Virtual Supervisor Module in VSB on the Cloud Services Platform

To change the memory reservations in the VSM VSB, use the following procedure:

Before You Begin

From the current release of Cisco Nexus 1000V software, the VSM requires 4-GB RAM and two vCPUs to accommodate the new scalability limits.

Procedure

Step 1 Login to the Cloud Services Platform command prompt.

Step 2 Enter the VSM configuration mode.

Step 3 Change the RAM size to 4 GB and change the vCPU number to 2.

Note With Cisco Nexus Cloud Services Platform Release 4.2(1)SP1(6.1) and later, the virtual service blades can remain powered on when you change the RAM size. In Cisco Nexus Cloud Services Platform releases earlier than 4.2(1)SP1(6.1), the primary/secondary virtual service blades must be powered off before you can change the RAM size.

Step 4 Copy the running configuration to the startup configuration.

Step 5 Reboot the secondary VSM VSB by using the **shut** and **no shut** commands.

Step 6 Check if the secondary VSM has 4-GB RAM and two vCPUs.

Step 7 Perform a system switch over from the primary VSM to make the secondary VSM as active with 4-GB RAM and two vCPUs.
The primary VSM reboots and is in the standby state with 4-GB RAM and two vCPUs.

Reserving the Memory and CPU for the Virtual Supervisor Module in VSB on the Cloud Services Platform Using the CLI

To change the memory reservations in the VSM VSB using the CLI, use the following procedure:

Before You Begin

From the current release of Cisco Nexus 1000V software, VSM requires 4 GB RAM to accommodate the new scalability limits.

Procedure

	Command or Action	Purpose
Step 1	CSP **configure terminal**	Enters the global configuration mode.
Step 2	CSP(config)# **virtual-service-blade** *VSM for the current release*	Enters the VSM configuration mode.
Step 3	CSP(config-vsb-config)# **ramsize** *4096*	Change the RAM size to 4 GB. **Note** The virtual service blade is powered ON. Restart the VSB to reflect the change in RAM size. Perform a shutdown using the **shutdown** and **no shutdown** commands.
Step 4	CSP(config-vsb-config)# **numcpu 2**	Changing the number of CPUs to 2.
Step 5	CSP(config-vsb-config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.
Step 6	CSP(config-vsb-config)# **shutdown secondary**	Shuts down the secondary VSB.
Step 7	CSP(config-vsb-config)# **no shutdown secondary**	Applies the RAM and vCPU changes.
Step 8	VSM# **system switchover**	Performs a system switch over from primary VSM to make the secondary VSM as active with 4 GB RAM and two vCPUs.
Step 9	**VSM(standby)# show system resources**	Displays that the secondary VSM has 4 GB of RAM and two vCPUs.

VSM Upgrade Procedures

Software Images

The software image install procedure is dependent on the following factors:

- Software images—The kickstart and system image files reside in directories or folders that you can access from the Cisco Nexus 1000V software prompt.
- Image version—Each image file has a version.
- Disk—The bootflash: resides on the VSM.
- ISO file—If a local ISO file is passed to the **install all** command, the kickstart and system images are extracted from the ISO file.

In-Service Software Upgrades on Systems with Dual VSMs

Note Performing an In-service Upgrade (ISSU) from Cisco Nexus 1000V Release 4.2(1)SV1(4x), 4.2(1)SV1(5.1x), 4.2(1)SV1(5.2x) to the current release of Cisco Nexus 1000V is not supported.

The Cisco Nexus 1000V software supports in-service software upgrades (ISSUs) for systems with dual VSMs. An ISSU can update the software images on your switch without disrupting data traffic. Only control traffic is disrupted. If an ISSU causes a disruption of data traffic, the Cisco Nexus 1000V software warns you before proceeding so that you can stop the upgrade and reschedule it to a time that minimizes the impact on your network.

Note On systems with dual VSMs, you should have access to the console of both VSMs to maintain connectivity when the switchover occurs during upgrades. If you are performing the upgrade over Secure Shell (SSH) or Telnet, the connection will drop when the system switchover occurs, and you must reestablish the connection.

An ISSU updates the following images:

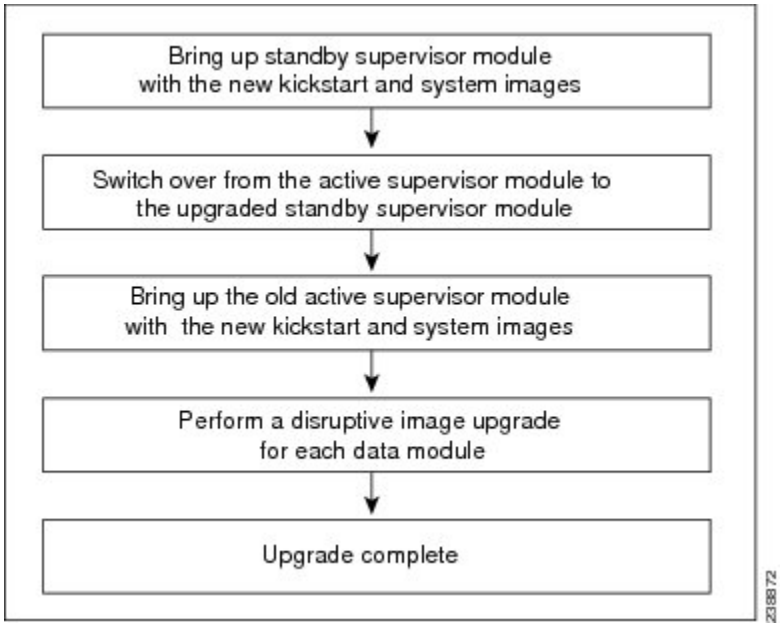
- Kickstart image
- System image
- VEM images

All of the following processes are initiated automatically by the upgrade process after the network administrator enters the **install all** command.

ISSU Process for the Cisco Nexus 1000V

The following figure shows the ISSU process.

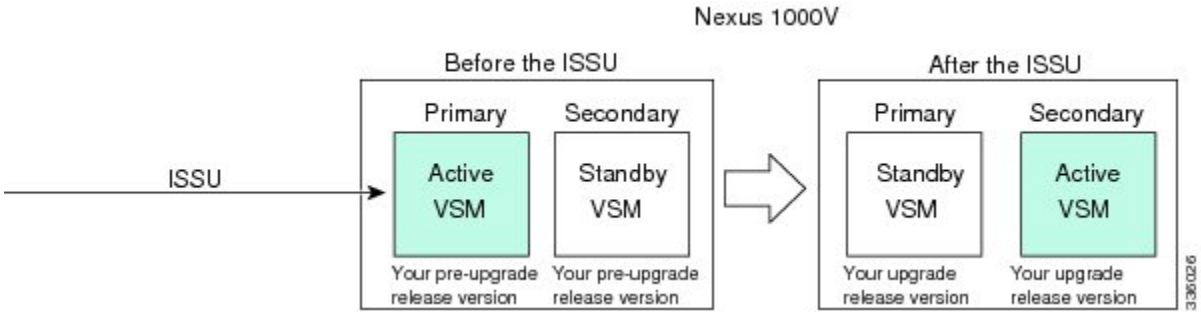
Figure 1: ISSU Process



ISSU VSM Switchover

The following figure provides an example of the VSM status before and after an ISSU switchover.

Figure 2: Example of an ISSU VSM Switchover



ISSU Command Attributes

Support

The **install all** command supports an in-service software upgrade (ISSU) on dual VSMs in an HA environment and performs the following actions:

- Determines whether the upgrade is disruptive and asks if you want to continue.
- Copies the kickstart and system images to the standby VSM. Alternatively, if a local ISO file is passed to the **install all** command instead, the kickstart and system images are extracted from the file.
- Sets the kickstart and system boot variables.
- Reloads the standby VSM with the new Cisco Nexus 1000V software.
- Causes the active VSM to reload when the switchover occurs.

Benefits

The **install all** command provides the following benefits:

- You can upgrade the VSM by using the **install all** command.
- You can receive descriptive information on the intended changes to your system before you continue with the installation.
- You have the option to cancel the command. Once the effects of the command are presented, you can continue or cancel when you see this question (the default is no):

```
Do you want to continue (y/n) [n]: y
```

- You can upgrade the VSM using the least disruptive procedure.
- You can see the progress of this command on the console, Telnet, and SSH screens:
  - After a switchover process, you can see the progress from both the VSMs.
  - Before a switchover process, you can see the progress only from the active VSM.
- The **install all** command automatically checks the image integrity, which includes the running kickstart and system images.
- The **install all** command performs a platform validity check to verify that a wrong image is not used.
- The Ctrl-C escape sequence gracefully ends the **install all** command. The command sequence completes the update step in progress and returns to the switch prompt. (Other upgrade steps cannot be ended by using Ctrl-C.)
- After running the **install all** command, if any step in the sequence fails, the command completes the step in progress and ends.

Upgrading VSMs from Releases 4.2(1)SV2(1.1) and Later Releases to Release 5.2(1)SV3(1.2) and Later Release

Procedure

Step 1 Log in to the active VSM.

Step 2 Log in to Cisco.com to access the links provided in this document. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

Note Unregistered Cisco.com users cannot access the links provided in this document.

Step 3 Access the Software Download Center by using this URL:
http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your system.
You see links to the download images for your switch.

Step 5 Choose and download the Cisco Nexus 1000V zip file and extract the kickstart and system software files to a server.

Step 6 Ensure that the required space is available for the image file(s) to be copied by entering the **dir bootflash:** command.

Tip We recommend that you have the kickstart and system image files for at least one previous release of the Cisco Nexus 1000V software on the system to use if the new image files do not load successfully.

Step 7 Verify that there is space available on the standby VSM by entering the **dir bootflash://sup-standby/** command .

