



Installing and Upgrading VMware

This chapter contains the following sections:

- [Upgrading from VMware Releases 5.x to VMware Release 6.0, page 1](#)
- [Installing VMware Release 5.x and 6.x Patches, page 9](#)
- [Verifying the Build Number and Upgrade, page 13](#)

Upgrading from VMware Releases 5.x to VMware Release 6.0

The steps to upgrade are as follows:



Note

Do not install VMware vSphere 5.5 Patch 2702864 with Cisco Nexus 1000V. The VMware vSphere 5.5 Patch 2702864 is not supported on Cisco Nexus 1000V.

SUMMARY STEPS

1. [Installing the vCenter Server, on page 2](#)
2. [Upgrading the vSphere Client, on page 3](#)
3. [Upgrading the vCenter Update Manager to Release 6.0, on page 3](#)
4. [Creating a Customized Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 5](#)
5. Installing VMware Release 5.x or 6.x Patches:
 - [Creating the Host Patch Baseline for 5.x or 6.x Patches, on page 9](#)
 - [Upgrading the ESXi Hosts to Release 5.x or 6.x Patches Using VMware Update Manager, on page 10](#)
 - [Upgrading the ESXi Hosts to Release 5.x or 6.x Using the CLI, on page 11](#)
6. [Verifying the Build Number and Upgrade, on page 13](#)

DETAILED STEPS

-
- Step 1** [Installing the vCenter Server](#) , on page 2
- Step 2** [Upgrading the vSphere Client](#) , on page 3
- Step 3** [Upgrading the vCenter Update Manager to Release 6.0](#), on page 3
- Step 4** [Creating a Customized Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image](#), on page 5
- Step 5** Installing VMware Release 5.x or 6.x Patches:
- [Creating the Host Patch Baseline for 5.x or 6.x Patches](#), on page 9
 - [Upgrading the ESXi Hosts to Release 5.x or 6.x Patches Using VMware Update Manager](#), on page 10
 - [Upgrading the ESXi Hosts to Release 5.x or 6.x Using the CLI](#) , on page 11
- Step 6** [Verifying the Build Number and Upgrade](#), on page 13
-

Installing the vCenter Server

Before You Begin

- Download the upgrade ISO file that contains the ESXi image and the Cisco Nexus 1000V software image files.
- 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.

-
- Step 1** Mount the vCenter Server 6.0 ISO image.
- Step 2** Unzip the ISO image.
- Step 3** If autorun doesn't start, double-click **autorun.exe**.
- Step 4** In the VMware vCenter Installer window, select **vCenter Server for Windows** and click **Install**.
- Step 5** Click **Next**.
- Step 6** Accept the license agreements.
- Step 7** Enter the vCenter Single Sign On password and the service account password if applicable and click **Next**.
- Step 8** After the pre-upgrade checks are complete, accept the default ports and click **Next**.
- Step 9** Check the box to verify that you have backed up this vCenter Server and its database and click **Upgrade**.
- Step 10** Click **Finish**.
-

What to Do Next

Complete the steps in [Upgrading the vSphere Client](#) , on page 3.

Upgrading the vSphere Client

- Step 1** Run the vSphere Client installer.
- Start the vCenter Server installer. Double-click the **autorun.exe** file and select **vSphere Client**.
 - If you downloaded the vSphere Client, double-click the **VMware-viclient-build number.exe** file.
- Step 2** Click **Next**.
- Step 3** Accept the terms in the license agreements and click **Next**.
- Step 4** Click **Next**.
- Step 5** Click **Install**.
- Step 6** Click **Finish** after the installation completes.
-

What to Do Next

Complete the steps in [Upgrading the vCenter Update Manager to Release 6.0](#), on page 3.

Upgrading the vCenter Update Manager to Release 6.0

Before You Begin

You have upgraded the vCenter Server to the vSphere Client to a compatible version.

