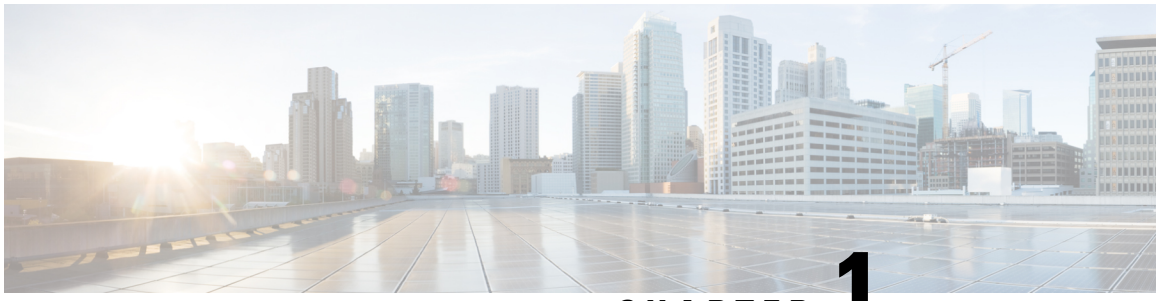
Cisco Nexus 1000VE Installation and Upgrade Guide, Release 5.2(1)SV5(1.3)

First Published: 2019-12-19

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



CHAPTER 1

Overview

This chapter contains the following sections:

About Cisco Nexus 1000VE

The Cisco Nexus 1000VE 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 1000VE is compatible with any upstream physical access layer switch that is compliant with the Ethernet standard, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000VE 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 ESXi host software.

About Virtual Supervisor Module

The Virtual Supervisor Module (VSM) is the control plane of the Cisco Nexus 1000VE. 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 VSE collectively represent the Cisco Nexus 1000VE. Cisco VSE is a module that switches data traffic.

The VSM, along with the VSEs that it controls, performs the following functions for the Cisco Nexus 1000VE system:

- Configuration

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

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

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

A single VSM can control up to 64 VSEs.

While using the VSG, it can control up to 32 VSES.

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

About Virtual Service Engine

A VSE is deployed for each hypervisor instance and it performs 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 VSE can be installed on an ESXi host at any time.

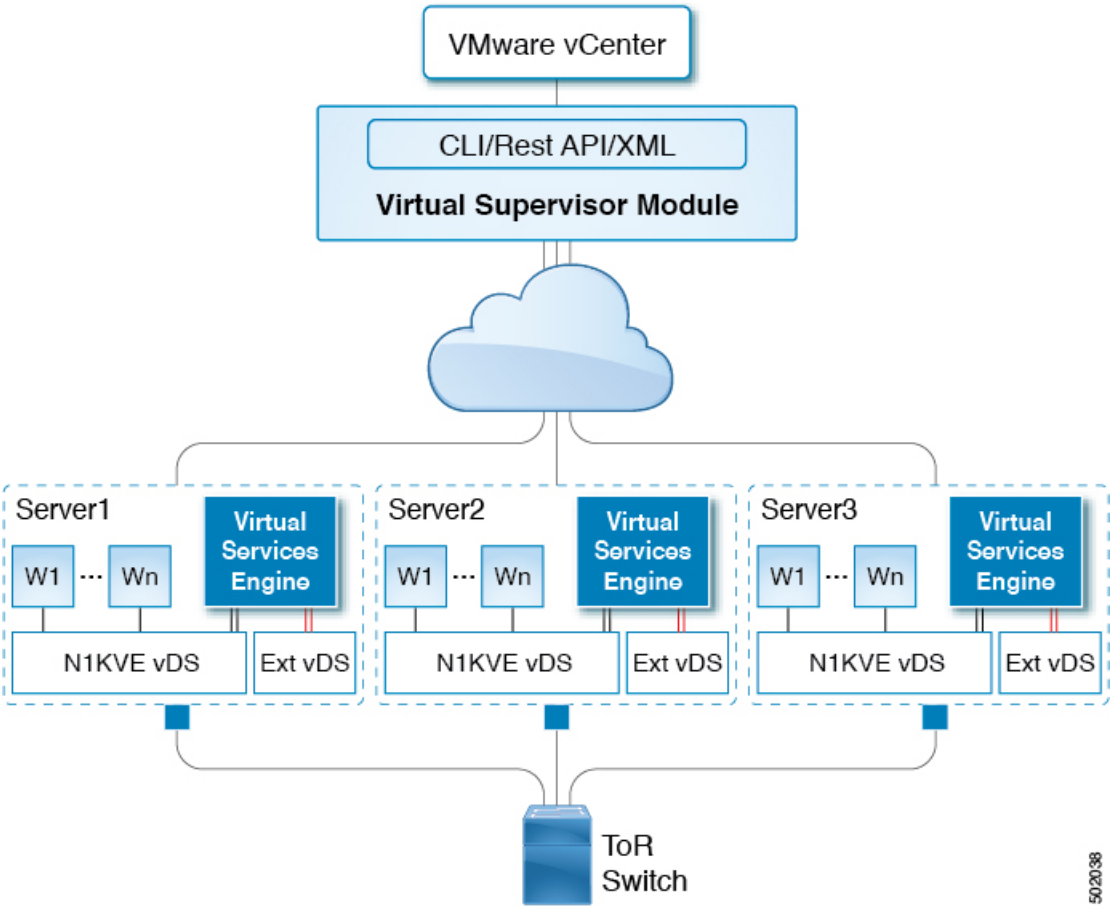
Note Cisco Nexus 1000VE VSE does not support ESXi custom TCP/IP stack and control traffic through the custom TCP/IP stack.

In the Cisco Nexus 1000VE, the traffic is switched between VMs locally at each VSE instance. Each VSE 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 VSE accordingly, but it never forwards packets.

In the Cisco Nexus 1000VE, the module slots 1 is for the primary VSM and module slot 2 is for the secondary VSM. Either module can act as active or standby. The first server or host is automatically assigned to module 3. The ports to which the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000VE where they are assigned with a global number.

The Cisco Nexus 1000VE architecture is shown in the following figure.

Figure 1: Cisco Nexus 1000VE Architecture



About VSM-to-VSE Communication

The VSM and the VSE can communicate over a Layer 3 network. These configurations are referred to as Layer 3 control modes.

Layer 3 Control Mode

Layer 3 control mode is the preferred method of communication between the VSM and the VSEs. In Layer 3 control mode, the VSEs can be in a different subnet than the VSM and from each other. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs.

Note You can configure IPv4 as transport mode for communication between VSE and VSM.

For more information about Layer 3 control mode, see the "Configuring the Domain" chapter in the *Cisco Nexus 1000VE System Management Configuration Guide*.

