Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1) SV1(4)

Revised: April 18, 2011
OL-21656-01

This document describes how to install and upgrade the Cisco Nexus 1000V Virtual Ethernet Module (VEM) software on a VMware ESX/ESXi 4.0.0 server or ESX/ESXi 4.1.0 server.

This document includes the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Audience

This document is intended for use by experienced server administrators who configure and maintain server software. Table 1 compares the roles of the network administrator and server administrator.

Table 1 Administrator Roles

Network Administrator	Server Administrator
• Creates, configures, and manages vswitches. • Creates, configures, and manages port profiles, including the following: – Security – Port channels – QoS policies	• Assigns the following to port groups: – Virtual network interface cards (VNICs) – vmkernel interfaces – Service console interfaces • Assigns physical NICs (PNICs) to vswitches on each host.

This document includes instructions for installing new VEM software as a fresh install or after upgrading the VSM software to a new version.

To install the Virtual Supervisor Module (VSM), see the following document:

Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4)

For detailed information about upgrading the software on the VSM and VEM, see the following document:

Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4)

Information About the Virtual Ethernet Module

This section provides information about the Virtual Ethernet Module and includes the following topics:

Introduction to Cisco Nexus 1000V and the Virtual Ethernet Module

The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is Ethernet standard compliant, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL).

Cisco and VMware jointly designed APIs that produced the Cisco Nexus 1000V. The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. This solution off-loads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy.

The Cisco Nexus 1000V has the following components that can virtually emulate a 66-slot modular Ethernet switch with redundant supervisor functions:

- Virtual Ethernet module (VEM) data plane—Each hypervisor is embedded with one VEM, a lightweight software component that replaces the virtual switch by performing the following functions:
  - Advanced networking and security
  - Switching between directly attached virtual machines
  - Uplinking to the rest of the network

Note There can be one and only one version of VEM installed on an ESX/ESXi host at any given time.

- Virtual supervisor module (VSM) control plane—The VSM is a virtual appliance which can be installed in either a standalone or active/standby HA pair which is the recommended configuration. The VSM performs the following functions for the Cisco Nexus 1000V system (that is, the combination of the VSM and all VEMs that it controls):
  - Configuration
  - Management

    A single VSM can manage up to 64 VEMs.
  - Monitoring
  - Diagnostics
  - Integration with VMware vCenter

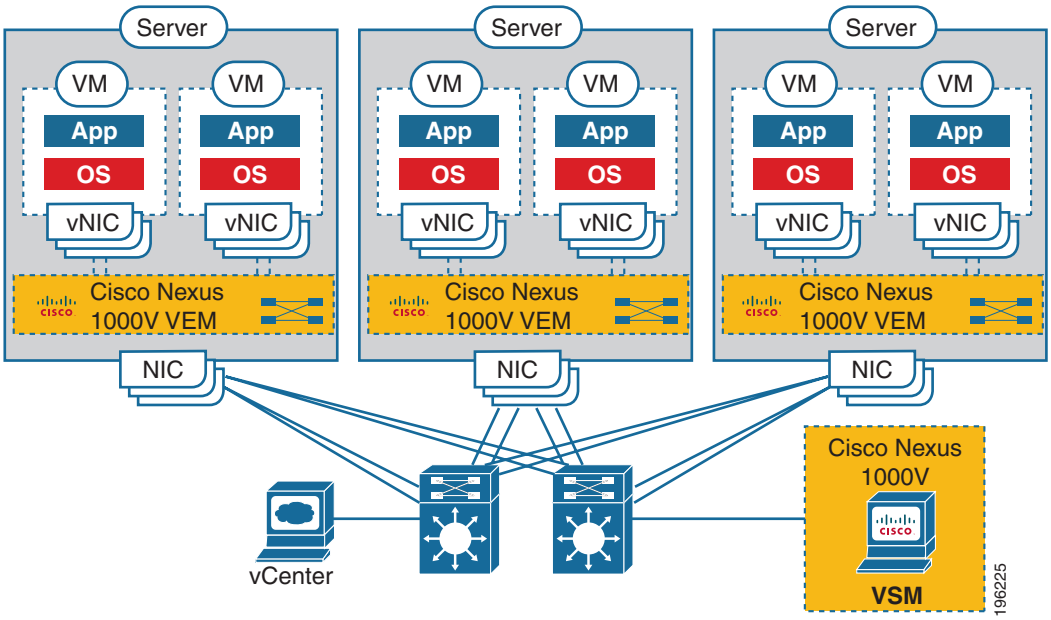
  Active-standby VSMs increase high availability

In the Cisco Nexus 1000V, traffic is switched between virtual machines locally at each VEM instance. Each VEM also interconnects the local virtual machine with the rest of the network through the upstream access-layer network switch (blade, top-of-rack, end-of-row, and so forth). The VSM runs the control plane protocols and configures the state of each VEM accordingly, but it never forwards packets.

In the Cisco Nexus 1000V, the module slots are primary module 1 and secondary module 2. Either module could act as active or standby. The first server or host is automatically assigned to Module 3. NIC ports are 3/1 and 3/2 (vmnic0 and vmnic1 on ESX/ESXi host). The ports to which the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000V where they are assigned a global number.

Figure 1 shows an example of the Cisco Nexus 1000V distributed architecture.

Figure 1 Cisco Nexus 1000V Distributed Switching Architecture



Obtaining the VEM Software

You can obtain the VEM software from the sources listed in Table 2.

Table 2 Obtaining VEM Software

Source	Description
VUM	If you are using the VMware vCenter Update Manager (VUM), then VUM obtains the VEM software from the VSM or from the VMware online portal. See the VMware and Cisco Nexus 1000V Software Compatibility table in the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* to identify which VEM bits are available on the VSM or posted on the VMware online portal[1].
VSM	After the VSM has been installed as a VM, copy the file containing the VEM software from the VSM homepage located at the following url: http://*VSM_IP_Address*/
VMware	Download the VEM software from the VMware website. Click **Download Vmware vSphere 4 Enterprise Plus > Download** Download the VMware patches if you are utilizing VMware releases with patches.
Cisco	Download the VEM software from the Cisco website.

1. VMware vCenter Update Manager 4.0 does not list Cisco Nexus 1000V patches or updates, but you can add a Cisco Nexus 1000V patch source using the VMware knowledge base procedure located at the following url:

   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1013134

   VMware vCenter Server 4.0 Update 1 with VUM P02 and later versions do not have this limitation.

VMware Patch Releases

The Cisco Nexus 1000V VEM software is updated to support VMware patch releases and is available on both the VMware and Cisco software download web sites. The Cisco Nexus 1000V software posted on these Web sites can be used for both installation and upgrade of the VEM for both the VMware Classic and VMware Embedded platforms.

For information about installing software on an ESX/ESXi host, see your VMware documentation.

For information about VEM software packages and compatibility, see the following document:

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4).

Prerequisites for Installing VEM Software

Before installing the Cisco Nexus 1000V VEM software, you must know or do the following:

Caution If the VMware vCenter Server is hosted on the same ESX/ESXi host as a Cisco Nexus 1000V VEM, then a VUM assisted upgrade on the host will fail. You should manually vMotion the VM to another host before performing the upgrade.

Note When performing any VUM operation on hosts which are a part of a cluster, ensure that VMWare High Availability (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.

- Before performing a VEM upgrade, make sure that there are no active VMs running on the host. When VMware patch ESX/ESXi400-201002001 or the ESX/ESXi400-201006201-UG is installed on the host, it puts the host in maintenance mode when performing a VEM upgrade. If you do not have and also use VMware vCenter Update Manager 4.0 Update 1 Patch 2, vCLI build 198790, and VSM Release 4.0(4)SV1(2) or later, in order to have a non-disruptive upgrade.
- You must install VMware patch ESX/ESXi400-201002001 or the ESX/ESXi400-201006201-UG on the host, and also use VMware vCenter Update Manager 4.0 Update 1 Patch 2, vCLI build 198790, and VSM Release 4.0(4)SV1(2) or later, in order to have a non-disruptive upgrade.
- 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 Table 2.
- If you are installing the VEM software for the first time, you can install it before the Virtual Supervisor Module (VSM) is installed; however, verification and configuration of the VEM can only be done after installing the VSM.
- You have already downloaded the correct VEM software based on the current ESX/ESXi host patch level. For more information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4).*
- If you install the VEM software on an ESXi host before adding the host to a vSphere Server, you need to reboot the host. The alternative is to add the host to vSphere Server first, and then install the VEM software.
- If using VUM for a first-time installation, no action is required by the server administrator. VUM automatically installs the VEM software.

- If you use a proxy server to connect VUM to the Internet, you may need to disable the proxy before starting a VUM upgrade. In VMware versions before VUM Update 1, the proxy prevents VUM from communicating locally with the VSM. For this reason, automatic VEM upgrades may fail if the proxy is not disabled first.
- On upstream switches the following configuration is **mandatory**:
  - cat6k IOS:
    (config-if) **portfast trunk**
    or
    (config-if) **portfast edge trunk**
  - n5k: (config-if) **spanning-tree port type edge trunk**
- On upstream switches it is **highly recommended** that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, it is highly recommended that you configure the following:
  - (config-if) **spanning-tree bpdu filter**
  - (config-if) **spanning-tree bpdu guard**
- For more information about configuring spanning-tree, BPDU, or portfast, see the documentation for your upstream switch.

Choosing a VEM Software Installation or Upgrade Procedure

There are two possible use cases:

- Upgrading the ESX/ESXi Host with VEM Software Installed
  - If you are using VUM to upgrade the host, you will have to create a host patch baseline and include the appropriate VMware patch or update bulletins and the corresponding Cisco Nexus 1000V VEM bulletin in the baseline. You can then upgrade the host by applying the baseline to the host and remediating. To determine which VUM upgrade procedure you should follow, see "Upgrading the ESX/ESXi Host With VEM Software Installed Using VUM" section on page 7.
  - If you are using the CLI, use the **vihostupdate** command or the **esxupdate** command. See the "Upgrading the ESX/ESXi Host with VEM Software Installed Using the CLI" section on page 40.
- Installing or Upgrading the VEM Software
  - If you are using VUM, then the Cisco Nexus 1000V VEM software will be installed automatically when the host is added to the Cisco Nexus 1000V DVS. When VEM upgrades are triggered from the VSM, the VEM software will be automatically upgraded on the host. To determine which VUM upgrade procedure you should follow, see Installing or Upgrading the VEM Software Using VUM, page 43.
  - If you are using the CLI, use the **vihostupdate** command or the **esxupdate** command. See the "Installing or Upgrading the VEM Software Using the CLI" section on page 44.

Upgrading the ESX/ESXi Host With VEM Software Installed Using VUM

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

This section describes the procedures for installing and upgrading from ESX/ESXi 4.0.0 Update 1 to ESX/ESXi 4.0.0 Update 1 Patch 04 and ESX/ESXi 4.0.0 to ESX/ESXi 4.1.0. Choose the procedure that is appropriate to your environment.

- Patching ESX/ESXi 4.0.0 Update 1 with ESX/ESXi400-201002001 (P04), page 7
- Upgrading from VMware Release 4.0 to VMware Release 4.1, page 17

Patching ESX/ESXi 4.0.0 Update 1 with ESX/ESXi400-201002001 (P04)

BEFORE YOU BEGIN

Before you begin this procedure, you must know or do the following:

Caution Disabling the HTTP server prevents VEM from upgrading the VEMs. For more information, see *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4)*.

- Make sure that you have the VMware Update Manager installed on your VMware vCenter Server. For more information, see the *VMware vCenter Update Manager Administration Guide*.
- All VMware patches require that the host be placed in maintenance mode.

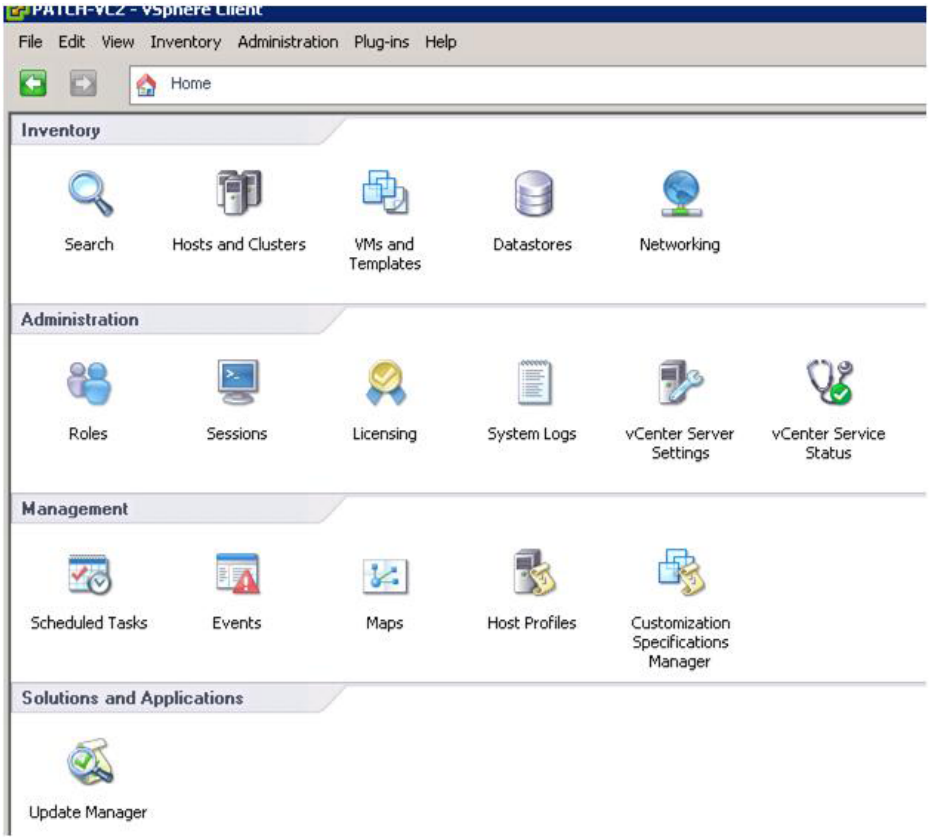
Note VUM U1-ESX400-P02 (282702) is mandatory for all upgrades.

- Determine which version of VMware you are upgrading from by running the **vem version** command on the ESX/ESXi hosts.
- Check *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)*.
- See Table 2 for software download locations.
- The entire Cisco zip bundle needs to be downloaded and extracted to get the appropriate VEM vib file. The file name is similar to Nexus1000v-4.2.1.SV1.4.zip.
- You are logged in to the VMware vSphere Client.

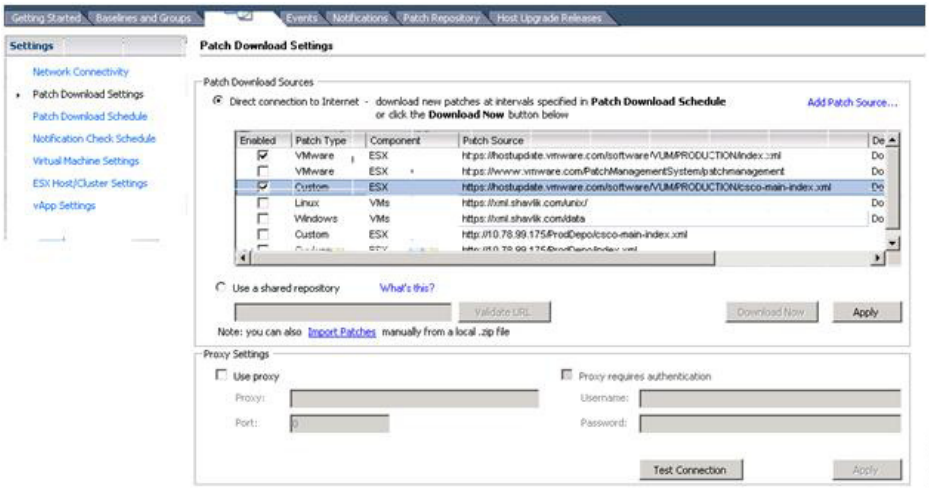
PROCEDURE

You can use the following procedure to upgrade the VEM software from ESX/ESXi 4.0.0 Update 1 to ESX/ESXi 4.0.0 Update 1 Patch 04.

