Send document comments to nexus1k-docfeedback@cisco.com.

# Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(1)

**November 21, 2012**
**Part Number: OL-19422-01**

This document describes how to install software for the Cisco Nexus 1000V Virtual Ethernet Module (VEM) for a VMware ESX or ESXi 4.0 server using remote login or VMware virtual CLI (vCLI).

**Note** The Cisco Nexus 1000V is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL), which is running VMWare vSphere 4.0 Enterprise Plus.

**Note** The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is Ethernet standard compliant, including Catalyst 6500 series switches Cisco Nexus switches, and switches from other network vendors.

This document includes the following topics:


- Audience, page 2
- Information About Cisco Nexus 1000V, page 2
- Obtaining VEM Software Releases, page 4
- Prerequisites, page 5
- Using the vCLI to Install the VEM Software, page 6
- Manually Installing the VEM Software, page 7
- Uninstalling the VEM Software, page 8
- Related Documentation, page 9


**Note** If you are using VUM, then the Cisco Nexus 1000V software is installed automatically. No action is required by the server administrator.

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

Send document comments to nexus1k-docfeedback@cisco.com.

# Audience

This document is for use by experienced server administrators who configure and maintain server software.

This document includes instructions for installing VEM software only. Installation instructions for the Virtual Supervisor Module (VSM) are found in the document, *Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(1)*.

## Administrator Roles

Table 1 describes the Cisco Nexus 1000V administrator roles.

***Table 1 Administrator Roles***

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

# Information About Cisco Nexus 1000V

Cisco and VMware jointly designed APIs that produced the Cisco Nexus 1000V—a distributed virtual switch solution that is fully integrated within 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 datacenter 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 effectively 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
- Virtual supervisor module (VSM)-control plane—The VSM is a standalone, external, physical or virtual appliance that performs the following functions for the Cisco Nexus 1000V system (that is, the combination of the VSM itself and all VEMs it controls):
  - Configuration.
  - Management. A single VSM can manage up to 64 VEMs.
  - Monitoring.
  - Diagnostics.

Send document comments to nexus1k-docfeedback@cisco.com.

- 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.

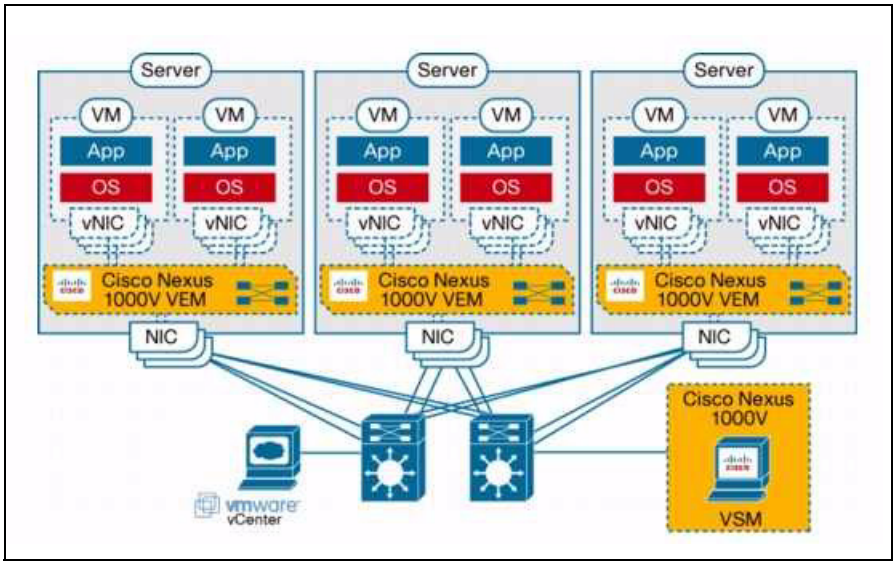
In Cisco Nexus 1000V, modules are numbered as follows:

- Module 1 is reserved for the Virtual Supervisor Module (VSM).
- Module 2 is reserved for the standby VSM in a dual supervisor system.
- The first server or host is automatically assigned to Module 3.
  NIC ports are 3/1 and 3/2.

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***



Send document comments to nexus1k-docfeedback@cisco.com.