Installation Overview

Information About Installing the Cisco Nexus 1000VE Manually

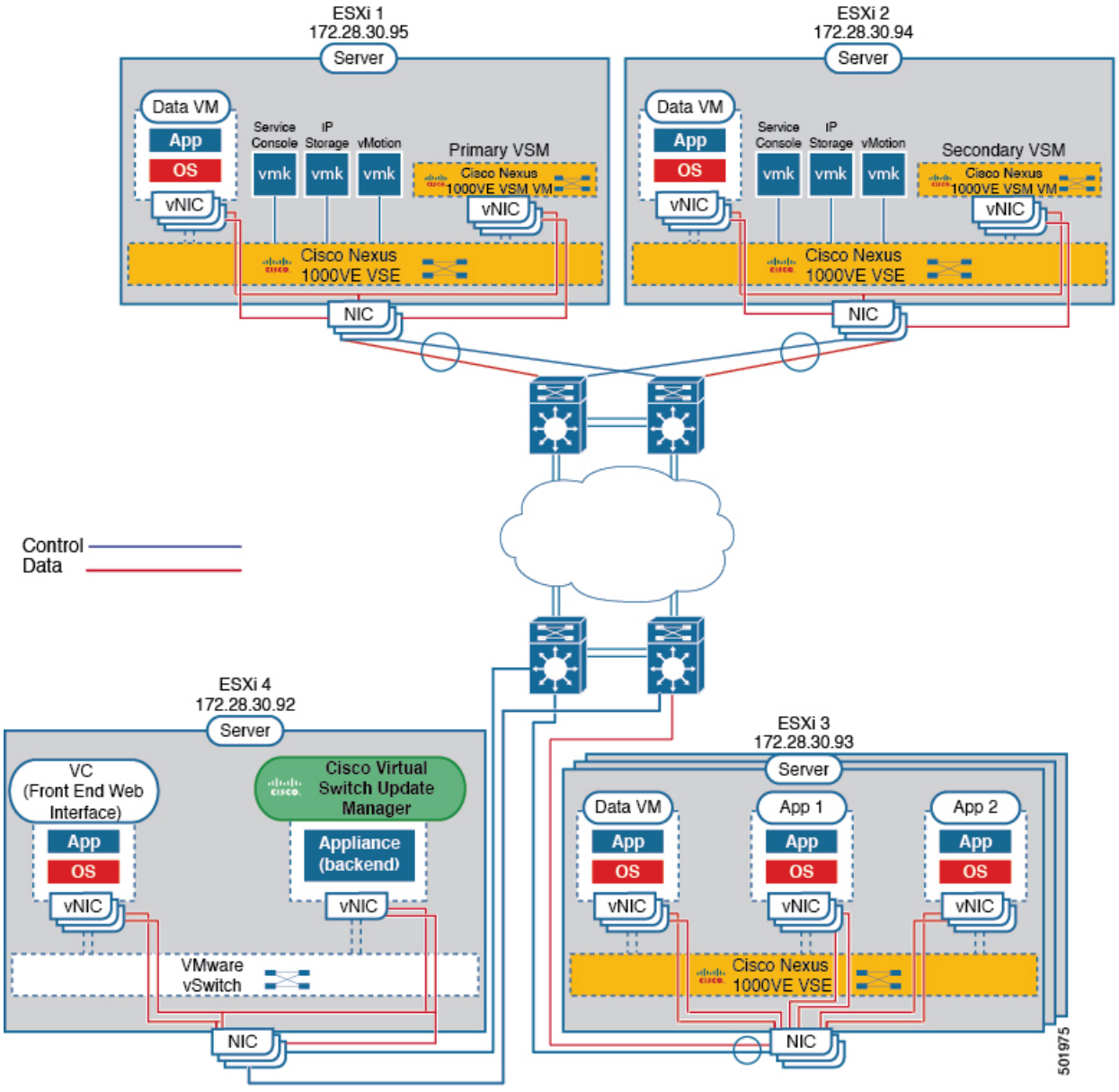
When you install the Cisco Nexus 1000VE manually, you download and install all of the necessary software. This installation method gives you the option of deploying Layer 3 connectivity between the VSM and VSEs. Layer 3 connectivity is the preferred method. For an example of the Layer 3 installation topology, see Topology for Layer 3 Control Mode, on page 4.

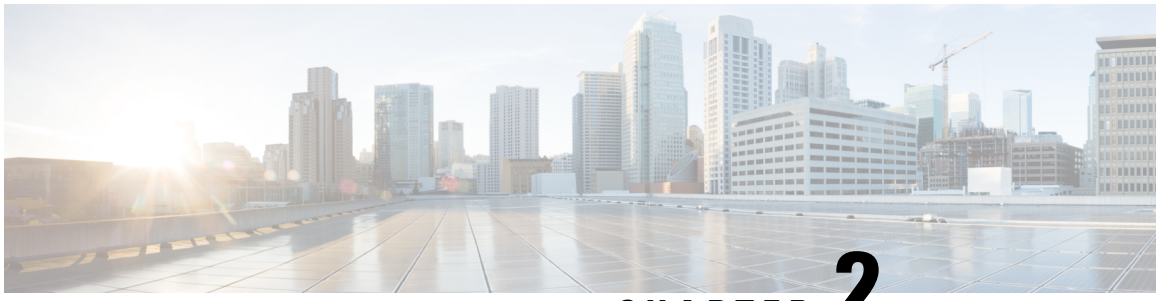
Recommended Topologies

Topology for Layer 3 Control Mode

Layer 3 control mode is the preferred method of communication between the VSM and VSEs. You can configure IPv4 addressing for Layer 3 control mode. This figure shows an example of a Layer 3 control mode topology (using IPv4 addressing) where redundant VSM VMs are installed. 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 Control Mode Topology Diagram





CHAPTER 2

Installing the Cisco Nexus 1000VE Software

This chapter contains the following sections:

Supported VMware vSphere ESXi Hypervisor Versions

Cisco Nexus 1000VE supports the following VMware vSphere ESXi Hypervisor version:

- 6.5U2 and later

Prerequisites for Installing the Cisco Nexus 1000VE

Prerequisites for Installing Nexus 1000 Virtual Edge (VE)

Cisco Nexus 1000 Virtual Edge installation have the following prerequisites:

- You have downloaded the Cisco Nexus 1000VE VSM and VSE images.
- You should have the VMware vCenter details and the administrator credentials.
- You have ESXi host to deploy the Cisco Nexus 1000VE VSM.
- At least one ESXi host is available to deploy VSE for Cisco Nexus 1000VE
- You have at least two IP addresses available for VSM and VSE (Virtual Services Engine).
- You have (N+1) IP addresses, where N is the number of ESXi hosts on which VSE is deployed.

ESXi Host Prerequisites

ESX or ESXi hosts have the following prerequisites:

- You have already installed and prepared vCenter Server for host management using the instructions from VMware.
- You have already installed the VMware Enterprise Plus license on the hosts.
- All VSE hosts must be running ESXi 6.5U2 or later releases.
- You have two physical NICs on each host for redundancy. Deployment is also possible with one physical NIC.
- If you are using a set of switches, make sure that the interswitch trunk links carry all relevant VLANs. The uplink should be a trunk port that carries all VLANs that are configured on the host.
- You must configure control and management VLANs on the host to be used for the VSM VM.
- Make sure that the VM to be used for the VSM meets the minimum requirements listed in the following table.
- All the vmnics should have the same configuration upstream.

⚠

Caution

- VSM hardware version 11 is not supported. See table below for supported versions.
- The VSM VM might fail to boot if RAM and CPU are not properly allocated. This document includes procedures for allocating RAM and setting the CPU speed.

This table lists the minimum requirements for hosting a VSM.

Table 1: Minimum Requirements for a VM Hosting a VSM

VSM VM Component	Minimum Requirement
VSM Hardware Version	7 **Note** VSM hardware versions 7, 8, 9, and 10 are supported. VSM hardware version 11 is not supported.
Platform	64 bit
Type	Other 64-bit Linux (recommended)
Processor	2
RAM (configured and reserved)	4 GB[1]
NIC	3
SCSI Hard Disk	3 GB with LSI Logic Parallel adapter
CPU speed	2048 MHz[2]

[1] If you are installing the VSM using an OVA file, the correct RAM setting is made automatically during the installation of this file. If you are using the CD ISO image, see Deploying Virtual Supervisor Module, on page 13 to reserve RAM and set the memory size.

[2] If you are installing the VSM using an OVA file, the correct CPU speed setting is made automatically during the installation. If you are using the CD ISO image, see Deploying Virtual Supervisor Module, on page 13 to reserve CPU and set the CPU reservation.

VSM Prerequisites

The Cisco Nexus 1000VE VSM software has the following are prerequisites:

- You have the VSM IP address.
- You have installed the appropriate VMware vCenter Server.
- If you are installing redundant VSMs, make sure that you first install and set up the software on the primary VSM before installing and setting up the software on the secondary VSM.
- If you are using the OVA file for installation, make sure that the CPU speed is 2048 MHz or greater. If the CPU speed is less than 2048 MHz, then use ISO image for installation.
- You have already identified the HA role for this VSM from the list in the following table.

Note You can provision VSM VM on a Cisco CSP 2100 or Cisco Nexus 1110 appliance also.

Table 2: HA Roles

HA Role	Single Supervisor System	Dual Supervisor System
Standalone (test environment only)	X	
HA		X

Note A standalone VSM is not supported in a production environment.

- You are familiar with the Cisco Nexus 1000VE topology diagram that is shown in Topology for Layer 3 Control Mode, on page 4.

VSE Prerequisites

The Cisco Nexus 1000VE VSE software has the following prerequisites:

- If the hosts are in ESXi stateless mode, enable the PXE booted ESXi host settings under **Home** > **Update Manager** > **Configuration** > **ESXi host/cluster**.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VSE software file.

- The ESXi server is capable of hosting VSE that reserves two vCPUs and 8 GB of memory.

Upstream Switch Prerequisites

The upstream switch from the Cisco Nexus 1000VE has the following prerequisites:

- If you are using a set of switches, make sure that the interswitch trunk links carry all relevant VLANs. The uplink must be a trunk port that carries all the VLANs that are configured on the host.
- The following spanning tree prerequisites apply to the upstream switch from the Cisco Nexus 1000VE on the ports that are connected to the VSE.
  - On upstream switches, the following configuration is mandatory:

    On your Catalyst series switches with Cisco IOS software, enter the **spanning-tree portfast trunk** or **spanning-tree portfast edge trunk** command.
  - On upstream switches we highly recommend that you enable Global BPDU Filtering and Global BPDU Guard globally.
  - On upstream switches, where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the **spanning-tree bpdu filter** and **spanning-tree bpdu guard**commands.