Step 1 From the VMware vSphere Client window, click the **Update Manager** icon.



The Update Manager Administration window opens.



Step 2 To configure the VMware Update Manager, click the **Configuration** tab and check the **Enabled** check boxes for the VMware patch source and the Cisco patch source.

The appropriate links are:

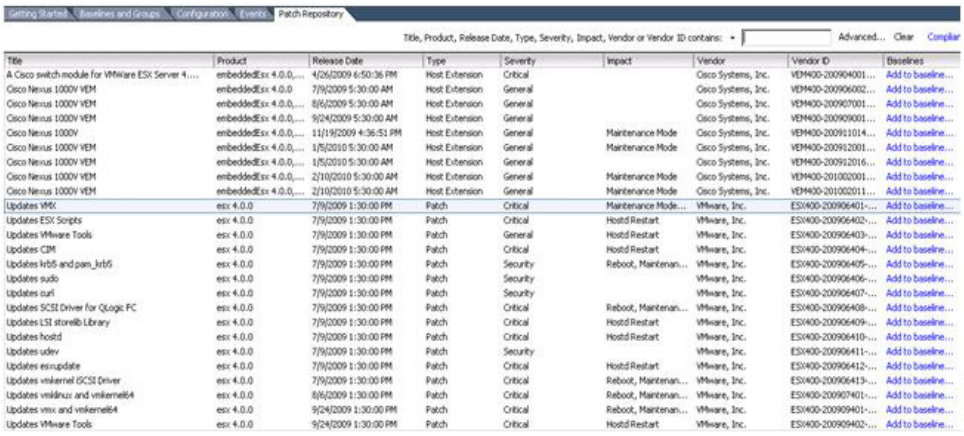
- https://hostupdate.vmware.com/software/VUM/PRODUCTION/index.xml
- https://hostupdate.vmware.com/software/VUM/PRODUCTION/csco-main-index.xml

Note If you are behind a proxy, you might need to specify the required proxy server settings to access the Internet.

Step 3 To apply the settings, click **Apply** and **Download Now**.

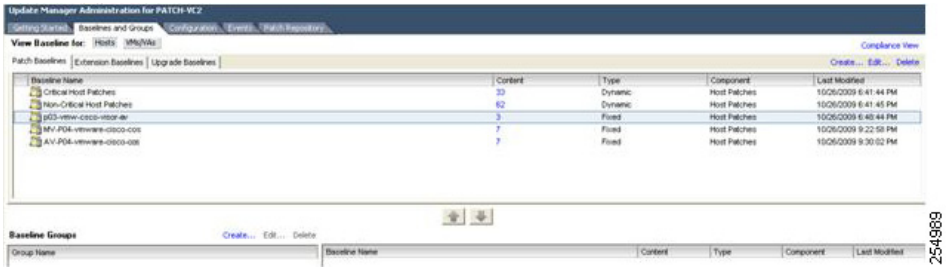
Step 4 To display the list of all available patches on the Cisco Nexus 1000V VSM and patches which are on the portals, click the **Patch Repository** tab.

The Patch Repository window opens where you can confirm that the patches are being downloaded.



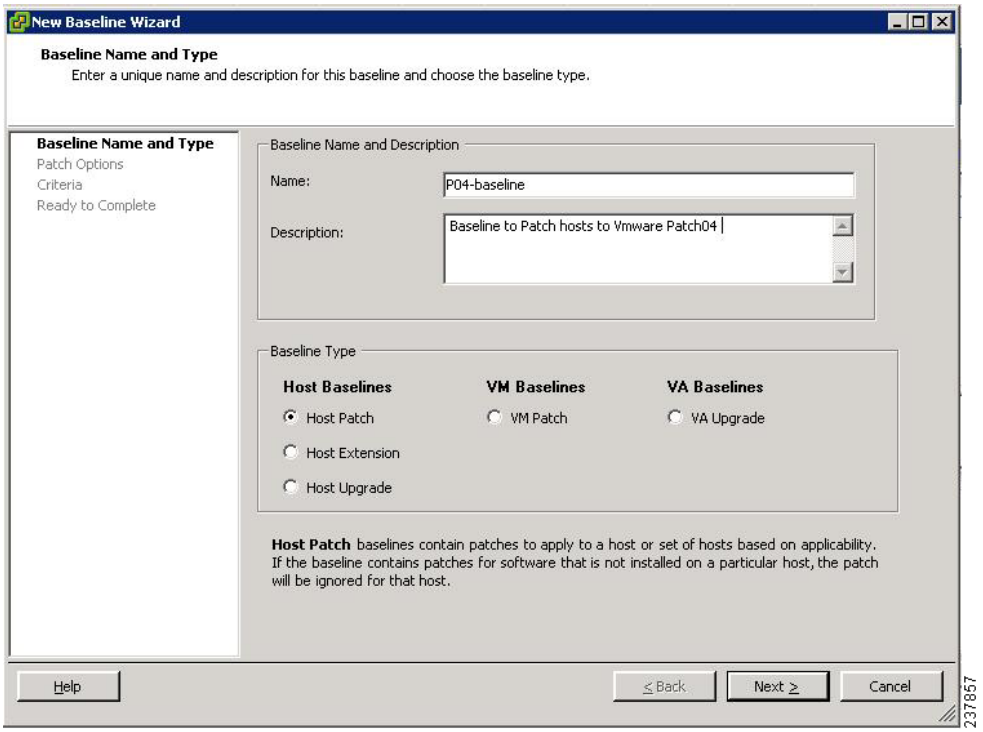
Step 5 To patch the ESX/ESXi host by using a baseline, click the **Baselines and Group** tab.

Note You need to select the bulletin numbers based on the patch that you are installing. Consult *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* and refer to the VEM Bundle for the VMware Software Version you are patching.



Step 6 To create a new baseline, click the **Create** link at the upper right-hand corner of the window.

The New Baseline Wizard screen opens.

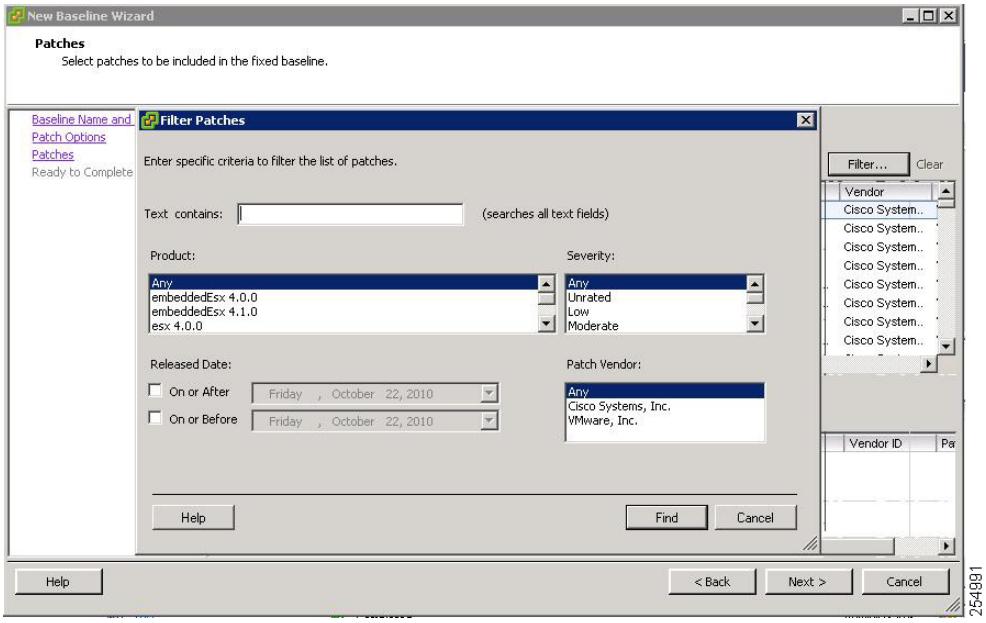


Step 7 Enter a name in the **Name** field, click the **Host Patch** radio button, and click **Next**.

The Patch Options screen opens.

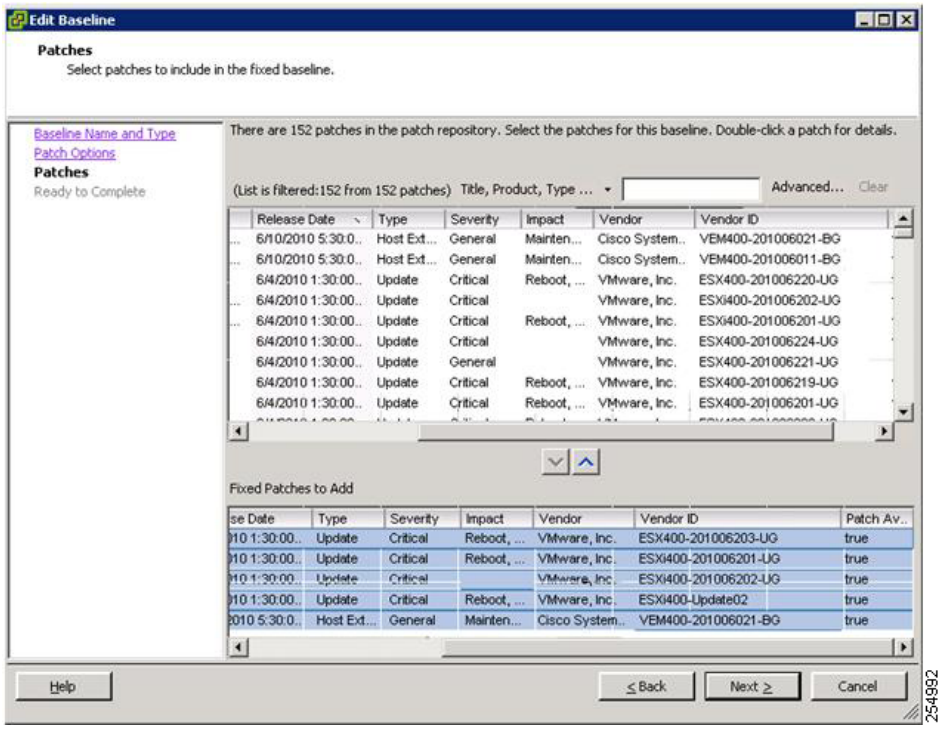
Step 8 In the Patch Options screen, click the **Fixed** radio button and click **Next**.

The Filter Patches screen opens.



Step 9 Select from the **Product** field for the product that matches your environment, choose the appropriate Patch Vendor, and click **Find**.

The Patches window opens.

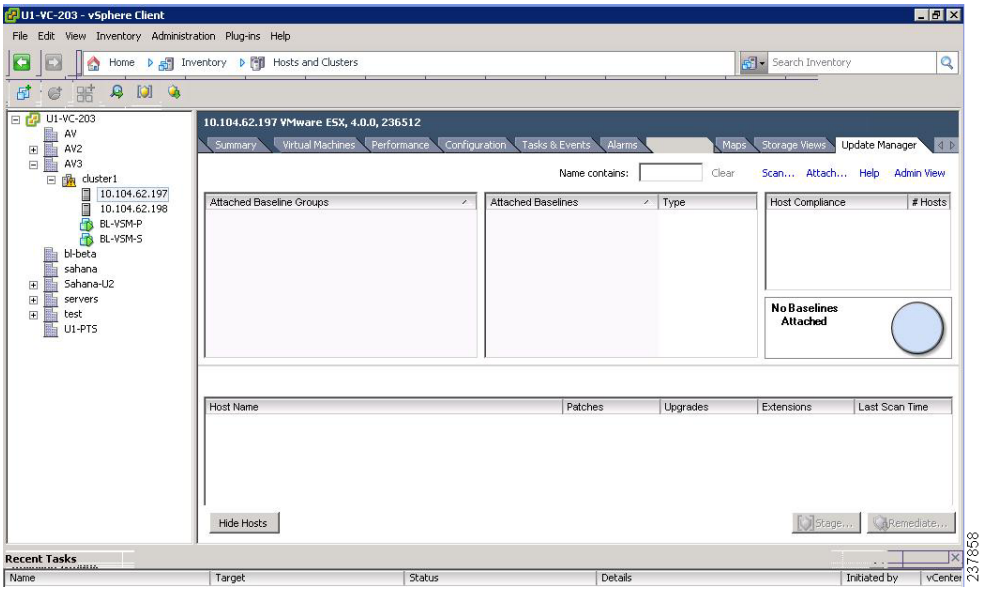


Step 10 To add patches to the baseline, select the appropriate patches from the upper half of the screen and click the down arrow.

The patch is added to the Fixed Patches to Add section.

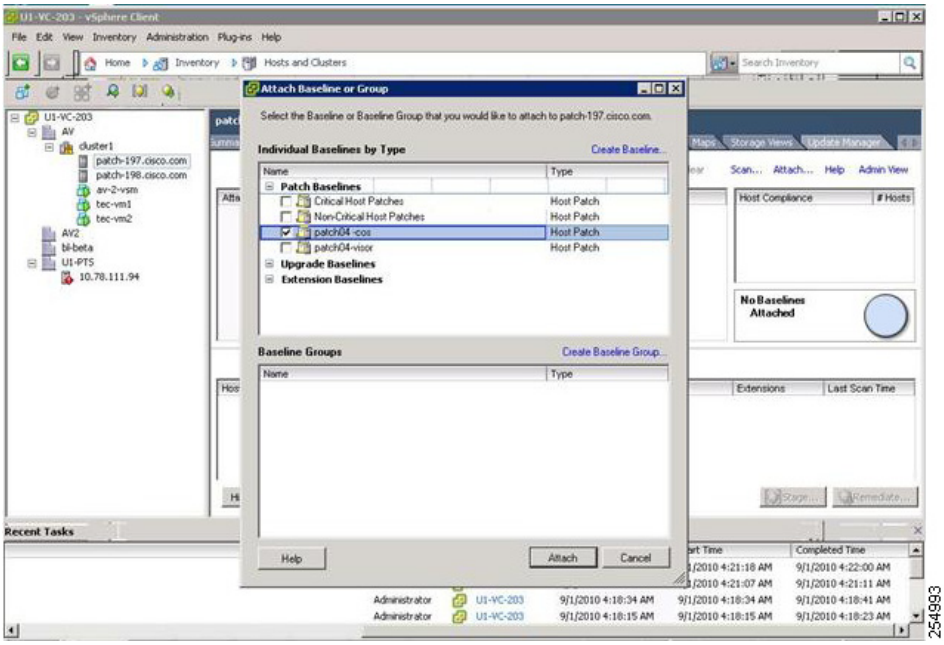
Step 11 When you have added all patches, click **Next**.

The Update Manager window opens.



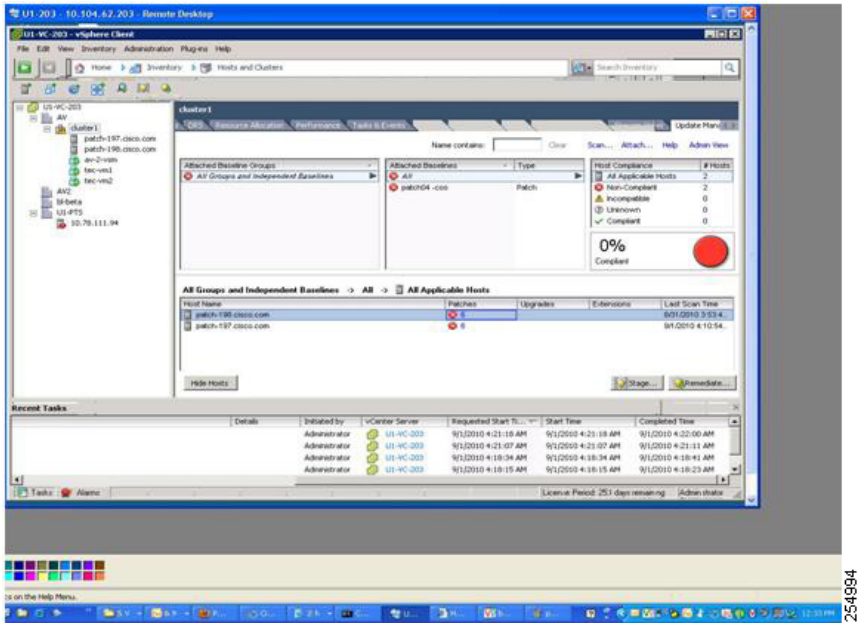
Step 12 Select either a host or cluster to be patched and click the **Attach** link.