# Obtaining VEM Software Releases

VEM software releases can be obtained from the sources shown in Table 2.

*Table 2 Obtaining VEM Software*

| Source | Description |
|---|---|
| VUM | If you are using VMware Update Manager (VUM), then VUM obtains the VEM software from the VSM through the web server hosted on the VSM. Then VUM installs the VEM software either during the VSM **Add Host** operation on the Cisco Nexus 1000V DVS, or after the VEM software is updated on the VSM.[1] |
| Cisco VEM CD | Copy the file containing the VEM software from the Cisco Nexus 1000V CD to the host where you installed the vCLI or to the ESX 4.0 host /tmp directory. |
| VSM | Copy the file containing the VEM software from the following url after the VSM has been installed as a VM:<br>http://<VSM-IP-ADDR>/ |
| VMware | Download the VEM software from the VMware web site.<br>Click **Download Vmware vSphere 4 Enterprise Plus > Download** |
| Cisco | Download the VEM software from the Cisco web site. |

1. 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 at the following url:

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

   vCenter Update Manager 4.0 Update 1 does not have this limitation.

# Information About VEM Software for VMware Patch Releases

Cisco Nexus 1000V VEM software is updated to support VMware patch releases and is available on both the VMware and Cisco 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 with the following exception:

- On the VMware Embedded platform, the Cisco Nexus 1000V bundle posted on the Cisco website can only be used for installation due to restrictions in the VMware Embedded platform manual install and upgrade utility.

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

For information about VEM software packages and compatibility, see the document, *Cisco Nexus 1000V and VMware Compatibility Information, Release 4.0(4)SV1(1)*.

Send document comments to nexus1k-docfeedback@cisco.com.

# Prerequisites

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

- The following are the disk and memory usage for the VEM software on an ESX/ESXi host:
  - 6.5 MB of disk space.
  - Maximum of 150 MB of RAM when all Cisco Nexus 1000V features are activated.
- You can install the VEM software before the Virtual Supervisor Module (VSM) is installed, however, verification and configuration of the VEM can only be done after installing the VSM.
- 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 you are using a proxy server to connect VUM to the Internet, you may need to disable the proxy before starting a VUM upgrade of your VEMs. Because in some VMware versions the proxy prevents VUM from communicating locally with the VSM, automatic VEM upgrades may fail if the proxy is not disabled first.

**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 upgrade the hosts in the cluster.

# Installation Methods

You can use any of the methods listed in Table 3 to install the VEM software.

*Table 3 Cisco Nexus 1000V VEM Software Installation Methods*

| | Server/Host | |
|---|---|---|
| **Install Method** | **ESX** | **ESXi** |
| VMware Virtual CLI (vCLI) | X | X |
| Remote Login Manual Installation | X | X[1] |
| VMware Update Manager (VUM)[2] | X | X |

1. SSH must be enabled on the host.
2. If using VUM, no action is required by the server administrator. VUM automatically installs the VEM software. VUM will not install the VEM software on a host where the vCenter resides. The vCenter must be migrated to another host before installing VEM software.

Send document comments to nexus1k-docfeedback@cisco.com.

# Using the vCLI to Install the VEM Software

You can install the Cisco Nexus 1000V VEM software with vCLI on an ESXi host.

## BEFORE YOU BEGIN

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

**Note** If you are using VUM, then the Cisco Nexus 1000V software will be installed automatically. No action is required by the server administrator.

- You have downloaded and installed the VMware vCLI. For information about installing vCLI, see the VMware vCLI documentation.
- 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.
- You are logged in to the remote host where vCLI is installed.
- The host is in maintenance mode.

## PROCEDURE

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

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

**Step 2** Using the **vihostupdate** utility and the correct name of the new VEM software file, install the VEM software.

```
[root@serialport tmp]# vihostupdate -i -b ./cisco-vem-v100-4.0.4.1.1.nn-0.4.nn.zip
--server fcs-visor1
Enter username: root
Enter password:
Host updated successfully.
[root@serialport tmp]#
```

**Step 3** Verify that the installation was successful.

```
[root@serialport tmp]# vihostupdate -q --server fcs-visor1
Enter username: root
Enter password:
-----Bulletin ID----- -----Installed----- ----------Summary----------
VEM400-20904000-BG    2009-J4-TO6:02:56    A Cisco switch module for VMware ESX Server
4.0.0 systems
[root@serialport tmp]#
```

**Step 4** Do one of the following:

- If the installation was successful, the procedure is complete.
- If not, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)*.