SUMMARY STEPS

1. In the VMware vCenter Installer window, select **vCenter Update Manager Server** and check **Use Microsoft SQL Server 2012 Express as the embedded database**.
2. Click **Install**.
3. Choose a language and click **OK**. The vCenter Update Manager Installer appears.
4. Click **OK**.
5. Click **Next** to begin the upgrade.
6. View the patent agreement and click **Next**.
7. Click the **I agree to the terms in the license agreement** radio button and click **Next**.
8. Verify the IP address and username in the VMware vCenter Server Information area .
9. In the Password field, enter your password and click **Next**.
10. Click **Next**.
11. Click the **Yes, I want to upgrade my Update Manager database** radio button and click **Next**.
12. Verify the Update Manager port settings and click **Next**.
13. Verify the proxy settings and click **Next**.
14. Click **Install** to begin the database upgrade.
15. Click **OK** to acknowledge that a reboot will be required to complete the setup. During the upgrade, the vSphere Client is disconnected.
16. Click **Cancel** for the attempt to reconnect.
17. Click **OK** in the Server Connection Invalid window.
18. Click **Finish**.
19. Reboot the vCenter Update Manager and vCenter Server.
20. Select **Other (Planned)** from the Option drop-down list in the Shut Down Windows dialog box and enter a value in the comment field.
21. Click **OK**.
22. After the system reboots, navigate to the C:\ProgramData\VMware Update Manager\Logs\ folder and open the vmware-vum-server-log4cpp file.
23. Choose **Manage Plug-ins** from the VMware vCenter Server's Plug-in menu.
24. Click **Download and Install for VMware vSphere Update Manager Extension** under Available Plug-ins..

DETAILED STEPS

Step 1 In the VMware vCenter Installer window, select **vCenter Update Manager Server** and check **Use Microsoft SQL Server 2012 Express as the embedded database**.

Note If the Installer window is not open, run the autorun.exe file.

- Step 2** Click **Install**.
- Step 3** Choose a language and click **OK**. The vCenter Update Manager Installer appears.
- Step 4** Click **OK**.
- Step 5** Click **Next** to begin the upgrade.
- Step 6** View the patent agreement and click **Next**.
- Step 7** Click the **I agree to the terms in the license agreement** radio button and click **Next**.
- Step 8** Verify the IP address and username in the VMware vCenter Server Information area .
- Step 9** In the Password field, enter your password and click **Next**.
- Step 10** Click **Next**.
- Step 11** Click the **Yes, I want to upgrade my Update Manager database** radio button and click **Next**.
- Step 12** Verify the Update Manager port settings and click **Next**.
- Step 13** Verify the proxy settings and click **Next**.
- Step 14** Click **Install** to begin the database upgrade.
- Step 15** Click **OK** to acknowledge that a reboot will be required to complete the setup. During the upgrade, the vSphere Client is disconnected.
- Step 16** Click **Cancel** for the attempt to reconnect.
- Step 17** Click **OK** in the Server Connection Invalid window.
- Step 18** Click **Finish**.
- Step 19** Reboot the vCenter Update Manager and vCenter Server.
- Step 20** Select **Other (Planned)** from the Option drop-down list in the Shut Down Windows dialog box and enter a value in the comment field.
- Step 21** Click **OK**.
- Step 22** After the system reboots, navigate to the C:\ProgramData\VMware Update Manager\Logs\folder and open the vmware-vum-server-log4cpp file.
- Step 23** Choose **Manage Plug-ins** from the VMware vCenter Server's Plug-in menu.
- Step 24** Click **Download and Install for VMware vSphere Update Manager Extension** under Available Plug-ins..
-

What to Do Next

Complete the steps in [Creating a Customized Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image](#), on page 5.

Creating a Customized 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.

-
- Step 1** Start the VMWare PowerCLI application.
- Step 2** Run the **Set-ExecutionPolicy unrestricted** command.
- Step 3** Connect to the vCenter Server by using the **Connect-VIServer IP_address -User Administrator -Password password_name** command.
- Step 4** Load the ESXi depot by using the **Add-ESXSoftwareDepot path_name\file_name** command.
- Step 5** Display the image profiles by using the **Get-ESXImageProfile** command.
- Step 6** 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 7** Load the Cisco Nexus 1000V VEM offline bundle by using the **Add-ESXSoftwareDepot VEM_offline_bundle** command.
- Step 8** Confirm that the n1kv-vib package is loaded by using the **Get-ESXSoftwarePackage -Name package_name** command.
- Step 9** Bundle the n1kv-package into the cloned image profile by using the **Add-ESXSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage cloned_image_profile** command.
- Step 10** Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile by entering the following commands.
- Simg = Get-ESXImageProfile n1kv-Image**
 - Simg.vibList**
- Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile.
- Step 11** 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\VEM550-201612340113-BG-release.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.         02/02/2016 7:... PartnerSupported
CN1-CY                               CISCO                4/22/2015 11:... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.         12/7/2015 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.         12/7/2015 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools          VMware, Inc.         8/2/2015 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.         12/7/2015 7:... PartnerSupported
ESXi-5.1.0-799733-standard          VMware, Inc.         8/2/2015 3:0... PartnerSupported