Step 8 Delete any unnecessary files to make space available if you need more space on the standby VSM.

Step 9 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart and system images or the ISO image to the active VSM by using a transfer protocol. You can use ftp:, tftp:, scp:, or sftp:. The examples in this procedure copies a kickstart and system image using scp:.

Note When you download an image file, change to your FTP environment IP address or DNS name and the path where the files are located.

a) switch# **copy scp://***filepath/kickstart_filename* **bootflash:***kickstart_filename*
Copy the ISO image.

b) switch# **copy scp://***filepath/system_filename* **bootflash:***system_filename*
Copy kickstart and system images.

Step 10 switch# **show install all impact kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename*
Verify the ISSU upgrade for the kickstart and system images or the ISO image. The example in this procedure shows the kickstart and system images.

Step 11 Read the release notes for the related image file. See the *Cisco Nexus 1000V Release Notes*.

Step 12 Determine if the Cisco Virtual Security Gateway (Cisco VSG) is configured in the deployment by using the **show vnm-pa status** command .

Note If an output displaying a successful installation is displayed as in the example, the Cisco VSG is configured in the deployment. You must follow the upgrade procedure in the *Cisco Virtual Security Gateway and Cisco Virtual Network Management Center Installation and Upgrade Guide*. If an output displaying that the policy agent has not installed is displayed, continue to Step 13.

Step 13 Save the running configuration to the startup configuration by using the **copy running-config startup-config** command.

Step 14 Save the running configuration on the bootflash and externally.

Note You can also run a VSM backup. See the "Configuring VSM Backup and Recovery" chapter of the *Cisco Nexus 1000V System Management Configuration Guide*.

a) Save the running configuration on the bootflash by using the **copy running-config bootflash:run-cfg-backup** command.

b) Save the running configuration externally by using the **copy running-config scp://***external_backup_location* command.

Step 15 Perform the upgrade on the active VSM using the ISO or kickstart and system images by using the **install all kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename* command. The example in this procedure shows the kickstart and system images.

Step 16 Continue with the installation by pressing Y.
If you press N, the installation exits gracefully.

Note As part of the upgrade process, the standby VSM is reloaded with new images. Once it becomes the HA standby again, the upgrade process initiates a switchover. The upgrade then continues from the new active VSM.

Step 17 After the installation operation completes, log in and verify that the switch is running the required software version by using the switch# **show version** command

Step 18 Copy the running configuration to the startup configuration to adjust the startup-config size by using the switch# **copy running-config startup-config** command

Step 19 Display the log for the last installation by entering the following commands.

a) switch# **show install all status**

b) switch# **attach** *module_name*

c) switch# **show install all status**

Step 20 Review information about reserving memory and CPU on the VSM VM at the following URL: Reserving the Memory and CPU on the Virtual Supervisor Module Virtual Machine.

Note You must review this information, to accommodate the new scalability limits.

VEM Upgrade Procedures

- VUM Upgrade Procedures
  - Generate an upgrade ISO. See Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image.
  - Set up VUM baselines. See Upgrading the ESXi Hosts to Release 5.x.
  - Initiate an upgrade from VUM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 30.
  - Upgrade VEM from VSM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 30.
- Manual upgrade procedures

- Upgrading VIB Manually from the CLI. See Upgrading the VEMs Manually from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 42Upgrading the VEMs Manually from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 42

- Installing or upgrading stateless ESXi. See Installing the VEM Software on a Stateless ESXi Host.

VEM upgrades fall into three types:

- An upgrade of an ESX or stateful ESXi host, without a migration from ESX (with a console OS) to ESXi. This upgrade type is described further in this section.
- An upgrade of a stateless ESXi host. This involves installing a new image on the host by updating the image profile and rebooting the host. The upgrade is described in Installing the VEM Software on a Stateless ESXi Host.
- An upgrade that involves a migration from ESX to ESXi (of the same or different vSphere version).

An upgrade of an ESX or stateful ESXi host without a migration from ESX (which has a console OS) to ESXi falls into two separate workflows.

1. Upgrade the VEM alone, while keeping the ESX/ESXi version intact. The first figure shows this flow.
2. Upgrade the ESX/ESXi without a change of the Cisco Nexus 1000V version. This process is addressed in the Workflow 2 figure.

The following figure shows Workflow 1 where Cisco Nexus 1000V Release 4.2(1)SV1(4.x) or 4.2(1)SV1(5.x) is upgraded to the current release, without a change of ESX versions.

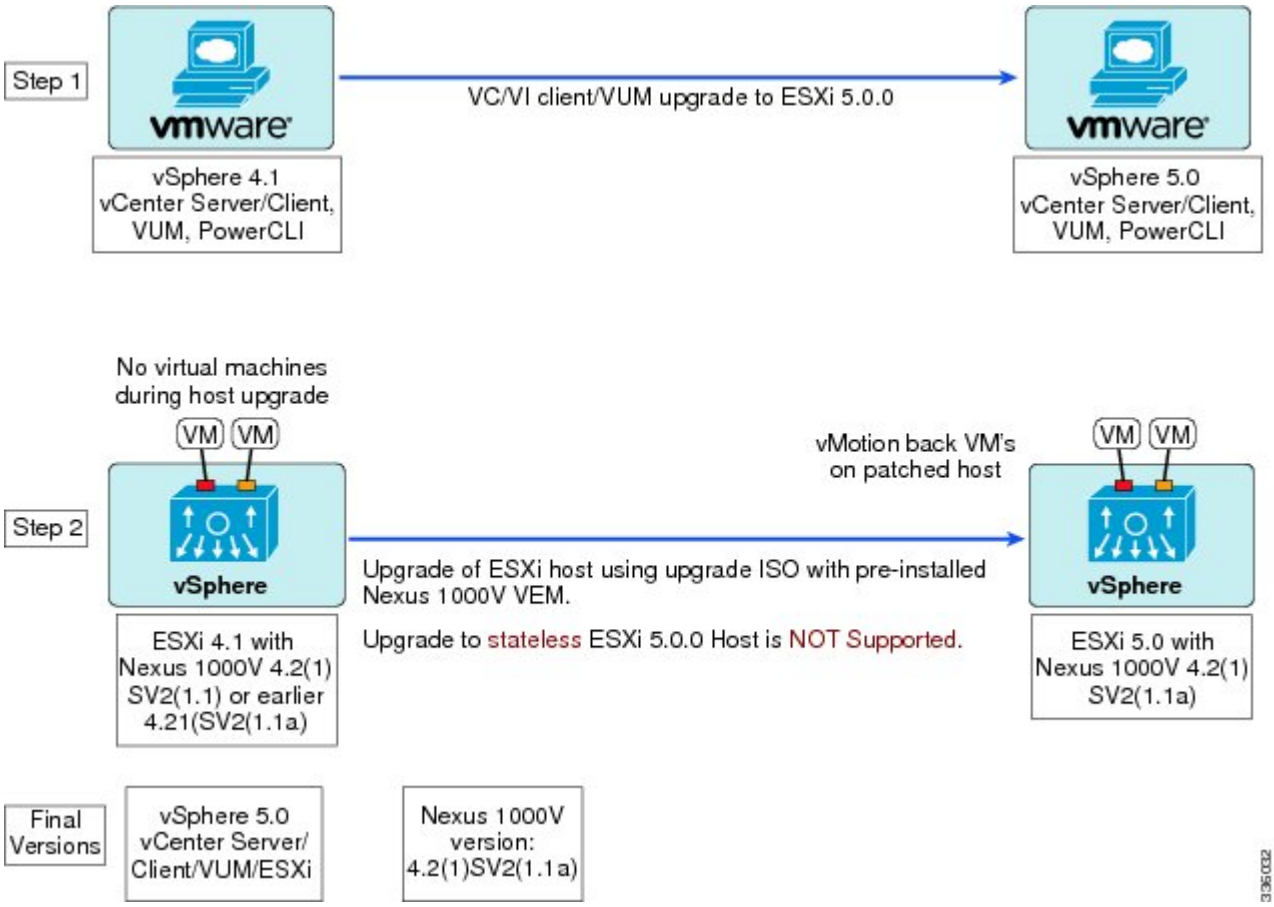
Figure 3: Workflow 1 with a Cisco Nexus 1000V Version 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), or SV1(5.2) Installed

If you are using VUM, set up a host patch baseline with the VEM's offline bundle. Then follow Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 30.

If you are upgrading from the command line, see Upgrading the VEMs Manually from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release, on page 42.

The following figure shows Workflow 2 where Cisco Nexus 1000VRelease 4.2(1)SV2(1.1) is installed and VMware 4.1 is upgraded to 5.0.

Figure 4: Workflow 2 with Cisco Nexus 1000V 4.2(1)SV2(1.1a) Installed and Upgrading ESX from 4.1 to 5.0



- If you are using VUM version 5.0 or later, use the following method (independent of whether the VEM version is being changed as well):
  - If you are upgrading the ESX host to a new update within a release, use a host upgrade baseline. For example, vSphere 5.0 GA to 5.0 U1.
  - If you are upgrading the ESX host to a major release (for example, vSphere 5.0 U1), generate an upgrade ISO and set up a host upgrade baseline. The upgrade ISO must have the desired final images for both ESX and VEM. The procedure to generate an upgrade ISO is in Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image.
  - You can upgrade the ESX version and VEM version simultaneously if you are using VUM 5.0 Update 1 or later. VUM 5.0 GA does not support a combined upgrade.

Note If you plan to perform Workflow 2 and manually update to vSphere 5.0 or later, you must boot the host from an upgrade ISO with both ESX and VEM images.

