Cisco Virtual Switch Update Manager Release 1.0 Getting Started Guide for Cisco Nexus 1000V

First Published: August 22, 2014

Last Modified: September 01, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface contains the following sections:

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

This guide is for network and server administrators with the following experience and knowledge:

- An understanding of virtualization
- An understanding of the corresponding hypervisor management software for your switch, such as VMware vSwitch, Microsoft System Center Virtual Machine Manager (SCVMM), or OpenStack.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).

Convention	Description
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Cisco Virtual Switch Update Manager

This section lists the documents used with the Cisco Virtual Switch Update Manager and available on Cisco.com at the following URL:

Cisco Nexus 1000V for VMware vSphere Documentation

General Information

Cisco Virtual Switch Update Manager Release Notes

Install and Upgrade

Cisco Virtual Switch Update Manager Getting Started Guide for Cisco Nexus 1000V

Cisco Virtual Switch Update Manager Getting Started Guide for Cisco Application Virtual Switch

Troubleshooting and Alerts

Cisco Virtual Switch Update Manager Troubleshooting Guide

Nexus 1000V Documentation

For the Cisco Nexus 1000V for VMware vSphere Documentation:

Cisco Nexus 1000V for VMware vSphere Documentation

Cisco Application Virtual Switch Documentation

Cisco Application Virtual Switch Documentation

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway Documentation

Prime Network Services Controller Documentation

Prime Network Services Controller

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to:

- nexus1k-docfeedback@cisco.com

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

CHAPTER 1

Overview

This chapter contains the following sections:

Information About the Cisco Virtual Switch Update Manager

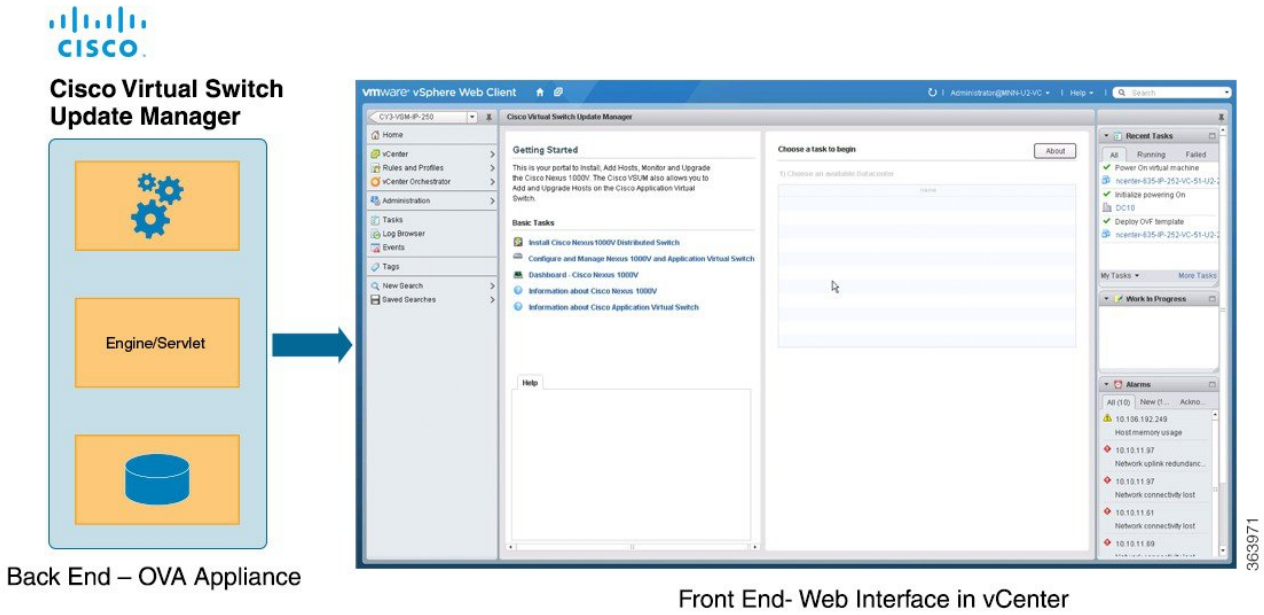
Cisco Virtual Switch Update Manager enables you to install, upgrade, and monitor the Cisco Nexus 1000V for VMware vSphere and also migrate hosts to the Cisco Nexus 1000V, using the VMware vSphere Web Client .

Cisco Virtual Switch Update Manager enables you to do the following:

- Install the Cisco Nexus 1000V switch.
- Migrate the VMware vSwitch and VMware vSphere Distributed Switch (VDS) to the Cisco Nexus 1000V.
- Monitor the Cisco Nexus 1000V.
- Upgrade the Cisco Nexus 1000V and added hosts from an earlier version to the latest version.
- Install the Cisco Nexus 1000V license.

- View the health of the virtual machines in your datacenter using the Dashboard - Cisco Nexus 1000V.

Figure 1: Cisco Virtual Switch Update Manager



Information About 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 offloads 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 is compatible with any upstream physical access layer switch that is compliant with Ethernet standard, 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 that is listed in the VMware Hardware Compatibility List (HCL).

Note We recommend that you monitor and install the patch files for the VMware ESX host software.

Cisco Nexus 1000V Components

The Cisco Nexus 1000V switch has the following components:

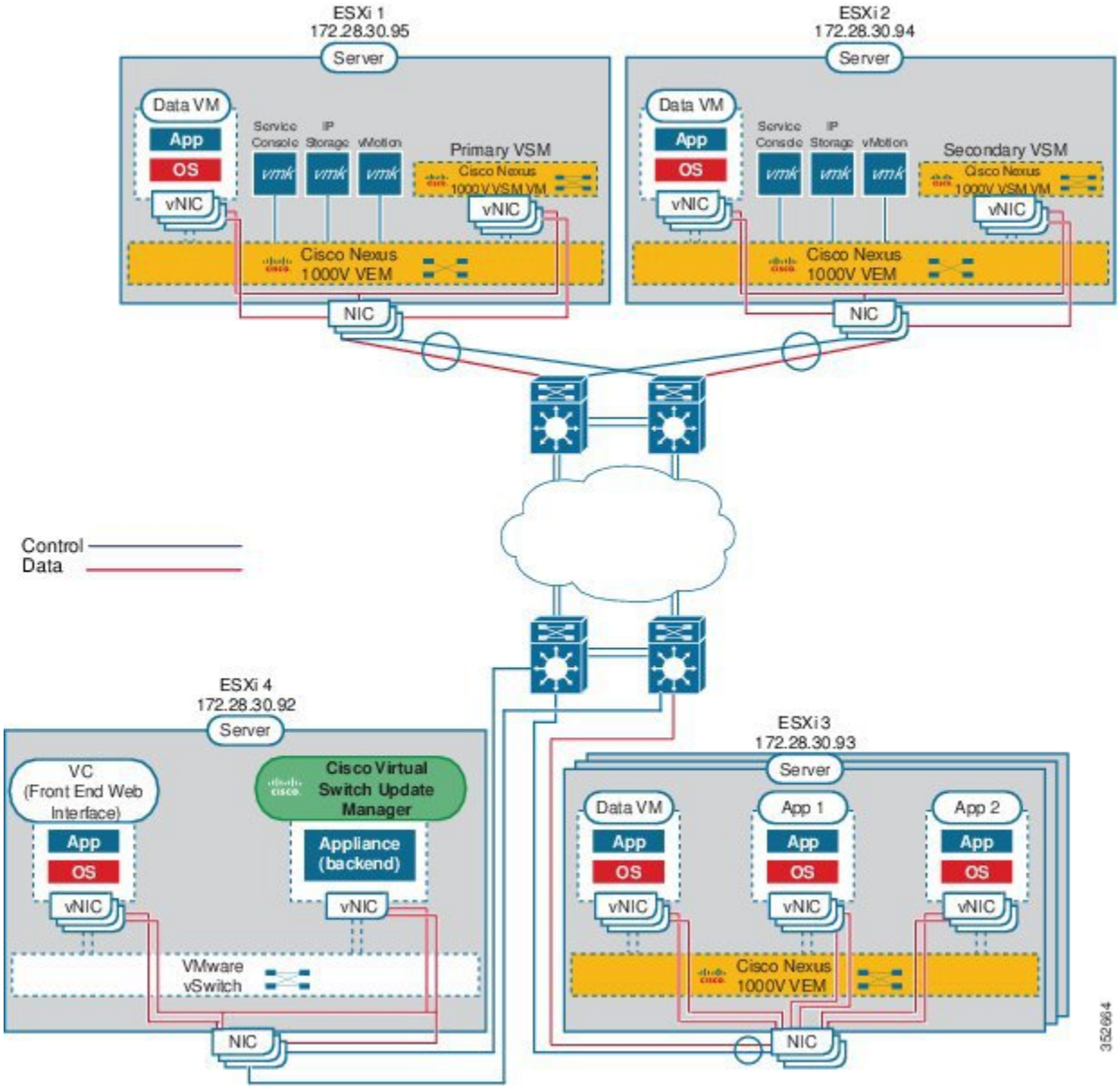
- Virtual Supervisor Module (VSM)—The control plane of the switch and a VM that runs Cisco NX-OS.

- Virtual Ethernet Module (VEM)—A virtual line card that is embedded in each VMware vSphere (ESX) host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the VEM Agent.

This figure shows the relationship between the VSM, VEMs and other Cisco Nexus 1000V components.

Layer 3 is the preferred method of communication between the VSM and the VEMs. This figure shows an example of a Layer 3 topology. The software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2.