  For more information about spanning tree and its supporting commands, see the documentation for your upstream switch.
- Enter the following commands on the upstream switch:

```
show running interface interface number
interface GigabitEthernet interface number
 description description of interface
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN native VLAN
switchport trunk allowed vlan list of VLANs
switchport mode trunk

end
```

Guidelines and Limitations for Installing the Cisco Nexus 1000VE

The Cisco Nexus 1000VE software installation has the following configuration guidelines and limitations:

- Virtual machine hardware version 11 is not supported.
- Do not enable VMware fault tolerance (FT) for the VSM VM because it is not supported. Instead, Cisco NX-OS HA provides high availability for the VSM.
- The VSM VM supports VMware HA. However, we strongly recommend that you deploy redundant VSMs and configure Cisco NX-OS HA between them. Use the VMware recommendations for the VMware HA.
- Do not enable VM monitoring for the VSM VM because it is not supported, even if you enable the VMware HA on the underlying host. Cisco NX-OS redundancy is the preferred method.

- Deploying VSMs on the Cisco Nexus 1000VE DVS is not recommended. Please deploy on VMware vSwitch or vDS.

  The VSM reboot is based on the following conditions:

  1. The number of modules attached to the VSM
     - If more modules are attached on one of the VSMs and there is no virtual channel (VC) connectivity on both VSMs, the VSM that has the smaller number of modules is rebooted.
     - If modules are attached to both VSMs and one of the VSMs 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, the software makes a selection that is based on the VC connectivity status.

       For example, this action is taken if both VSMs have two modules attached or both VSMs have no modules attached.
  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.

- To improve redundancy, install primary and secondary VSM VMs on separate hosts that are connected to different upstream switches.
- The Cisco Nexus 1000VE VSM always uses the following three network interfaces in the same order as specified below:
  1. Control Interface
  2. Management Interface
  3. Packet Interface
- We recommend that you deploy the VMware vCenter server and VSM in the same physical data center. If you choose to deploy the vCenter server and VSM in different physical data centers, be aware of the following guidelines and limitations:

- The VSM HA pair must be located in the same site as their storage and the active vCenter Server.
- Quality of Service bandwidth guarantees for control traffic over the DCI link.
- Limit the number of physical data centers to two.
- A maximum latency of 10 ms is supported for VSM-VSM control traffic when deployed across datacenters.
- A maximum latency of 100 ms is supported for VSM-VSE control traffic.
- Support for deployments where vCenter and VSM are in different data centers, provided the number of hosts does not exceed 35 and the link latency does not exceed 200 ms. In these types of deployments, we recommend that you do not edit port profiles when the VSM and the vCenter are disconnected.

- We recommend that you monitor and install all the relevant patch applications from VMware ESX host server.
- The ESXi host maintenance events are not managed by the Cisco Nexus1000VE VSM and VSE modules. During the maintenance process, the system/network administrators must manually power-off/on the VMs that belong to Cisco Nexus1000VE switches.
- We recommend to configure vmknics for management, NFS/iSCSI and vMotion on external VDS instead of Nexus1000VE VDS.

Information Required for Installation

Before installing the software, make topology decisions and gather any necessary information, as follows:

- Decide whether to deploy the VSM as a VM on a vSphere host or cluster or on a CSP.
- Decide whether the management and Layer 3 control ports will be unified or separate.
- Determine the domain ID.
- Determine the management, subnet, and gateway IP addresses for the VSM.
- Determine the administrative password for the VSM and VSEs.

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

- openssl
- base64

Before you install the Nexus1000v.5.2.1.SV5.1.3.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.5.2.1.SV5.1.3.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:

Procedure

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

- Nexus1000v.5.2.1.SV5.1.3.zip

  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

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

```
Authenticity of Cisco-signed image Nexus1000v.5.2.1.SV5.1.3.zip has been successfully
verified!
```

Installing the Cisco Nexus 1000VE Software Using ISO or OVA Files

Deploying Virtual Supervisor Module

Before you begin

- Know the location and image name of the installation image you require for the installation.
- You have already read the Prerequisites for Installing the Cisco Nexus 1000VE, on page 7.
- The VSM VM requires the following and this procedure includes steps for updating these properties:
  - We recommend 4 Gigabyte of RAM reserved and allocated.
  - We recommend 2048 MHz of CPU speed.

Procedure

Step 1 Log into VMware vCenter server.

Step 2 Right click the Host to deploy the VSM OVA and select **Deploy OVF Template** option from the pop-up menu.

Note OVA deployment fails with VMware vCenter Webclient version 6.5 U2 if there are 4000 port groups created on VDS. Use power CLI or vCenter API to install OVA files.

Step 3 In the **Deploy OVF Template** window complete the following steps:

a) In the **Select Template** page, select **Local file** option and click **Browse** to navigate to the location of the VSM OVA. Select the applicable VSM OVF file and click **Ok**. Click **Next** to continue.

b) In the **Select name and location** page, enter a name for VSM in the **Name** text field and click **Browse** tab to navigate to select the datacenter to deploy the VSM.

c) Click **Next**.

d) In the **Select a resource** page, click **Browse** tab and select the ESXi host to deploy the VSM. Click **Next** to continue.

e) In the **Review details** page, verify the OVA details and click **Next** to continue.

f) In the **Accept license agreements** page, click **Accept** and then click **Next** to continue.

g) In the **Select configuration** page, from the **Configuration** drop-down menu select **Nexus 1000v Installer** and click **Next** to continue.

Note You can select **Manually configure Nexus 1000v** from the **Configuration** drop-down list and configure the parameters from the VSM boot prompt.

h) In the **Select storage** page, select the storage to be used and click **Next** to continue.

i) In the **Select networks** page, select the networks to use for Management destination Networks. Click **Next** to continue.

j) In the **Customize template** page, do the following

1. In the **Enter the Domain Id** text field, enter Domain ID for the VSM.

   Note Cisco N1KVE domain ID should be different from N1KV VSM Domain ID.

2. In the **Enter password** and **Confirm password** fields, enter the password for the VSM.

3. Click **Show Next** and enter Management IP Address, Management IP Subnet Mask, and Management IP Gateway. Click **Next** to continue.

k) In the **Ready to complete** page, verify all the details and click **Finish** to start VSM deployment.

Power on the VSM after the VSM deployment is complete. Connect to VSM using SSH to continue further configuration.

Configuring VSM Switch Name

To change the VSM switch name, use the switchname command. For example:

```
switch#
switch# conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# switchname N1KV-NG
N1KV-NG(config)# exit
N1KV-NG# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
N1KV-NG#
```

Creating VDS in VMware vCenter

To create Nexus 1000VE VDS in the VMware vCenter, run the following commands from VSM. For example:

```
N1KV-NG# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N1KV-NG(config)# svs connection vcenter65   // SVS Connection Name
N1KV-NG(config-svs-conn)# remote ip address 10.29.176.180 // vCenter IP Address
N1KV-NG(config-svs-conn)# vmware dvs datacenter-name TME-POD2 // Datacenter Name
N1KV-NG(config-svs-conn)# protocol vmware-vim
N1KV-NG(config-svs-conn)# register-plugin remote username administrator@vsphere.local
password Cisco123@ // vCenter administrator credentials
N1KV-NG(config-svs-conn)# connect
N1KV-NG(config-svs-conn)# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
N1KV-NG(config-svs-conn)# exit
N1KV-NG(config-svs)
```

Note The **connect** command may return the following message, `SVS connection service is busy. Please try again later.`

Note The VDS is deployed and managed by the VSM.

A VDS is created in the vCenter with the specified name and inside-trunk port group and internal port group are created. The VDS does not have any physical NICs associated with it. All the traffic from the VM's within this VDS is sent through the VSE and to the Outside trunk.

Configuring Promiscuous Mode for the Port Group

To configure promiscuous mode for the outside trunk port group, complete the following steps:

Procedure

Step 1 Right click the port group and select Edit Settings option from the pop-up menu.

Step 2 In the Outside trunk Edit Settings window, click Security.

Step 3 3. In the Security page, do the following:.

a) Promiscuous Mode: Select Accept
b) MAC address changes: Leave as default
c) Forged transmits: Select Accept.

d) Click Ok to complete the promiscuous mode configuration for port group.