VUM Upgrade Procedures

Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image

Before You Begin

- Install the VMware PowerCLI on a Windows platform. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform, where the VMware PowerCLI is installed, do one of the following:
  - Download the ESX depot, which is a .zip file, to a local file path.
  - Download the VEM offline bundle, which is a .zip file, to a local file path.

Procedure

Step 1 Start the VMWare PowerCLI application.

Step 2 Connect to the vCenter Server by using the **Connect-VIServer** *IP_address* **-User Administrator -Password** *password_name* command.

Step 3 Load the ESX depot by using the **Add-ESXSoftwareDepot** *path_name\file_name* command.

Step 4 Display the image profiles by using the **Get-EsxImageProfile** command.

Step 5 Clone the ESX standard image profile by using the **New-ESxImageProfile -CloneProfile** *ESXImageProfile_name* **-Name** *clone_profile* command.

Note The image profiles are usually in READ-ONLY format. You must clone the image profile before adding the VEM image to it.

Step 6 Load the Cisco Nexus 1000V VEM offline bundle by using the **Add-EsxSoftwareDepot** *VEM_offline_bundle* command.

Step 7 Confirm that the n1kv-vib package is loaded by using the **Get-EsxSoftwarePackage -Name** *package_name* command.

Step 8 Bundle the n1kv-package into the cloned image profile by using the **Add-EsxSoftwarePackage -ImageProfile** *n1kv-Image* **-SoftwarePackage** *cloned_image_profile* command.

Step 9 Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile by entering the following commands.

a) **$img = Get-EsxImageProfile** *n1kv-Image*

b) **$img.vibList**

Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile.

Step 10 Export the image profile to an ISO file by using the **Export-EsxImageProfile -ImageProfile** *n1kv-Image* **-FilePath** *iso_filepath* command.

This example shows how to create an upgrade ISO with a VMware ESX image and a Cisco VEM image.

Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
vSphere PowerCLI> Connect-VIServer 10.105.231.40 -User administrator -Password 'XXXXXXXX'

Working with multiple default servers?

    Select [Y] if you want to work with more than one default servers. In this
case, every time when you connect to a different server using Connect-VIServer,
 the new server connection is stored in an array variable together with the
previously connected servers. When you run a cmdlet and the target servers
cannot be determined from the specified parameters, the cmdlet runs against all
 servers stored in the array variable.
    Select [N] if you want to work with a single default server. In this case,
when you run a cmdlet and the target servers cannot be determined from the
specified parameters, the cmdlet runs against the last connected server.

    WARNING: WORKING WITH MULTIPLE DEFAULT SERVERS WILL BE ENABLED BY DEFAULT
IN A FUTURE RELEASE. You can explicitly set your own preference at any time by
using the DefaultServerMode parameter of Set-PowerCLIConfiguration.

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Name                           Port  User
----                           ----  ----
10.105.231.40                  443   administrator

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-5.1.0-799733-depot.zip'

Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-...

vSphere PowerCLI> Get-EsxImageProfile

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.1.0-20121201001s-no-... VMware, Inc.    12/7/2012 7:... PartnerSupported
CN1-CY                         CISCO           4/22/2013 11... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools     VMware, Inc.    8/2/2012 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-standard     VMware, Inc.    8/2/2012 3:0... PartnerSupported

vSphere PowerCLI> New-EsxImageProfile -CloneProfile ESXi-5.1.0-799733-standard -Name FINAL

cmdlet New-EsxImageProfile at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Vendor: CISCO

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           8/2/2012 3:0... PartnerSupported

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229
\VEM510-201502172106-BG-release.zip
```

```
Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1...

vSphere PowerCLI> Get-EsxSoftwarePackage cisco*

Name                     Version                          Vendor              Creation Date
                                                                          e
----                     -------                          ------              ------------
cisco-vem-v172-esx    5.2.1.3.1.3.0-3.0.1          Cisco PartnerSupported    2015-02-04

vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v170-esx -ImageProfile
 FINAL

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           8/24/2014 3:... PartnerSupported

vSphere PowerCLI> $img = Get-EsxImageProfile FINAL

vSphere PowerCLI> $img.vibList

Name                     Version                          Vendor     Creation Dat
                                                                     e
----                     -------                          ------     ------------
scsi-bnx2i               1.9.1d.v50.1-5vmw.510.0.0.7...   VMware     8/2/2012 ...
sata-sata-promise        2.12-3vmw.510.0.0.799733         VMware     8/2/2012 ...
net-forcedeth            0.61-2vmw.510.0.0.799733         VMware     8/2/2012 ...
esx-xserver              5.1.0-0.0.799733                 VMware     8/2/2012 ...
misc-cnic-register       1.1-1vmw.510.0.0.799733          VMware     8/2/2012 ...
net-tg3                  3.110h.v50.4-4vmw.510.0.0.7...   VMware     8/2/2012 ...
scsi-megaraid-sas        5.34-4vmw.510.0.0.799733         VMware     8/2/2012 ...
scsi-megaraid-mbox       2.20.5.1-6vmw.510.0.0.799733     VMware     8/2/2012 ...
scsi-ips                 7.12.05-4vmw.510.0.0.799733      VMware     8/2/2012 ...
net-e1000e               1.1.2-3vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-ahci                3.0-13vmw.510.0.0.799733         VMware     8/2/2012 ...
sata-sata-svw            2.3-3vmw.510.0.0.799733          VMware     8/2/2012 ...
net-cnic                 1.10.2j.v50.7-3vmw.510.0.0....   VMware     8/2/2012 ...
net-e1000                8.0.3.1-2vmw.510.0.0.799733      VMware     8/2/2012 ...
ata-pata-serverworks     0.4.3-3vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-mptspi              4.23.01.00-6vmw.510.0.0.799733   VMware     8/2/2012 ...
ata-pata-hpt3x2n         0.3.4-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-s2io                 2.1.4.13427-3vmw.510.0.0.79...   VMware     8/2/2012 ...
esx-base                 5.1.0-0.0.799733                 VMware     8/2/2012 ...
net-vmxnet3              1.1.3.0-3vmw.510.0.0.799733      VMware     8/2/2012 ...
net-bnx2                 2.0.15g.v50.11-7vmw.510.0.0...   VMware     8/2/2012 ...
cisco-vem-v171-esx       5.2.1.3.1.2.0-3.1.2              Cisco      2014-11-10
scsi-megaraid2           2.00.4-9vmw.510.0.0.799733       VMware     8/2/2012 ...
ata-pata-amd             0.3.10-3vmw.510.0.0.799733       VMware     8/2/2012 ...
ipmi-ipmi-si-drv         39.1-4vmw.510.0.0.799733         VMware     8/2/2012 ...
scsi-lpfc820             8.2.3.1-127vmw.510.0.0.799733    VMware     8/2/2012 ...
ata-pata-atiixp          0.4.6-4vmw.510.0.0.799733        VMware     8/2/2012 ...
esx-dvfilter-generic-... 5.1.0-0.0.799733                 VMware     8/2/2012 ...
net-sky2                 1.20-2vmw.510.0.0.799733         VMware     8/2/2012 ...
scsi-qla2xxx             902.k1.1-9vmw.510.0.0.799733     VMware     8/2/2012 ...
net-r8169                6.011.00-2vmw.510.0.0.799733     VMware     8/2/2012 ...
sata-sata-sil            2.3-4vmw.510.0.0.799733          VMware     8/2/2012 ...
scsi-mpt2sas             10.00.00.00-5vmw.510.0.0.79...   VMware     8/2/2012 ...
sata-ata-piix            2.12-6vmw.510.0.0.799733         VMware     8/2/2012 ...
scsi-hpsa                5.0.0-21vmw.510.0.0.799733       VMware     8/2/2012 ...
ata-pata-via             0.3.3-2vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-aacraid             1.1.5.1-9vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-rste                2.0.2.0088-1vmw.510.0.0.799733   VMware     8/2/2012 ...
ata-pata-cmd64x          0.2.5-3vmw.510.0.0.799733        VMware     8/2/2012 ...
ima-qla4xxx              2.01.31-1vmw.510.0.0.799733      VMware     8/2/2012 ...
net-igb                  2.1.11.1-3vmw.510.0.0.799733     VMware     8/2/2012 ...
scsi-qla4xxx             5.01.03.2-4vmw.510.0.0.799733    VMware     8/2/2012 ...
block-cciss              3.6.14-10vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-aic79xx             3.1-5vmw.510.0.0.799733          VMware     8/2/2012 ...
tools-light              5.1.0-0.0.799733                 VMware     8/2/2012 ...
uhci-usb-uhci            1.0-3vmw.510.0.0.799733          VMware     8/2/2012 ...
sata-sata-nv             3.5-4vmw.510.0.0.799733          VMware     8/2/2012 ...
sata-sata-sil24          1.1-1vmw.510.0.0.799733          VMware     8/2/2012 ...
```

```
net-ixgbe                3.7.13.6iov-10vmw.510.0.0.7... VMware     8/2/2012 ...
ipmi-ipmi-msghandler     39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-adp94xx             1.0.8.12-6vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-fnic                1.5.0.3-1vmw.510.0.0.799733    VMware     8/2/2012 ...
ata-pata-pdc2027x        1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
misc-drivers             5.1.0-0.0.799733               VMware     8/2/2012 ...
net-enic                 1.4.2.15a-1vmw.510.0.0.799733  VMware     8/2/2012 ...
net-be2net               4.1.255.11-1vmw.510.0.0.799733 VMware     8/2/2012 ...
net-nx-nic               4.0.558-3vmw.510.0.0.799733    VMware     8/2/2012 ...
esx-xlibs                5.1.0-0.0.799733               VMware     8/2/2012 ...
net-bnx2x                1.61.15.v50.3-1vmw.510.0.0.... VMware     8/2/2012 ...
ehci-ehci-hcd            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
ohci-usb-ohci            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-r8168                8.013.00-3vmw.510.0.0.799733   VMware     8/2/2012 ...
esx-tboot                5.1.0-0.0.799733               VMware     8/2/2012 ...
ata-pata-sil680          0.4.8-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ipmi-ipmi-devintf        39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-mptsas              4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...