Figure 2: Layer 3 Installation Diagram for Installing Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager



Information About the Cisco Nexus 1000V Virtual Supervisor Module

The Virtual Supervisor Module (VSM) is the control plane of the Cisco Nexus 1000V. It is deployed as a virtual machine.

You can install the VSM in either a standalone or active/standby high-availability (HA) pair. We recommend that you install two VSMs in an active-standby configuration for high availability.

VSM and VEM collectively represent the Cisco Nexus 1000V. The switch supports the following operations:

- Configuration
- Management
- Monitoring
- Diagnostics
- Integration with VMware vCenter Server

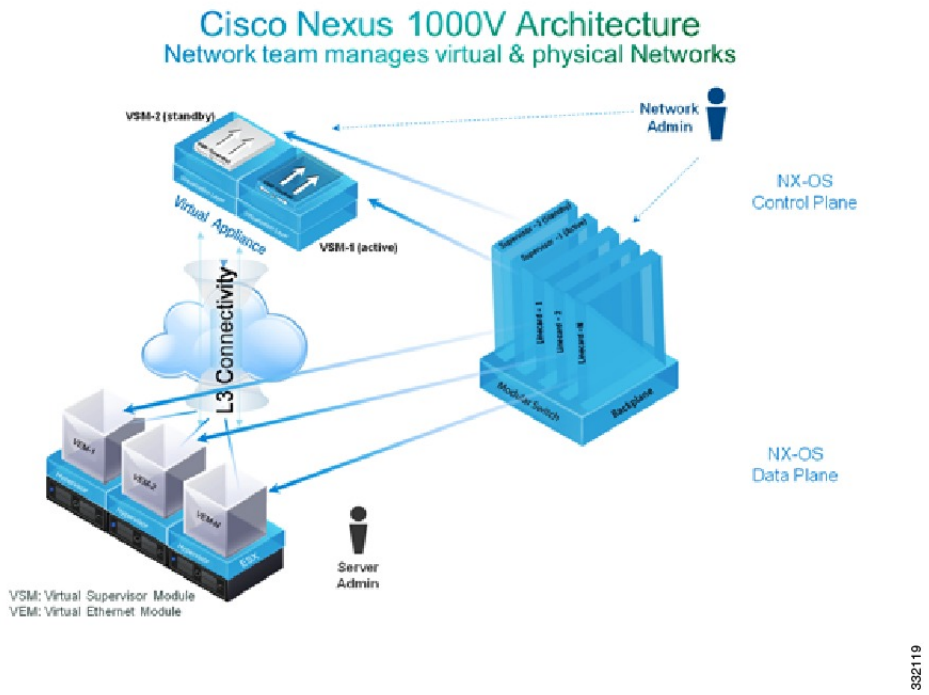
The VSM uses an external network fabric to communicate with the VEMs. The VSM runs the control plane protocols and configures the state of each VEM, but it never actually forwards packets. The physical NICs on the VEM server are the uplinks to the external fabric. VEMs switch traffic between the local virtual Ethernet ports that are connected to the VM vNICs but do not switch the traffic to other VEMs. Instead, a source VEM switches packets to the uplinks that the external fabric delivers to the target VEM.

A single Cisco Nexus 1000V instance, including dual-redundant VSMs and managed VEMs, forms a switch domain. Each Cisco Nexus 1000V domain within a VMware vCenter Server must be distinguished by a unique integer called the domain identifier.

See the *Cisco Nexus 1000V Resource Availability Reference* for information about scale limits.

The Cisco Nexus 1000V architecture is shown in this figure.

Figure 3: Cisco Nexus 1000V Architecture



Information About the Virtual Ethernet Module

Each hypervisor is embedded with one VEM which replaces the virtual switch by performing the following functions:

- Advanced networking and security
- Switching between directly attached VMs
- Uplinking to the rest of the network

Note Only one version of the VEM can be installed on an ESX/ESXi host at any given time.

In the Cisco Nexus 1000V, the traffic is switched between VMs locally at each VEM instance. Each VEM also interconnects the local VM 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 for the primary module 1 and secondary module 2. Either module can act as active or standby. The first server or host is automatically assigned to module 3. The network interface card (NIC) ports are 3/1 and 3/2 (vmnic0 and vmnic1 on the ESX/ESXi host). The ports to which

the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000V where they are assigned with a global number.

Workflow for Installing Cisco Nexus 1000V

Installing Cisco Nexus 1000V using Cisco Virtual Switch Update Manager consists of the following steps:

Step 1 Installing Cisco Virtual Switch Update Manager.
See Installing the Cisco Virtual Switch Update Manager, on page 10.

Step 2 Installing Cisco Nexus 1000V VSM.
See Installing the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager, on page 17.

Step 3 Migrating hosts to Cisco Nexus 1000V.
See Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager, on page 25.

CHAPTER 2

Installing Cisco Virtual Switch Update Manager

This chapter contains the following sections:

Information About Cisco Virtual Switch Update Manager

Cisco Virtual Switch Update Manager is a virtual appliance that is registered as a plug-in to VMware vCenter Server. The Cisco Virtual Switch Update Manager graphical user interface (GUI) is an integral part of VMware vSphere Web Client; it can only be accessed by logging into the VMware vSphere Web Client.

The Cisco Virtual Switch Update Manager enables you to install, migrate, monitor, and upgrade the VSMs in high availability (HA) or standalone mode and the VEMs on ESX/ESXi hosts.

The Cisco Virtual Switch Update Manager software is available at the download URL location that is provided with the software.

Compatibility Information for Cisco Virtual Switch Update Manager

The following table lists the compatibility information for Cisco Virtual Switch Update Manager.

Table 1: Version Compatibility for Cisco Virtual Switch Update Manager for Cisco Nexus 1000V

Minimum Required Cisco Nexus 1000V Release for Various Features	VMware vCenter Server Version (Includes Patches and Updates)	VMware Software Release Version (Includes Patches and Updates)
Cisco Virtual Switch Update Manager supports installations of the following releases: • Release 5.2(1)SV3(1.1) • Release 4.2(1)SV2(2.3) • Release 4.2(1)SV2(2.2) • Release 4.2(1)SV2(1.1a) • Release 4.2(1)SV1(5.2b) Cisco Virtual Switch Update Manager supports the migrations from Release 4.2(1)SV1(5.1) and later releases. Cisco Virtual Switch Update Manager supports upgrades from Release 4.2(1)SV1(4b) and later releases. Cisco Virtual Switch Update Manager supports the monitoring functionality from Release 4.2(1)SV2(1.1) and later releases.	5.1, 5.5	ESXi 4.1 ESXi 5.0 ESXi 5.1 ESXi 5.5

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

System Requirements

- VMware ESXi 4.1, 5.0, 5.1, 5.5
- All the web–based GUI client requirements as required by VMware vShpere Web Client.
- The memory requirement is 4 GB RAM.
- The CPU requirement is 2.

- The disk space requirement is 80 GB.

Prerequisites

Cisco Virtual Switch Update Manager has the following prerequisites:

- You have installed the VMware Enterprise Plus license on the hosts.
- You have installed the vCenter Server 5.1 or 5.5 with Web Client.
- You must have administrative credentials for vCenter Server.
- You must have a username, IP address, subnet mask, and a gateway IP address for deploying the OVA.
- Cisco Virtual Switch Update Manager must have IP connectivity on port 443 to all ESXi hosts.
- Ensure that ports 80 and 443 are open in the vCenter to communicate with the host.
- Ensure that the IP address used for deploying the OVA can communicate with the IP address of vCenter Server.

Verifying the Authenticity of the Cisco-Signed Image (Optional)

Before you install the Nexus1000v-vsum.1.0.zip image, you have the option to validate the authenticity of it. In the zip file, there is a signature.txt file that contains a SHA-512 signature and an executable script that can be used to verify the authenticity of the Nexus1000v-vsum.1.0.zip image.

Note Verifying the authenticity of an image is optional. You can still install the image without validating its authenticity.

Before You Begin

You need to be running a Linux machine with the following utilities installed:

- openssl
- base64

Step 1 Copy the following files to a directory on the Linux machine:

- Nexus1000v-vsum.1.0.zip image
- signature.txt file
- cisco_n1k_image_validation_v_1_1 script

Step 2 Ensure that the script is executable.
chmod 755 cisco_n1k_image_validation_v_1_1

Step 3 Run the script.
./cisco_n1k_image_validation_v_1_1 -s signature.txt Nexus1000v-vsum.1.0.zip

Step 4 Check the output. If the validation is successful, the following message displays:

```
Authenticity of Cisco-signed image Nexus1000v-vsum.1.0.zip has been successfuly verified!
```

Installing the Cisco Virtual Switch Update Manager

You can install the Cisco Virtual Switch Update Manager OVA using the following steps.

Before You Begin

- Ensure that the Cisco Virtual Switch Update Manager OVA image is available in the file system.
- Ensure that you have the IP address, subnet mask, gateway IP address, domain name, DNS server, and vCenter IP address and credentials for deploying the OVA.

Note It is important that you use the credentials that you use for the thick client and vCenter Managed Object Browser (MOB) while installing Cisco Virtual Switch Update Manager.

Step 1 Log in to VMware vSphere Web Client.

Step 2 Choose the host on which to deploy the Cisco Virtual Switch Update Manager OVA.

Step 3 From the **Actions** menu, choose **Deploy OVF Template**.

Step 4 In the **Deploy OVF Template** wizard, complete the information as described in the following table.