Creating VLANs on VSM

Use the **vlan** command to create required VLANs on the VSM. For example:

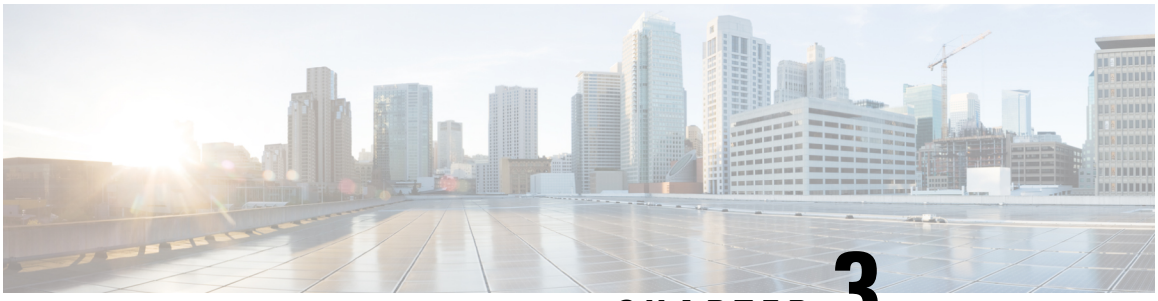
```
N1KV-NG# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N1KV-NG(config)# vlan 300-350
N1KV-NG(config-vlan)# no shut
N1KV-NG(config-vlan)# exit
N1KV-NG(config)#
```

Creating vEthernet Port Group for the Workload VMs

You need to create vEthernet port groups for the workload VMs. Use the **port-profile type vethernet** command to create vEthernet port groups. For example:

```
N1KV-NG(config)# port-profile type vethernet app-300
N1KV-NG(config-port-prof)# switchport mode access
N1KV-NG(config-port-prof)# switchport access vlan 300
N1KV-NG(config-port-prof)# no shut
N1KV-NG(config-port-prof)# state enabled
N1KV-NG(config-port-prof)# vmware port-group
N1KV-NG(config-port-prof)# end
N1KV-NG#
N1KV-NG(config)# port-profile type vethernet db-301
N1KV-NG(config-port-prof)# switchport mode access
N1KV-NG(config-port-prof)# switchport access vlan 301
N1KV-NG(config-port-prof)# no shut
N1KV-NG(config-port-prof)# state enabled
N1KV-NG(config-port-prof)# vmware port-group
N1KV-NG(config-port-prof)# end
N1KV-NG#
Save the configuration by running copy r s
N1KV-NG# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
N1KV-NG#
```

Note The port-profiles created on VSM are available on the N1KVE-VDS. These can be assigned to workload VMs.



CHAPTER 3

VSE Deployment Using Cisco Nexus 1000VE Manager vCenter Plugin

This chapter contains the following sections:

Cisco Nexus 1000VE Manager vCenter Plugin Software Requirements

This section lists Cisco Nexus 1000VE Manager vCenter plugin software requirements.

Note Cisco Nexus 1000VE Manager vCenter Plugin is Flex based on vCenter versions 6.0, 6.5, and 6.7U1, and HTML5 based plugin for vCenter version 6.5U2 and above.

Table 3: Cisco Nexus 1000VE Manager VCenter Plugin Software Requirements

Platform	Recommended Release
VMware vCenter	• 6.5 U2 Linux Appliance • 6.5 U2 Windows • 6.7 U1 Linux Appliance • 6.7 U1 Windows • 6.7 U2 Linux Appliance • 6.7 U2 Windows • 6.7 U3 Linux Appliance • 6.7 U3 Windows
Cisco Nexus 1000VE VSM	5.2(1)SV5(1.3)

Installing the Cisco Nexus 1000VE Manager vCenter Plugin

This section describes how to install the Cisco Nexus 1000VE vCenter Plugin. Ensure that you have HTTPS connection between the vCenter and Cisco Nexus 1000VE VSM to download the plugin directly from the VSM.

If you cannot establish HTTPS connection between vCenter and Cisco Nexus 1000VE VSM, you can use alternate method of hosting the Cisco Nexus 1000VE vCenter Plugin zip file to a Web Server. You need to download the plugin zip from Cisco Nexus 1000VE VSM available at `https://<N1KVE-VSM-IP>/` and place it on the Web Server path accessible through HTTPS. There are two plugins, that is Flex based (supported on vCenter 6.0/6.5/6.7U1) and HTML5 based (supported on vCenter 6.5U2 or above). You must download the corresponding plugin according to currently installed vCenter version.

Before you begin, note the following:

- Ensure that you have Python environment (version 3.7.0 or greater) in your network.
- Ensure that you have copied the deploy_n1kve_plugin_v3.py script to a python environment where pyvmomi package is installed.

You can use one of the following two methods to install the Cisco Nexus 1000VE vCenter Plugin:.

- Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 1 , on page 19
- Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2, on page 20

Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 1

Procedure

Step 1 Download the deploy_n1kve_plugin_v3.py python script from `https://<N1KVE-VSM-IP>/` to the Python environment.

Example:

Step 2 Run the Python script, deploy_n1kve_plugin_v3.py, to register the N1KVE Manager vCenter plugin and enter the following details when prompted:

- vCenter IP: IP address of the VMware vCenter server to install the plugin.
- vCenter Username: User with administrator privileges.
- Password: password.
- Plugin zip file URL: URL where the vCenter downloads the plugin. There are two zip files corresponding Flex(6.0/6.5/6.7) and for HTML for vCenter (6.5u2 or above). Please provide respective file path depending upon your vCenter version and preference.
  - If vCenter can reach Cisco Nexus 1000VE VSM over HTTP/HTTPS, then provide the URL similar to `http://N1KVE-VSM-IP/vcplugin/n1kve-vcenter-plugin-flex-1.0.3.zip` for flex based vSphere client or `http://N1KVE-VSM-IP/vcplugin/n1kve-vcenter-plugin-html-2.0.1.zip` for HTML5 based vSphere client (Supported for vCenter v6.5u2 or above).
  - If the Zip file is placed in any other webserver, then provide the URL for the same. For example, `http://WEB-SERVER-IP/Relative-path-if-any-to-Zip-file/n1kve-vcenter-plugin-flex-1.0.3.zip` for flex based vSphere client OR `http://WEB-SERVER-IP/Relative-path-if-any-to-Zip-file/n1kve-vcenter-plugin-html-2.0.1.zip` for HTML based vSphere client.
  - If the Zip file is placed in any other webserver, then provide the URL for the same `https://<WEB-SERVER-IP>/<Relative-path-if-any-to-Zip-file>/n1kve-vcenter6.X-plugin-1.0.2.zip`

  Note Ensure you have not renamed the .zip file.

- HTTPS Server Thumbprint(fingerprint): If you are using HTTPS, enter the HTTPS SHA1 Thumbprint from the Web Server else leave this field empty. For more information about how to retrieve HTTPS SHA1 Thumbprint, see Retrieving HTTPS SHA1 Thumbprint.

```
C:\>python deploy_n1kve_plugin_v3.py

================================================================
.:|:.:|:. Cisco Systems Inc
================================================================
N1KVE Plugin for the vSphere Web Client deployment tool
----------------------------------------------------------------
NOTE: Please go through the DeployPlugin-ReadMe.txt file on your VSM and ensure that all
the pre-requisites are taken care of.

In order to install the N1KVE Plugin for the vSphere Web Client,
the following wizard will prompt you the following information:

- vCenter IP : The IP address of the vCenter where the plugin needs to be installed.
```

```
- vCenter Username / password : SSO login credentials
- vCenter Username / password : The login information of a user with root privileges
- Plugin version number : The version of the plugin to deploy
- Plugin zip file URL : The URL where the vCenter will be able to download the N1KVE Plugin
 zip archive (HTTP or HTTPS).
- Https server Thumbprint: The SHA thumbprint of the HTTPS server where the zip archive is
 located

vCenter IP: 10.126.129.75
vCenter Username: administrator@vsphere.local
Password:
Plugin zip file URL: http://10.126.129.100/vcplugin/n1kve-vcenter-plugin-html-2.0.1.zip
Select one of the following:-
1. Windows VCenter
2. VCenter Server Appliance
Enter 1 or 2
Choice: 1
Administrator password:
Successful connection to 10.126.129.75
Connecting to the vCenter 10.126.129.75...
Fetching service instance content ...
Checking the API version ...
Checking if any version of HTML plugin is already present ...
Installing the plugin ...

The plugin information was successfully installed on the vCenter 10.126.129.75


--- Please Read ---
The information provided was successfully pushed to the vCenter, but plugin installation
is not over.
You need to login into the vSphere Web Client and check for the Cisco N1KVE Plugin icon to
 ensure that the installation is successful
If the plugin does not appear in the UI, check the vSphere Web Client log file to see what
 went wrong
Checking if all files were installed successfully...
Pushing files to the VCenter. Please wait for sometime...
It is considered that all VCenter related files are installed in C drive...

Please restart vmon service from the task manager
```

Step 3 Log into the vSphere Web Client after the registration process completes. If you were logged into vSphere Web Client before the script was run, logout and login again back. For Flex based vSphere clients, the plugin appears as theCisco Nexus 1000VE Manager icon and is added under the **Operations and Policies** section on the **Home** tab. For HTML5 based vSphere clients, the plugin appears as The Cisco Nexus 1000VE Manager icon and is added under **Main Menu** > **Shortcuts**.