vSphere PowerCLI> Export-EsxImageProfile -ImageProfile FINAL -FilePath 'C:\Documents and
Settings\Administrator\Desktop\FINAL.iso' -ExportToIso
```

Upgrading the vCenter Server

Note This upgrade procedure applies to vCenter Server 5.0, 5.0 Update 1 and later, 5.1, and 5.5 versions.

Before You Begin

- Download the upgrade ISO file that contains your desired ESXi image and the desired Cisco Nexus 1000V image.
- See the *Cisco Nexus 1000V and VMware Compatibility Information* document to determine the correct VIB Version, VEM Bundle, Host Build, vCenter Server, and Update Manager versions.

Procedure

Step 1 Navigate to the VMware vSphere installation file.

Note If you have the ISO image, you should mount it on the host.

Step 2 Double-click **autorun.**

Step 3 In the **VMware vCenter Installer** screen, click **vCenter Server**.

Step 4 Click **Install**.

Step 5 Choose a language and click **OK.**

Step 6 Click **Next.**

Step 7 In the **Patent Agreement** screen, click **Next.**

Step 8 In the **License Agreement** screen, click the **I agree to the terms in the license agreement** radio button.

Step 9 Click **Next.**

Step 10 In the **Database Options** screen, click **Next.**

Step 11 Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\.** check box.

Step 12 From the **Windows Start** Menu, click **Run.**

Step 13 Enter the name of the folder that contains the vCenter Server database and click **OK.**

Step 14 Drag a copy of the parent folder (SSL) to the desktop as a backup.

Step 15 Return to the installer program.

Step 16 Click **Next.**

Step 17 In the **vCenter Agent Upgrade** screen, click the **Automatic** radio button.

Step 18 Click **Next.**

Step 19 In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box.

Step 20 Click **Next.**

Step 21 Review the port settings and click **Next.**

Step 22 In the **vCenter Server JVM Memory** screen based on the number of hosts, click the appropriate memory radio button.

Step 23 Click **Next.**

Step 24 Click **Install.**

Step 25 Click **Finish.**
This step completes the upgrade of the vCenter Server.

Step 26 Upgrade the VMware vSphere Client to your desired ESXi version.

Step 27 Open the VMware vSphere Client.

Step 28 From the **Help** menu, choose **About VMware vSphere**.

Step 29 Confirm that the vSphere Client and the VMware vCenter Server are both the same VMware versions.

Step 30 Click **OK**, and exit the VMware vSphere Client.

What to Do Next

Complete the steps in Upgrading the vCenter Update Manager to Release 5.5.

Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release

Caution If removable media is still connected (for example, if you have installed the VSM using ISO and forgot to remove the media), host movement to maintenance mode fails and the VUM upgrade fails.

Before You Begin

When using VUM, the **feature http-server enable** command must be enabled.

Procedure

Step 1 switch# **show vmware vem upgrade status**
Display the current configuration.

Step 2 switch# **vmware vem upgrade notify**
Coordinate with and notify the server administrator of the VEM upgrade process.

Step 3 switch# **show vmware vem upgrade status**
Verify that the upgrade notification was sent.

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.

Step 4 switch# **show vmware vem upgrade status**
Verify that the server administrator has accepted the upgrade in the vCenter. For more information about how the server administrator accepts the VEM upgrade, see Accepting the VEM Upgrade, on page 33. Coordinate the notification acceptance with the server administrator. After the server administrator accepts the upgrade, proceed with the VEM upgrade.

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.

Step 5 Initiate the VUM upgrade process with the following commands.

Note Before entering the following commands, communicate with the server administrator to confirm that the VUM process is operational.

The vCenter Server locks the DVS and triggers VUM to upgrade the VEMs.

a) switch# **vmware vem upgrade proceed**
b) switch# **show vmware vem upgrade status**

Note The DVS bundle ID is updated and is highlighted.

If the host is using ESXi 5.0.0 or a later release and your DRS settings are enabled to allow it, VUM automatically VMotions the VMs from the host to another host in the cluster and places the ESXi in maintenance mode to upgrade the VEM. This process is continued for other hosts in the DRS cluster until all the hosts are upgraded in the cluster. For details about DRS settings required and vMotion of VMs, visit the VMware documentation related to Creating a DRS Cluster.

Step 6 switch# **show vmware vem upgrade status**
Check for the upgrade complete status.

Step 7 Clear the VEM upgrade status after the upgrade process is complete with the following commands.

a) switch# **vmware vem upgrade complete**

b) switch# **show vmware vem upgrade status**

Step 8 switch# **show module**
Verify that the upgrade process is complete.

The upgrade is complete.

The following example shows how to upgrade VEMs using VUM.

Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
switch# show vmware vem upgrade status

# sh vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201401164100-BG
switch#
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.
switch# show vmware vem upgrade status

sh vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201401164100-BG

switch# show vmware vem upgrade status

2015 Feb  4 10:24:12 BL vms[3609]: %VMS-5-DVS_UPGRADE_INFO: VEM Upgrade Notification has
been accepted by vCenter Admin.
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201401164100-BG

switch#
```

```
switch# vmware vem upgrade proceed
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time: Wed Feb  4 10:25:57 2015
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201502172101-BG

switch#
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time: Wed Feb  4 10:25:57 2015
Upgrade End Time(vCenter): Wed Feb  4 09:10:21 2015
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201502172101-BG

switch#
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG
    DVS: VEM500-201502172101-BG

switch#
switch# show module
switch# sh module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    1022   Virtual Ethernet Module           NA                  ok
5    1022   Virtual Ethernet Module           NA                  ok
6    1022   Virtual Ethernet Module           NA                  ok


Mod  Sw                 Hw
---  -----------------  ------------------------------------------------
1    5.2(1)SV3(1.3)     0.0
2    5.2(1)SV3(1.3)     0.0
3    5.2(1)SV3(1.3)     VMware ESXi 5.1.0 Releasebuild-1065491 (3.1)
5    5.2(1)SV3(1.3)     VMware ESXi 5.5.0 Releasebuild-2068190 (3.2)
6    5.2(1)SV3(1.3)     VMware ESXi 5.0.0 Releasebuild-914586 (3.0)


Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.197.133.108   NA                                   NA
2    10.197.133.108   NA                                   NA
3    10.197.132.44    7b1a5e63-bcd0-11e0-bd1d-30e4dbc2c3ae  10.197.132.44
5    10.197.132.42    e0829a21-bc61-11e0-bd1d-30e4dbc2ba66  NA
6    10.197.132.45    8d8ff0e8-b565-11e0-bd1d-30e4dbc297da  10.197.132.45

switch#
```

Note The lines with the bold characters in the preceding example display that all VEMs are upgraded to the current release.

Accepting the VEM Upgrade

Before You Begin

- The network and server administrators must coordinate the upgrade procedure with each other.
- You have received a notification in the vCenter Server that a VEM software upgrade is available.

Procedure

Step 1 In the vCenter Server, choose **Inventory > Networking**.

Step 2 Click the **vSphere Client DVS Summary** tab to check for the availability of a software upgrade.

Figure 5: vSphere Client DVS Summary Tab

Step 3 Click **Apply upgrade**.
The network administrator is notified that you are ready to apply the upgrade to the VEMs.

Required Task After Upgrade—Changing the VEM Feature Level

After upgrading to Release 5.2(1)SV3(1.x), you must update the VEM feature level to the corresponding Release. After you perform this task, the new features in Release 5.2(1)SV3(1.x) are available on the Cisco Nexus 1000V and you have the option to increase the VLAN and port channel resource limits.

Before You Begin

- VSM and VEM have been upgraded to Release 5.2(1)SV3(1.x).

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# **show system vem feature level**
Displays the current VEM feature level. The current feature level should be 5.2(1)SV3(1.x).

Step 3 switch(config)# **vdc** *switch-name*
Enters VDC configuration mode for the specified switch.

Step 4 switch(config-vdc)# **limit-resource port-channel minimum** *value* **maximum** *value*
Configures the port channel resource limit.

Step 5 switch(config-vdc)# **limit-resource vlan minimum** *value* **maximum** *value*
Configures the VLAN resource limit

Step 6 switch(config-vdc)# **show resource**
Displays the updated values.

Step 7 switch(config-vdc)# **exit**
Exists the current configuration mode.

Step 8 (Optional) switch(config)# **copy running-config startup-config**
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to update the VEM feature level after upgrading from Release 4.2(1)SV2(1.1) to Release 5.2(1)SV3(1.x).