Window	Action
Source	Choose the Cisco Virtual Switch Update Manager OVA.
OVF Template Details	Review the details.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Enter a name and choose a location for the appliance.
Host or Cluster	Choose the host or cluster to run the OVA template.
Datastore	Choose the datastore for the VM.
Disk Format	Choose either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks. We recommend that you store the VM virtual disks in the **Thick provisioned format**.

Window	Action
Network Mapping	Choose the network mapping for the VM.
Properties	Provide the following information: • VM IP address • IP subnet mask • Gateway IP address • DNS server IP address • vCenter IP or fully qualified domain name (FQDN) • DNS entry to resolve FQDN • vCenter username • vCenter password • HTTP cleartext port and HTTPS port
Ready to Complete	Review the deployment settings. **Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, gateway information, and vCenter credentials.

Step 5 Click **Finish**.

Step 6 After Cisco Virtual Switch Update Manager is successfully deployed, click **Close**.

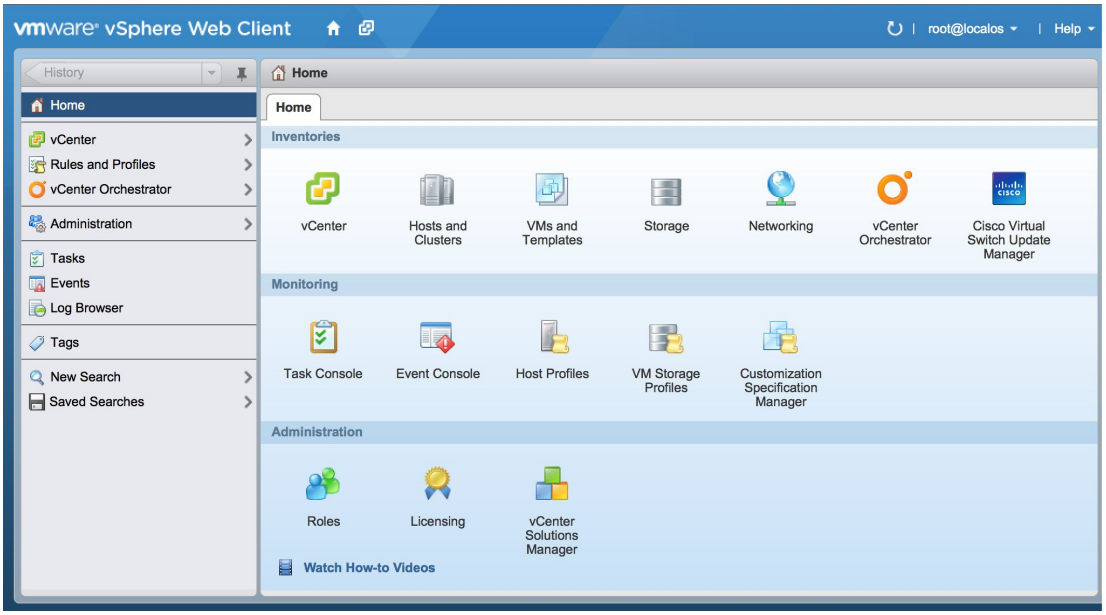
Step 7 Power on the Cisco Virtual Switch Update Manager VM.
It might take 5 minutes for Cisco Virtual Switch Update Manager to be installed and registered as a vSphere Web Client plug-in.
If the Web Client session was open during this installation, you must log out and log in again to view the Cisco Virtual Switch Update Manager plug-in.

About the Cisco Virtual Switch Update Manager GUI

Cisco Virtual Switch Update Manager is a virtual appliance that is registered as a plug-in to VMware vCenter Server. It can only be accessed by logging into VMware vSphere Web Client.

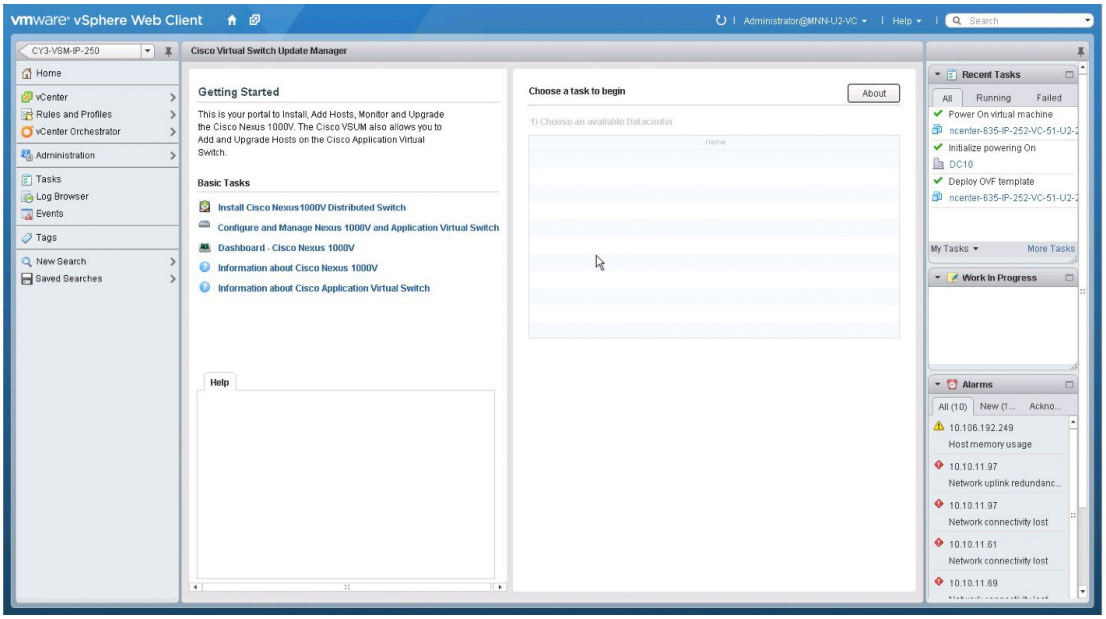
The Cisco Virtual Switch Update Manager is the graphical user interface (GUI) that you use to install, migrate, monitor, and upgrade the VSMs in high availability (HA) or standalone mode and the VEMs on ESX/ESXi hosts.

Figure 4: VMware vSphere Web Client—Home Page



363894

Figure 5: Cisco Virtual Switch Update Manager—Home Page



363972

Replacing Cisco Virtual Switch Update Manager—Windows vCenter Server

Use this procedure to replace an existing Cisco Virtual Switch Update Manager in the VMware vSphere Web Client.

Before You Begin

Ensure that you power off the current Cisco Virtual Switch Update Manager before you begin this procedure.

Step 1 Power off the current active Cisco Virtual Switch Update Manager VM.

Step 2 Enter `https://VCIP/mob` and log in with the default credentials.

Step 3 In a web browser, choose **Content** > **Extension Manager** > **UnregisterExtension**.

Step 4 Enter **com.cisco.n1kv** and click **Invoke method**.

Step 5 Choose **Start** > **Run** > **services.msc**.

Step 6 Right click the VMware vSphere Web Client and click **stop**.

Step 7 From the `C:\ProgramData\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity` directory, delete the **com.cisco.n1kv** folder.

Step 8 Choose **Start** > **Run** > **type service.msc**.

Step 9 Right click the VMware vSphere Web Client and click **Start**.

Step 10 Install the new version of the Cisco Virtual Switch Update Manager VM.

Step 11 After Cisco Virtual Switch Update Manager is successfully deployed, login to the VMware vSphere Web Client to view the Cisco Virtual Switch Update Manager plugin.

ReplacingCiscoVirtualSwitchUpdateManager—LinuxvCenter Appliance

Use this procedure to replace an existing Cisco Virtual Switch Update Manager in the VMware vSphere Web Client.

Before You Begin

Ensure that you power off the current Cisco Virtual Switch Update Manager before you begin this procedure.

Step 1 Power off the current active Cisco Virtual Switch Update Manager VM.

Step 2 Enter `https://VCIP/mob` and log in with the default credentials.

Step 3 In a web browser, choose **Content** > **Extension Manager** > **UnregisterExtension**.

Step 4 Enter **com.cisco.n1kv** and click **Invoke method**.

Step 5 Enter the **rm -rf /var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.cisco.n1kv-1.0/** command.

Step 6 Enter the **/etc/init.d/vsphere-client restart** command.

Step 7 Install the new version of the Cisco Virtual Switch Update Manager VM.

Step 8 After Cisco Virtual Switch Update Manager is successfully deployed, login to the VMware vSphere Web Client to view the Cisco Virtual Switch Update Manager plugin.

Feature History for Installing Cisco Virtual Switch Update Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Installing Cisco Virtual Switch Update Manager	Release 1.0	This feature was introduced.

CHAPTER 3

Installing Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This chapter contains the following sections:

Information About Installing Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

The Cisco Virtual Switch Update Manager is the graphical user interface (GUI) that you use to install the VSMs in high availability (HA) or standalone mode and the VEMs on ESX/ESXi hosts. The Cisco Virtual Switch Update Manager GUI is an integral part of the VMware vSphere Web Client and can only be accessed by logging into the VMware vSphere Web Client.

Cisco Virtual Switch Update Manager enables you to install the following versions of the Release 5.2(1)SV3(1.1) VSM:

- Release 4.2(1)SV1(5.2b)
- Release 4.2(1)SV2(1.1a)
- Release 4.2(1)SV2(2.3)
- Release 4.2(1)SV2(2.2)

See Migrating Hosts to Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager, on page 23 to install VEM using Cisco Virtual Switch Update Manager.