vSphere PowerCLI> New-EsxImageProfile -CloneProfile VEM550-201612340113-BG-release.zip
ESXi-5.1.0-799733-standard -Name ESXi-N1Kv-bundle

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
----                               -
ESXi-N1Kv-bundle                   CISCO                09/09/2016 3:0... PartnerSupported

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229
\VEM510-201612340107-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
----                               -
cisco-vem-v320-esx                5.2.1.3.2.5.0-3.2.1 Cisco Partner Supported 2016-09-09

vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v170-esx -ImageProfile
ESXi-N1Kv-bundle

Name                               Vendor                Last Modified      Acceptance Level
----                               -
ESXi-N1Kv-bundle                   CISCO                09/09/2016 3:... PartnerSupported

vSphere PowerCLI> $img = Get-EsxImageProfile ESXi-N1Kv-bundle

vSphere PowerCLI> $img.vibList

Name                               Version              Vendor              Creation Date
----                               -
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-cnuc-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-bnx215-esx 5.2.1.3.2.5.0-3.1.2 Cisco 2016-09-09
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 ESXi-N1Kv-bundle -FilePath
'C:\Documents and Settings\Administrator\Desktop\ESXi-N1Kv-bundle.iso' -ExportToIso

```


Installing VMware Release 5.x and 6.x Patches

Creating the Host Patch Baseline for 5.x or 6.x Patches

Before You Begin

- VMware release 5.x or 6.x must be installed prior to installing a patch.
- Ensure you configure the VMware Update Manager Download settings with proxy enabled and VMware production portal links for VMware ESX/ESXi in connected state and download those images into the VUM patch repository.



Note Do not install VMware vSphere 5.5 Patch 2702864 with Cisco Nexus 1000V. The VMware vSphere 5.5 Patch 2702864 is not supported on Cisco Nexus 1000V.

Step 1 Under **Home > Solutions and Applications > Update Manager**, select **Baselines and Groups** tab.

Step 2 Under **Baseline**, click **Create** to create a baseline.

Step 3 In the **Baseline Name and Type** window, enter a name for the baseline, select the **Host Patch** radio button and click **Next**.

Step 4 In the **Patch Options** window, select the **Fixed** radio button and click **Next**.

Step 5 In the **Patches** window, select the required patch to upgrade to and move the selected patch to **Fixed patches to Add** column and click **Next**.

Note To find the 6.x or 5.1 update 1 and later patches, refer to <http://www.vmware.com/patchmgr/findPatch.portal>.

Note In the combined upgrade scenario, add the required Cisco Nexus 1000V VEM patch that corresponds to 6.x and 5.x releases to the **Fixed patches to Add** column along with ESXi 6.x and 5.x patches. You can get the required Cisco Nexus 1000V VEM patches into the VUM patch repository either from www.cisco.com, VMWare production portal links or through the VSM home page.

Upgrading the ESXi Hosts to Release 5.x or 6.x Patches Using VMware Update Manager



Note Follow the same procedure to upgrade ESXi hosts 5.0 to 5.0 Update 1 and later.

-
- Step 1** In the vSphere Client, choose **Home > Hosts and Clusters** .
- Step 2** From the left navigation pane, select the host or cluster that needs to be upgraded and click **Update Manager**.
- Step 3** Click **Attach**.
- Step 4** In the Individual Baselines by Type area, select your Patch baseline's radio button check box.
- Step 5** Click **Attach**.
- Step 6** Click **Scan**.
- Step 7** In the Confirm Scan dialog box, check the **Patches and extensions box** and click **Scan**. Verify if all the hosts are non-compliant.
- Step 8** Click **Stage**.
- Step 9** In Baseline Selection window, keep the default selected baseline and click **Next**.
- Step 10** In Patch and Extension exclusion window, keep the default selected baseline and click **Next**.
- Step 11** Click **Finish**.
- Step 12** Click **Remediate** and click **Next**.
- Step 13** In Patch and Extension exclusion window, keep the default selected baseline and click **Next**.
- Step 14** Click **Next**.
- Step 15** In the Host Remediate Options window, under Maintenance Mode Options, select the **Disable any removable media devices connected to the virtual machines on the host** check box.
- Note** If you have stateless host in your setup, select **Enable Patch Remediation on Powered on PXE booted ESXi hosts** radio button.
- Step 16** Click **Next**.
- Step 17** In the Cluster Remediation Options window, select all the check boxes and click **Next**.
- Step 18** Click **Finish** to begin the remediation.
- To check the host versions, on the left-hand pane, click on each host to confirm if version 6.x and 5.x appears in the top-left corner of the right-hand pane and the version information matches the information provided under the *Cisco Nexus 1000V and VMware Compatibility Information* guide.
- You can also confirm if the upgrade was successful by executing the **show module** command on the VSM and check if the VEMs are running the correct build.
-

Upgrading the ESXi Hosts to Release 5.x or 6.x Using the CLI

You can upgrade an ESXi host by installing a VMware patch or update with the compatible Cisco Nexus 1000V VEM software.


Note

Do not install VMware vSphere 5.5 Patch 2702864 with Cisco Nexus 1000V. The VMware vSphere 5.5 Patch 2702864 is not supported on Cisco Nexus 1000V.

Before You Begin

- 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 when the vCLI is installed.


Note

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

Step 1 Download the VEM software and copy them to the local host.

Step 2 Determine the upgrade method that you want to use.

If you are using the vCLI, enter the `esxcli` command and install the ESXi and VEM software simultaneously.

esxcli software vib install -v full-path-to-vib

Note When using the `esxcli software VIB install` command, you must log in to each host and enter the command. ESXi expects the VIB to be in the `/var/log/vmware` directory if the absolute path is not specified.