The Attach Baseline or Group window opens.



Step 13 Select the check box of the baseline that you previously created and click **Attach**.

The Update Manager window opens.



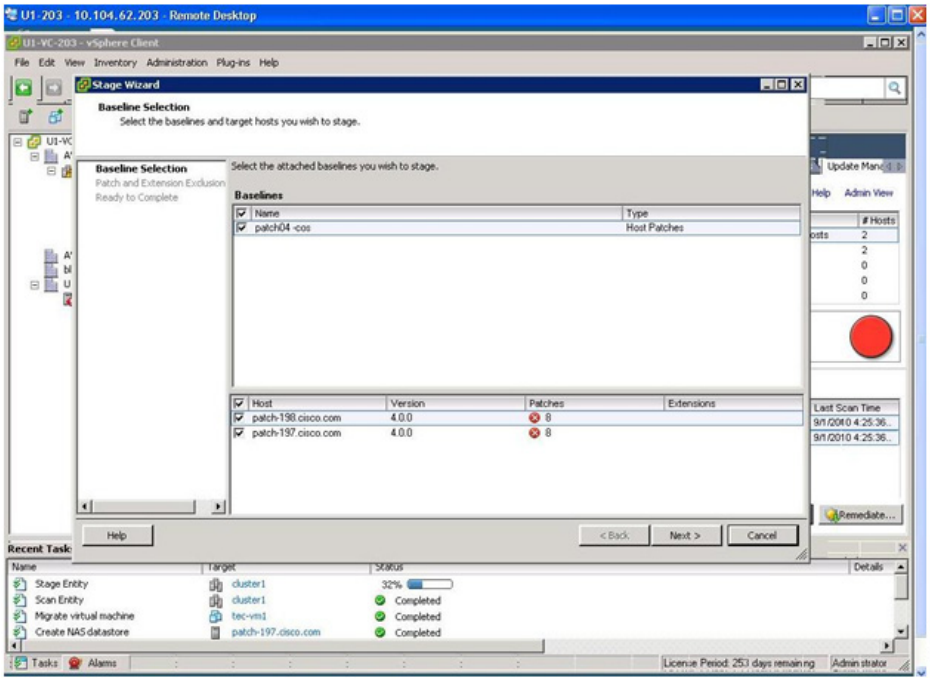
Step 14 In the Update Manager window, click the **Scan** link.

The Confirm Scan window opens.

Step 15 Click the **Scan** button.

Step 16 In the Update Manager window, click **Stage**.

The Stage Wizard screen opens.

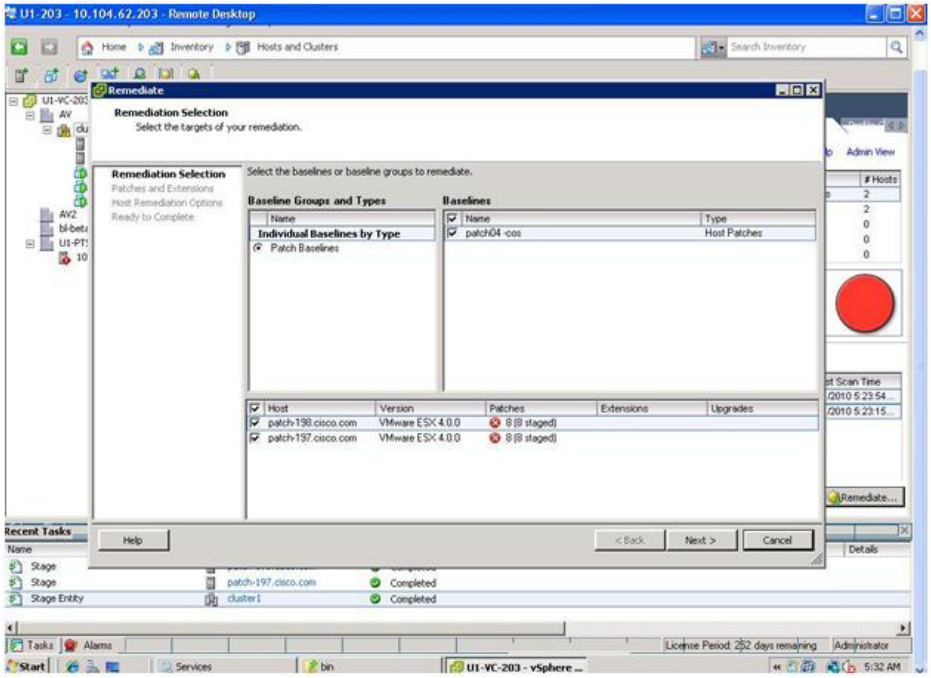


Step 17 Click **Next** and click **Finish.**

Note The Staging process will take some time to complete depending on the patches. Once staging is complete, look for the patches displaying a staged status.

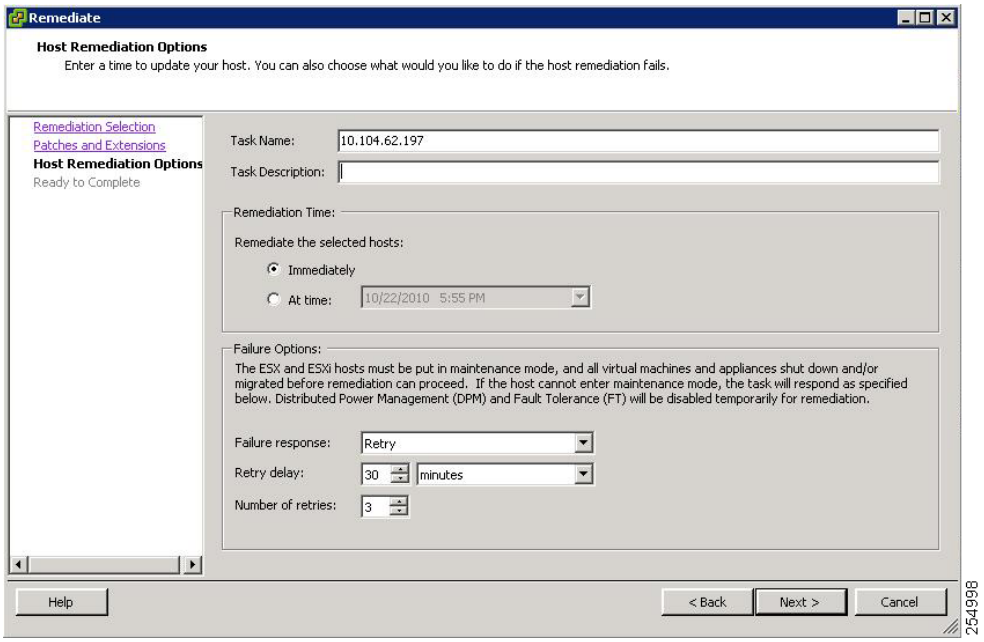
Step 18 Click **Remediate** in the Update Manager window.

The Remediate window opens.



Step 19 Click **Next** in the Remediation Selection window.

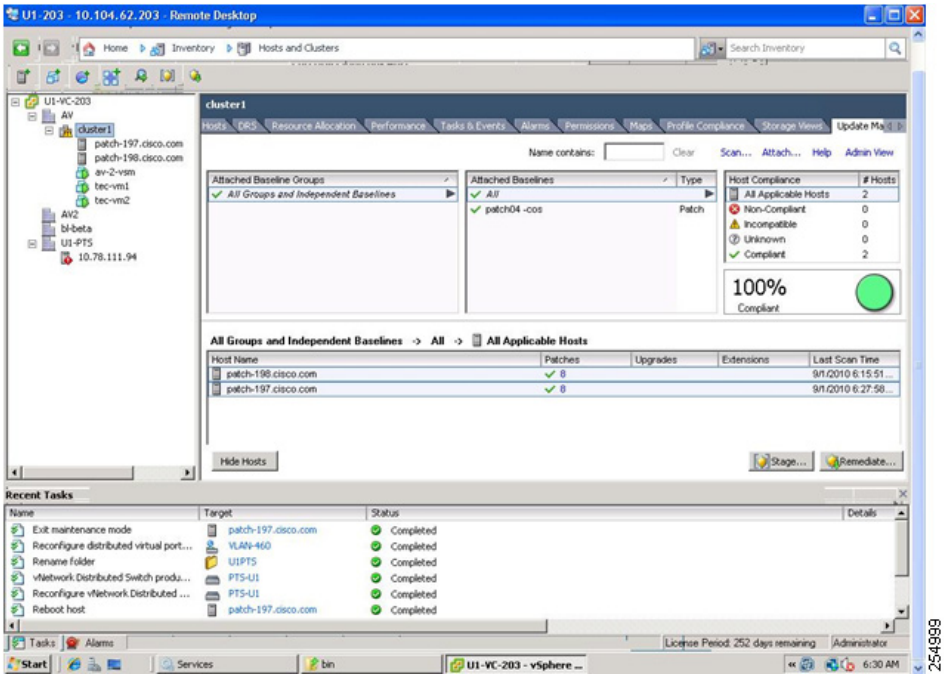
The Host Remediation Options window opens.



Step 20 Click **Next**.

Step 21 To remediate the baseline, click **Next**.

Note This process will take time to complete based on the clusters, the number of hosts in the clusters, and on the patch that is being applied. This process involves automatically putting the host in maintenance mode, applying the patch, rebooting the host, and removing the host from maintenance mode.

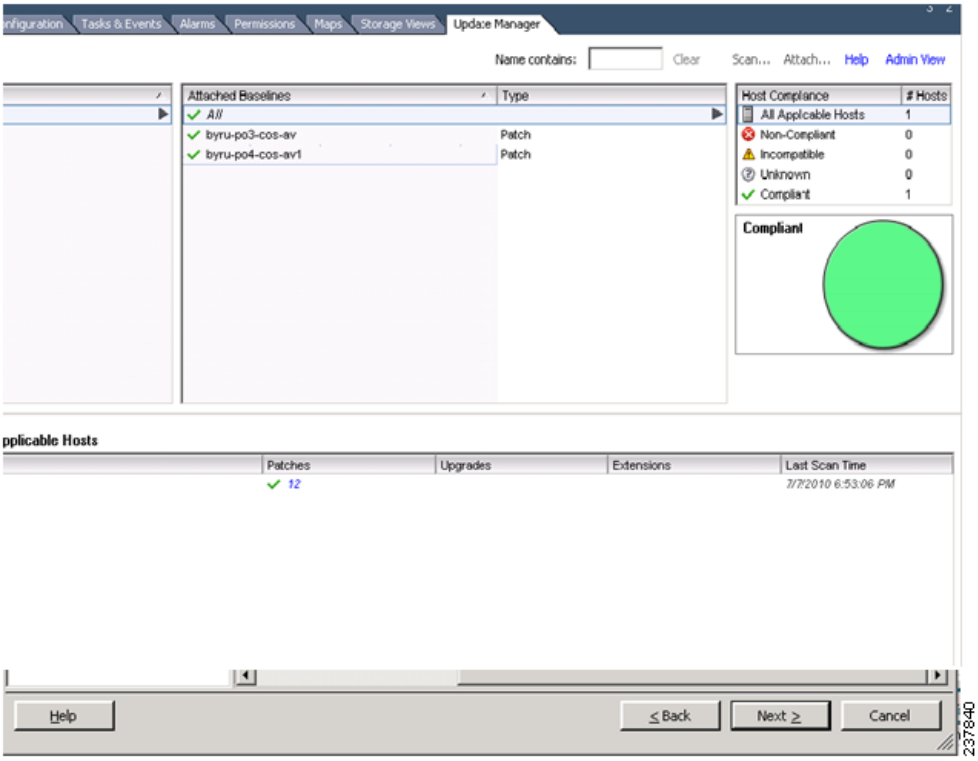


Step 22 Once remediation is complete, the Update Manager window displays 100% complete.

You have completed the patching procedure.

Verifying the Patch Upgrade on VUM

Step 1 Click the **Update Manager** tab.



The status of the applied patch and the compliance view are displayed.

Step 2 To verify the build number on the ESX/ESXi host, run the following commands:

```
[root@hostname~] # rpm -qa | grep vmkernel | awk -F. '{print $5}'
236512

~ # vmware -v
VMware ESXi 4.0.0 build-236512
```

Upgrading from VMware Release 4.0 to VMware Release 4.1

You can use this procedure to upgrade from VMware Release 4.0 to VMware Release 4.1.

BEFORE YOU BEGIN

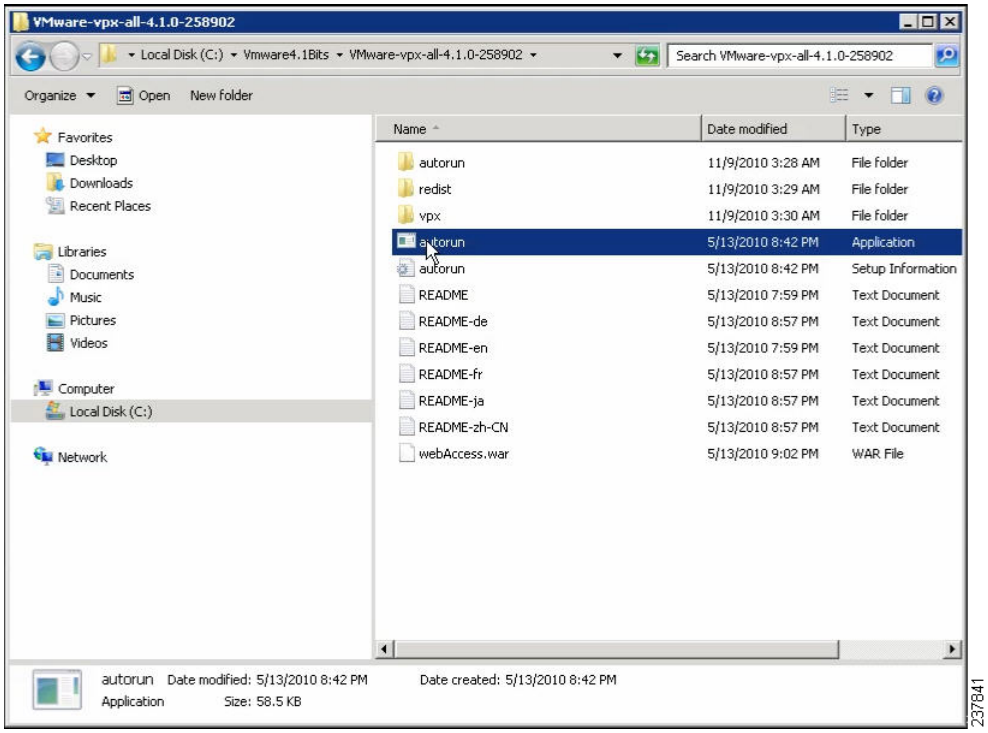
Before beginning this procedure, you must know or do the following:

- ESX/ESXi 4.1.0 vCenter Server and ESX/ESXi 4.1.0 Update Manager
- Download the upgrade ZIP bundle to a local desktop or vCenter Server.
  - For ESX, download upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip
  - For ESXi, download upgrade-from-ESXi4.0-to-4.1.0-0.0.260247-release.zip
  - For Cisco Nexus 1000V, download the bundle from www.cisco.com (VEM-4.1.0-GA-v120.zip)

- Consult the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* document to determine the correct VIB Version, VEM Bundle, Host Build, vCenter Server, and Update Manager versions.
- Upgrading the ESX/ESXi hosts consists of the following procedures:
  - Upgrading the vCenter Server, page 18
  - Upgrading the vCenter Update Manager, page 23
  - Upgrading the ESX/ESXi Hosts, page 27

Upgrading the vCenter Server

Step 1 Navigate to the VMware-vpx-all-4.1.0-258902 folder.