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# system update vem feature ?
  level  Updating vem feature level

switch(config)# system update vem feature level ?
  <CR>
  <1-50>  Version number index from the list above

switch(config)# system update vem feature level
Feature      Version
Level        String
--------------------
1          4.2(1)SV2(2.1)
2          4.2(1)SV2(2.2)
3          4.2(1)SV2(2.3)
4          5.2(1)SV3(1.1)
5          5.2(1)SV3(1.2)
6          5.2(1)SV3(1.3)
switch(config)#
switch(config)# system update vem feature level 6
switch(config)# copy running-config startup-config
```

Upgrading Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

Information About Upgrading the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

Cisco Virtual Switch Update Manager is the graphical user interface (GUI) that you can use to upgrade the Virtual Supervisor modules (VSMs) and the VEMs on ESX/ESXi hosts.

An interactive upgrade tool has been provided to assist you in determining the correct upgrade steps based on your current environment and the one to which you want to upgrade.

See the *Cisco Nexus 1000V and VMware Compatibility Information* for more information on the compatibility information for Cisco Nexus 1000V.

You can obtain your upgrade-related software for the current release of the Cisco Nexus 1000V software from cisco.com.

With Cisco Virtual Switch Update Manager, you can upgrade Cisco Nexus 1000V version only with the vSphere version intact.

See the *Cisco Nexus 1000V Installation and Upgrade Guide* for information about how to upgrade both vSphere and Cisco Nexus 1000V versions together and how to upgrade the vSphere version only, with the Cisco Nexus 1000V version intact.

Supported Upgrade Paths: With Cisco Virtual Switch Update Manager, you can upgrade Cisco Nexus 1000V from Release 4.2(1)SV1(4b) and later releases.

Unsupported Upgrade Paths: Using Cisco Virtual Switch Update Manager, you cannot upgrade the following releases of Cisco Nexus 1000V to the current release, Release 5.2(1)SV3(1.x):

- Release 4.2(1)SV1(4)
- Release 4.2(1)SV1(4a)
- Release 4.2(1)SV1(3x) series

Note Upgrades from Release 4.0(4)SV1(1), 4.0(4)SV1(2), and 4.0(4)SV1(3x) are no longer supported. VMware 4.0 and 4.1 are also not supported with this Cisco Nexus 1000V release.

Guidelines and Limitations for Upgrading the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

Caution During the upgrade process, the Cisco Nexus 1000V does not support any new additions such as modules, virtual NICs (vNICs), or VM NICs and does not support any configuration changes. VM NIC and vNIC port-profile changes might render VM NICs and vNICs in an unusable state.

Note We recommend that you use vSphere 5.0 Update 1 or later instead of vSphere 5.0.

Upgrading the Cisco Nexus 1000V with Cisco Virtual Switch Update Manager has the following guidelines and limitations:

- You are upgrading the Cisco Nexus 1000V software to the current release.
- Schedule the upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- Avoid power interruptions to the hosts that run the VSM VMs during any installation procedure.

Before you upgrade the VEMs, note these guidelines and limitations:

- During the VEM upgrade process, VEMs reattach to the VSM.
- Connectivity to the VSM can be lost during a VEM upgrade when the interfaces of a VSM VM connect to its own distributed virtual switch (DVS).

Prerequisites for Upgrading Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

Upgrading the Cisco Nexus 1000V with Cisco Virtual Switch Update Manager has the following prerequisites:

- Close any active configuration sessions before upgrading the Cisco Nexus 1000V software.
- Save all changes in the running configuration to the startup configuration.
- Save a backup copy of the running configuration in the external storage.
- Perform a VSM backup. For more information, see the "Configuring VSM Backup and Recovery" chapter in the *Cisco Nexus 1000V System Management Configuration Guide*.
- Use the VSM management IP address to log into VSM and perform management tasks.

Important If you connect to a VSM using the VSA serial port or the connect host from the Cisco Integrated Management Control (CIMC), do not initiate commands that are CPU intensive, such as copying images from the TFTP server to bootflash or generating a lot of screen output or updates. Use the VSA serial connections, including CIMC, only for operations such as debugging or basic configuration of the VSA.

- If you need to migrate a vSphere host from ESX to ESXi, do it before the Cisco Nexus 1000V upgrade.
- You have placed the VEM software file in `/tmp` on the vSphere host. Placing it in the root (/) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space by entering the **vdf** command.
- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series switches with the Cisco IOS software, enter the **portfast trunk** command or the **portfast edge trunk** command.
  - On Cisco Nexus 5000 Series switches with the Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:
  - **spanning-tree bpdu filter**
  - **spanning-tree bpdu guard**

- You must have the Distributed Switch—Create and Modify privilege permission enabled on the vCentre.
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

Upgrading the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

You can upgrade the Cisco Nexus 1000V using Cisco Virtual Switch Update Manager.

Procedure

Step 1 Log in to the VMware vSphere Web Client.

Step 2 In the vSphere Client, choose **Cisco Virtual Switch Update Manager** > **Nexus 1000V** > **Configure and Manage Nexus 1000V and Application Virtual Switch** > **Datacenter** > **Distributed Virtual Switch** > **Manage**.

Note If the switch is not managed by Cisco Virtual Switch Update Manager, you are prompted to enter the switch credentials in the **Make Managed** window.

Step 3 In the switch pane, click **Upgrade**.

Step 4 (Optional) In case of multiple vCenter Servers, choose **Home** > **Cisco Virtual Switch Update Manager** > **vCenter Server** > **Configure**.

Step 5 (Optional) You can also access the Cisco Virtual Switch Update Manager in the vSphere Client by navigating to **vCenter** > **Distributed Switches**.

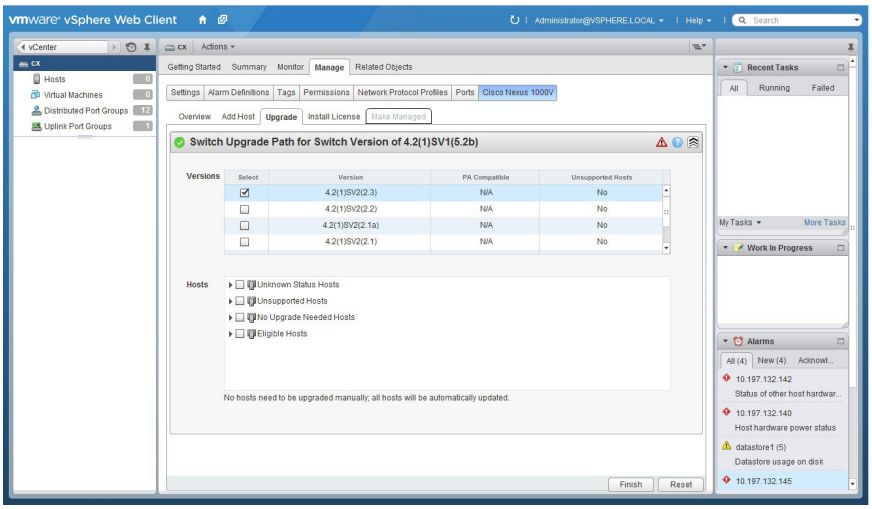
Step 6 (Optional) In the switch pane, click **Manage** > **Cisco Nexus 1000V** > **Upgrade**.

Note If the policy agent has been installed on the VSM, then do the following:

1. Enter the PNSC version number in the PNSC field.
2. Enter the VSG version number in the VSG field.
3. Click **OK**. The upgrade path displays the selected PNSC version and PA Compatible option as **Yes**.
4. From the Eligible Hosts drop-down list, choose the host and click **Finish**. This upgrades the VSMs along with the Policy Agent and the VEM.

Step 7 In the **Switch Upgrade Path** area, the **Switch Upgrade Path** for the selected switch displays the switch to be upgraded.

Figure 6: Cisco Virtual Switch Update Manager—Upgrading Cisco Nexus 1000V



Step 8 In the **Versions** area, the following information is pre configured.

Name	Description
Suggested Upgrade field	Displays if the upgrade is supported .
Version field	Displays the version number of the Cisco Nexus 1000V switch suggested for upgrade.
PA Compatble field	Displays if the Cisco PNSC version is compatible with the Cisco Nexus 1000V switch version suggested for upgrade.
Unsupported Hosts field	Displays if the ESXi host has to be upgraded manually.

Step 9 In the **Hosts** area, the hosts that are associated with the Cisco Nexus 1000V version suggested for upgrade are displayed.
The hosts are represented in the following four categories

- Unknown Status Hosts—The status of the host is in nonresponding state.
- Unsupported Hosts—The ESX/ESXi version of the host is not compatible with the ESX/ESXi version of the host that is associated with the Cisco Nexus 1000V version suggested for upgrade. The unsupported hosts should be upgraded manually to the ESX/ESXi versions supported by the Cisco Nexus 1000V. See the *Cisco Nexus 1000V and VMware Compatibility Information* for more information about supported ESX/ESXi versions.
- No Upgrade Needed Hosts—The hosts already have the correct VEM version installed.

- Eligible Hosts—The ESX/ESXi version of the host is compatible with the ESX version of the host that is associated with the Cisco Nexus 1000V version suggested for upgrade. During the upgrade process, Cisco Virtual Switch Update Manager upgrades the VEM version installed on the hosts to the specified version.

Step 10 Click **Finish** to upgrade the Cisco Nexus 1000V.

Step 11 In vSphere Web Client, choose **vCenter** > **Datacenter** > **Switch** > **Monitor** > **Tasks** to view the status of the upgrade. You can also view the tasks in the vSphere Web Client by choosing **Cisco Virtual Switch Update Manager** > **Select vCenter Host** > **Manage DVS** > **Select Datacenter** > **Select Switch** > **Monitor** > **Tasks**. A typical upgrade of the host takes a few minutes. In vCenter Web Client, you can view the tasks by the task object, user, or task status.

Manual Upgrade Procedures

Upgrading the VEM Software Using the vCLI

You can upgrade the VEM software by using the vCLI.

Before You Begin

- If you are using vCLI, do the following:
  - You have downloaded and installed the VMware vCLI. For information about installing the vCLI, see the VMware vCLI documentation.
  - You are logged in to the remote host where the vCLI is installed.

Note The vSphere command-line interface (vCLI) command set allows you to enter common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also enter most vCLI commands against a vCenter Server system and target any ESX/ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- If you are using the **esxupdate** command, you are logged in to the ESX host.
- Check *Cisco Nexus 1000V and VMware Compatibility Information* for compatible versions.
- You have already copied the VEM software installation file to the `/tmp` directory. Do not copy the files to the root (/) folder.
- You know the name of the VEM software file to be installed.

Procedure

Step 1 [root@serialport -]# **cd tmp**
Go to the directory where the new VEM software was copied.

Step 2 Determine the upgrade method that you want to use and enter the appropriate command.

- **vihostupdate**
  Installs the ESX/ESXi and VEM software simultaneously if you are using the vCLI.
- **esxupdate**
  Installs the VEM software from the ESX host /tmp directory.
  Note You must log in to each host and enter this command. This command loads the software manually on the host, loads the kernel modules, and starts the VEM agent on the running system.

Step 3 For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.

a) ~ # **esxcli software vib install -d** */absolute-path/VEM_bundle*
b) ~ # **esxcli software vib install -v** */absolute-path/vib_file*

Note You must specify the absolute path to the *VEM_bundle* and *vib_file* files. The absolute path is the path that starts at the root of the file system such as `/tmp/vib_file`.

Step 4 Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.

a) [root@serialport tmp]# **vmware -v**
b) root@serialport tmp]# # **esxupdate query**
c) [root@host212 ~]# . ~ # **vem status -v**
d) [root@host212 ~]# **vemcmd show version**

Step 5 switch# **show module**
Display that the VEMs were upgraded by entering the command on the VSM.

If the upgrade was successful, the installation procedure is complete.

The following example shows how to upgrade the VEM software using the vCLI.

Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
esxupdate -b [VMware offline update bundle] update
~ # esxcli software vib install -d /tmp/VEM500-201502172101-BG-release.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v172-5.2.1.3.1.3.0-3.0.1.VIB
   VIBs Removed:
   VIBs Skipped:
~ #
```

```
~ # esxcli software vib install -v /tmp/cross_cisco-vem-v172-5.2.1.3.1.3.0-3.0.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v172-5.2.1.3.1.3.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
~ #
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-843203
root@serialport tmp]# # esxupdate query
------Bulletin ID------- -----Installed----- --------------Summary---------------
VEM500-201502172101 2014-08-27T08:18:22 Cisco Nexus 1000V 5.2(1)SV3(1.3)


~ # vem status -v
Package vssnet-esxmn-ga-release
Version 5.2.1.3.1.3.0-3.0.1
Build 1
Date Tue Feb 3 18:23:50 PST 2015

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         6           128               1500    vmnic5
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
BL               1024        59          1024              1500    vmnic4,vmnic3
                                    ,vmnic2,vmnic1

VEM Agent (vemdpa) is running


~ # vemcmd show version
VEM Version: 5.2.1.3.1.3.0-3.0.1
VSM Version: 5.2(1)SV3(1.3)
System Version: VMware ESXi 5.0.0 Releasebuild-914586
ESX Version Update Level: 2

~ #
switch# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    1022   Virtual Ethernet Module           NA                  ok
5    1022   Virtual Ethernet Module           NA                  ok
6    1022   Virtual Ethernet Module           NA                  ok


Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    5.2(1)SV3(1.3)      0.0
2    5.2(1)SV3(1.3)      0.0
3    5.2(1)SV3(1.3)      VMware ESXi 5.1.0 Releasebuild-1065491 (3.1)
5    5.2(1)SV3(1.3)      VMware ESXi 5.5.0 Releasebuild-2068190 (3.2)
6    5.2(1)SV3(1.3)      VMware ESXi 5.0.0 Releasebuild-914586 (3.0)


Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.197.133.108   NA                                    NA
2    10.197.133.108   NA                                    NA
3    10.197.132.44    7b1a5e63-bcd0-11e0-bd1d-30e4dbc2c3ae  10.197.132.44
5    10.197.132.42    e0829a21-bc61-11e0-bd1d-30e4dbc2ba66  NA
6    10.197.132.45    8d8ff0e8-b565-11e0-bd1d-30e4dbc297da  10.197.132.45

switch#
```