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

See the corresponding *Cisco Nexus 1000V Installation and Upgrade Guide* to manually install the Cisco Nexus 1000V versions that are not supported by the Cisco Virtual Switch Update Manager.

Prerequisites for Installing the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

The Cisco Nexus 1000V installation using Cisco Virtual Switch Update Manager has the following prerequisites:

- You have installed Cisco Virtual Switch Update Manager.
- You have installed and prepared vCenter Server for host management using the instructions from VMware.
- You have installed VMware vSphere Web Client.
- You have installed the VMware Enterprise Plus license on the hosts.
- You are familiar with the Cisco Nexus 1000V topology diagram.
- You must create port groups for the Control and Management VLANs on the Cisco Nexus 1000V.
- You must have the Distributed Switch—Create, Extension-Register, Update privilege permissions enabled on the vCenter Server.
- ESXi host must be running 4.1 or later releases.

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

The Cisco Nexus 1000V installation using Cisco Virtual Switch Update Manager has the following guidelines and limitations:

- We recommend that you install the VSMs in a high availability mode on the Cisco Nexus 1000V. For information about high availability and redundancy, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide*. Cisco Virtual Switch Update Manager supports standalone mode, but we do not recommend that you use this mode in a production environment.
- Cisco Virtual Switch Update Manager always deploys with VSM HA pairs by default. We recommend that you install primary and secondary VSM VMs on separate hosts.
- Only Layer 3 mode of deployment is supported by the Cisco Virtual Switch Update Manager with ESXi host only.
- The Cisco Nexus 1000V VSM always uses the following two network interfaces in the same order as follows:

  1 Control Interface

2 Management Interface

- The VM hardware version has no dependencies; so the VM hardware version can be upgraded if required.
- Do not deploy vCenter server and VSM in different data centers. It is not supported.
- We recommend that you monitor and install all the relevant patch applications from the VMware ESX host server.

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

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

Before You Begin

Know the following about the switch:

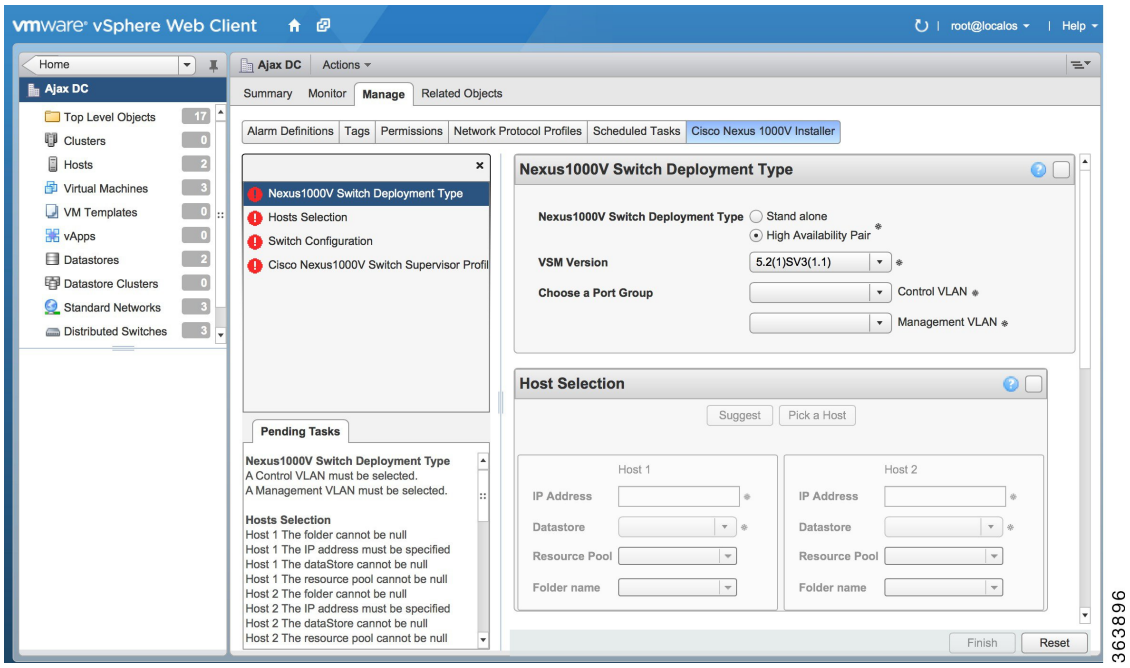
- VM port group for the control traffic of the switch
- VM port group for the management traffic of the switch
- IP address for management
- Subnet mask
- Gateway IP address
- Datacenter in which the switch will be installed
- Domain ID (a unique ID for the switch)

- Password

Step 1 Log in to VMware vSphere Web Client.

Step 2 In the vSphere Client, choose **Cisco Virtual Switch Update Manager** > **Install Cisco Nexus 1000V Distributed Switch** > **Datacenter**. The Cisco Nexus 1000V Installer pane appears.

Figure 6: Cisco Nexus 1000V Installer Pane



Step 3 (Optional) You can also access the Cisco Nexus 1000V Installer in vSphere Client by choosing **vCenter** > **Datacenter**.

Step 4 Choose **Manage** > **Cisco Nexus 1000V Installer**.

Step 5 In the **Cisco Nexus 1000V Switch Deployment Type** area, complete the following fields:

Name	Description
HIgh Availability Pair radio button	Installs the switch as a HA pair. By default, the **High Availability Pair** is selected.
Standalone radio button	Installs the switch in a standalone mode. **Note** We recommend that you install the Cisco Nexus 1000V in an HA pair.
VSM Version drop-down list	Select the Cisco Nexus 1000V version to be installed. By default, the latest version is selected.
Control VLAN drop-down list	Choose the control port group for the switch. The control port group is used for the control traffic.

Name	Description
Management VLAN drop-down list	Choose the management port group for the switch. **Note** The Cisco Nexus 1000V VSM uses the management network to communicate with vCenter server and ESXi.

Step 6 Click **Suggest**. This will automatically select two hosts based on the details provided in the Cisco Nexus 1000V Switch deployment type area.

Step 7 In the **Host Selection** area, complete the following fields:

Name	Description
IP Address field	The IP address of the hosts on which the switch will be deployed. The primary switch is deployed on Host 1 and the secondary switch is deployed on Host 2. You can override system choices by dragging and dropping hosts. Click **Pick a host** to drag and drop hosts.
Datastore drop-down list	Choose the system-selected datastore that you want to override. Choose a datastore for each host.
Resource Pool drop-down list	Choose the resource pool for each host. **Note** If you do not choose a resource pool and the host is a cluster, the resource pool for the switch is the root resource pool of the cluster. If you do not choose a resource pool and the host is in a standalone mode, then the resource pool for the switch will be the root resource pool of the host.
Folder Name drop-down list	Choose the folder name for each host. **Note** If the folder name is not displayed in the drop-down list, the switch VM is created in the root VM folder of the datacenter.

Step 8 In the **Switch Configuration** area, complete the following fields:

Name	Description
Domain ID field	The domain ID for the switch. The domain ID is common for both the primary and secondary switches and it should be unique for every new switch. The range for the domain is from 1 to 1023.

Name	Description
Deployment Type radio button	Configures the deployment type. By default, **Management IP Address** is selected. **Note** • If you select the Management IP address, then this IP address is used for both, the VSM management operations as well as the VSM to VEM communications. • If you select the Control IP address, then this IP address is used only for the VSM to VEM communications.
Control:IP/Name field	The IP address for switch connectivity.
Control: Mask field	The sub net mask.
Control: Gateway IP/Name field	The gateway IP address.
Default Port Profile checkbox	If checked, the default port profile is enabled and this creates sample port profiles for the different features in the VSM, and pushes it to the VSM. The sample port profiles are created as user references and includes default and mandatory commands that are required to configure this feature. You can modify the port profiles based on the network configuration.

Step 9 In the **VIrtual Supervisor Module (VSM) configuration** area, complete the following fields:

Name	Description
Switch Name field	The name of the switch. The name must: have the following: • Start with a letter (A-Z, a-z). • Contain up to 32 case-sensitive letters (A-Z, a-z), numbers (0-9), or hyphens (-). • Not contain any other special characters or spaces. When a switch VM is created in the vCenter, the same name is used for the primary and the secondary switch. For a standalone deployment, the VSM VM is the *switch name*. For a HA deployment, the primary VSM VM is the *switch name_primary* and the secondary switch is the *switch name_secondary*.

Name	Description
IP Address field	The IP address of the switch. The IP address is used for the management of the Cisco Nexus 1000V switch.
Subnet Mask field	The subnet mask for the above entered IP address.
Gateway Address field	The gateway IP address for the above entered IP address.
Username field	By default, the user name is admin. This field is not editable.
Password field	The admin user password. This password is used to log in to the switch for administration.
Confirm Password field	The admin user password that you reenter for confirmation.

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

Step 11 In the vSphere Web Client, choose **Home** > **vCenter** > **Datacenters** > **Select Datacenter** > **Monitor** > **Tasks** to view the status of the Cisco Nexus 1000V switch installation.
A typical installation of the switch takes about four minutes. In the vCenter Web Client, you can view the tasks by the task object, user, or the task status.

What to Do Next

Install VEM as described in the procedure Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager, on page 25.

Feature History for Installing Cisco Nexus 1000V using Cisco Virtual Switch Update Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Installing Cisco Nexus 1000V for VMware vSphere using Cisco Virtual Switch Update Manager	Release 1.0	This feature was introduced.