Note First login to VMware vSphere Web Client may take longer because the vCenter downloads and deploys the plugin from the Web Server.

Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2

Procedure

Step 1 Log into VMware vCenter Managed Object Browser (MOB).

Step 2 Click **Content** under the **Properties** section.

Step 3 Click **Extension Manger**.

Step 4 Under **Methods**, click **RegisterExtensions** to open **Register Extension Pop-up**.

Step 5 Copy the following information by changing the version, URL, serverThumbprint tags according to your setup and then paste it in the **Value** Text field:

uu

- For Flex based vSphere clients, use following extension key:

```
<extension>
   <description>
      <label>N1KVE Plugin</label>
      <summary>Deployment for the N1KVE plugin</summary>
   </description>
   <key>com.cisco.plugin.n1kveui</key>
   <company>Cisco Systems Inc.</company>
   <version>1.0.3</version>
   <server>
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter-plugin-flex-1.0.3.zip</url>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
      <adminEmail>string</adminEmail>

<serverThumbprint>6c:47:83:8f:18:e2:a6:12:c7:f1:ce:ac:72:e2:6c:c9:a2:b5:70:05</serverThumbprint>

   </server>
   <client>
      <version>1.0.3</version>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.3.zip</url>
   </client>
   <lastHeartbeatTime>2019-05-16T00:00:00Z</lastHeartbeatTime>
   <shownInSolutionManager>false</shownInSolutionManager>
</extension>
```

- For HTML based vSphere clients use following extension key:

```
<extension>
   <description>
      <label>N1KVE Plugin</label>
      <summary>Deployment for the N1KVE plugin</summary>
   </description>
   <key>com.cisco.n1kve.plugin</key>
   <company>Cisco Systems Inc.</company>
   <version>2.0.1</version>
   <server>
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter-plugin-html-2.0.1.zip</url>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
```

```
      <adminEmail>string</adminEmail>

<serverThumbprint>3D:E7:9A:85:01:A9:76:DD:AC:5D:83:1C:0E:E0:3C:F6:E6:2F:A9:97</serverThumbprint>

   </server>
   <client>
      <version>2.0.1</version>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter-plugin-html-2.0.1.zip</url>
   </client>
   <lastHeartbeatTime>2018-01-10T00:00:00Z</lastHeartbeatTime>
   <shownInSolutionManager>false</shownInSolutionManager>
</extension>
```

Step 6 Click **Invoke method** to register the plugin with the VMware vCenter. You must log out and logi again into the VMware vCenter inorder to apply the changes.

Step 7 Logout from VMware vCenter and login again into VMware vCenter. The plugin tool initiates automatically.

Retrieving HTTPS SHA1 Thumbprint

You need HTTPS SHA1 Thumbprint for secured communication between vCenter and VSM.

Using Firefox to Retrieve HTTPS SHA1 Thumbprint

Follow these intruction so retreive HTTPS SHA1 Thumbprint using Firefox:

1. Open the following URL in the Web browser: `https://<N1KVE-VSM-IP>/`.
2. Click the **Lock** icon on the address bar.
3. Click on the arrow on the right, and click on **More Information**.
4. Click **View Certificate** button in the **Page Info** dialog-box.
5. Copy the content of the **SHA1 Fingerprint** field on the **Certificate Viewer** dialog-box

Using Google Chrome to Retrieve HTTPS SHA1 Thumbprint

Follow these intruction so retreive HTTPS SHA1 Thumbprint using Google Chrome:

1. Open the following URL in the Web browser: `https://<N1KVE-VSM-IP>/`.
2. Click the **Lock** icon on the address bar or the Not Secure icon besides the URL.
3. Click **Certificate** in the drop-down list.
4. Scroll down to the Thumbprint Field and copy the content.
5. Click the **Details** tab in the pop-up window.

Installing VSE Using the Cisco Nexus 1000VE Manager vCenter Plugin

Complete these steps to install VSE using Ciso Nexus 1000VE Manager vCenter plugin. You can also use the migrate option avialble on the Nexus 1000VE Manager vCenter plugin to install VSEs and to migrate the configuration from all existing Nexus 1000V instances.

Note The installation procedure is the same for the Flex and HTML based plugins.

Before you begin

- Ensure that you have configured a static IP pool or a DHCP server in the VMware vCenter. If both, a static IP pool and a DHCP server are configured, static IP pool is considered.You must make sure that the IP pool contains enough number of IP addresses to assign to all VSEs. If none are selected or no network profiles are mapped, then the DHCP server is used.
- Ensure that VSM is already deployed.
- The network IP address pool for the VSE must be configured with a maximum of one DNS server IP address.

Procedure

Step 1 Navigate to **Home** on VMware vCenter Web Client. If a content library has already been created with the required VSE image, go to Step 6. If not, proceed to step 2.

Step 2 On the **Navigator** Pane, click **Content Libraries** to open the **Content Libraries** page. For some HTML based vCenter client versions where the content libraries are not supported, use Flex based vCenter client to import the same.

Step 3 On the **Getting Started** tab, click **Create new content library**.

Step 4 In the **New Content Library** dialog box, do the following:

a) On the **Name and Location** page, enter the content library name in the **Name** text field and select vCenter Server IP address from the **vCenter Server** drop-down list
b) Click **Next**.
c) On the **Configure content library** page, verify that the default option, **Local content library** is selected
d) Click **Next**.
e) On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.
f) Click **Next**.
g) On the **Ready to complete** page, click **Finish**.
h) On the **Navigator** tab, select the new content library that you just created
i) On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box

j) Choose **Local file** option and click **Browse** and navigate to the location of the VSE OVF file. Select the VSE OVF file and click **Open**.
k) In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.
l) On the **Select referenced files** dialog box, click **Ok**.
m) On the **New Content Library – Import Library Item** dialog-box, click **Ok**.
n) On the **Home** page, click **Recent Tasks** tab at the bottom to check VSE file upload progress.

Step 5 Navigate to **Home** tab on VMware vSphere Web Client.

Step 6 Click **N1KVE Manager**, and enter the VMware vCenter password and click **Login**. The N1KVE Manager page opens.

Step 7 On the **Installation** tab, select a data center from the **Select a DC** drop-down list.

Step 8 Select a N1KVE vDS from the **Select a VDS** drop-down list to list the available Hosts.

Step 9 Select the check-box for a Host from the list of Hosts and click Physical Adapter icon to open **Select PNICS for Outside VDS** dialog-box

Step 10 In the **Select PNICSs for OUTSIDE VDS** dialog box, select a physical adapter and click **Submit**.

Step 11 Select an OVF file from the **OVF File** drop-down list.

Step 12 Enter VSM IP address for **VSM IP** text field.

Step 13 Enter domain Id for **Domain ID** text field.

Step 14 Select an uplink port profile from the **Uplink Port Profile** drop-down list.

Step 15 Select a management port group from the **Management Port Group** drop-down list.

Step 16 Select **Auto** for **Datastore** drop-down list.

Step 17 Enter VSE administrator password in the **VSE Admin Password** text-field.

Step 18 Confirm the password in the **Confirm Password** text field.

Step 19 Click **Install**.

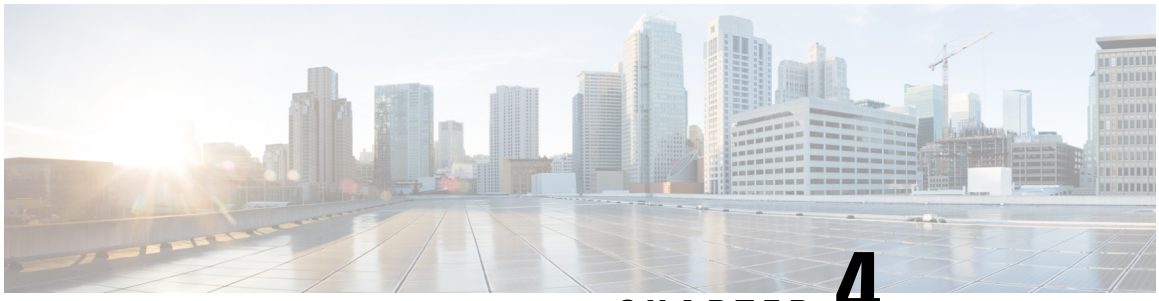
Step 20 In the **Install** dialog box, click **Yes**.