```
# esxcli software vib update -d /var/tmp/update-from-esxi5.1-5.1_update01.zip
Installation Result
  Message: The update completed successfully, but the system needs to be rebooted for the
  changes to be effective.
  Reboot Required: true
  VIBs Installed: VMware_bootbank_esx-base_5.1.0-0.12.1065491,
  VMware_locker_tools-light_5.1.0-0.12.1065491
  VIBs Removed: VMware_bootbank_esx-base_5.1.0-0.3.799733,
  VMware_locker_tools-light_5.0.0-0.0.799733
  VIBs Skipped: VMware_bootbank_ata-pata-amd_0.3.10-3vmw.510.0. 3.799733,
  VMware_bootbank_ata-pata-atiixp_0.4.6-3vmw.510.0. 3.799733,
```

```
VMware_bootbank_scsi-qla4xxx_5.01.03.2-3vmw.510.0.3.799733.,
VMware_bootbank_uhci-usb-uhci_1.0-3vmw.510.0.3.799733
```

Upgrading the VMware DVS Version Using the VSM CLI

You can upgrade the VMware DVS version from the current version (4.0 or 5.0) to 5.0 and above using the VSM commands.

Before You Begin

- You have upgraded the VSM to the current Cisco Nexus 1000V release.



Note

The VMware ESXi host should be compatible with the new DVS version. Supported DVS versions are 5.0.0, 5.1.0, 5.5.0 or 6.0.0. If the ESXi host is incompatible with the new DVS version, the upgrade process fails.

- Step 1** Log in to **svs-connection** command mode in the VSM.
- Step 2** Configure the DVS version using **vmware dvs-version *version_no*** command.
- ```
vsm(config-svs-conn)#
vsm(config-svs-conn)# vmware dvs-version 5.1.0
```
- Step 3** Verify the DVS version upgrade using **show svs connections** command.
- ```
vsm(config-svs-conn)# show svs connections
```