Step 2 Double-click **autorun**.

The VMware vCenter Installer window opens.

Step 3 Click **vCenter Server**.

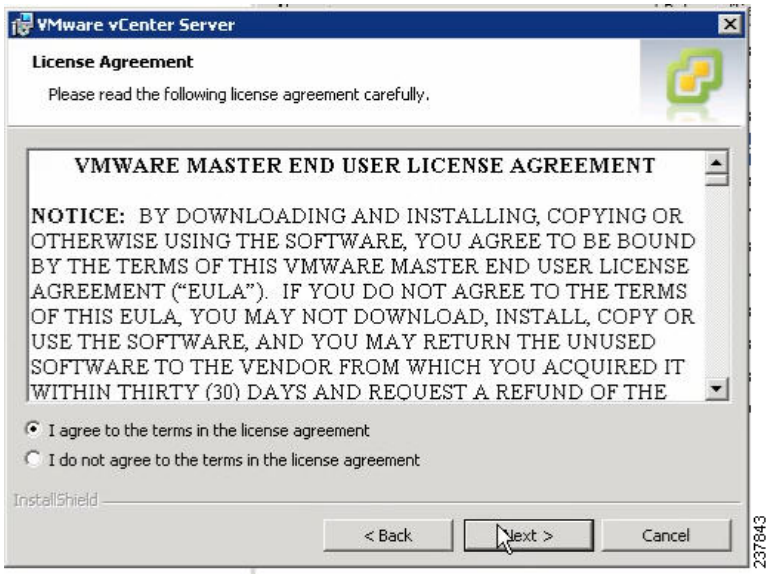
Step 4 Select a language and click **OK**.

The Installation Wizard opens.

Step 5 Click **Next**.

Step 6 In the Patent Agreement window, click **Next**.

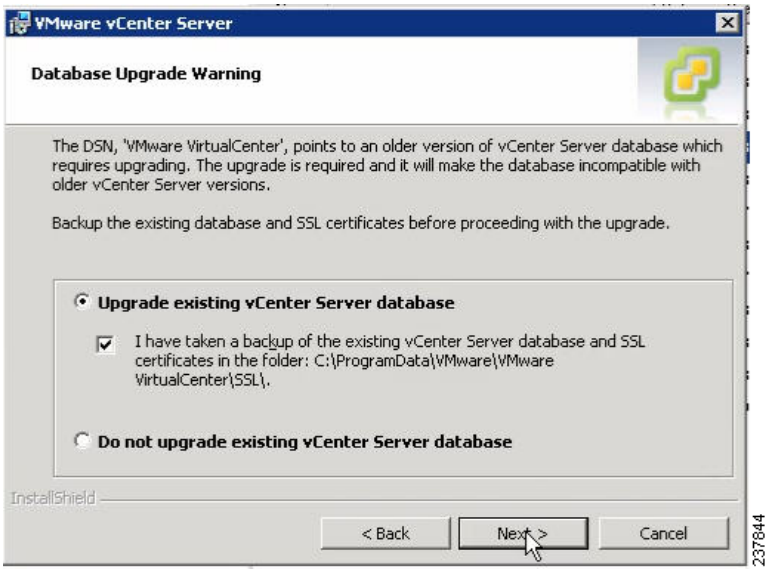
The License Agreement window opens.



Step 7 Click the **I agree to the terms in the license agreement** radio button and click **Next**.

Step 8 In the Database Options window, click **Next**.

The Database Upgrade Warning window opens.



Step 9 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 10 From the Windows Start Menu, click **Run**.

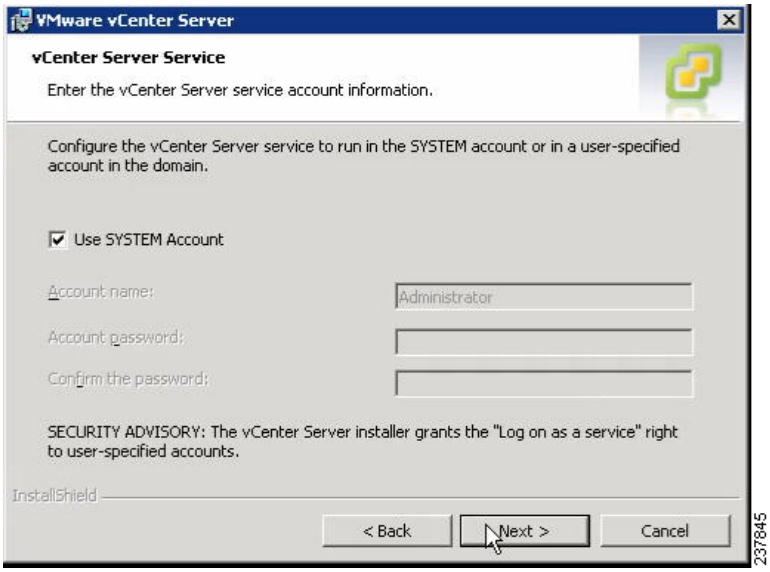
Step 11 Enter the name of the folder that contains the vCenter Server database and click **OK**.

Step 12 Drag a copy of the parent folder (SSL) to the Desktop as a backup.

Step 13 Return to the installer program and click **Next**.

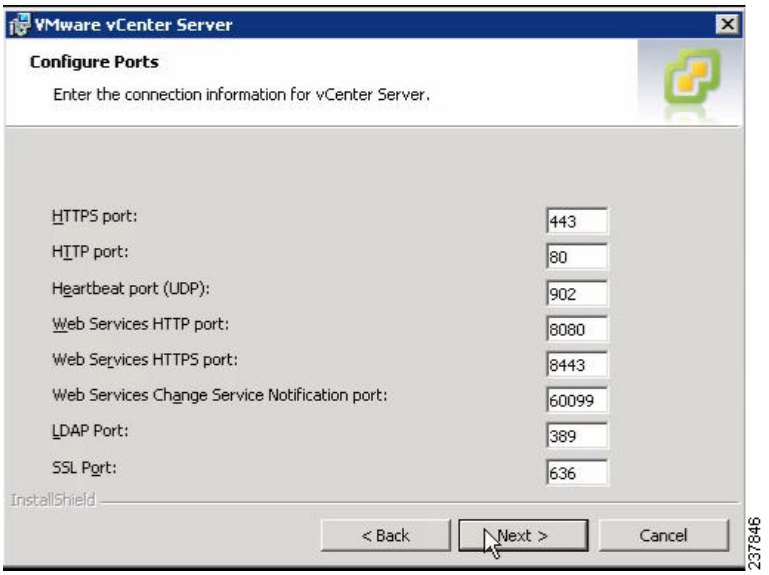
Step 14 In the vCenter Agent Upgrade window, click the **Automatic** radio button and click **Next**.

The vCenter Server Service window opens.



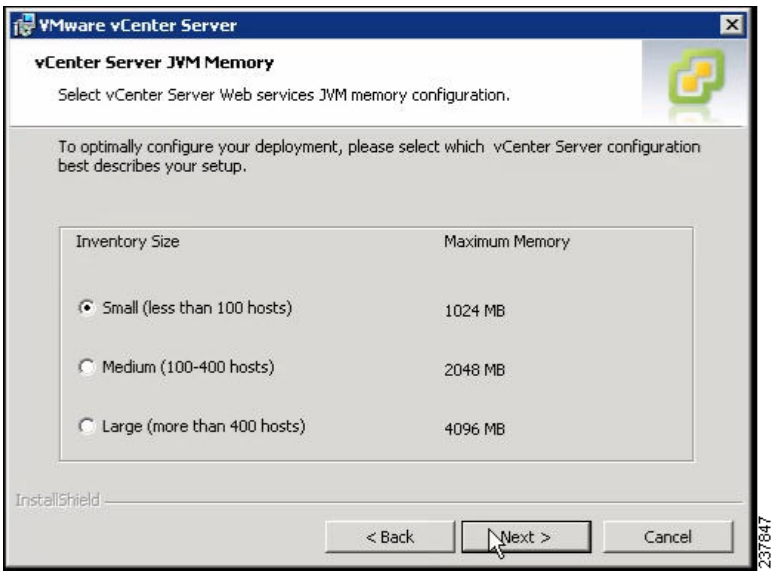
Step 15 Check the **Use SYSTEM Account** check box and click **Next**.

The Configure Ports window opens.



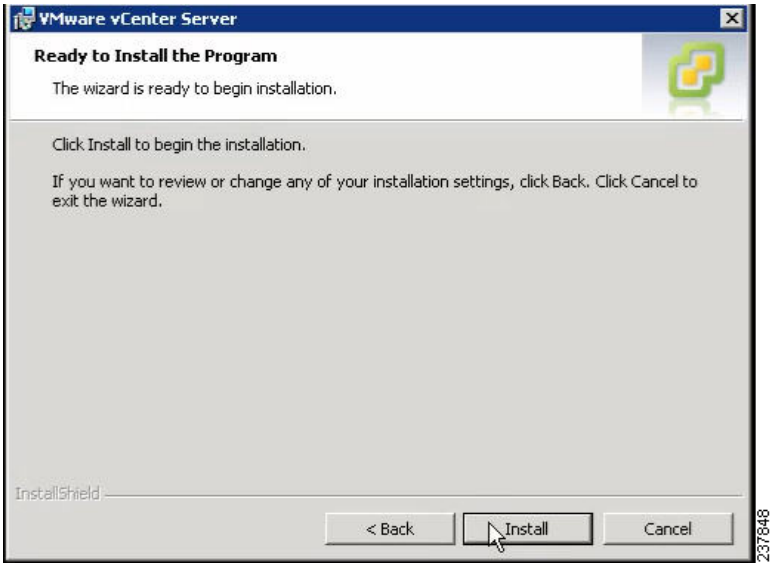
Step 16 Review the port settings and click **Next**.

The vCenter Server JVM Memory window opens.



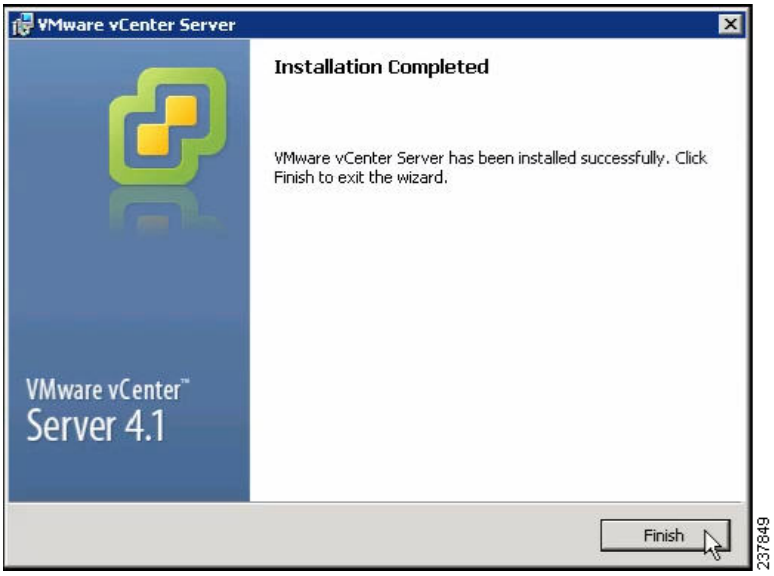
Step 17 Based on the number of hosts, click the appropriate memory radio button and click **Next**.

The Ready to Install the Program window opens.



Step 18 Click **Install**.

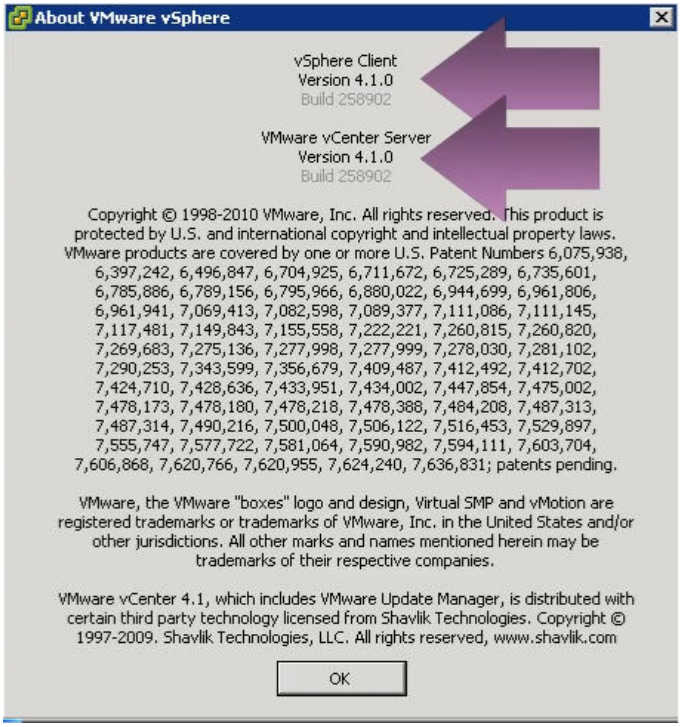
The Installation Completed window appears.



Step 19 Click **Finish**.

Step 20 Open the VMware vSphere Client.

Step 21 From the Help menu, choose **About VMware vSphere**.



Step 22 Confirm that the vSphere Client and the VMware vCenter Server are both version 4.1.0, Build 258902, click **OK**, and exit the VMware vSphere Client.

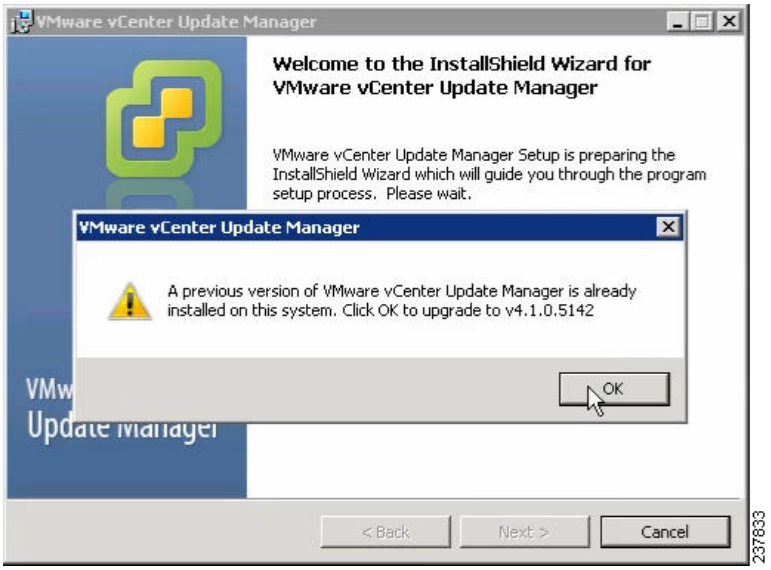
Upgrading the vCenter Update Manager

Step 1 Copy the VUM bundle to the local drive.

Step 2 On the local drive, double-click **VMware-UpdateManager**.

Step 3 Select a language and click **OK**.

The Update Manager Installer opens.



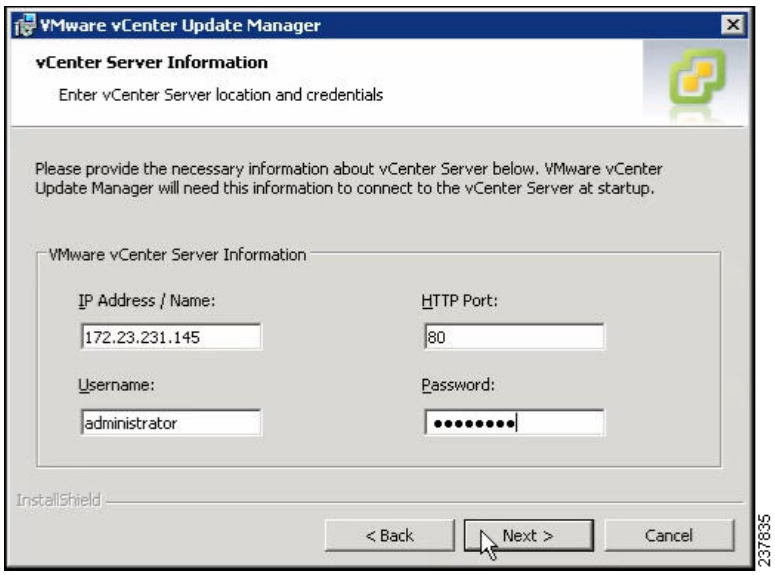
Step 4 Click **OK** to upgrade to 4.1.