You have completed this procedure.

Send document comments to nexus1k-docfeedback@cisco.com.

# Manually Installing the VEM Software

You can manually install the Cisco Nexus 1000V VEM software on an ESX host.

## BEFORE YOU BEGIN

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

**Note** If you are using VUM, then the Cisco Nexus 1000V software will be installed automatically. No action is required by the server administrator.

- You are logged in to the ESX host
- You have already copied the VEM software installation file to the ESX host /tmp directory.
- You know the name of the VEM software file to be installed.
- The host is in maintenance mode.

## PROCEDURE

**Step 1** From the ESX 4.0 host /tmp directory, using the **esxupdate** command and the correct name of the VEM software file, install the VEM software as shown in the following example.

```
[root@cos1-]# esxupdate -b ./cross_cisco-vem-v100-4.0.4.1.1.nn-0.4.nn-release.vib update
cross_cisco-vem-v100-4.0.4.1.1.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 2** Verify that the installation was successful by checking for the statement, **VEM Agent is running**, in the output of the **vem status** command.

```
[root@cos1-]# vem status
VEM modules are loaded
Switch Name   Num Ports   Used Ports  Configured Ports  MTU   Uplinks
vSwitch0      32          3           32                1500  vmnic0

VEM Agent is running
[root@cos1-]#
```

**Step 3** Do one of the following:

- If the installation was successful, the procedure is complete.
- If not, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)*.

You have completed this procedure.

Send document comments to nexus1k-docfeedback@cisco.com.

# Uninstalling the VEM Software

You can 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 host remotely using SSH.

## PROCEDURE

**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.

**Example**:
```
[root@fcs-cos2 ~]# vem-remove -d
Watchdog-vemdpa: Terminating watchdog with PID 6651
Removing CIsco VEM VIB from COS system
Removing VIB cross_cisco-vem-v100-esx_4.0.4.1.1.27-0.4.2
Removing cisco-vem-v100-esx ############################### [100%]
Running [/usr/sbin/vmkmod-install.sh]...
Ok.
root@fcs-cos2 ~]#
```

**Example:**
```
~ # vem-remove -d
watchdog-vemdpa: Terminating watchdog with PID 8815
Removing Cisco VEM VIB from visor system
Removing VIB cross_cisco-vem-v100-esx_4.0.4.1.1.27-0.4.2
Removing packages :cisco-vem-v100-esx ############################ [100%]
Running [/usr/sbin/vmkmod-install.sh]...
ok.
Cleaning up running visor system
~ #
```

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

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

------------------VIB ID------------------ Package State -----------Timestamp-----------
cross_cisco-vem-v100-esx_4.0.4.1.1.27-0.4.2 retired      2009-07-02T15:26:45.994264-05:00
root@fcs-cos2 -]#
```

**Example**:
```
~ # esxupdate --vib-view query

------------------VIB ID------------------ Package State -----------Timestamp-----------
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
cross_cisco-vem-v100-esx_4.0.4.1.1.27-0.4.2 retired      2009-07-02T05:20:47.860404+00:00

~ #
```

**Step 3** Do one of the following:

- If the removal was successful, the procedure is complete.
- If not, see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)*.

You have completed this procedure.

# Related Documentation

Cisco Nexus 1000V includes the following documents available on Cisco.com:

### General Information

*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V and VMware Compatibility Information, Release 4.0(4)SV1(1)*

### Install and Upgrade

*Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0(4)SV1(1)*

### Configuration Guides

*Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V  Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0(4)SV1(1)*

### Reference Guides

*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V MIB Quick Reference*

### Troubleshooting and Alerts

*Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(1)*

*Cisco Nexus 1000V Password Recovery Guide*

Send document comments to nexus1k-docfeedback@cisco.com.

*Cisco NX-OS System Messages Reference*

# Obtaining Documentation and Submitting a Service Request

For information about 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.

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 "Related Documentation" section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.