```
connection nlk-vc:
  hostname: -
  ip address: 103.3.176.26
  ipv6 address: -
  remote port: 80
  transport type: ipv4
  protocol: vmware-vim https
  certificate: default
  datacenter name: dc-tb22
  admin:
  max-ports: 12000
  DVS uuid: a4 a7 0f 50 c8 79 ba a2-85 86 75 fd 53 7f d9 25
  dvs version: 5.1.0
  config status: Enabled
  operational status: Connected
  sync status: Complete
  version: VMware vCenter Server 6.0.0 build-2559268
  vc-uuid: 4fd42386-8cba-4055-8872-6340e2f61d86
  ssl-cert: self-signed or not authenticated
```

Verifying the Build Number and Upgrade



Note The examples in the procedure 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.

Before You Begin

- You have upgraded the VSMs and VEMs to the current Cisco Nexus 1000V release.



Note The VSM upgrade will not proceed if ESX/ESXi 4.0 or 4.1 is part of the DVS. You must either remove ESX 4.0 or 4.1 from the DVS and proceed with VSM upgrade or upgrade ESX 4.0 or 4.1 to 5.0 or later releases and proceed with the VSM upgrade.

- You have upgraded the vCenter Server.
- You have upgraded the VMware Update Manager.
- You have upgraded your ESX/ESXi hosts.

Step 1 Verify the build number on the ESXi host.

```
~ # vmware -v -l
VMware ESXi 5.5.0 build-2068190
VMware ESXi 5.5.0 Update 2
~ #
```

Step 2 Verify the VIB installed

```
~ # esxcli software vib list |grep cisco
cisco-vem-v340-esx          5.2.1.3.2.8.0-3.2.1          Cisco   PartnerSupported
2016-09-12
~ #
```

Step 3 Verify VEM status.

```
~ # vem status -v
Package vssnet-esxesx2013-release
Version 5.2.1.3.2.8.0-3.2.1
Build 1
Date Wed Sep 16:27:37 PST 2016
```

VEM modules are loaded

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
vSwitch0	2432	106	128	1500	vmnic0
DVS Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
BL	1024	22	1024	1500	vmnic5,vmnic4,vmnic7

VEM Agent (vemdpa) is running

```
~ #
```

Step 4 Verify VEM version.

```
~ # vemcmd show version
VEM Version: 5.2.1.3.2.8.0-3.2.1
VSM Version: 5.2(1)SV3(2.8)
System Version: VMware ESXi 5.5.0 Releasebuild-2068190
```

```
ESX Version Update Level: 0
~ #
```

Step 5

Verify the upgrade on the Cisco Nexus 1000V VSM.

```
switch# show module
```

Mod	Ports	Module-Type	Model	Status
1	0	Virtual Supervisor Module	Nexus1000V	active *
2	0	Virtual Supervisor Module	Nexus1000V	ha-standby
3	1022	Virtual Ethernet Module	NA	ok
4	1022	Virtual Ethernet Module	NA	ok
5	1022	Virtual Ethernet Module	NA	ok
6	1022	Virtual Ethernet Module	NA	ok
7	1022	Virtual Ethernet Module	NA	ok

Mod	Sw	Hw
1	5.2(1)SV3(2.8)	0.0
2	5.2(1)SV3(2.8)	0.0
3	5.2(1)SV3(2.8)	VMware ESXi 5.1.0 Releasebuild-2323236 (3.1)
4	5.2(1)SV3(2.8)	VMware ESXi 6.0.0 Releasebuild-3620759 (6.0)
5	5.2(1)SV3(2.8)	VMware ESXi 5.1.0 Releasebuild-2323236 (3.1)
6	5.2(1)SV3(2.8)	VMware ESXi 6.0.0 Releasebuild-3620759 (6.0)
7	5.2(1)SV3(2.8)	VMware ESXi 5.5.0 Releasebuild-2068190 (3.2)

Mod	Server-IP	Server-UUID	Server-Name
1	10.197.132.57	NA	NA
2	10.197.132.57	NA	NA
3	10.197.132.42	e0829a21-bc61-11e0-bd1d-30e4dbc2ba66	NA
4	10.197.132.43	e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba	NA
5	10.197.132.44	7b1a5e63-bcd0-11e0-bd1d-30e4dbc2c3ae	NA
6	10.197.132.45	8d8ff0e8-b565-11e0-bd1d-30e4dbc297da	NA
7	10.197.132.46	db8b80ac-af1d-11e0-a4e7-30e4dbc26b82	NA

* this terminal session