Step 5 Click **Next** to begin.

Step 6 Click **Next** at the Patent Agreement.

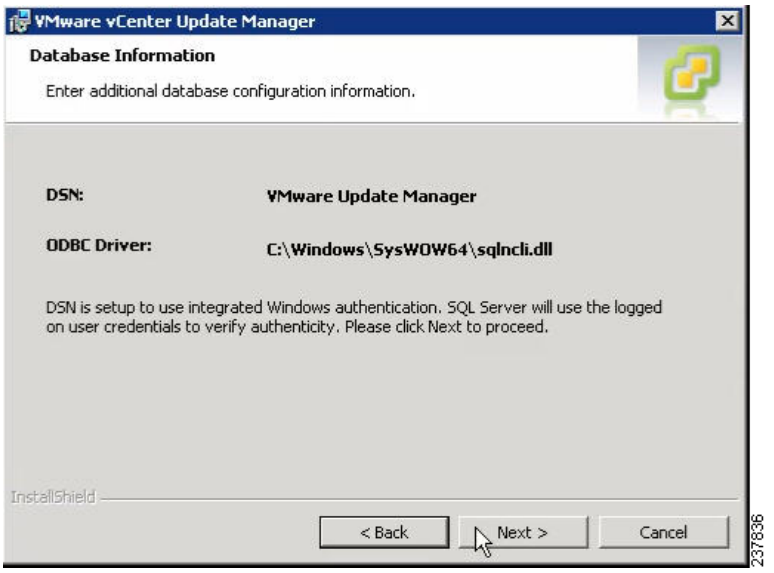
Step 7 Click the **I agree to the terms in the license agreement** radio button and click **Next**.

The vCenter Server Information window opens.



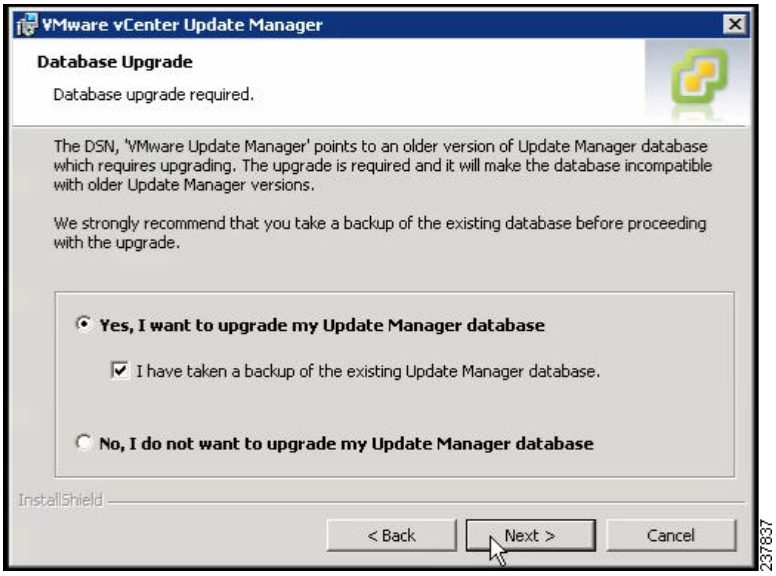
Step 8 Verify the IP Address and Username, enter the Password and click **Next**.

The Database Information window opens.



Step 9 Click **Next.**

The Database Upgrade window opens.



Step 10 Click the **Yes, I want to upgrade my Update Manager database** radio button and click **Next**.

Step 11 Verify the Update Manager port settings and click **Next**.

Step 12 Verify the Proxy Settings and click **Next**.

Step 13 Click **Install** to begin the upgrade.

Step 14 Click **OK** to acknowledge that a reboot will be required to complete the setup.

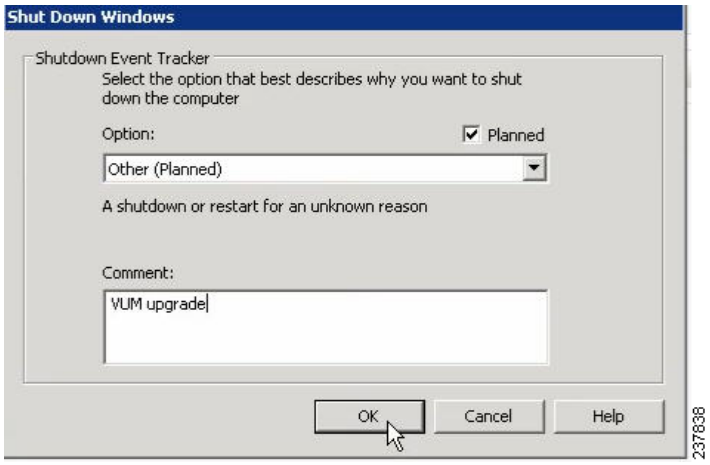
Step 15 During the upgrade, the vSphere Client is disconnected. Click **Cancel** for the attempt to reconnect.

Step 16 Click **OK** in the **Server Connection Invalid** dialog box.

Step 17 Click **Finish**.

Step 18 Reboot the local PC.

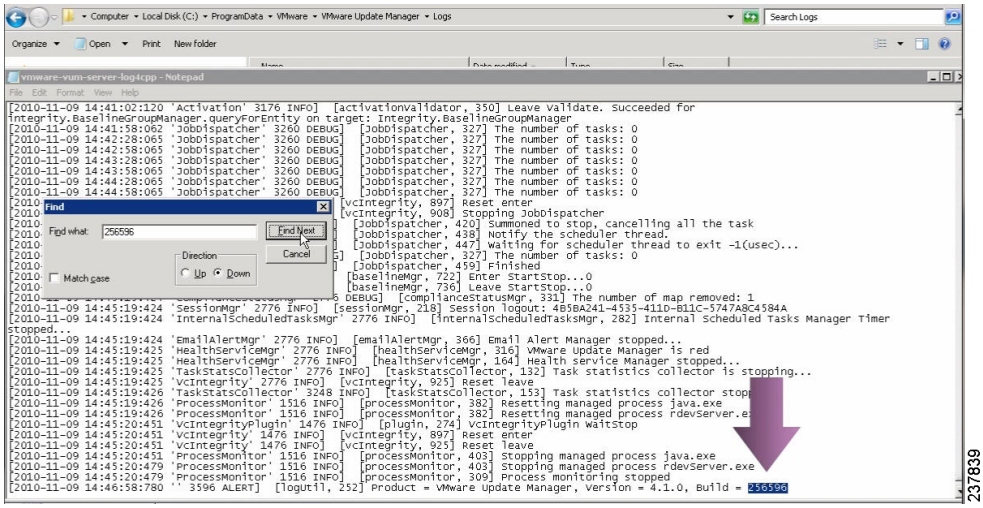
The Shut Down Windows window opens.



Step 19 From the Option drop-down list, choose **Other (Planned)**, enter a value in the comment field, and click **OK**.

Step 20 After the system has rebooted, browse to the **C:\ProgramData\VMware\VMware Update Manager\Logs** folder.

Step 21 Open the vmware-vum-server-log4cpp file.

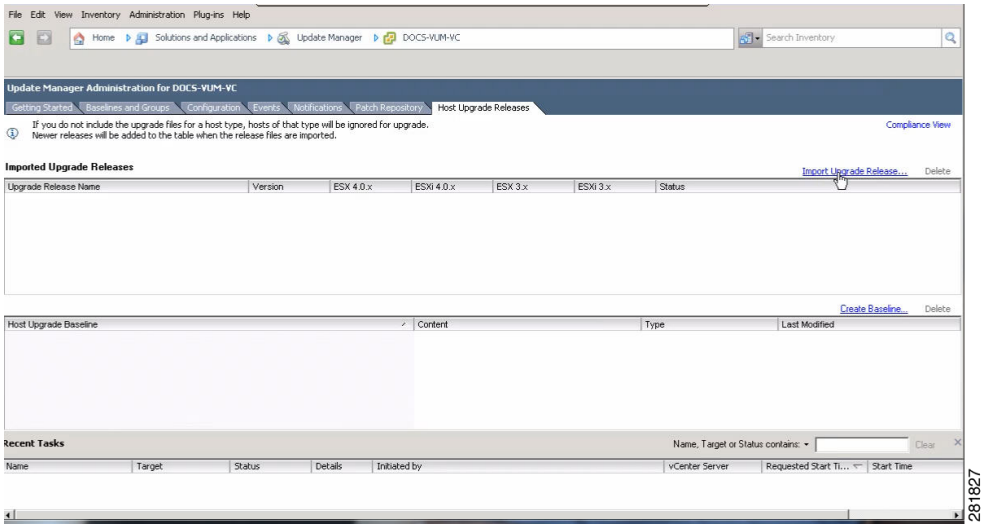


Step 22 Verify the Update Manager version in the log files by searching for the Update Manager build number of 256596.

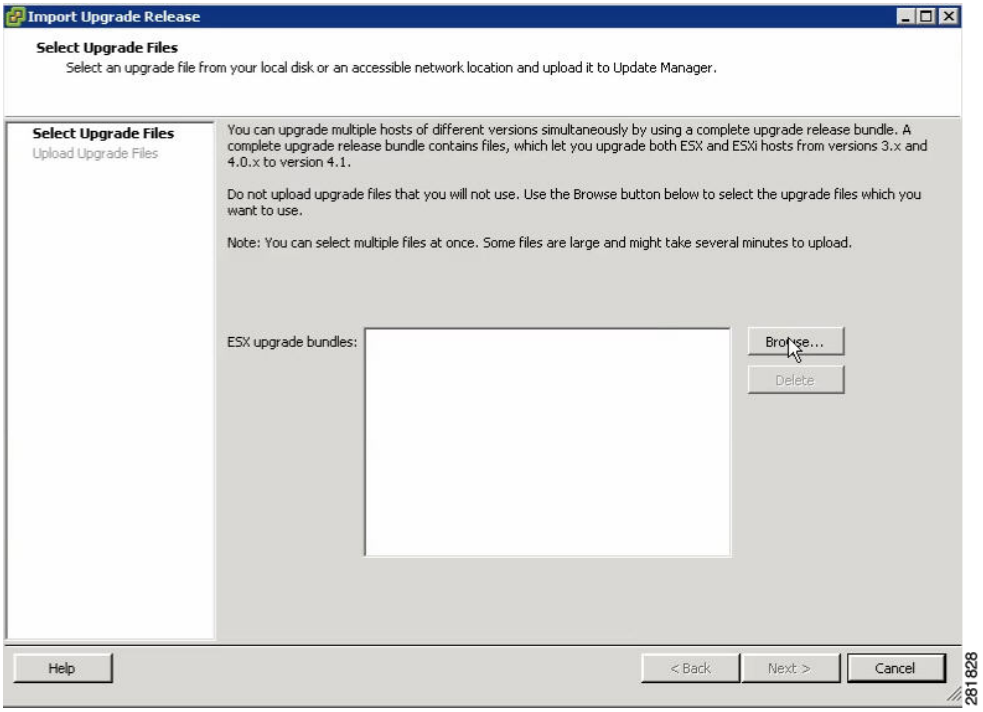
Upgrading the ESX/ESXi Hosts

Step 1 In the vSphere Client, click **Home** and click **Update Manager**.

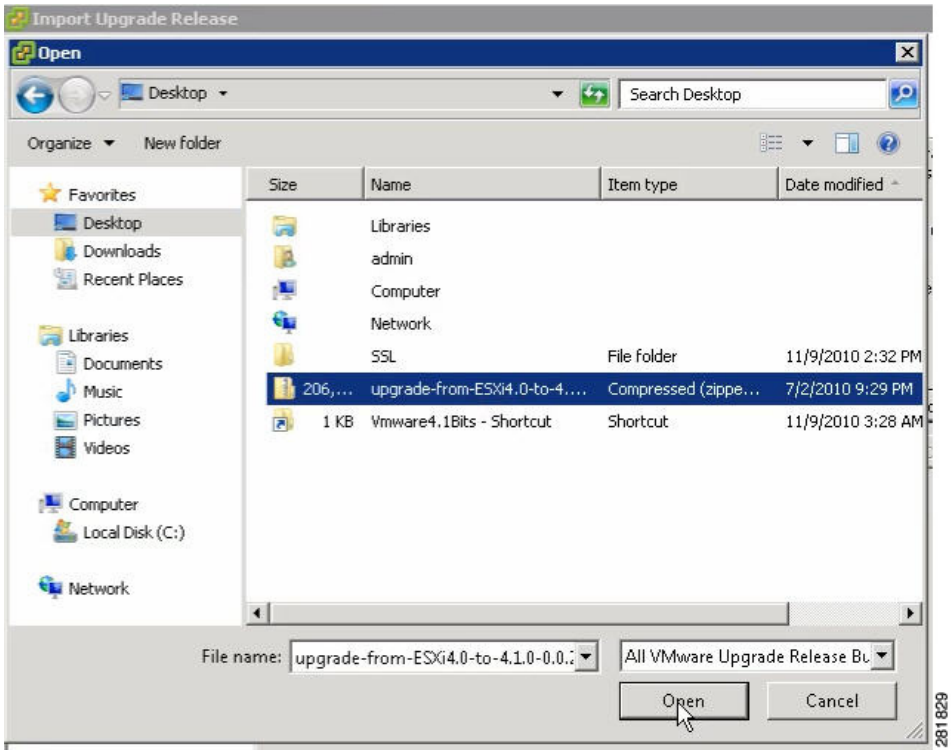
Step 2 Click the **Host Upgrade Releases** tab.



Step 3 Click **Import Upgrade Release**.

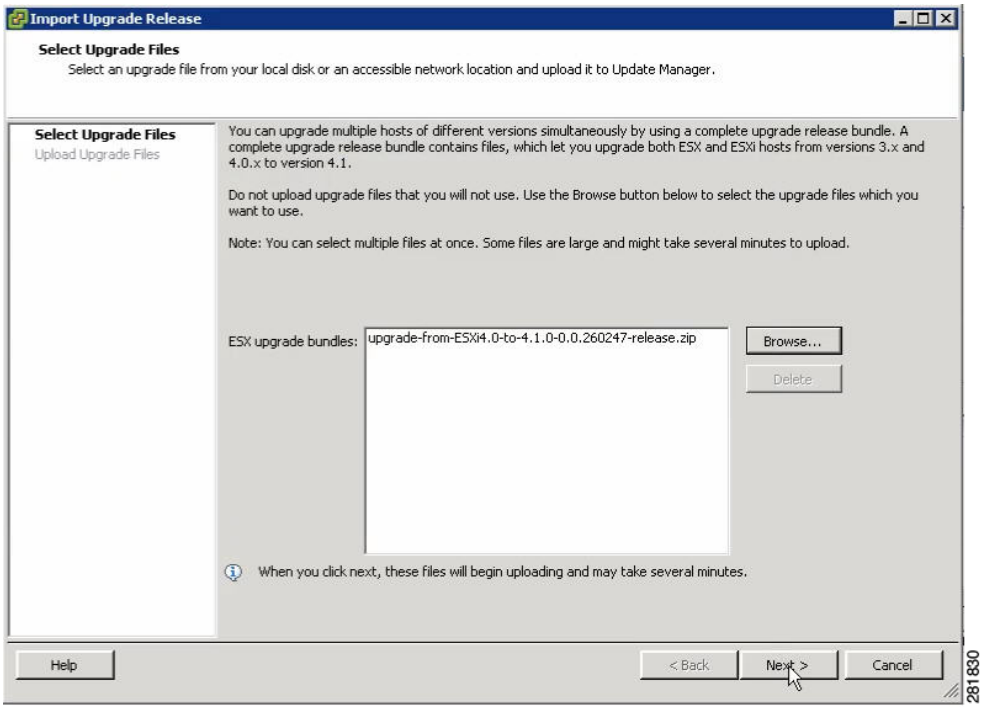


Step 4 Click **Browse** and navigate to the location of the upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip Zip bundle.