You can check the installation progress in the **Recent Tasks** tab at the bottom of VMware vCenter.

Unsupported Features

Cisco Nexus 1000VE Release 5.2(1)SV5(1.3) does not support the following features:

- Link Aggregation Control Protocol (LACP)
- L3 Forwarding
- Dynamic Host Configuration Protocol (DHCP)
- Netflow
- Network Segmentation Manager



CHAPTER 4

VSE Deployment Using VSE-Passthrough

This chapter contains the following sections:

About VSE-Passthrough

Pasthrough devices provide means to use the host network resources more efficiently and improve performance in VSE.By passing through the PCI network device to VSE, the control of traffic is given from the host to VSE over that PCI device for uplink configuration of nexus 1000ve VSE switch. This helps to improve the performance of VSE in traffic handling.

Guidelines and Limitations for VSE-Passthrough

VSE-Passthrough has the following guidelines and limitations:

- The live migration option in case of suspension and subsequent migration of a VM to a new physical host is not available.
- You cannot suspend or migrate the VM with vMotion or take snapshots of the VSE.
- You must ensure that a VMNIC (other thanthe passthrough enabled VMNICs) is available for host to handle the management traffic.

Note If passthrough is activated on all the VMNICs, the host will get disconnected. When you reset the host configuration, you cannot recover the host configuration.

- Adding the ESX host to an external-DVS should be avoided if the VSE is deployed with passthrough in that host. An external DVS in the host for the Cisco Nexus 1000VE configuration is not needed in this case.

- The VSE-Passthrough feature is verified successfully only with the Intel network adapters. The Cisco, Broadcom, and Emulex adapters are not supported or recommended for using Cisco Nexus 1000VE VSE with the corresponding PCI devices.
- You can install the VSE VM manually with the VSE-Passthrough feature.
- After the VSE VM is installed, the PCI devices must be added before you power on the VM.

Enabling Passthrough Devices

You must enable the Passthrough devices in the ESX Host before using the PCI device in VSE.

Note You cannot install VSE with the PCI devices passthrough option without enabling them in ESX Host, where the VSE is installed.

Before you begin

Before you enable the Passthrough devices, you must do the following:

- Login in to ESX Host.
- Enable the PCI devices in the host.
- Ensure the link state of the VMNICs are up, for which passthrough is activated.

Procedure

Step 1 Login and navigate to **Home** on VMware vCenter Web Client.

Step 2 Click **Manage** > **Settings**.

Step 3 From the **Hardware** tab, click **PCI Devices**.

Step 4 Select the network device to be used for passthrough and click **OK**. Alternatively, click **Toggle Passthrough**.

Step 5 Click **Reboot** to reboot the host to make the PCI network device available for use.

Installing VSE with PCI-Passthrough

Before you begin

You must do the following before you install VSE:

- Know the OVF image location and name that are required for the VSE installation.
- Ensure that VSM is already deployed as per the requirement.

Procedure

Step 1 Log into VMware Vsphere web client.

Step 2 Right click the Host to deploy the VSE OVA and select the **Deploy OVF Template** option from the pop-up menu.

Step 3 In the **Deploy OVF Template** window, complete the following steps:

a) In the **Select Template** page, select the **Local file**option and click **Browse** to navigate to the location of the VSE OVF. Select the applicable VSE OVF file and click **OK**. Click **Next** to continue.

b) In the **Select name and location** page, enter a name for VSE in the Name text field and click the **Browse** tab to navigate, and then select the datacenter to deploy the VSE.

c) Click **Next**.

d) In the **Select a resource** page, click the **Browse** tab, and then select the ESXi host to deploy the VSE. Click **Next** to continue.

e) In the **Review details** page, verify the OVA details, and then click **Next** to continue.

f) In the **Select storage** page, select the storage to be used, and then click **Next** to continue.

g) In the **Select networks** page, select the networks to use for Management destination Networks.

h) Select **VM Network** for Outside Networks, and click **Next** to continue.

i) In the **Customize template** page, do the following:

1. In the **Enter the Domain Id** text field, enter Domain ID for the VSM.

   Note The Cisco Nexus 1000VE domain ID should be the same as the domain iD of the Cisco Nexus 1000V VSM.

2. In the **L3 Control IP Address** text field, enter the VSM IP.
3. In the **IP Setting(static/dhcp)** text field, enter static.
4. In the **ESX host IP address** text field, enter the HOST IP address.
5. In the **Network 1 IP Address** text field, assign proper IP for VSE.
6. In the **Network 1 Netmask** text field, enter network mask.
7. In the **Default Gateway** text field, enter gateway IP address.
8. In the **DNS**, **DNS Domain**, and the **Uplink Port-profile** fields, retain the default strings.
9. In the **Admin password** text field, enter the password for VSE.
10. In the **Outside Trunk Mode(passthrough/uplink**) text field, enter the mode as passthrough.
11. In the **Number of Passthrough nics configured** text field, enter the number of Passthrough enabled NICs that are going to be used for this VSE.
12. In the **Passthrough dev-prof map 1** field, enter a uplink trunk-profile name, which is used to forward traffic to outside network using Passthrough. In similar way, fill the fields Passthrough dev-prof map x, with same or different uplink trunk-profiles upto the count given in the Step 11 or all the Passthrough enabled VMNICs(maximum 5).
13. Click **Next**.
14. In the **Ready to complete** page, verify all the details, and then click **Finish** to start VSE deployment.

Note VSE must not be powered on at this stage before completing the VSE VM deployment.

Configuring VSM

Configure all the Ethernet Port-groups/profiles in VSM with the same name as given in the Passthrough dev-prof map-1 to 8 fields while deploying VSE. These Profiles are called as Passthrough Profiles.

Ensure that the physical uplinks are trunk ports that should carry all the VLANs that are configured in the Passthrough Profiles.

Use the **port-profile type ethernet** command to create Ethernet port groups. For example:

```
N1KV-NG(config)# port-profile type ethernet < Passthrough dev-prof >
N1KV-NG(config-port-prof)# switchport mode trunk
N1KV-NG(config-port-prof)# switchport trunk vlan 300
N1KV-NG(config-port-prof)# no shut
N1KV-NG(config-port-prof)# state enabled
N1KV-NG(config-port-prof)# vmware port-group
N1KV-NG(config-port-prof)# end
N1KV-NG#
Save the configuration by running copy r s
N1KV-NG# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
N1KV-NG#
```

Note The veth port-profiles created on the VSM are available on the N1KVE-VDS. These can be assigned to workload VMs.

Attaching PCI Passthrough Devices in VSE

Procedure

Step 1 Login and navigate to **Home** on VMware vCenter Web Client.

Step 2 From the Inventory panel, select the VSE.

Step 3 Right click the VSE and select **Edit Settings**.

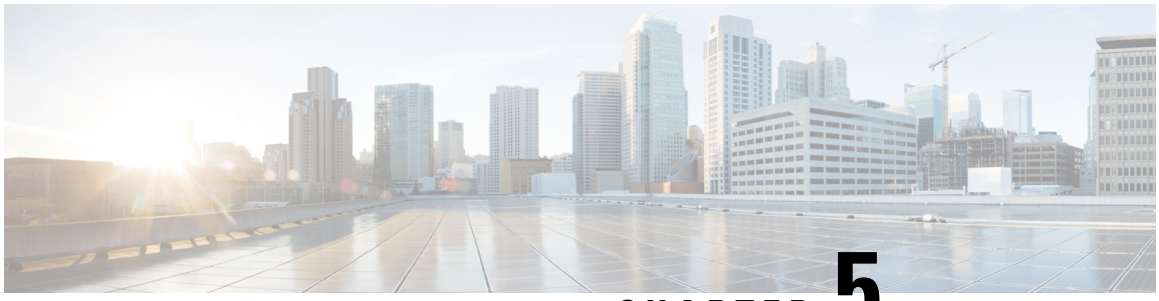
Step 4 On the Virtual Hardware tab, in the the New Device field, select **PCI Device**.

Step 5 Click **Add**.

Step 6 From the **New PCI Device** drop-down, select the appropriate passthrough device to use.

Step 7 Select **Reserve all memory**.

Step 8 Power on the VSE.