CHAPTER 4

Migrating Hosts to Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This chapter contains the following sections:

Information About Migrating Hosts to the Cisco Nexus 1000V Switch Using Cisco Virtual Switch Update Manager

You can use the Cisco Virtual Switch Update Manager GUI to migrate hosts from the VMware vSwitch and VMware distributed virtual switch (DVS) to the Cisco Nexus 1000V switch.

Cisco Virtual Switch Update Manager enables you to do the following:

- Add hosts and/or Migrate multiple hosts.
- Migrate each VMware port group or kernel NIC to the correct port profile.
- Migrate each physical NIC from the VMware vSwitch or VMware DVS to the correct uplink on the Cisco Nexus 1000V.
- Migrate VM NICs from the VMware vSwitch or VMware DVS to the corresponding uplink on the Cisco Nexus 1000V.

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

Prerequisites for Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

The migration of hosts to the Cisco Nexus 1000V using Cisco Virtual Switch Update Manager has the following prerequisites:

- The host must have one or more physical NICs on each VMware vSwitch/VMware DVS in use.
- You must have administrative privileges for vCenter Server.
- You must have the Distributed Switch—Create and Modify privilege permission enabled on the vCentre.

Guidelines and Limitations for Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

When you move the ESX/ESXi host that runs the Virtual Supervisor module (VSM) from the VMware vSwitch or VMware DVS to the Cisco Nexus 1000V, the connectivity between the active and standby VSM might get temporarily lost. In that situation, both active and standby VSMs assume the active role.

The reboot of the VSM is based on the following conditions:

1. The number of modules attached to the VSM
   - If a VSM has more modules attached than the other VSMs, and there is no virtual channel (VC) connectivity on either VSM, the VSM that has fewer modules is rebooted.
   - If modules are attached to both VSMs and one VSM has VC connectivity, the VSM without connectivity is rebooted.
2. VC connectivity

Note This option is invoked when the previous condition is not met.

   - If both VSMs have the same number of modules or no modules, the software makes a selection that is based on the VC connectivity status.
3. Last configuration change

Note This condition is invoked when the previous two conditions are not met.

   - If both VSMs have the same number of modules and no VC connectivity, the VSM with the latest configuration remains active and the other VSM is rebooted.

4 Last active VSM

- If the previous three conditions are not met, the VSM that became active most recently is rebooted.

Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

You can install a Cisco Nexus 1000V Virtual Ethernet module (VEM) using Cisco Virtual Switch Update Manager. When the Cisco Virtual Switch Update Manager installs VEMs, it migrates all VM kernels and their corresponding VM NICs across vSwitches to the Cisco Nexus 1000V VEMs.

Before You Begin

Know the following information about the switch:

- vCenter IP address
- vCenter user ID
- vCenter password
- Cisco Nexus 1000V switch username
- Cisco Nexus 1000V switch password

Step 1 Log in to the VMware vSphere Web Client.

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

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

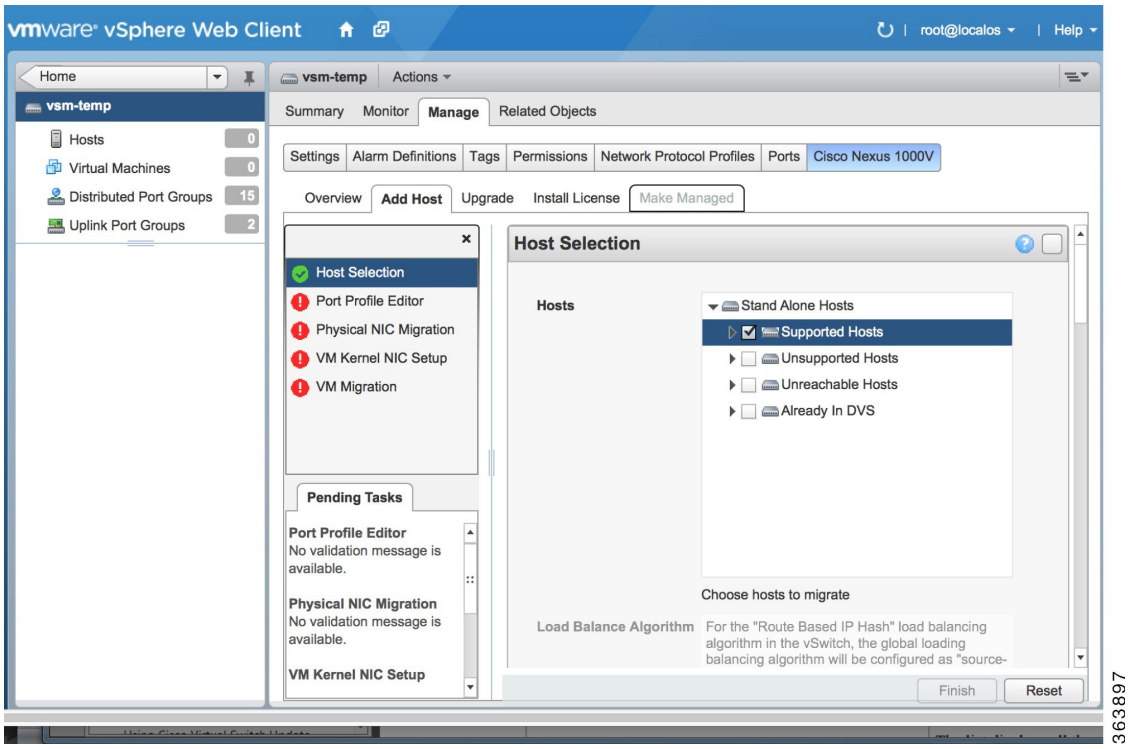
Step 3 In the switch pane, click **Add Host**.

Step 4 (Optional) In case of multiple vCenter Servers, choose **Home** > **Cisco Virtual Switch Update Manager** > **vCenter Server** > **Configure and Manage Nexus 1000V and Application Virtual Switch** .

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

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

Figure 7: Cisco Virtual Switch Update Manager—Migrating Hosts



Step 7 In the **Host Selection** area, review the following fields.

Name	Description
Clustered hosts drop-down list	Choose the hosts to be migrated. The clustered hosts list displays all the hosts that are in HA pair.
Standalone hosts drop-down list	Choose the hosts to be migrated.
Supported Hosts check box	If checked, displays the lists of hosts that can be migrated to the current version of the Cisco Nexus 1000V.

Name	Description
Unsupported Hosts check box	If checked, displays the list of hosts that cannot be migrated to the current version of the Cisco Nexus 1000V. For information on the list of hosts that are not supported, see the Cisco Nexus 1000V and VMware Compatibility Documentation, at: http://www.cisco.com/c/en/us/support/switches/nexus-1000v-switch-vmware-vsphere/products-device-support-tables-list.html.
Unreachable Hosts check box	If checked, displays the list of hosts that are in a unreachable state.
Already in DVS check box	If checked, displays the list of hosts that are already migrated to the Cisco Nexus 1000V.

Step 8 Click **Suggest**.
Cisco Virtual Switch Update Manager displays the list of existing and proposed port profiles and suggests appropriate port profiles for each VMKNIC, VM NIC, and physical NICs.

Step 9 Review the port profile populated in the **Port Profile Editor** area. You can edit the fields based on your requirements. To edit the fields, you must use the **Port Profile Editor**.
The port profiles that are already available on the VSM are not editable. You can edit only those port profiles that are suggested by the Cisco Virtual Switch Update Manager. Click the **Duplicate** button to create a new port profile from an existing or from a suggested port profile.

Step 10 In the **Port Profile Editor** area, complete the following fields.

Name	Description
Port Profile Editor drop-down list	The list of existing port profiles or new port profiles to be created are displayed. Choose the port profile. • In Use—Displays true, when the port profile is in use on the current Add Host screen. Displays False when the port profile is not in use on the current Add Host screen. • Valid—Displays true when all the port profile fields are completed. Displays false when one or more of the port profile fields is incomplete. • Editable—Displays true if the port profile is editable. Displays false if the port profile is not editable. • Profile Name—Displays the name of the port profile.
Uplink check box	If checked, displays the uplink associated with the port profile.

Name	Description
Trunk check box	If checked, displays the trunk associated with the port profile.
L3 Capable check box	If checked, the L3 capability is associated with the port profile.
ISCSI Multipath check box	If checked, the ISCSI Multipath is associated with the port profile.
Neither L3 nor ISCSI check box	If checked, then neither the L3 or the ISCSI is associated with the port profile.
Channel-group auto mode check box	If checked, the channel group auto mode is associated with the port profile.
Mac-pinning check box	If checked, the channel group auto mode on mac-pining is associated with the port profile.
Name field	The name of the port profile.
VLANs field	Choose the VLAN.
Native VLAN field	The native VLAN associated with the port profile.
Duplicate button	Clones an existing port profile configuration to create a new port profile .

Step 11 Scroll down to view the host profile populated in the **Physical NIC Migration** area.

Step 12 In the **Physical NIC Migration** area, review the following fields.

Name	Description
Physical NIC check box	Review the physical NIC that has been automatically selected by the Cisco Virtual Switch Update Manager. Check/uncheck to select/deselect the VMNIcs for the migration. You must ensure that at least one physical NIC is selected for the migration.
Profile drop-down list	Review the port profile associated with the physical NICs. Alternatively, you can choose the required port profile from the profile drop-down list, to associate it with the physical NIC. You must ensure that all the necessary VLANs are allowed in the selected port profile.
Source column	The vSwitch or VDS port group that the PNIC is currently assigned to.