Step 5 Select the Zip file and click **Open**.

The Select Upgrade Files window opens.



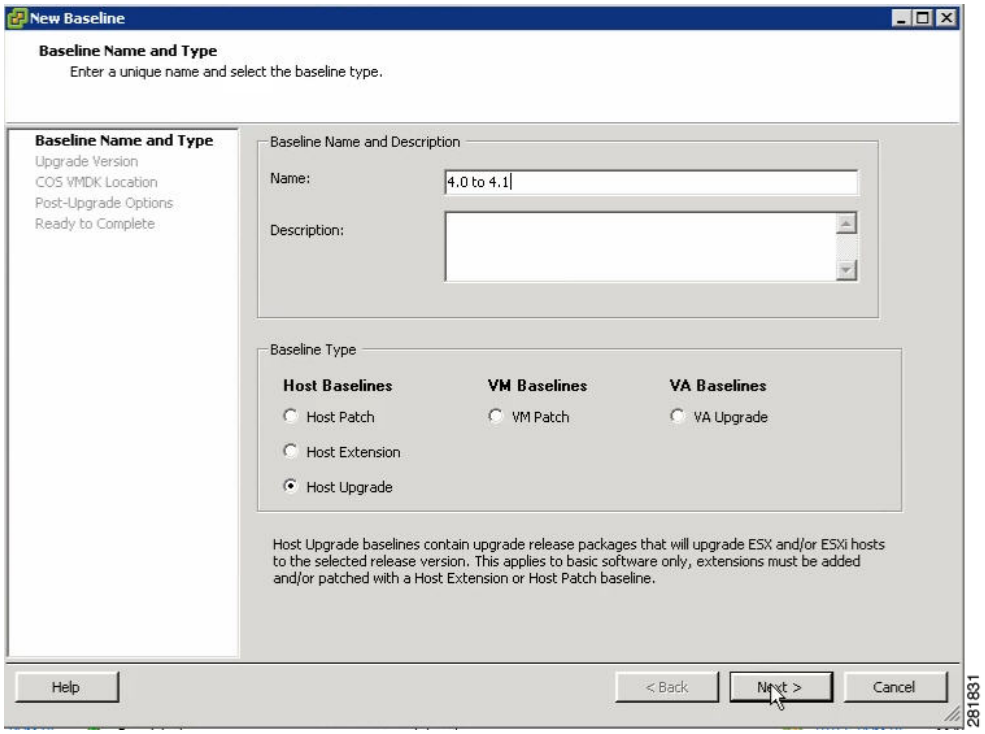
Step 6 Click **Next**.

Step 7 If you receive a Security Warning about the certificate, you can install the certificate or ignore the warning.

Step 8 When the upload is successful, click **Finish**.

Step 9 To create a baseline, in the **Host Upgrade Releases** tab, click **Create Baseline**.

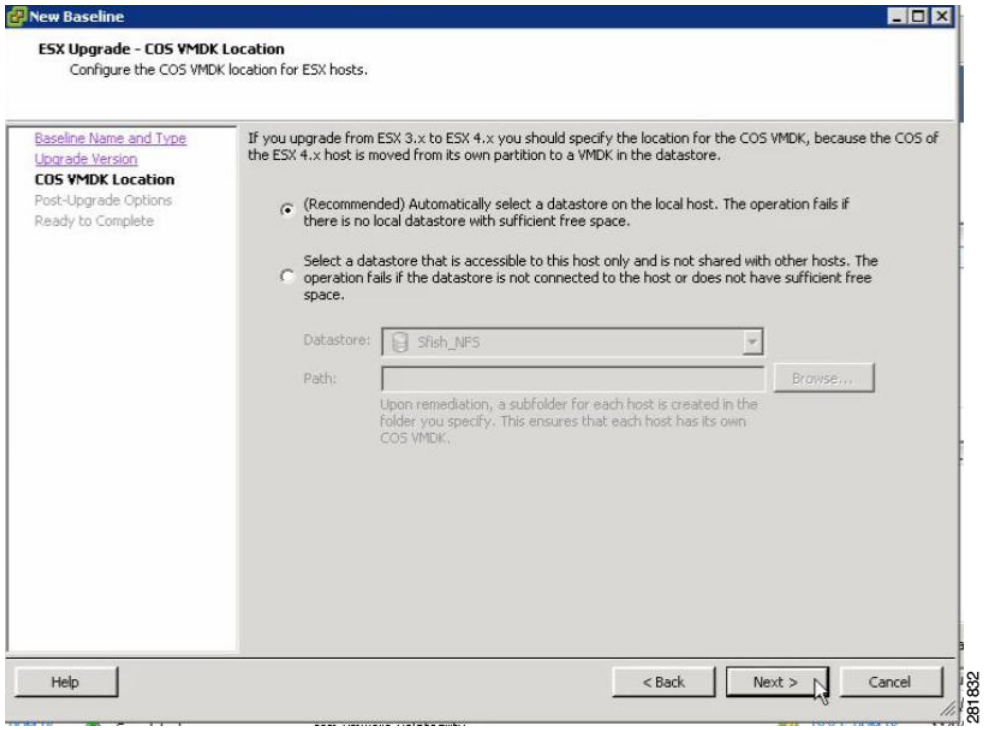
When you create a baseline and attach it to a host or cluster, the Update Manager can remediate the device applying all updates needed to bring it into compliance with the baseline.



Step 10 Enter a Name, click the **Host Upgrade** radio button and click **Next**.

Step 11 Click the Host Upgrade Release and click **Next**.

The COS VMDK Location window opens.



Step 12 Click **Next**.

Step 13 Click the **Try to reboot the host and roll back the upgrade in case of failure** check box and click **Next**.

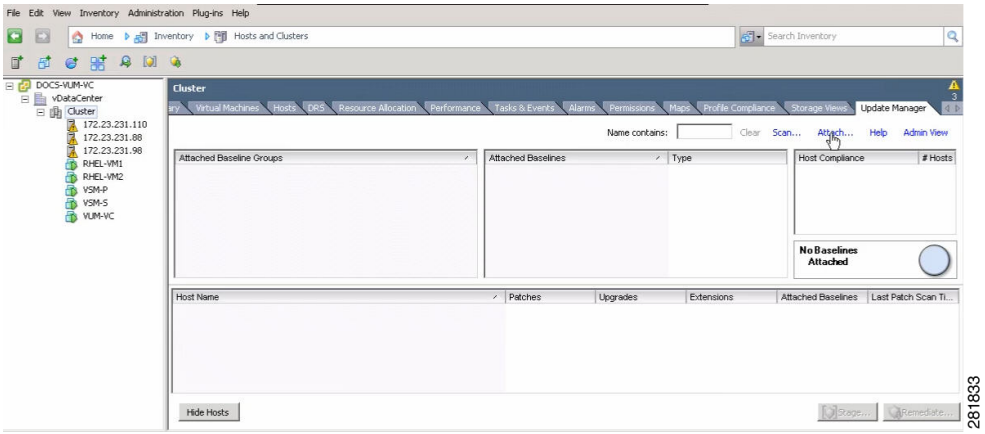
Step 14 Review the upgrade information and click **Finish**.

The baseline has been created.

Step 15 Click **Home** and click **Host and Cluster Inventory** tab.

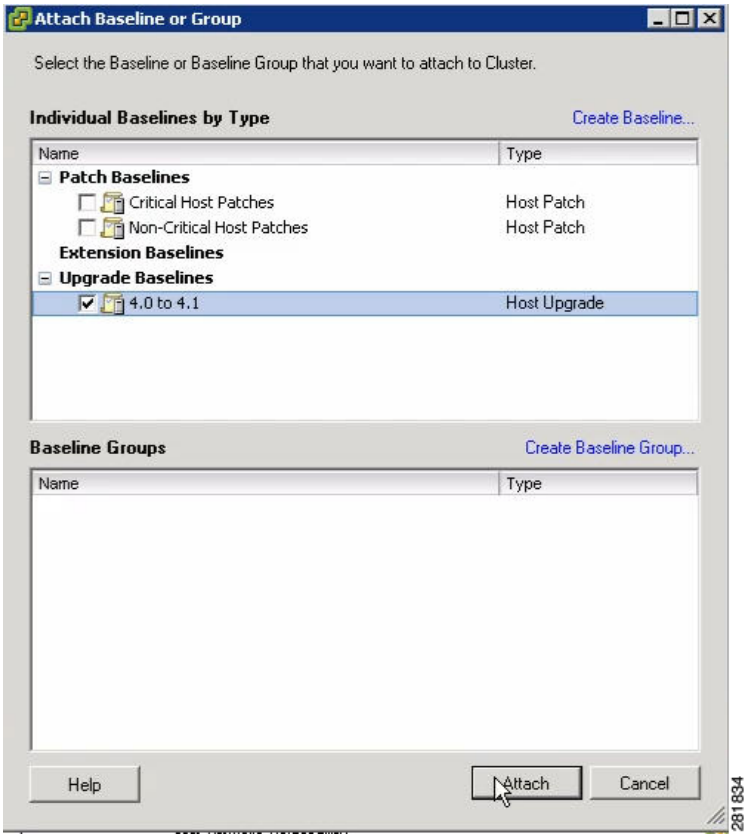
Step 16 Click the **Cluster** icon to upgrade all hosts in the cluster.

Step 17 Click the **Update Manager** tab.

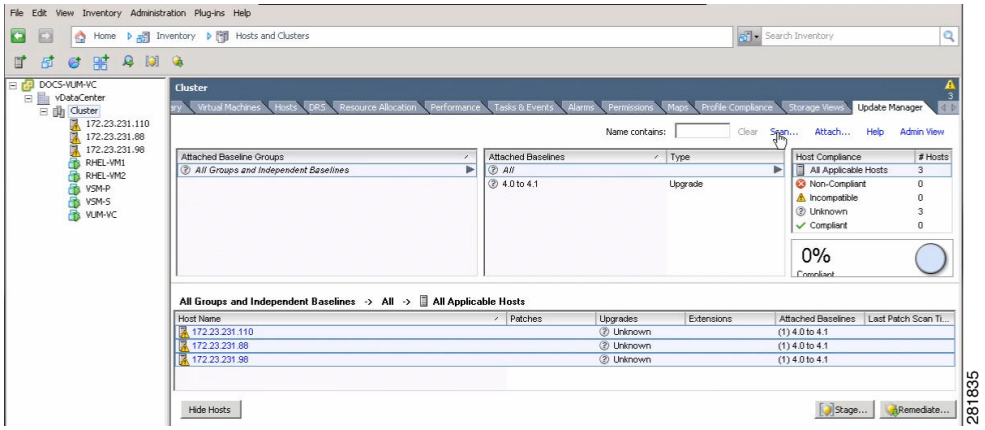


Step 18 Click **Attach**.

The Attach Baseline or Group window opens.

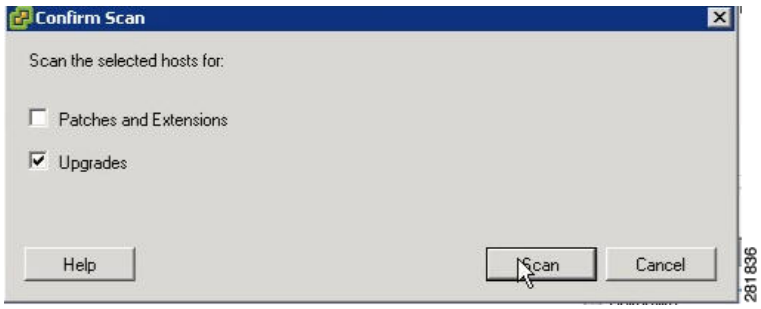


Step 19 Check the **4.0 to 4.1** check box and click **Attach**.

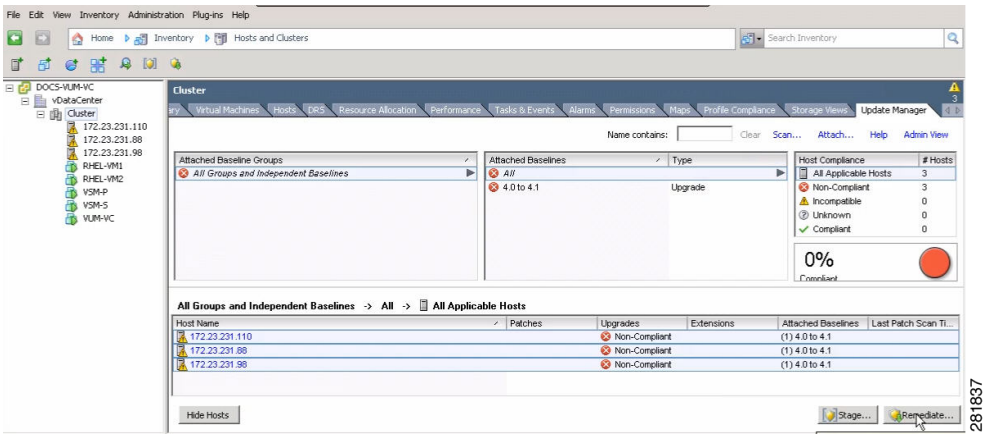


Step 20 Click **Scan** to test the cluster's compliance to the baseline.

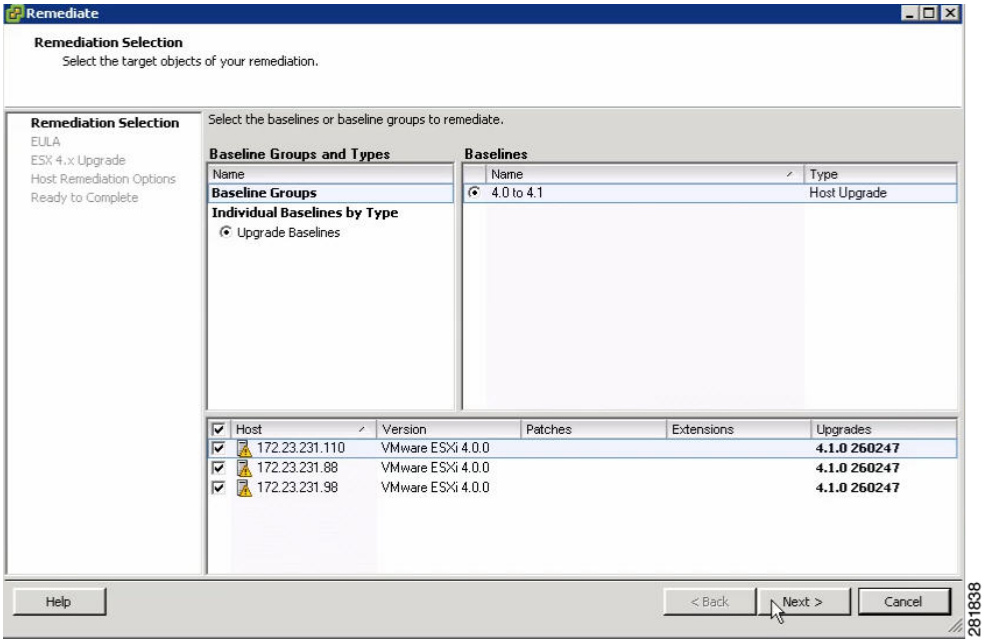
The Confirm Scan window opens.



Step 21 Check the **Upgrades** check box, uncheck the **Patches and Extensions** check box, and click **Scan**.



Step 22 Verify that all hosts are Non-Compliant and click **Remediate**.