CHAPTER 5

Upgrading the Cisco Nexus 1000VE

This chapter contains the following sections:

Pre-requisites and Usage Guidelines

Follow these prerequisites and usage guidelines before upgrading Cisco Nexus 1000VE to release 5.2(1)SV5(1.3):

- Ensure that the current Nexus 1000VE release instance is up and running in the existing setup.
- Cisco Nexus 1000VE release 5.2(1)SV5(1.3) supports VMware vCenter v6.7. If you are upgrading ESXi hosts and VMWare vCenter Server to release v6.7, we recommend you to follow the upgrade steps in the specified sequence.
- Ensure that you have sufficient maintenance period during the upgrade process because a service disruption is expected during the upgrade process.

Upgrading the Cisco Nexus 1000VE VSMs

Software Images

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

- Software images—The kickstart and system image files reside in directories or folders that you can access from the Cisco Nexus 1000VE software prompt.
- Image version—Each image file has a version.
- Disk—The bootflash: resides on the VSM.

- ISO file—If a local ISO file is passed to the **install all** command, the kickstart and system images are extracted from the ISO file.

In-Service Software Upgrades on Systems with Dual VSMs

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

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

An ISSU updates the following images:

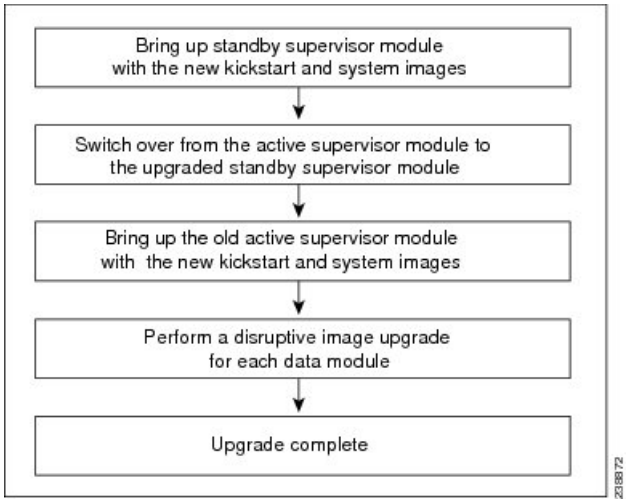
- Kickstart image
- System image
- VEM images

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

ISSU Process for Cisco Nexus 1000VE

The following figure shows the ISSU process.

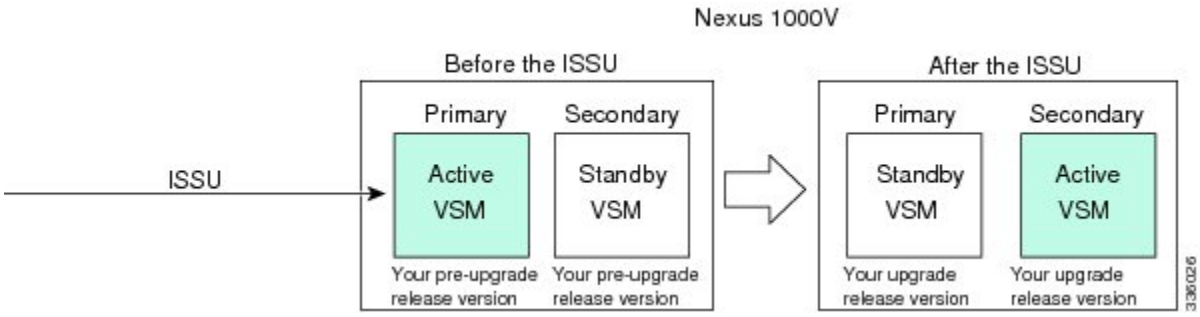
Figure 3: ISSU Process



ISSU VSM Switchover

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

Figure 4: Example of an ISSU VSM Switchover



ISSU Command Attributes

Support

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

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

Benefits

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

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

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

- You can upgrade the VSM using the least disruptive procedure.
- You can see the progress of this command on the console, Telnet, and SSH screens:
  - After a switchover process, you can see the progress from both the VSMs.
  - Before a switchover process, you can see the progress only from the active VSM.

- The **install all** command automatically checks the image integrity, which includes the running kickstart and system images.
- The **install all** command performs a platform validity check to verify that a wrong image is not used.
- The Ctrl-C escape sequence gracefully ends the **install all** command. The command sequence completes the update step in progress and returns to the switch prompt. (Other upgrade steps cannot be ended by using Ctrl-C.)
- After running the **install all** command, if any step in the sequence fails, the command completes the step in progress and ends.

Upgrading VSM from Release 5.2(1)SV5(1.2) to Release 5.2(1)SV5(1.3)

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

Procedure

Step 1 Log in to the active VSM.

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

Step 3 Access the Software Download Center by using this URL:

http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your system.

You see links to the download images for your switch.

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

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

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

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

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

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

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

a) switch# **copy scp://***filepath/kickstart_filename* **bootflash:***kickstart_filename*

Copy the ISO image.

b) switch# **copy scp://***filepath/system_filename* **bootflash:***system_filename*

Copy kickstart and system images.

Step 10 switch# **show install all impact kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename*

Verify the ISSU upgrade for the kickstart and system images or the ISO image. The example in this procedure shows the kickstart and system images.

Step 11 Read the release notes for the related image file. See the *Cisco Nexus 10000VE Release Notes*.

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

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

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

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

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

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

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

Step 16 Continue with the installation by pressing **Y**.

If you press **N**, the installation exits gracefully.

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

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

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

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

a) switch# **show install all status**
b) switch# **attach** *module_name*
c) switch# **show install all status**

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

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

Upgrading Cisco Nexus 1000VE Manager vCenter Plugin

To upgrade the Cisco Nexus 1000VE Manager vCenter Plugin, see Installing the Cisco Nexus 1000VE Manager vCenter Plugin, on page 18.

Upgrading the Cisco Nexus 1000VE VSEs

You can upgrade the Cisco Nexus 1000VE VSEs using two methods:

- Using Cisco Nexus 1000VE Manager vCenter Plugin
- Manually

Upgrading VSE using Cisco Nexus 1000VE Manager vCenter Plugin

Complete these steps to upgrade VSE using Cisco Nexus 1000VE Manager vCenter Plugin.

Before you begin

Make sure that new plugin corresponding to 5.2(1)SV5(1.3) is installed on vCenter.

Procedure

Step 1 Download the new VSE images, cisco-vse-5.2.1.SV5.1.3.ovf and cisco-vse-5.2.1.SV5.1.3-disk1.vmdk, to VMware vCenter content library.

Step 2 Navigate to **Home** on VMware vCenter Web Client. If a content library has already been created with the required VSE image, go to Step 6. If not, proceed to step 2.

Step 3 On the **Navigator** pane, click **Content Libraries** to open the **Content Libraries** page.

Step 4 On the **Getting Started** tab, click **Create new content library**.

Step 5 In the **New Content Library** dialog box, do the following:

a) On the **Name and Location** page, enter the content library name in the **Name** text field and select vCenter Server IP address from the **vCenter Server** drop-down list
b) Click **Next**.
c) On the **Configure content library** page, verify that the default option, Local content library is selected.
d) Click **Next**.
e) On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.
f) Click **Next**.
g) On the **Ready to complete** page, click **Finish**.
h) On the **Navigator** tab, select the new content library that you just created.

i) On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box.
j) Choose Local file option and click **Browse** and navigate to the location of the VSE OVF file. Select the VSE OVF file and click **Open**.
k) In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.
l) On the **Select referenced files** dialog box, click **Ok**.
m) On the **New Content Library – Import Library Item** dialog-box, click **Ok**.
n) On the **Home** page, click **Recent Tasks** tab at the bottom to check VSE file upload progress.

Step 6 Navigate to **Home** tab on **VMware vSphere Web Client**.

Step 7 Click **N1KVE Manager**, and enter the VMware vCenter password and click **Login**. The **N1KVE Manager** page opens.

Step 8 On the **Installation** tab, select a Data Center from the **Select a DC** drop-down list.

Step 9 Select N1KVE vDS from the **Select a VDS** drop-down list to list the available Hosts.

Step 10 Select a Host to upgrade from the list of **Hosts**.

Step 11 Select an OVF file from the **OVF File** drop-down list.

Step 12 Enter VSM IP address for **VSM IP** text-field.

Step 13 Enter domain Id for **Domain ID** text-field.

Step 14 Select an uplink port profile from the **Uplink Port Profile** drop-down list.

Step 15 Select a management port group from the **Management Port Group** drop-down list.

Step 16 Select **Auto** or choose from **Datastore** drop-down list for all hosts.

Step 17 Enter VSM and VSE credentials in respective fields.

Step 18 Click **Upgrade**.