Name	Description
Select All button	Migrates all the physical NICs associated with the host.
Select None button	Deselects all the selected values for the physical NICs associated with the host.

Step 13 Scroll down to view the host profile populated in the **VM Kernel NIC Setup** area.

Step 14 In the **VM Kernel NIC Setup** area, complete the following fields.

Name	Description
VM Kernel NIC check box	If checked, displays the port profile configuration that will be created on Cisco Nexus 1000V and associated with the VMkernel NIC. Review the selected VMkernel NICs. You can also uncheck the VMkernel NIC check boxes if you do not want the VMKs to be migrated to the Cisco Nexus 1000V. You must ensure that at least one VMkernel NIC is selected to migrate to the Cisco Nexus 1000V which will carry the L3 traffic. **Note** Do not uncheck any of the VMkernel NIC checkboxes, unless and until the required VMkernel NIC is associated with the Layer3 port profile.
L3 Capable column	Displays whether the VMkernel NIC is Layer 3 capable. Only one VMkernel NIC is Layer3 capable. By default, the VMK0 is selected as the Layer3 control. **Note** To change the VMkernel to Layer3 port profile, do the following: • From the **Port Profile** drop-down list, choose the non Layer3 port profile for VMk0. In absence of non Layer3 veth profile, you can create non Layer3 port profiles as follows: ◦ Select the Layer3 port profile and click **Duplicate**. ◦ Check the **Neither L3 nor ISCSI** radio button and click **OK**. You can edit the list of the supported VLANs. • Select the L3 enabled PP for any one VMkernel NICs, which you want to use for the L3 control traffic.

Name	Description
Profile drop-down list	Choose the port profile associated with the VMkernel NIC.
Source Profile column	Displays the vSwitch or VDS port group that the VMkernel NIC is currently assigned to.
Select None button	Deselects all the selected VMkernel NICs associated with the host.
New button	Adds a new VMkernel NIC for Layer 3 control. Enter the IP address and net mask for the new VMkernel NIC and click **OK**. After the VMKernel NIC is created, select the appropriate port profile for the VMKernel NIC from the port profile drop-down list. **Note** Ensure that the host is selected before you create the new VMkernel NIC.
Edit button	Edits the IP address and subnet mask for a newly created VMkernel NIC.

Step 15 Scroll down to view the host profile populated in the **VM Migration** area.

Step 16 In the **VM Migration** area, review the following fields.

Area	Action
Virtual Machine NICs check box	If checked, displays the VSMs and the network adapters associated with the VM.
Profile drop-down list	Choose the port profile associated with the Virtual NIC.
Source Profile column	The source associated with the port profile.
Select None button	Deselects all the VMs associated with the host.

Step 17 Click **Finish** to migrate the host from the VMware vSwitch to the Cisco Nexus 1000V switch.

Step 18 In the vSphere Client, choose **vCenter** > **Datacenter** > **Switch** > **Monitor** > **Tasks** to view the status of the migration. You can also view the tasks in the vSphere Web client by navigating to **Cisco Virtual Switch Update Manager** > **Select vCenter Host** > **Manage DVS** > **Select Datacenter** > **Select Switch** > **Monitor** > **Tasks**.
A typical migration of the host takes about 2 minutes. In the vCenter Client, you can view the tasks by the task object, user, or task status.

Feature History for Migrating Hosts to the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Migrating hosts to the Cisco Nexus 1000V using Cisco Virtual Switch Update Manager	Release 1.0	This feature was introduced.

CHAPTER 5

Upgrading Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This chapter contains the following sections:

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

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

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

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

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

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

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

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

Unsupported Upgrade Paths: Using Cisco Virtual Switch Update Manager, you cannot upgrade the following releases of Cisco Nexus 1000V to the current release:

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

See the *Cisco Nexus 1000V Installation and Upgrade Guide* to upgrade the Cisco Nexus 1000V to the current version using the CLI.

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

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

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

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

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

- If you need to migrate a vSphere host from ESX to ESXi, do it before the Cisco Nexus 1000V upgrade.
- You have placed the VEM software file in `/tmp` on the vSphere host. Placing it in the root (/) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space by entering the **vdf** command.

- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series switches with the Cisco IOS software, enter the **portfast trunk** command or the **portfast edge trunk** command.
  - On Cisco Nexus 5000 Series switches with the Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:
  - **spanning-tree bpdu filter**
  - **spanning-tree bpdu guard**
- You must have the Distributed Switch—Create and Modify privilege permission enabled on the vCentre.
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

Upgrading VSM to a 3-GB HDD Before Upgrading Cisco Nexus 1000V

If you are upgrading Cisco Nexus 1000Vfrom a previous release to Release 5.2(1)SV3(1.x) and you have a VSM 2-GB HDD, you must upgrade VSM to a 3-GB HDD before you upgrade Cisco Nexus 1000V. Follow one of the following sets of instructions to upgrade VSM.

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

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

Before You Begin

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

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

Step 1 Remove the existing standby VSM.

a) Right-click on the VSM VM and power off the VM.

b) Remove it from the Virtual Center inventory.

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

a) Confirm that the same port profiles are used as the primary VSM for 3 network interfaces.

b) Provision a 3-GB HDD with a minimum of 2 GB of RAM reserved and allocated, and has a minimum CPU speed of 1600 MHz.

See the section "Installing the Software from the ISO Image" in the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Step 3 Power on the standby VSM.

a) Confirm the HA role is set as Secondary.

b) Configure the Domain ID is the same as the Primary VSM.

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

Step 5 Remove the current standby VSM.

a) Right-click on the VSM VM and power off the VM.

b) Remove it from the Virtual Center inventory.

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

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

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

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

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

What to Do Next

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

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

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

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

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

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

N1110#
```

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

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

a) N1110# **configure terminal**

b) N1110#(config)**virtual-service-blade** name switch

c) N1110#(config-vsb-config)**shutdown secondary**

d) N1110#(config-vsb-config)**no enable secondary**

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

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

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

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

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

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

N1110#
```

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

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

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

N1110(config-vsb-config#
```

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

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

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

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

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

Step 8 Bring up the new VSB with Release 4.2(2)SV2(1.1) using ISO.

See the Cisco Nexus 1100 Series Virtual Services Appliances Deployment Guide White Paper for more information.

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

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

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

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

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

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

Mount-on                 1K-blocks      Used   Available   Use%  Filesystem
        /                  307200     87628      219572     29   /dev/root
        /proc                   0         0           0      0   proc
        /isan                614400    243076      371324     40   none
        /var/sysmgr          512000     18896      493104      4   none
        /var/sysmgr/ftp      204800        40      204760      1   none
        /dev/shm             358400     30268      328132      9   none
        /volatile             20480         0       20480      0   none
        /debug                 2048         8        2040      1   none
        /dev/mqueue               0         0           0      0   none
        /mnt/cfg/0           326681      8360      301455      3   /dev/hda5
        /mnt/cfg/1           326681      8359      301456      3   /dev/hda6
        /var/sysmgr/startup-cfg 409600   1168      408432      1   none
        /dev/pts                  0         0           0      0   devpts
        /mnt/pss             326671      8625      301178      3   /dev/hda3
        /bootflash          3122988    151756     2812592      6   /dev/hda4
        /bootflash_sup-remote 3122992  151760     2812592      6   127.1.1.1:/mnt/bootflash/
```

What to Do Next

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

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

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

Step 1 Display the system internal flash.

```
switch# show system internal flash
Mount-on                 1K-blocks      Used   Available   Use%  Filesystem
```

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

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

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

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

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

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

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

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

- During the VEM upgrade process, VEMs reattach to the VSM.

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

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

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

Step 1 Log in to the VMware vSphere Web Client.

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

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

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

Step 4 (Optional) In case of multiple vCenter Servers, choose **Home** > **Cisco Virtual Switch Update Manager** > **vCenter Server** > **Configure and Manage Nexus 1000V and Application Virtual Switch** .

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

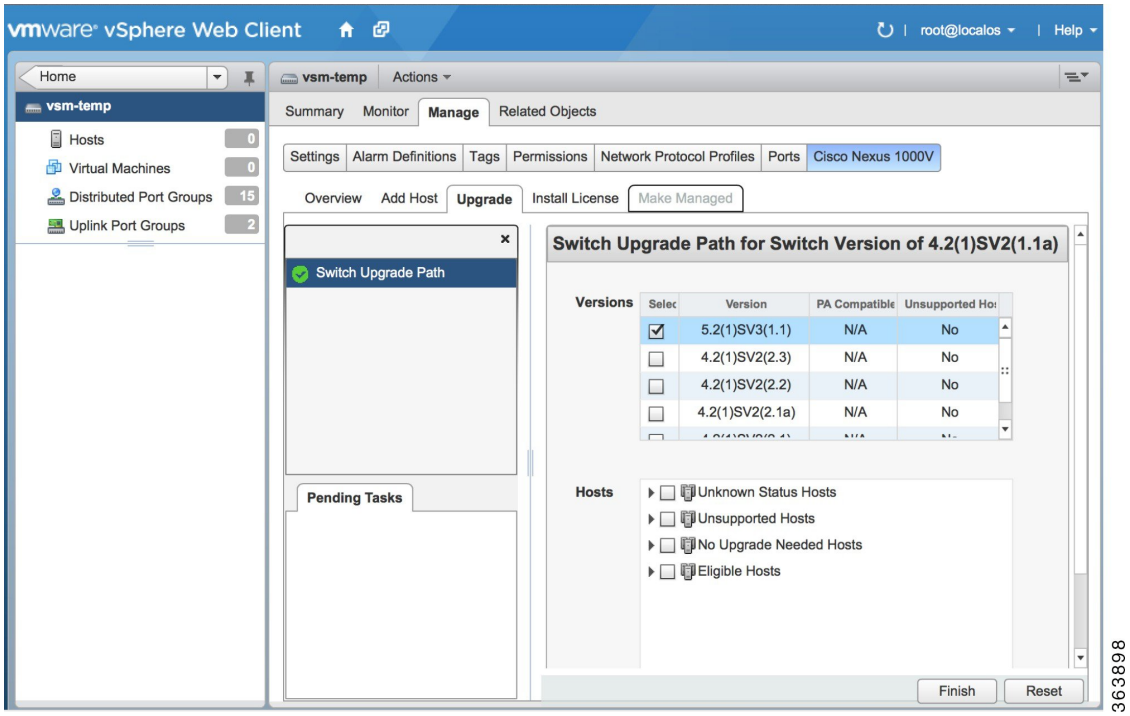
Step 6 (Optional) In the switch pane, click **Manage** > **Cisco Nexus 1000V** > **Upgrade**.