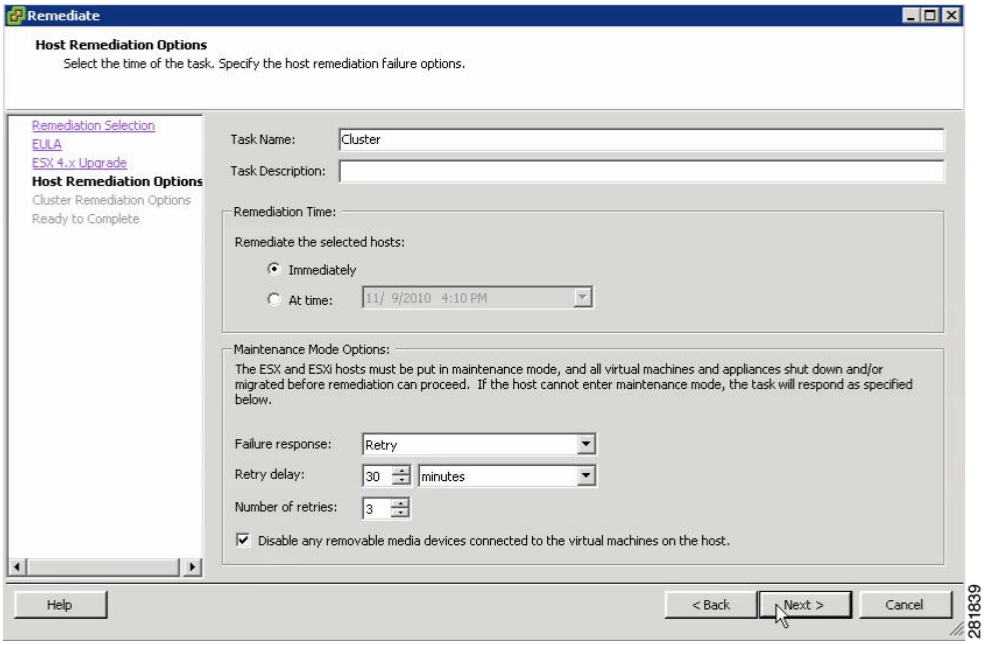


Step 23 Click **Next** in the Remediation Selection window.

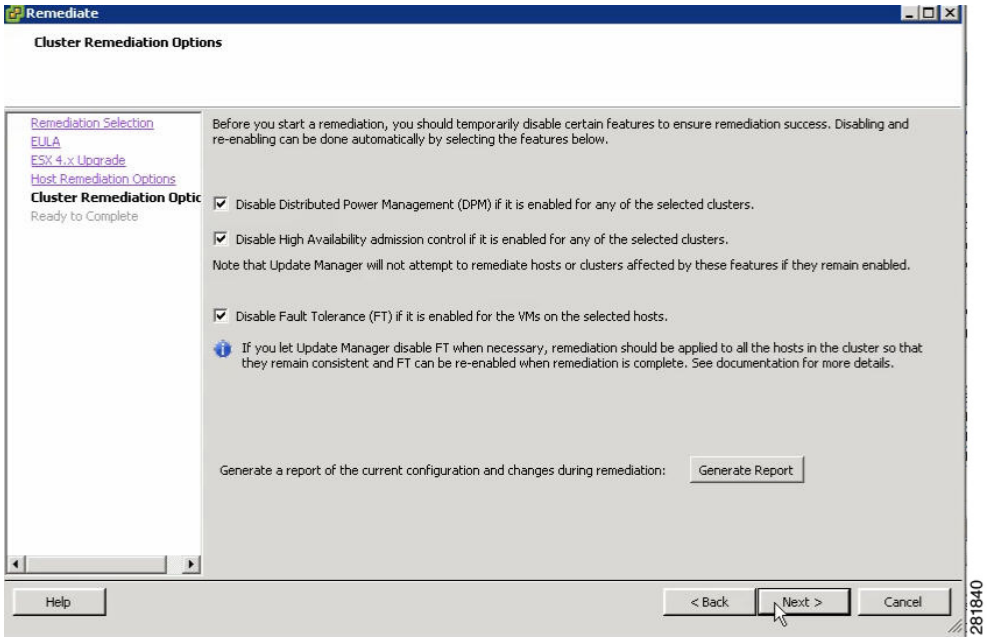
Step 24 Click the **I agree to the term in the license agreement** radio button and click **Next**.

Step 25 In the ESX 4.x Upgrade window, click **Next**.

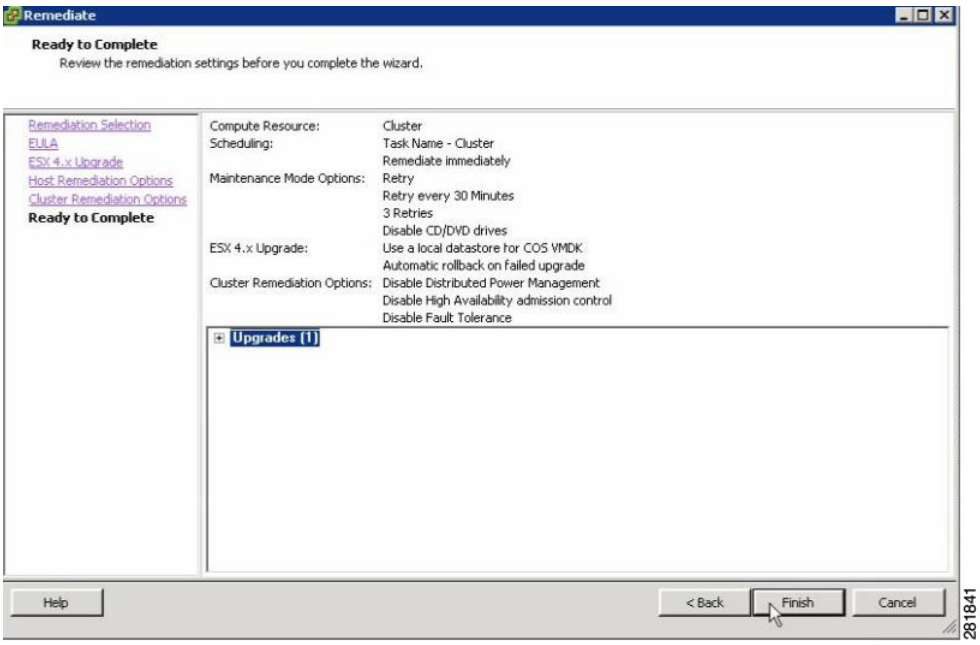
The Host Remediation Options window opens.



Step 26 Check the **Disable any removable media devices connected to the virtual machines on the host** check box and click **Next**.



Step 27 In the Cluster Remediation Options window, check all check boxes and click **Next**.



Step 28 Click **Finish** to begin the remediation.

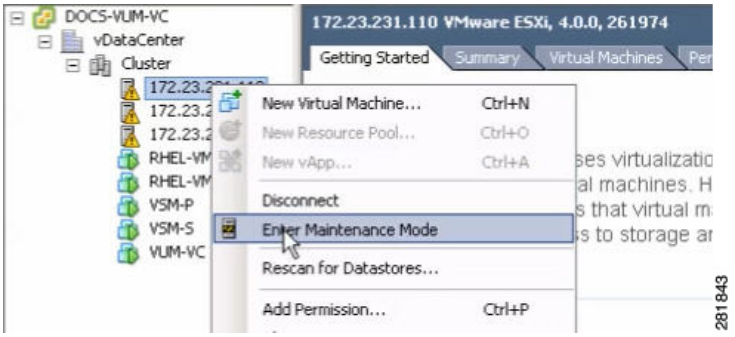
You can monitor remediation progress in the Recent Tasks section.

Step 29 To check the host versions, click each host in the left-hand pane and confirm that 4.1.0, 260247 appears in the top-left corner of the right-hand pane.

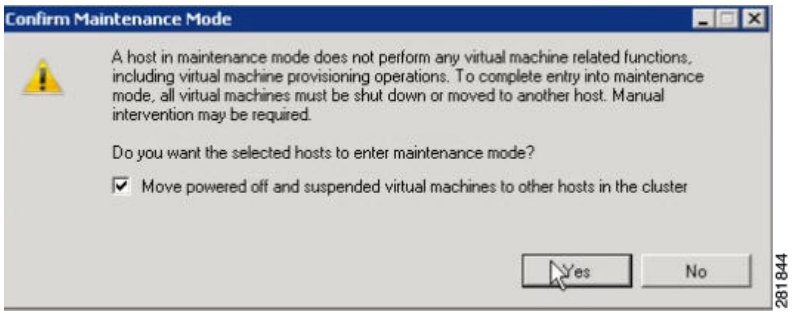
Step 30 Determine upgrade completion:

a. If all hosts have been upgraded, the upgrade is complete.

b. If any one of the hosts was not upgraded, perform Step 31 through Step 39for each host that requires an upgrade.



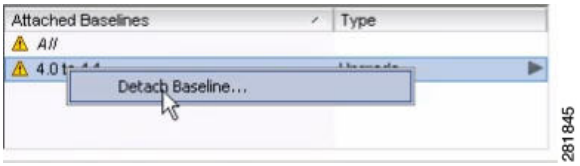
Step 31 Right-click on the host's IP address and choose Maintenance Mode.



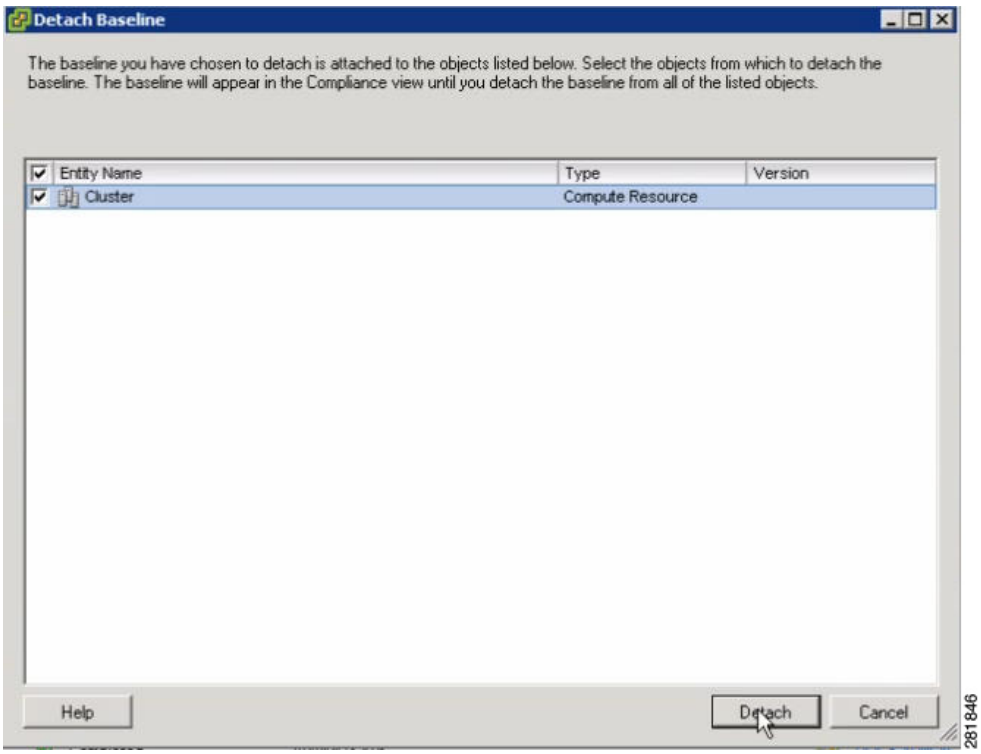
Step 32 Click **Yes** in the Confirm Maintenance Mode dialog box.

The host's VMs are migrated.

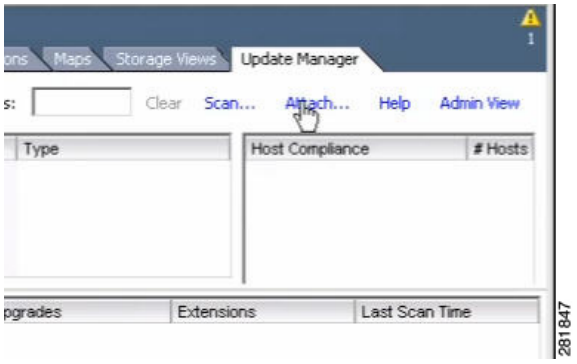
Step 33 Click the **Update Manager** tab.



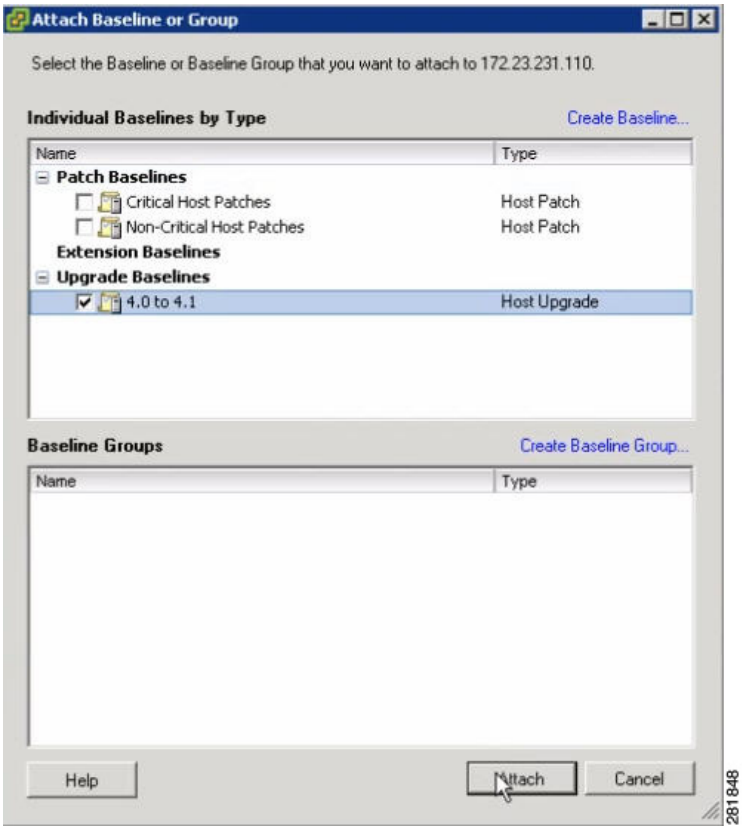
Step 34 Right-click on the 4.0 to 4.1 baseline and select **Detach Baseline**.



Step 35 Check the **Cluster** check box and click **Detach**.



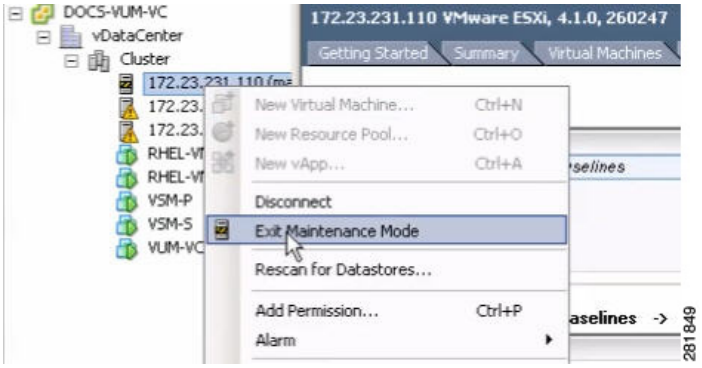
Step 36 To attach the baseline to the host that did not upgrade, click **Attach**.



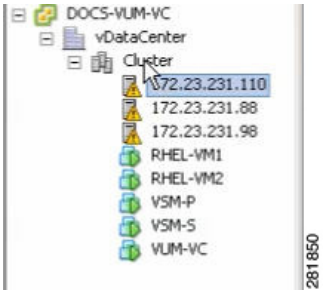
Step 37 Check the **4.0 to 4.1** check box and click **Attach**.

Step 38 Perform Step 22 through Step 28.

Step 39 When the remediation is complete, confirm that the host is compliant in the Host Compliance section.