Note The highlighted text in the previous command output confirms that the upgrade was successful.

Upgrading the VEMs Manually from Release 4.2(1)SV2(1.1x) and Later Releases to the Current Release

Before You Begin

Note If VUM is installed, it should be disabled.

To manually install or upgrade the Cisco Nexus 1000V VEM on an ESXi host, follow the steps in Upgrading the VEM Software Using the vCLI.

To upgrade the VEMs manually, perform the following steps as network administrator:

Note This procedure is performed by the network administrator. Before proceeding with the upgrade, make sure that the VMs are powered off if you are not running the required patch level.

Caution If removable media is still connected, (for example, if you have installed the VSM using ISO and forgot to remove the media), host movement to maintenance mode fails and the VEM upgrade fails.

Procedure

Step 1 switch# **vmware vem upgrade notify**
Coordinate with and notify the server administrator of the VEM upgrade process.

Step 2 switch# **show vmware vem upgrade status**
Verify that the upgrade notification was sent.

Step 3 switch# **show vmware vem upgrade status**
Verify that the server administrator has accepted the upgrade in vCenter Server. For details about the server administrator accepting the VEM upgrade, see Accepting the VEM Upgrade, on page 33. After the server administrator accepts the upgrade, proceed with the VEM upgrade.

Step 4 Perform one of the following tasks:

- If the ESXi host is not hosting the VSM, proceed to Step 5.
- If the ESXi host is hosting the VSM, coordinate with the server administrator to migrate the VSM to a host that is not being upgraded. Proceed to Step 5.

Step 5 switch# **vmware vem upgrade proceed**
Initiate the Cisco Nexus 1000V Bundle ID upgrade process.

Note If VUM is enabled in the vCenter environment, disable it before entering the **vmware vem upgrade proceed** command to prevent the new VIBs from being pushed to all the hosts.

Enter the **vmware vem upgrade proceed** command so that the Cisco Nexus 1000V Bundle ID on the vCenter Server gets updated. If VUM is enabled and you do not update the Bundle ID, an incorrect VIB version is pushed to the VEM when you next add the ESXi to the VSM.

Note If VUM is not installed, the "The object or item referred to could not be found" error appears in the vCenter Server task bar. You can ignore this error message.

Step 6 switch# **show vmware vem upgrade status**
Check for the upgrade complete status.

Step 7 Coordinate with and wait until the server administrator upgrades all ESXi host VEMs with the new VEM software release and informs you that the upgrade process is complete.
The server administrator performs the manual upgrade by using the **vihostupdate** command or the **esxcli** command. For more information, see Upgrading the VEM Software Using the vCLI.

Step 8 switch# **vmware vem upgrade complete**
Clear the VEM upgrade status after the upgrade process is complete.

Step 9 switch# **show vmware vem upgrade status**
Check the upgrade status once again.

Step 10 switch# **show module**
Verify that the upgrade process is complete.

Note The line with the bold characters in the preceding example display that all VEMs are upgraded to the current release.

The upgrade is complete.

The following example shows how to upgrade VEMs manually.

Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG-
    DVS: VEM500-201401164100-BG-
switch#
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.

switch# show vmware vem upgrade status

Upgrade Notification has been accepted by vCenter Admin.
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
```

```
    VSM: VEM500-201502172101-BG-
    DVS: VEM500-201401164100-BG

switch#
switch# vmware vem upgrade proceed
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time: Wed Feb  4 10:25:57 2015
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG-
    DVS: VEM500-201502172101-BG-

switch# show vmware vem upgrade status
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Wed Feb  4 10:23:33 2015
Upgrade Status Time(vCenter): Wed Feb  4 09:04:09 2015
Upgrade Start Time: Wed Feb  4 10:25:57 2015
Upgrade End Time(vCenter): Wed Feb  4 09:10:21 2015
Upgrade Error:
Upgrade Bundle ID:

    VSM: VEM500-201502172101-BG-
    DVS: VEM500-201502172101-BG-

switch#
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201502172101-BG-
    DVS: VEM500-201502172101-BG-

switch#
switch# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------  -----------------  ------------
1    0      Virtual Supervisor Module        Nexus1000V         ha-standby
2    0      Virtual Supervisor Module        Nexus1000V         active *
3    1022   Virtual Ethernet Module          NA                 ok
5    1022   Virtual Ethernet Module          NA                 ok
6    1022   Virtual Ethernet Module          NA                 ok


Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SV3(1.3)    0.0
2    5.2(1)SV3(1.3)    0.0
3    5.2(1)SV3(1.3)    VMware ESXi 5.1.0 Releasebuild-1065491 (3.1)
5    5.2(1)SV3(1.3)    VMware ESXi 5.5.0 Releasebuild-2068190 (3.2)
6    5.2(1)SV3(1.3)    VMware ESXi 5.0.0 Releasebuild-914586 (3.0)


Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.197.133.108   NA                                   NA
2    10.197.133.108   NA                                   NA
3    10.197.132.44    7b1a5e63-bcd0-11e0-bd1d-30e4dbc2c3ae  10.197.132.44
5    10.197.132.42    e0829a21-bc61-11e0-bd1d-30e4dbc2ba66  NA
6    10.197.132.45    8d8ff0e8-b565-11e0-bd1d-30e4dbc297da  10.197.132.45
```