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

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

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

Figure 8: Cisco Virtual Switch Update Manager—Upgrading Cisco Nexus 1000V



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

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

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

- Unknown Status Hosts—The status of the host is in nonresponding state.
- Unsupported Hosts—The ESX version of the host is not compatible with the ESX version of the host that is associated with the Cisco Nexus 1000V version suggested for upgrade. The unsupported hosts should be upgraded

manually to the ESX versions supported by the Cisco Nexus 1000V. See the *Cisco Nexus 1000V and VMware Compatibility Information* for more information about supported ESX versions.

- No Upgrade Needed Hosts—The hosts already have the correct VEM version installed.
- Eligible Hosts—The ESX version of the host is compatible with the ESX version of the host that is associated with the Cisco Nexus 1000V version suggested for upgrade. During the upgrade process, Cisco Virtual Switch Update Manager upgrades the VEM version installed on the hosts to the specified version.

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

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

Feature History for Upgrading the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Upgrading Cisco Nexus 1000V using Cisco Virtual Switch Update Manager	Release 1.0	This feature was introduced.

CHAPTER 6

Monitoring Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager

This chapter contains the following sections:

Information about Monitoring

Cisco Virtual Switch Update Manager provides the server administrators with a view of the virtual network and visibility into the networking aspects of the Cisco Nexus 1000V.

It allows the administrators to view the configuration aspects of the VSM, export networking details from vCenter server, investigate the root cause of and prevent networking issues, and deploy the virtual machines with policies. The administrators can monitor and manage the resources effectively with the network details that are provided in the Cisco Virtual Switch Update Manager.

Cisco Virtual Switch Update Manager displays the following switch information:

- **Dashboard tab—**Displays the summary of the system, network statistics, and license information.
- **Switch tab—**Displays hosts, VMs, port groups, and VNIC and PNIC information at the switch level.
- **Hosts/VEM tab—**Displays hosts, VMs, port groups, and VNIC and PNIC information at the host level.

Note TACACS users cannot monitor the Cisco Nexus 1000V switch on the Cisco Virtual Switch Update Manager.

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

You can view the Virtual Supervisor module (VSM) and Virtual Ethernet module (VEM) details of the Cisco Nexus 1000V switch.

Step 1 Log in to VMware vSphere Web Client.

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

Note You are prompted to enter your credentials if the switch is not managed by Cisco Virtual Switch Update Manager. If the switch is managed by Cisco Virtual Switch Update Manager, you can monitor the switch automatically.

Note If you register Cisco Virtual Switch Update Manager with vCenter when the vCenter plug-in is already installed, you might not see the **Cisco Nexus 1000V** tab under Monitor. If you do not see this tab, reboot VMware vSphere Web Client.

Step 3 (Optional) You can also access the **Cisco Nexus 1000V Monitor** pane in the vSphere Client by choosing **vCenter** > **Distributed Switches**.

Step 4 (Optional) In the switch pane, choose **Monitor** > **Cisco Nexus 1000V** .

Step 5 Click **Dashboard**.

The **Dashboard** pane displays following non configurable summary of the Cisco Nexus 1000V:

Name	Description
System	
Switch Name field	The name of the switch.
NX-OS Version field	The Cisco NX-OS version and the build that the switch is using.
VSM IP field	The IP address of the Virtual Supervisor Module (VSM).
DC Name field	The name of the data center.
Connectivity Mode field	The mode of connectivity between the VSMs and the VEMs .
VC Connectivity field	The status of vCenter connectivity
VSM HA field	The Virtual Supervisor Module (VSM) high availability mode
Network Statistics	
VNICs vs Max field	The maximum number of virtual network interface cards (VNICs) that are supported and their current usage

Name	Description
Hosts vs Max field	The maximum number of server hosts that are supported and their current usage.
Port-Groups vs Max field	The maximum number of port groups that are supported and their current usage.
Veths/Host Max field	The maximum number of vEthernet ports per host that are supported and their current usage.
VLAN vs Max field	The maximum number of VLANs that are supported and their current usage.
VXLAN vs Max field	The maximum number of VXLANs that are supported and their current usage.
Licenses	The information of the license installed.
License Type field	The type of the license
Licenses Available field	The licenses that are available to use.
Licenses Used field	The licenses that are actually used.
Earliest Expiration field	The earliest expiration time of the license.
Status field	The status of the license.

Step 6 Click **Switch**.

Step 7 Click **Host/VEM**.
The **Host/VEM** pane displays the following non configurable details of the host.

Name	Description
Host Name field	The name of the host.
NX-OS Version field	The Cisco NX-OS version and the build that the host is using.
Host IP field	The IP address of the host.
License field	The license details of the host.
Host/Module field	The number of modules per host.
VMs/Host field	The number of VMs per host.

Name	Description
VNICs / Host field.	The number of VNICs per host.

Step 8 Click **VM Info**.
The **VM Info** pane displays the following non configurable details.

Name	Description
VMs field	The name of the VM.
vNICs field	The name of the vNIC associated to the VM.
Adapter field	The name of the adapter.
Status field	The status of the VM.
Port Group field	The port group associated with the VM.
VLANs field	The VLAN associated with the VM.
Host ID field	The module number of the host at VSM.

Step 9 Click **Port Groups**.
The **Port Groups** pane displays the following non configurable details.

Name	Description
Port Group field	The name of the port profile.
Type field	The type of port profile.
VLANs field	The VLANs associated with the port profile.
System VLANs field	The system VLANs associated with the port profile.
Port Max field	The maximum number of ports available.
Port Min field	The minimum number of ports available.
Port Used field	The total number of the ports used.

Step 10 Click **vNICS**.
The **vNICs** pane displays the following non configurable details.

Name	Description
vNICs field	The name of the vNIC.
VM field	The name of the VM.
Adapter field	The name of the adapter.
Status field	The status of the vNIC.
Port Group field	The port group associated with the vNICs.
VLANs field	The VLANs associated with the vNICs.
Host ID field	The module number of the host at the VSM.

Step 11 Click **Uplinks**.
The Uplinks pane displays the details of the Uplinks as described in the table below:

Name	Description
Switch Interface field	The name of the port.
Status field	The status of the uplink.
Port Channel field	The port channel associated with the uplink.
Host IDfield	The module number of the host at the VSM.
Port Group field	The port group associated with the uplink.
VLANs field	The VLANs associated with the uplink .
CDP Uplinks field	The CDP uplink information.

Step 12 Click **Hosts/VEM**.
The Systems area in the Host/VEM pane displays the details of the host as described in the table below:

Name	Description
Host Name field	The name of the host.
NX-OS Version field	The Cisco NX-OS version and the build that the host is using.
Host IP field	The IP address of the host.

Name	Description
License field	The license details of the host.
Host/Module field	The number of modules per host.
VMs/Host field	The number of VMs per host .
VNIC/Host field	The number of VNICs per host.

Step 13 Click **VM Info**.
The **VM Info** area provides the following host details:

Name	Description
VMs field	The name of VMs per host.
VNICs field	The name of the vNICs per host.
Adapter field	The name of the adapter.
Status field	The status of the host.
Port Group field	The port group associated with the VM of the host.
VLANs field	The VLANs associated with the VMs of the host.
Host ID field	The module number of the host at the VSM.

Step 14 Click **Port Groups**.
The **Port Groups** area provides the following host details:

Name	Description
Port Group field	The name of the port group.
Type field	The type of the port group.
VLAN field	The VLANs associated with the host.
System VLAN field	The system VLAN associated with the host.
Ports Max field	The maximum number of port per host.
Ports Min field	The minimum number of ports per host.
Ports Used field	The total number of ports used.

Step 15 Click **vNICS**.
The **vNICs** area provides the following host details:

Name	Description
VNICs field	The name of the VNICs associated to the host.
VMs field	The name of the VM associated to the host .
Adapter field	The name of the adapter.
Status field	The status of the vNIC associated to the host.
Ports Group field	The name of the port group associated to the host.
VLANs field	The VLANs associated with the host.
Host ID field	The module number of the host at the VSM.

Step 16 Click **Uplinks**.
The **Uplinks** area provides the following host details:

Name	Description
Switch Interface field	The name of the port.
Status field	The status of the uplink interface.
Port Channel field	The port channel associated with the uplink.
Host ID field	The module number of the host at the VSM.
Ports Group field	The name of the port group per host.
VLANs field	The VLANs associated with per host.
CDP Uplink field	The CDP Uplink information.