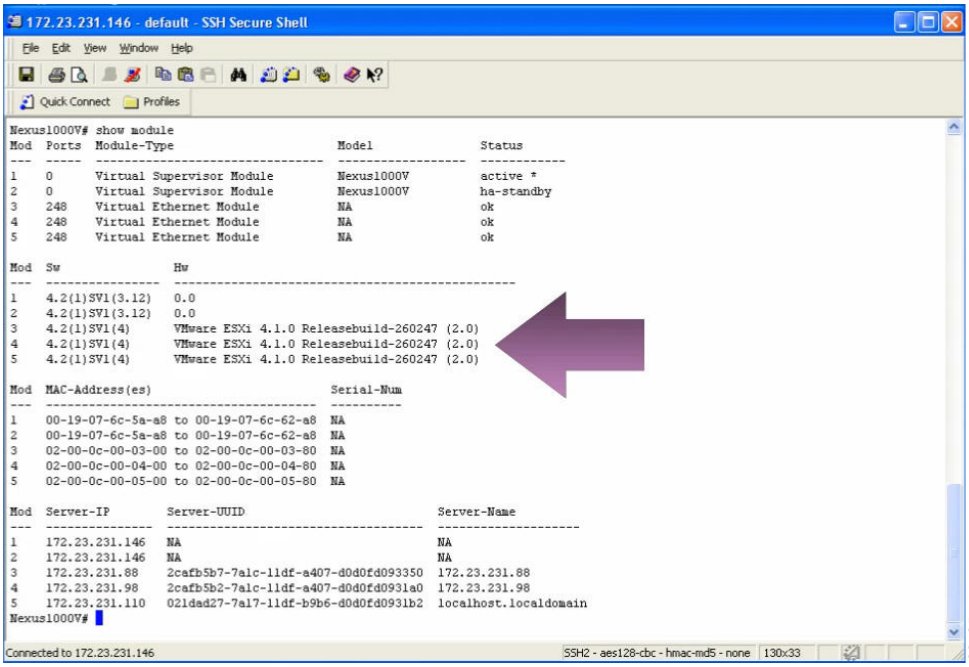
Step 40 Right-click on the host and choose **Exit Maintenance Mode**.



Step 41 Select **Cluster** to scan the entire cluster for compliance.

Step 42 Detach the baseline from the host and attach it to the cluster.

Step 43 The upgrade can also be confirmed by running the **show module** command on the VSM and observing that the VEMs are on the correct build.



The upgrade is complete.

Verification After the Upgrade

Step 1 To verify the build number on the ESX host, run the following commands:

```
[root@hostname~] # rpm -qa | grep vmkernel | awk -F. '{print $5}'
260402

~ # vmware -v
VMware ESXi 4.1.0 build-260402
```

```
[root@hostname ~] # rpm -qa | grep vmkernel | awk -F. '{print $5}'
260402

~ # vmware -v
VMware ESXi 4.1.0 build-260402

On Nexus 1000v side:
Refer to the Compatibility matrix

#  show mod

# vem status -v
```

Step 2 To verify the upgrade on the Cisco Nexus 1000V, run the following commands.

```
switch# show mod

vem status -v
```

Upgrading the ESX/ESXi Host with VEM Software Installed Using the CLI

You can use this procedure to upgrade an ESX or ESXi host by installing a VMware patch or update along with the compatible Cisco Nexus 1000V VEM software.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

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

Note The vSphere Command-Line Interface (vSphere CLI) command set allows you to run common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also run most vSphere CLI commands against a vCenter Server system and target any ESX/ESXi system that the vCenter Server system manages. vSphere CLI 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 the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* for compatible versions.
- You have already copied the ESX or ESXi host software and VEM software installation file to the /tmp directory.
- You know the name of the ESX or ESXi, and VEM software file to be installed.

DETAILED STEPS

Step 1 Go to the directory where the new VEM software was copied.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
```

Step 2 Determine which upgrade method you want to use and run the appropriate command:

- If you are using vCLI, run the **vihostupdate** command and install the ESX/ ESXi and VEM software simultaneously.

  vihostupdate --install --bundle "[path to VMware Update offline bundle]","[path to Cisco updated VEM offline bundle]" **--server** [vsphere host IP address]

Note Put the host is maintenance mode prior to running the following command.

Example:

```
[root@serialport tmp]# vihostupdate --install --bundle ESXi-4.0.0-update01.zip,
VEM400-201007301.zip --server 192.0.2.0
Enter username: root
Enter password:
Please wait installation in progress  …
The update completed successfully, but the system needs to be rebooted for the changes
to be effective.
[root@serialport tmp]#
```

- If you are using the **esxupdate** command, from the ESX host /tmp directory, install the VEM software as shown in the following example:

Note When using the **esxupdate** command, you must log in to each host and run the command.

esxupdate --bundle=[Updated 1000V VEM offline bundle] **--bundle**=[VMware offline update bundle] **update**

Example:

```
~ # esxupdate --bundle=/vmfs/volumes/datastore1/upgrade-from-esxi4.0-4.0_update02.zip
--bundle=/vmfs/volumes/datastore1/VEM400-201008401.zip update
Unpacking cross_cisco-vem-v130-esx_4.2.1.1.3.9-1.9.1
########################################################################### [100%]

Unpacking deb_vmware-esx-firmware_4.0.0-2.17.261974
########################################################################### [100%]

Unpacking deb_vmware-esx-viclient_4.0.0-2.17.261974
########################################################################### [100%]

Unpacking deb_vmware-esx-tools-light_4.0.0-2.17.261974
########################################################################### [100%]

Removing packages :vmware-esx-tools-light vmware-esx-viclient
########################################################################### [100%]

Installing packages :deb_vmware-esx-firmware_4.0.0-2.17.261974
########################################################################### [100%]

Installing packages :cross_cisco-vem-v130-esx_4.2.1.1.3.9.0-1.9.1
########################################################################### [100%]
```

```
Installing packages :deb_vmware-esx-viclient_4.0.0-2.17.261974, deb_..
########################################################################################## [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
The update completed successfully, but the system needs to be rebooted for the
changes to be effective.

~ #
```

This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

Step 3 Reboot the host.

Step 4 Verify that the installation was successful.

```
[root@serialport tmp]# vmware -v
VMware ESXi 4.0.0 build-236512
root@serialport tmp]# esxupdate --vib-view query | grep cisco
cross_cisco-vem-v120-esx_4.0.4.1.3.0.0-1.9.2 retired
2010-07-18T16:56:00.787147+00:00
cross_cisco-vem-v130-esx_4.2.1.1.3.9.0-1.9.1 installed
2010-07-18T17:06:53.675403+00:00
[root@serialport tmp]# esxupdate query
-----Bulletin ID----- -----Installed----- ----------Summary----------
ESXi400-200911203-UG      2010-07-18T14:30:58 VI Client update for 4.0 U1 release
ESXi400-Update01          2010-07-18T14:30:58 VMware ESXi 4.0 Update 1
ESXi400-201002401-BG      2010-07-18T17:07:14 Updates Firmware
ESXi400-201002402-BG      2010-07-18T17:07:14 Updates VMware Tools
VEM400-201004265454109-BG 2010-07-18T17:07:14 Cisco Nexus 1000V 4.0(4)SV1(3a)
[root@serialport tmp]# vem status -v
Package vssnet-esx4.1.2-00000-release
Version 4.0.4.1.3.0.0-1.11.2
Build 2
Date Mon Apr 26 21:47:24 PDT 2010
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          3           64                1500    vmnic0
DVS Name       Num Ports   Used Ports  Configured Ports  Uplinks
nexus          256         50          256               vmnic3
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Note If the VEM Agent is not running, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

Step 5 Run the following command from the VSM.

```
bldvs3# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw               Hw
---  ---------------  ------------------------------------------------
1    4.2(1)SV1(4)     0.0
4    4.2(1)SV1(4)     VMware ESXi 4.0.0 Releasebuild-261974 (1.20)

Mod  MAC-Address(es)                         Serial-Num
```

```
---  ------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    172.23.180.101   NA                                    NA
4    172.23.181.70    2ae7ac00-e805-11de-acef-3f85ac766493  172.23.181.70
```

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

Step 6 Do one of the following:

- If the installation was successful, the installation procedure is complete.
- If not, see the *Recreating the Cisco Nexus 1000V Installation* section in *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

You have completed this procedure.

Installing or Upgrading the VEM Software Using VUM

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

When installing or upgrading the VEM software, VMware Update Manager (VUM) will automatically select the correct VEM software to be installed on the host.

VEM software is installed on the host in one of the following procedures:

- When upgrading the VEM software, the VUM operation is initiated by the network administrator when he executes the **vmware vem upgrade proceed** command.
- VUM operation is initiated by the server administrator when adding a new host to the Nexus 1000V DVS.

Note Make sure you read Prerequisites for Installing VEM Software, page 5 to ensure that the VUM operation proceeds without failure.

  - If you are using VUM, then the Cisco Nexus 1000V VEM software will be installed automatically when the host is added to the Cisco Nexus 1000V DVS. When VEM upgrades are triggered from the VSM, the VEM software will be automatically upgraded on the host. To determine which VUM upgrade procedure you should follow, see Installing or Upgrading the VEM Software Using VUM, page 43.

Installing or Upgrading the VEM Software Using the CLI

You can use this procedure to install the Cisco Nexus 1000V VEM software on an ESX/ESXi host.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

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

Note The vSphere Command-Line Interface (vCLI) command set allows you to run common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also run 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 the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)* for compatible versions.
- You have already copied the VEM software installation file to the /tmp directory.
- You know the name of the VEM software file to be installed.

PROCEDURE

Step 1 Go to the directory where the new VEM software was copied.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
```

Step 2 Determine which upgrade method you want to use and run the appropriate command:

- If you are using vCLI, run the **vihostupdate** command and install the ESX/ ESXi and VEM software simultaneously.

```
vihostupdate --install --bundle [path to Cisco updated VEM offline bundle]" --server
[vsphere host IP address]
```

Note Put the host is maintenance mode prior to running the following command.

Example:

```
[root@serialport tmp]# vihostupdate -i --bundle cisco-vem-v130-4.2.1.1.3.9.0-1.9.1.zip
--server 192.0.2.0
Enter username: root
Enter password:
Please wait installation in progress …
The update completed successfully, but the system needs to be rebooted for the changes
to be effective.
```

```
[root@serialport tmp]#
```

- If you are using the **esxupdate** command, from the ESX host /tmp directory, install the VEM software as shown in the following example:

Note When using the **esxupdate** command, you must log in to each host and run the command.

```
esxupdate --bundle [VMware offline update bundle] update
Example:

[root@cos1-]# esxupdate -b ./cross_cisco-vem-v130-4.2.1.1.3.9.0-1.9.1.vib update
cross_cisco-vem-v130-4.2.1.1.1.nn-0.4.nn..   ###################################
[100%]
Unpacking cross_cisco-vem-v100-esx_4..        ###################################
[100%]
Installing cisco-vem-v100-esx                 ###################################
[100%]
Running [/usr/sbin/vmkmod-install.sh]...
ok.
[root@cos1-]#
```

This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

Step 3 Run the following commands and compare the output with the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4).*

```
[root@serialport tmp]# vmware -v
VMware ESXi 4.0.0 build-208167
[root@serialport tmp]# esxupdate --vib-view query | grep cisco
cisco-vem-v130-4.2.1.1.3.9.0-1.9.1 installed     2010-07-18T16:56:00.787147+00:00
```

The highlighted text shows the upgraded Cisco VEM.

```
root@serialport tmp]# esxupdate query
-----Bulletin ID----- -----Installed----- ----------Summary----------
ESXi400-Update01    2010-07-18T14:30:58    VMware ESXi 4.0 Update 1
VEM400-201004265419109-BG 2010-07-18T16:56:00 Cisco Nexus 1000V 4.0(4)SV1(3a)
root@serialport tmp]# vem status -v
Package vssnet-esx4.1.0-00000-release
Version 4.2.1.1.3.9.0-1.9.1
Build 2
Date Mon Apr 26 21:47:24 PDT 2010
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          3           64                1500    vmnic0
DVS Name       Num Ports   Used Ports  Configured Ports  Uplinks
nexus          256         50          256               vmnic3
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Step 4 Run the following command from the VSM.

```
switch# show mod
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module        Nexus1000V         active *
2    0      Virtual Supervisor Module        Nexus1000V         standby
3    248    Virtual Ethernet Module          NA                 ok
Mod  Sw               Hw
---  ---------------  ------
```

```
1    4.0(4)SV1(3)     0.0
2    4.0(4)SV1(3)     0.0
3    4.2(1)SV1(4)     VMware ESXi 4.0.0 build-208167 (1.9)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.62.220    NA                                    NA
4    10.104.62.217    3fa746d4-de2f-11de-bd5d-c47d4f7ca460  visor
```

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

Step 5 Do one of the following:

- If the installation was successful, the installation procedure is complete.
- If not, see the *Recreating the Cisco Nexus 1000V Installation* section in *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

You have completed this procedure.

Uninstalling the VEM Software

You can use this procedure to uninstall the Cisco Nexus 1000V software from a VEM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Make sure the host is not currently a part of any DV switch by removing all of the following active ports from the DV switch:
  - VMware kernel NICs
  - Virtual switch interfaces
  - Virtual NICs
- You are logged in to the ESX/ESXi host remotely using SSH.

DETAILED STEPS

Step 1 Uninstall the VEM software using the **vem-remove -d** command.

This command removes the software from the host, removes the kernel modules, and stops the VEM Agent on the running system.

Note The following example is being run on ESX.

```
[root@fcs-cos2 ~]# vem-remove -d
```

```
watchdog-vemdpa: Terminating watchdog with PID 14574
Module vem-v130-stun being unloaded..
Module vem-v130-stun unloaded..
Module vem-v130-vssnet being unloaded..
Module vem-v130-vssnet unloaded..
Module vem-v130-n1kv being unloaded..
Module vem-v130-n1kv unloaded..
Module vem-v130-l2device being unloaded..
Module vem-v130-l2device unloaded..
Removing CIsco VEM VIB from COS system
Removing VIB cross_cisco-vem-v130-esx_4.2.1.1.3.9.0-1.11.3
Removing cisco-vem-v130-esx
########################################################################################################
# [100%]

Running [/usr/sbin/vmkmod-install.sh]...

ok.
root@fcs-cos2 ~]#
```

Note The following example is being run on ESXi.

```
~ # vem-remove -d
watchdog-vemdpa: Terminating watchdog with PID 14574
Module vem-v130-stun being unloaded..
Module vem-v130-stun unloaded..
Module vem-v130-vssnet being unloaded..
Module vem-v130-vssnet unloaded..
Module vem-v130-n1kv being unloaded..
Module vem-v130-n1kv unloaded..
Module vem-v130-l2device being unloaded..
Module vem-v130-l2device unloaded..
Removing CIsco VEM VIB from visor system
Removing VIB cross_cisco-vem-v130-esx_4.2.1.1.3.9.0-1.11.3
Removing cisco-vem-v130-esx
########################################################################################################
# [100%]

Running [/usr/sbin/vmkmod-install.sh]...

ok.
```

Step 2 Verify that the software was successfully removed by checking for the output of the **esxupdate --vib-view query** command:

```
[root@fcs-cos2 -]# esxupdate --vib-view query

~ # esxupdate --vib-view query | grep cisco | grep retired

------------------VIB ID------------------ Package State -----------Timestamp------------
cross_cisco-vem-v130-4.2.1.1.3.12.0-2.0.3.vib retired 2009-07-02T15:26:45.994264-05:00
root@fcs-cos2 -]#
~ #
```

Step 3 Do one of the following:

- If the removal was successful, reboot the host and your uninstall is complete.
- If not, see the *Recreating the Cisco Nexus 1000V Installation* section in *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)*.

You have completed this procedure.

Available Documents

This section lists the documents used with the Cisco Nexus 1000 and available on Cisco.com at the following url:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(2)

Install and Upgrade

Cisco Nexus 1000V Virtual Supervisor Module Software Installation Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide

Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(2)

Configuration Guides

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(2)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(4)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)

Cisco Nexus 1000V MIB Quick Reference

Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(2)

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4)

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG(1)

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(1)

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(1)

Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(1)

Virtual Network Management Center

Release Notes for Cisco Virtual Network Management Center, Release 1.0.1

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1

Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1

Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1

Network Analysis Module Documentation

Cisco Network Analysis Module Software Documentation Guide, 4.2

Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide

Network Analysis Module Command Reference Guide, 4.2

User Guide for the Cisco Network Analysis Module Virtual Service Blades, 4.2

Cisco Network Analysis Module Software Release Notes, 4.2

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the section.