```
switch#
```

Simplified Upgrade Process

Combined Upgrade

You can upgrade the VEM and ESX version simultaneously. It requires vSphere version 5.0 Update1 and later versions. It is supported in Cisco Nexus 1000V Release 4.2(1)SV1(5.2) and later. This upgrade can be implemented manually or by using VUM.

Selective Upgrade

You can upgrade a selective set of VEMs and a few hosts or clusters at a time in a single maintenance window. This enables incremental upgrades during short maintenance windows. It is supported with combined upgrades of VEM and ESX, and also with manual upgrades of VEMs only. It is supported for VUM-based combined upgrades with select hosts or clusters using the GUI. It is not supported with VUM-based upgrades of VEMs alone. To upgrade manually using this procedure follow these general steps:

- Identify the cluster or set of hosts in a cluster
- Place the selected hosts in maintenance mode (to vacate the VMs)
- Upgrade the VEM image on the hosts using the manual command or scripts
- Take the hosts out of maintenance mode, allowing Distributed Resource Scheduler (DRS) to rebalance VMs

Allowed Infrastructure Operations Under Selective Upgrade

These operations are allowed under selective upgrades:

- vMotion of VMs with the following releases:
  - pre-5.2(1)SV3(1.x) to 5.2(1)SV3(1.x)
  - 5.2(1)SV3(1.x) to pre-5.2(1)SV3(1.x)
  - 5.2(1)SV3(1.x) to 5.2(1)SV3(1.x)
  - pre5.2(1)SV3(1.x) to pre-5.2(1)SV3(1.x)
- VEM restart
- Host Reboot
- Add modules in 5.2(1)SV3(1.x)
- Add or remove ports vEth ports
- Shut or no-shut on port
- Migrate ports to or from vSwitch
- Add or delete VLAN or VLAN ranges

Background Upgrade

You can upgrade VEMs without a maintenance window for VEMs. You use the manual procedure to upgrade VEMs during production. Place the host in maintenance mode, upgrade the VEM, and remove the host from the maintenance mode. You do not have to shut off HA Admission Control and such (as you would during VUM upgrades). You must ensure the spare capacity in the cluster and perform a health check before the upgrade. To upgrade using this procedure follow these general steps:

- Upgrade the VSM first as usual. This may be done in a maintenance window
- Place one host at a time in maintenance mode (to vacate the VMs)
- Upgrade the VEM image on that host using manual commands or scripts
- Take the host out of maintenance mode, allowing the DRS to rebalance the VMs.
- Repeat the same procedure for every host in the DVS.

Note Make sure there is enough spare capacity for HA and that all required ports have system profiles (such as mgmt vmk). Check the host health before upgrading.

Extended Upgrade

You can modify configurations between the upgrade maintenance windows. VSM configuration changes are allowed where you can add or remove modules, port configurations, VLANs, and other similar changes. If a set of hosts are upgraded to the latest VEM version using the Selective Upgrade or the Background Upgrade, the remaining set of hosts will remain in older VEM versions. During that time, various Cisco Nexus 1000V configuration changes are allowed between maintenanance windows.

Note Do not make configuration changes during a maintenance window when the VEMs are being upgraded.

The list of allowed configuration changes are as follows:

- Add or remove modules
- Add or remove ports (ETH and VETH)
- Shut or no-shut a port
- Migrate ports to or from a vswitch
- Change port modes (trunk or access) on ports
- Add or remove port profiles
- Modify port profiles to add or remove specific features such as VLANS, ACLs, QoS, or PortSec.
- Change port channel modes in uplink port profiles
- Add or delete VLANs and VLAN ranges
- Add or delete static MACs in VEMs

Note Queuing configuration changes are not supported on QoS.

Upgrading from Releases 4.2(1)SV1(4x), 4.2(1)SV1(5.1x), or 4.2(1)SV1(5.2x) to the Current Release

Upgrading from Releases 4.2(1)SV1(4x), 4.2(1)SV1(5.1x), or 4.2(1)SV1(5.2x) to the current release is a two-step process.

Procedure

Step 1 See the Upgrading from Releases 4.2(1)SV1(4x), 4.2(1)SV1(5.1x), or 4.2(1)SV1(5.2x) to the Current Release section in the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV2(1.1)*.

Step 2 See Upgrade Procedures.

Migrating from Layer 2 to Layer 3

Layer 3 Advantages

The following lists the advantages of using a Layer 3 configuration over a Layer 2 configuration:

- The VSM can control the VEMs that are in a different subnets.
- The VEMs can be in different subnets.
- Because the VEMs can be in different subnets, there is no constraint on the physical location of the hosts.
- Minimal VLAN configurations are required for establishing the VSM-VEM connection when compared to Layer 2 control mode. The IP address of the VEM (Layer 3 capable vmknic's IP address) and the VSM's control0/mgmt0 interface are the only required information.
- In the VSM, either the mgmt0 or the control0 interface can be used as the Layer 3 control interface. If mgmt0 is used, there is no need for another IP address as the VSM's management IP address is used for VSM-VEM Layer 3 connection.
- If the management VMKernel (vmk0) is used as the Layer 3 control interface in the VEM, there is no need for another IP address because the host's management IP address is used for VSM-VEM Layer 3 connectivity.

Note These advantages are applicable only for ESX-Visor hosts. On ESX-Cos hosts, a new VMKernel must be created.

Layer 2 to 3 Conversion Tool

About VSM-VEM Layer 2 to 3 Conversion Tool

Use the VSM-VEM Layer 2 to 3 Conversion Tool as an optional, simplified method to migrate from Layer 2 to Layer 3 mode. The tool enables you to do the following:

- Check whether the prerequisites are met for the migration from L2 to L3 mode.
- Migrate the VSM from Layer 2 to Layer 3 Mode, with user interaction.

  In the process of migration, the tool creates a port profile. You can use port profiles to configure interfaces, which you can assign to other interfaces to give them the same configuration. The VSM-VEM Layer 2 to 3 Conversion Tool also gives you the option of retrieving the IP addresses from a local file (static).

Prerequisites for Using VSM-VEM Layer 2 to 3 Conversion Tool

The L2-L3_CT.zip file contains the applications required to run VSM-VEM Layer 2 to 3 Conversion Tool

Before you begin:

- Log in as administrator to use this conversion tool script.
- Download the L2-L3_CT.zip file from the CCO Download Center.
- Install Tool Conversion Language (TCL) version 8.4 or later on the workstation.
- Install VMware PowerShell API version 5.0 or later on both the vCenter and the workstation.
- Install OpenSSH on the workstation.
- In the workstation environment variables, add `installation_directory_for_OpenSSH\bin` directory to the end of the Windows path variable.
- Ensure that VLANs are allowed on the uplinks.

Note You must install vCenter, VSM, and OpenSSH with admin privileges.

Using VSM-VEM Layer 2 to 3 Conversion Tool

Procedure

Step 1 On your workstation, unzip the L2-L3_CT.zip file to any folder.
When you unzip the file, a Pre-Migrate-Check-Logs folder is created that holds all the running logs. Debugging log files will be created in this folder.

Step 2 Inside the L2-L3_CT folder, run migration.bat as an administrator.
This starts the VSM-VEM Layer 2 to 3 Conversion Tool.

Step 3 Enter the VSM IP address.

Step 4 Enter the VSM username.

Step 5 Enter the vCenter IP.

Step 6 Enter the vCenter username.

Step 7 Enter the VSM password.

Step 8 Enter the vCenter password.
The migration tool begins creating the .csv file for the user, and then checks for a port profile with layer 3 capability.

Step 9 If there is no layer 3-capable port profile, the tool will prompt for the creation of one. If you don't want to create a layer-3 capable port profile, skip to the next step.

a) Enter yes to confirm when asked to create 1 layer 3-capable port profile.
b) Enter a layer 3 port profile name.
c) Enter access VLAN ID

This creates a port profile with the required configuration. You can select this port profile when prompted by the tool. The migration tool checks for connectivity between VSM, vCenter, and VEM modules. Wait for the message to display that all connectivity is fine.

Step 10 Enter yes to continue when asked if you want to continue.
The migration tool proceeds to create an extract .csv file.

Step 11 Open the extract.csv file (in `C:\Windows\Temp`).

Step 12 Enter the vmknic IP details at the end of the text, delimited by semicolons, and save the file as convert.csv.

Step 13 Press any key to continue.

Step 14 Enter yes to confirm when asked if you are sure you completed the required steps.

Step 15 Enter the VSM password.

Step 16 Enter the vCenter password.
The migration tool connects to the vCenter and VSM of the user.

Step 17 Enter yes to confirm when asked if you want to continue.
The migration process continues.

Step 18 Enter the port profile name from the list of port profiles that appears at the prompt.

Once the port profile is selected, the max port value is automatically changed to 128.

Step 19 Enter yes to confirm when asked if you have updated convert.csv file as per the instructions.

Step 20 Enter yes to confirm, when asked if you want to continue.
The tool checks the connectivity between VSM, vCenter, and VEM modules. A message is displayed that the addition to vmknics are successful and all connectivity is fine. The **VmkNicAddingToHost** window will remain open until the configuration is complete.

Step 21 Enter yes to confirm that you would like to proceed with mode change from L2 to L3.

Step 22 Enter yes to confirm when asked if you wish to continue.
Wait for the SUCCESSFULLY COMPLETED MIGRATION message to display. The migration from layer 2 to layer 3 is now complete. The operating mode should now be listed as L3.

Using Extract Mode

You can use Extract Mode to extract the attached VEM states and save them to the Extract.csv file, which is located in `C:\Windows\Temp`.

Procedure

	Command or Action	Purpose
Step 1	Choose extract mode when prompted by VSM-VEM Layer 2 to 3 Conversion Tool. You can now view the data in the Extract.csv file in the Windows temp folder of your workstation.	This mode will not migrate the VSM.

Using Convert Mode

You can use Convert Mode to migrate the VSM from Layer 2 to Layer 3.

Procedure

	Command or Action	Purpose
Step 1	Rename the Extract.csv file to Convert.csv	The migration tool will retrieve the data from the Convert.csv file.
Step 2	Populate your Convert.csv file (in `C:\Windows\Temp`) with the vmknic IP address and netmask.	
Step 3	Run migration.bat.	This will migrate the VSM mode from Layer 2 to Layer 3 .

Example

The following example shows how to use the VSM-VEM Layer 2 to 3 Conversion Tool.