Feature History for Cisco Virtual Switch Update Manager Monitoring Feature

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Cisco Virtual Switch Update Manager Monitoring Feature	Release 1.0	This feature was introduced.

CHAPTER 7

Installing a License Using Cisco Virtual Switch Update Manager

This chapter contains the following sections:

Information About Installing Licenses Using Cisco Virtual Switch Update Manager

Cisco Virtual Switch Update Manager is the graphical user interface (GUI) that you can use to install and upload a license on the Virtual Supervisor Module (VSM) to mark the VSM as licensed. The Cisco Virtual Switch Update Manager GUI is an integral part of the VMware vSphere Web Client and it can only be accessed by logging into VMware vSphere Web Client.

The license file is shared by both Virtual Supervisor Modules (VSMs) in an HA pair. A license file contains the number of licenses ordered for your VSM. One license is required for each CPU socket on each VEM, but you do not need a license for the VSM itself. A VSM can have more than one license file depending on the number of CPU sockets on each VEM.

If the license checkout fails, the module is marked as unlicensed and the virtual Ethernet (vEth) interfaces that are attached to that module are not allowed to come up. For software upgrades, if the switch is still in the default licensing period, it is extended for another 60 days from the software upgrade date.

See the *Cisco Nexus 1000V Platform Multi-Hypervisor Licensing Guide* for more information about the Cisco Nexus 1000V licensing model.

Installing a License Using Cisco Virtual Switch Update Manager

You can install and upload Cisco Nexus 1000V licenses using Cisco Virtual Switch Update Manager.

Before You Begin

- You have installed Cisco Virtual Switch Update Manager.
- You have the license file accessible to Cisco Virtual Switch Update Manager.
- You have the Distributed Switch - Create and Modify privilege enabled on the VMware vSphere Distributed Switch (VDS).

Step 1 Log in to VMware vSphere Web Client.

Step 2 Choose **Home** > **Cisco Virtual Switch Update Manager** > **Configure and Manage Nexus 1000V and Application Virtual Switch**.

Step 3 Choose the datacenter and the switch that is associated in the datacenter and click **Manage**.

Step 4 In the switch pane, click **Cisco Nexus 1000V** > **Install License**. The Cisco Nexus 1000V License pane appears.

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

Step 5 (Optional) You can also access the Cisco Nexus 1000V License by choosing **vCenter** > **Distributed Switches**.

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

Step 7 Click **Copy** to copy the VSM license host ID .

Step 8 Browse to the desired location to install the license file.

Step 9 Click **Install the License** to upload the license to the VSM.
After the license is installed, you can verify the count and expiry date of the license using the Monitor functionality of the Cisco Virtual Switch Update Manager . See Monitoring the Cisco Nexus 1000V Using Cisco Virtual Switch Update Manager, on page 44

Feature History For Installing a License Using the Cisco Virtual Switch Update Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Installing a license using the Cisco Virtual Switch Update Manager	Release 1.0	This feature was introduced.

CHAPTER 8

Dashboard-Cisco Nexus 1000V

This chapter contains the following sections:

Information About the Dashboard–Cisco Nexus 1000V

The dashboard in Cisco Virtual Switch Update Manager displays the health of the Cisco Nexus 1000V switch and the hosts and the virtual machines that it manages in your datacenter. The dashboard enables you to detect errors and warnings and fix any potential issues in your datacenter.

Cisco Virtual Switch Update Manager supports the dashboard functionality from Release 4.2(1)SV2(1.1a) and later releases..

In the Dashboard–Cisco Nexus 1000V, the following conditions are classified as warnings:

- When the Cisco Nexus 1000V switch reaches 90 percent of its Virtual Ethernet module (VEM) limit.
- When the Cisco Nexus 1000V switch reaches 90 percent of its VNIC limit.
- When the secondary Virtual Supervisor module (VSM) is not operational.
- If the number of Cisco Nexus 1000V licenses available is less than 5.
- When 90 percent of the VNIC limit is used in the host.
- If the license is going to expire in 10 days.

In the Dashboard–Cisco Nexus 1000V, the following conditions are classified as errors:

- When the Cisco Nexus 1000V reaches its VEM limit.
- When the Cisco Nexus 1000V reaches its module limit.
- If the switch is not managed by Cisco Virtual Switch Update Manager
- If the version of the switch is not supported.
- If the switch is not connected to vCenter Server.

- If the switch is not reachable.
- If the number of licenses is available is zero.
- If the licenses have expired.
- If the host is not connected as a module to the VSM.
- If the VNIC limit is used on the host.
- If one or more uplinks are not connected on the host.
- If the VMK NICs are not connected on the host.
- If the VNICs are not connected on the host.

Using the Dashboard-Cisco Nexus 1000V

The **Dashboard–Cisco Nexus 1000V** pane enables you to view the inventory of the components in your datacenter which are managed by the Cisco Virtual Switch Update Manager, the status of your datacenter, and a detailed summary of the errors and warnings associated with the components in your datacenter.

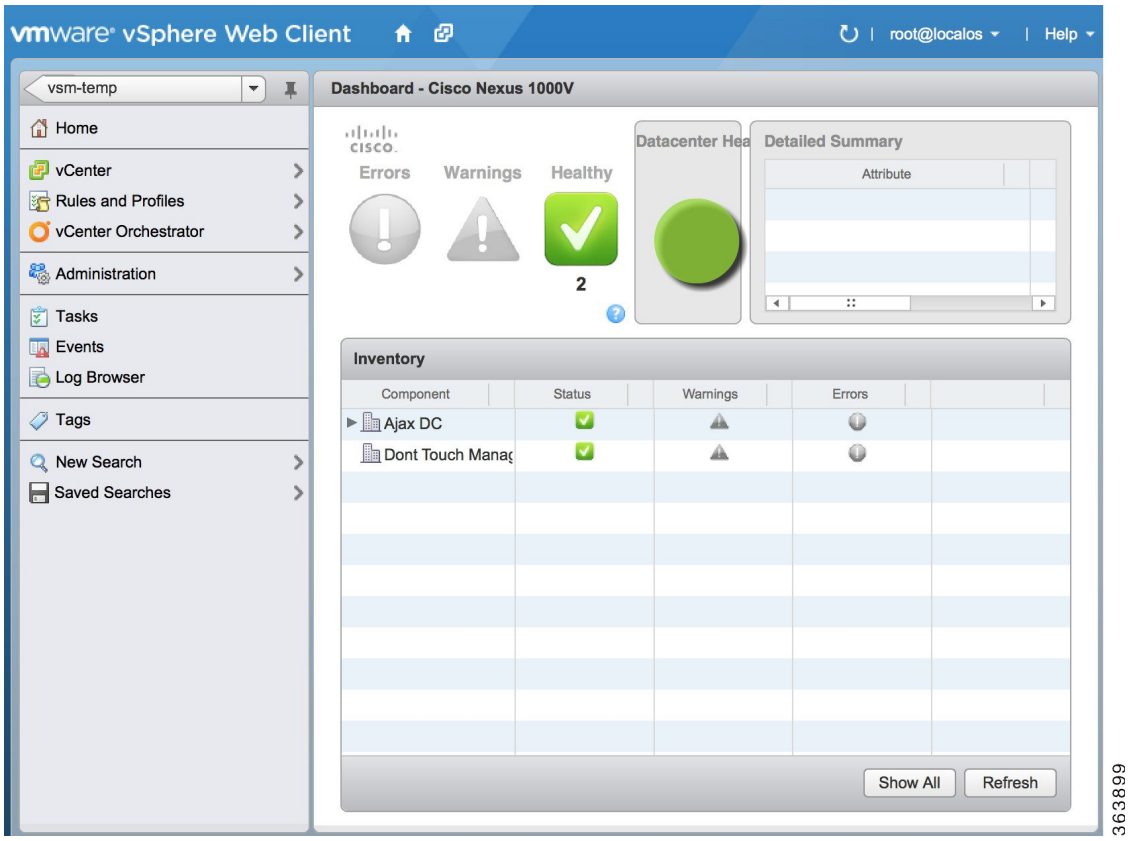
Before You Begin

- You have already installed the Cisco Virtual Switch Update Manager.
- The Cisco Nexus 1000V switch is managed by Cisco Virtual Switch Update Manager.

Step 1 Log in to the VMware vSphere Web Client .

Step 2 Choose **Home** > **Cisco Virtual Switch Update Manager** > **Dashboard – Cisco Nexus 1000V**.
The Dashboard - Cisco Nexus 1000V pane appears.

Figure 9: Dashboard–Cisco Nexus 1000V



Step 3 From the **Component** column, in the **Inventory** table, choose the data center.
You can view the following status of your datacenter in the **Status** column:

- A green icon indicates that the datacenter is healthy.
- A yellow icon indicates that there are errors associated with the components in the datacenter.
- A red icon indicates that there are warnings associated with the components in the datacenter.

See Information About the Dashboard–Cisco Nexus 1000V, on page 53 for information about the conditions that are classified as errors or warnings.

Step 4 From the **Component** drop-down list, choose the component in your datacenter.
In the **Detailed Summary** window, you can view the summary of the component such as the component type, component state, errors, or warnings that are associated with the component.

Step 5 Click **Refresh** to refresh the data.

Feature History For Dashboard–Cisco Nexus 1000V

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Dashboard–Cisco Nexus 1000V	Release 1.0	This feature was introduced.