Step 19 In the **Upgrade** dialog box, click **Yes** to complete the VSE upgrade process.

Step 20 Log in to Cisco N1KVE VSM and reload the system using the **reload** command. After the VSM boots up, you should be able to see the modules are up with new version.

Note Module indices change after upgrading VSE.

Example:

```
N1KVE-VSM# show module
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby
5 332 Virtual Service Engine NA ok
6 332 Virtual Service Engine NA ok

Mod Sw Hw
--- ------------------ ------------------------------------------------
1 5.2(1)SV5(1.3) 0.0
2 5.2(1)SV5(1.3) 0.0
5 5.2(1)SV5(1.3) NA
6 5.2(1)SV5(1.3) NA

Mod Server-IP Server-UUID Server-Name
--- --------------- ------------------------------------ --------------------
1 10.XXX.XXX.XXX NA NA
2 10.XXX.XXX.XXX NA NA
9 10.XXX.XXX.XXX XXXXXXXX-YYYY-ZZZZ-XXXX-YYYYYYYYYYYY localhost.localdomain
10 10.XXX.XXX.XXX AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE localhost.localdomain
```

```
Mod VSE-IP Host-IP
--- --------------- ------------------------------------
9 10.XXX.XXX.XXX 10.XXX.XXX.XXX
10 10.XXX.XXX.XXX 10.XXX.XXX.XXX
```

Upgrading VSE Manually

Complete the following steps to upgrade VSE manually. You need to manually upgrade all the VSEs.

Procedure

Step 1 Download the new VSE image, cisco-vse-5.2.1.SV5.1.3.ova, to the local system.

Step 2 Login to VSM.

Step 3 Use the **show module** command to identify the module to upgrade.

Step 4 Log into VMware vCenter using VMWare vSphere Web Client. For each host under the VSM complete the following steps:

a) Browse over **Hosts and Clusters** tab and Select a **Host**.

b) Select the **VSE Virtual Machine**, under the **Host**. Typically the VSE VMs are named as *N1KVE_VSE_<HOST_IP_ADDRESS>*.

c) Right-click the VSE and select **Edit Settings**. Note down the port-profiles for following network adapters required in future steps: Network Adapter 1 (Management), Network Adapter 2 (inside-trunk1), Network Adapter 3 (inside-trunk2), and Network Adapter 4 (Outside).

d) Right-click **Power** and select **Power-off**.

e) Right-click and select **Delete from the disk**.

Note Module will go offline in VSM.

Step 5 Login to VSM using administrator credentials and delete VSE module using the **no vse** command.

Example:

```
#no vse module_no
// for deleted VSE module
```

Step 6 Reboot the VSM to clear the stale VSE entry.

Step 7 Deploy the new VSE VM with the saved configuration settings. Login to VMware vCenter using VMWare vSphere Web Client.

a) In the **VMware vCenter WebClient**, select the **Host**.

b) Right-click the host and select **Deploy OVF Template** > **Local file** > **Browse**.

c) In the **Browse** dialog box, choose the cisco-vse-5.2.1.SV5.1.3.ova file from local system and click **Next**.

d) Enter VSE VM name, follow the standard naming convention, *N1KVE_VSE_<HOST_IP_ADDRESS>*.

e) Choose the same datacentre and click **Next**.

f) Choose the host and click **Next**.

g) Click **Next**.

h) In the **Select Networks** window, select **Destination Network** corresponding to inside-trunk1, inside-trunk2, Management and Outside Network Adapters as noted in Step 4c.

i) Enter the details in the **Customize Template** window:

- **Admin password**: Provide VSE administrator password.
- **Controller DomainId**: Provide domain id. Use **show svs domain** command to get domain Id.
- **DNS**: Provide DNS server IP address.
- **DNS Domain**: Provide DNS domain if required.
- **Default Gateway**: Default gateway IP Address.
- **ESX Host IP Address**: Host IP Address.
- **IP Setting(static/dhcp)**: Enter dhcp or static.
- **L3-Control IP Address**: Provide VSM IP address.
- **Network 1 IP Address**: Provide VSE IP Address. This IP address should be unused and available.
- **Network 1 Netmask**: Subnet mask for VSE adapter.
- **Uplink Port-Profile**: Provide the outside-trunk. Use the **show runnning-config port-profile outside-trunk** command on VSM to verify.

j) Click **Next**.
k) Review the detail of custom template and click **Finish** to deploy VSE on the selected host.
l) After deployment is completed, power on the VSE. Wait for some time to allow VSE to bootup.
m) Reload Cisco N1KVE VSM using the **reload** command and verify whether VSE is online.

Step 8 Verify the updated VSE using the **show module** command on VSM.

Example:

```
N1KVE-VSM# show module
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby
5 332 Virtual Service Engine NA ok
6 332 Virtual Service Engine NA ok

Mod Sw Hw
--- ------------------ ------------------------------------------------
1 5.2(1)SV5(1.3) 0.0
2 5.2(1)SV5(1.3) 0.0
5 5.2(1)SV5(1.3) NA
6 5.2(1)SV5(1.3) NA

Mod Server-IP Server-UUID Server-Name
--- --------------- ------------------------------------ --------------------
1 10.XXX.XXX.XXX NA NA
2 10.XXX.XXX.XXX NA NA
9 10.XXX.XXX.XXX XXXXXXXX-YYYY-ZZZZ-XXXX-YYYYYYYYYYYY localhost.localdomain
10 10.XXX.XXX.XXX AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE localhost.localdomain

Mod VSE-IP Host-IP
--- --------------- ------------------------------------
9 10.XXX.XXX.XXX 10.XXX.XXX.XXX
10 10.XXX.XXX.XXX 10.XXX.XXX.XXX
```

Changing the VSE Feature Level

After upgrading to Release 5.2(1)SV5(1.3), you must update the VSE feature level.

Before you begin

- VSM and VSE have been upgraded to Release 5.2(1)SV5(1.3) .

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **show system VSE feature level**

Displays the current VSE feature level. The current feature level should be 5.2(1)SV5(x).

Step 3 switch(config)# **system update VSE feature level** *value*

Configures the VSE feature level.

Note When you run the **system update VSE feature level** command after upgrading from Release 5.2(1)SV5(1.2) to Release 5.2(1)SV5(1.3), it displays the following versions:

- 5.2(1)SV5(1.3)

You must select 5.2(1)SV5(1.3) to update the VSE feature level to Release 5.2(1)SV5(1.3).

Step 4 (Optional) switch(config)# **copy running-config startup-config**

Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to update the VSE feature level after upgrading to Release 5.2(1)SV5(1.3).

```
N1KVE-VSM#
N1KVE-VSM# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    332    Virtual Service Engine            NA                  ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
2    5.2(1)SV5(1.3)    0.0
3    5.2(1)SV5(1.3)    NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
2    10.126.129.80    NA                                    NA
```

```
3    10.126.129.63    4206ECC3-9820-CF49-4778-31BEF6680657  localhost.localdomain

Mod  VSE-IP           Host-IP
---  ---------------  ------------------------------------
3    10.126.129.63    10.126.129.109

* this terminal session
N1KVE-VSM#
N1KVE-VSM# module vse 3 execute vemcmd show feature level
VSE Feature Level: 5.2(1)SV5(1.2)
N1KVE-VSM#
N1KVE-VSM# show system vse feature level
Current feature level: 5.2(1)SV5(1.2)
N1KVE-VSM# configure
Enter configuration commands, one per line.  End with CNTL/Z.
N1KVE-VSM(config)#
N1KVE-VSM(config)# system update vse feature level
Feature      Version
Level        String
--------------------
1            5.2(1)SV5(1.3)
N1KVE-VSM(config)# system update vse feature level 1
 Note: Run the command 'enable l3sec' under svs-domain for robust VSM-VSE
 security
 Note: Run following commands under 'vdc <switch-name>' to take full advantage
 of scale offered by this release:
 'limit-resource port-channel minimum <min-value> maximum <max-value>'
 'limit-resource vlan minimum <min-value> maximum <max-value>'
N1KVE-VSM(config)# end
N1KVE-VSM#
N1KVE-VSM# show system vse feature level
Current feature level: 5.2(1)SV5(1.3)
N1KVE-VSM#
N1KVE-VSM# system update vse feature level
Current feature level is the only one compatible with the inserted VSEs
N1KVE-VSM#
N1KVE-VSM# module vse 3 execute vemcmd show feature level
VSE Feature Level: 5.2(1)SV5(1.3)
N1KVE-VSM#
```

Upgrading VMware ESXi Hosts

Refer to VMware documentation to upgrade VMware ESXi host from release 6.5 to 6.7. For more information, see https://www.vmware.com/support/pubs/