```
Enter VSM IP:
enter VSM Username:
Enter VC IP:
enter VC Username:
Enter VSM password:
Enter VC password:
create the Csv File for User I/P: C:\windows\temp\extract.csv
#### VSM DETAILS STARTS ##########
.........
..............
#### VC DETAILS END ##########
..............
.................
Operating Mode : L2
Operatoinal Mode is L2 Currently ......
################################################################################
List of port profiles on VSM:
----------------------------
################################################################################
=========
 CHECK 1: Checking for a port profile with capability l3control set and Enabled.
.................
=========
There is not even One L3 Capable Port Profile

Do you want to Create One L3 Capable Port Profile
Please Give Option (Yes/No):Yes
Please Enter L3 PortProfile Name: L3-Control
Please Give Access Vlan Id :5
Creating L3 Port Profile : L3-Control with Access Vlan : 5
.....................................
.....................................................
L3 capable port profiles: L3-Control
Modules Registered:[10.105.228.116]
=========
 CHECK 3:  Checking for connectivity between VSM and VC, VSM and VEM Modules
=========
.....................
.....................................

## All connectivity is fine
################################################################################
Please wait for a few minutes.
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
Creating csv file: C:\windows\temp\extract.csv
Modules : 10.105.228.116
##########################################################
Modules Registered:[3 10.105.228.116]
##########################################################

##########################################################
################################################################################
Extraction of VEM connection status has been dumped in: C:\windows\temp\extract.
csv
Please rename this file before using Convert Mode
Update the VMKNic IP and NetMask for all disconnected entries
################################################################################
!#############################################################################
########!
!Open c:\windows\temp\Extract.csv and save as Convert.csv (in the same directory
)
!Enter the VMKNic IP and netmask in the Convert.csv file as shown below
!VEM_Host_IP;PPConnectionStatus;Vem_Vmk_IP;NetMask!
!PPConnectionStatus Should not be changed!
!10.10.10.12;DisConnected;10.10.10.100;255.255.255.0!
!After Updating the IP and Netmask, save the file in the same directory
!#############################################################################
```

```
########!
Press any key to continue . . .
Are you sure you completed the above steps? (yes/no):yes

################################################################################

##Tool expects this File have an IP/Netmask given for disconnected VEM in the co
rrect format : C:\windows\temp\Convert.csv

##10.10.10.12;DisConnected;10.10.10.100;255.255.255.0

################################################################################
VSM password required 10.105.228.115:

VC password required 10.105.228.113:

create the Csv File for User I/P: C:\windows\temp\extract.csv
.....................
.............................
## All connectivity is fine

################################################################################
Please wait for a few minutes.
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
..........................
.....................................................
#########################################################
Name the port profile you want to proceed with : [l3-pp]
Please type any port profile mentioned above       ||:l3-pp
You Selected : l3-pp
..................
..............................
#####################################################################
## Have you created a Convert.csv file with a proper VMKNic IP and NetMask?
## In the C:\windows\temp\Convert.csv file for disconnected VEMs.
#####################################################################
Have you Updated C:\windows\temp\Convert.csv as per the above instructions?(Yes)
:yes
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
.........................
.................................................

Addition to VmKNics are successful
## All connectivity is Fine
.............................
...................................
################################################################################

Would You Like to Proceed with Mode Change from L2 to L3....(yes/no):yes
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
..................
.....................
switch#
Operating Mode : L3
Operatoinal Mode is L3 Currently
Svs Connection Mode : L3
Vem IP : 10.10.10.108 Connected Back
.................
.....................
All VEMs are back: pass
 ==============SUCCESSFULLY COMPLETED MIGRATION==========================
```

Interface Comparisons Between mgmt0 and control0

The following describes the differences between using a mgmt0 interface or a control0 interface:

- On the VSM, there are two ways of connectivity via the mgmt0 or control0 interface.
- Setting mgmt0 as Layer 3 interface uses the mgmt0 interface on the VSM.
- The control0 interface is a special interface created for Layer 3 connectivity.
- The Layer 3 interface on the VEM is selected by designating the interface with the Layer 3 control capability.
- The egress control traffic route is decided by the VMware routing stack.
- On a VEM, the management vmknic (vmk0) can be used for Layer 3 control connectivity if it is managed by the Cisco Nexus 1000V and is designated with the Layer 3 control capability.

Configuring the Layer 3 Interface

Configure either the control0 (see Step 1) or mgmt0 interface (see Step 2).

Procedure

Step 1 Configuring the control0 interface.

Note When using control0 as the control interface on the VSM, the control0 interface must be assigned with an IP address.

a) Configure the IP address.

```
switch# configure terminal
switch(config)# interface control 0
switch(config-if)# ip address 5.5.5.2 255.255.255.0
```

b) Display the running configuration of the control0 interface.

```
switch# show running-config interface control 0
!Command: show running-config interface control0
!Time: Mon Dec 12 02:41:47 2011
version 4.2(1)SV1(5.1)
interface control0
  ip address 5.5.5.2/24
```

Step 2 Configure the mgmt0 interface.

Note When using mgmt0 as the control interface, no configuration on the VSM is required as the mgmt0 interface is assigned with the host's management IP address.

a) Display the running configuration of the mgmt0 interface.

```
switch# show running-config interface mgmt 0
!Command: show running-config interface mgmt0
!Time: Mon Dec 12 02:43:25 2011
version 4.2(1)SV1(5.1)
interface mgmt0
  ip address 10.104.249.37/27
```

Creating a Port Profile with Layer 3 Control Capability

Before You Begin

- You are creating a port profile with Layer 3 control capability.
- Allow the VLAN that you use for VSM to VEM connectivity in this port profile.
- Configure the VLAN as a system VLAN.

Note VEM modules will not register to the VSM before a vmkernel interface (vmk) is migrated to a Layer 3 control capable port profile. You must migrate a vmk to the Layer 3 port profile after migrating host vmnics to Ethernet port profiles. Migrate your management vmkernel interface into the Layer 3 capable port profile. Do not use multiple vmkernel interfaces on the same subnet.

Procedure

Step 1 Create a Layer 3 port profile.

```
VSM_1# configure terminal
VSM_1(config)# port-profile type vethernet l3_control
VSM_1(config-port-prof)# switchport mode access
VSM_1(config-port-prof)# switchport access vlan 3160
VSM_1(config-port-prof)# capability l3control
VSM_1(config-port-prof)# vmware port-group
VSM_1(config-port-prof)# state enabled
VSM_1(config-port-prof)# no shutdown
```

Step 2 Display the port profile.

```
VSM_1# show port-profile name l3_control
port-profile l3_control
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 min-ports: 1
 inherit:
 config attributes:
  switchport mode access
  switchport access vlan 3160 (Allow the VLAN in access mode.)
  no shutdown
 evaluated config attributes:
  switchport mode access
  switchport access vlan 3160
  no shutdown
 assigned interfaces:
  Vethernet1
 port-group: l3_control
 system vlans: 3160 (Configure the VLAN as a system VLAN.)
 capability l3control: yes (Configure capability l3 control.)
 capability iscsi-multipath: no
```

```
capability vxlan: no
capability l3-vn-service: no
port-profile role: none port-binding: static
```

Creating a VMKernel on the Host

Procedure

Step 1 Log in to the vCenter Server.

Step 2 Choose **Home > Inventory > Hosts and Clusters**.

Step 3 Choose the host.

Step 4 Click the **Configuration** tab.

Step 5 In the Hardware pane, choose **Networking**.

Step 6 Click the **vSphere Distributed Switch** button.

Step 7 Go to **Manage Virtual Adapters**.

Step 8 Add and create a new VMKernel.

Note The management vmkernel can also be used as a Layer 3 control interface. For ESX-Visor hosts only. Migrate your management vmkernel interface into the Layer 3 capable port profile. Do not use multiple vmkernel interfaes on the same subnet.

Step 9 Assign the VMkernel to the port profile created in Creating a Port Profile with Layer 3 Control Capability.

Step 10 Assign an IP address.

Configuring the SVS Domain in the VSM

Before You Begin

The control0 or mgmt0 interface can be assigned as the Layer 3 control interface.

Procedure

Step 1 Disconnect the VSM to vCenter Server connection.

```
switch# configure terminal
switch(config)# svs connection toVC
switch(config-svs-conn)# no connect
switch(config-svs-conn)# exit
```

Step 2 (Optional) Remove the control and the packet VLAN configuration.

```
switch(config)# svs-domain
switch(config-svs-domain)# no control vlan
switch(config-svs-domain)# no packet vlan
```

Step 3 Change the svs mode from Layer 2 to Layer 3 with the mgmt0 interface as the Layer 3 control interface.

```
switch(config-svs-domain)# svs mode l3 interface mgmt0
switch(config-svs-domain)# exit
```

Note If the control0 interface is being used as the Layer 3 control interface, enter the **svs mode l3 interface control0** command:

Step 4 Restore the VSM to vCenter Server connection.

```
switch(config)# svs connection toVC
switch(config-svs-conn)# connect
switch(config-svs-conn)# end
```

Note After entering the **svs connection toVC** command, the module is detached and reattached in Layer 3 mode. If this delay is more than six seconds, a module flap occurs. This does not affect the data traffic.

Step 5 Display the SVS domain configuration.

```
switch# show svs domain
SVS domain config:
  Domain id:    3185
  Control vlan: NA
  Packet vlan:  NA
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful.

Note: Control VLAN and Packet VLAN are not used in L3 mode.
```

Feature History for Upgrading the Cisco Nexus 1000V

The following table lists the release history for upgrading the Cisco Nexus 1000V.

Feature Name	Releases	Feature Information
Combined Upgrade	4.2(1)SV1(5.2)	The ability to perform a simultaneous upgrade of the VEM and ESXi host.
Upgrading the Cisco Nexus 1000V	4.0(4)SV1(2)	Introduced in this release.