



Cisco Nexus 1000VE Installation, Migration, and Upgrade Guide, Release 5.2(1)SV5(1.2)

First Published: 2019-05-24

Last Modified: 2019-06-03

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 1

- Information About Cisco Nexus 1000VE 1
 - Information About the Cisco Nexus 1000VE Virtual Supervisor Module 1
 - Information About the Virtual Service Engine 3
 - Information About VSM-to-VSE Communication 4
 - Layer 3 Control Mode 4
- Information About System Port Profiles and System VLANs 4
 - System Port Profiles 4
 - System VLANs 5
- Installation Overview 5
 - Information About Installing the Cisco Nexus 1000VE Manually 5
- Recommended Topologies 6
 - Topology for Layer 3 Control Mode 6

CHAPTER 2

Installing the Cisco Nexus 1000VE Software 7

- Supported VMware vSphere ESXi Hypervisor Versions 7
- Prerequisites for Installing the Cisco Nexus 1000VE 7
 - Prerequisites for Installing Nexus 1000 Virtual Edge (VE) 7
 - ESXi Host Prerequisites 8
 - VSM Prerequisites 9
 - VSE Prerequisites 9
 - Upstream Switch Prerequisites 10
- Guidelines and Limitations for Installing the Cisco Nexus 1000VE 10
- Information Required for Installation 12
- Verifying the Authenticity of the Cisco-Signed Image (Optional) 12
- Installing the Cisco Nexus 1000VE Software Using ISO or OVA Files 13

Deploying Virtual Supervisor Module	13
Configuring VSM Switch Name	14
Creating VDS in VMware vCenter	14
Configuring Promiscuous Mode for the Port Group	15
Creating VLANs on VSM	15
Creating vEthernet Port Group for the Workload VMs	16

CHAPTER 3**VSE Deployment Using Cisco Nexus 1000VE Manager vCenter Plugin 17**

Cisco Nexus 1000VE Manager vCenter Plugin Software Requirements	17
Installing the Cisco Nexus 1000VE Manager vCenter Plugin	18
Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 1	18
Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2	20
Retrieving HTTPS SHA1 Thumbprint	21
Installing VSE Using the NIKVE Manager vCenter Plugin	21
Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin	23
Migration Work Flow	23
Prerequisites for Migrating Cisco VSG, Cisco PNSC, and Cisco Nexus 1000V to Nexus 1000VE Environment	24
Usage Guidelines and Limitations	25
Unsupported Features	26
Compatibility Matrix - Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Environment	26
Migrating ESX Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using NIKVE Manager vCenter Plugin	27
Verifying the Host Migration	30
Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment	37
Registering Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC	38
Creating Firewall Object for Nexus 1000VE VSG on PNSC	39
Migrating Cisco VSG and Cisco PNSC with ESXi Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using NIKVE Manager vCenter Plugin	39
Verifying vService Nodes	43
Upgrading PNSC	44
Verifying Cisco PNSC Upgrade	46

Re-registering Cisco Nexus 1000VE VSM PA AND VSG PA	46
Registering PNSC with VMware vCenter Version 6.7(U1)	47

CHAPTER 4

Upgrading the Cisco Nexus 1000V	53
Pre-requisites and Usage Guidelines	53
Upgrading Nexus 1000VE Virtual Supervisor Module	53
Upgrading VMWare vCenter Server	55
Upgrading Cisco Nexus 1000VE Manager vCenter Plugin	56
Upgrading VSE using Cisco Nexus 1000VE Manager vCenter Plugin	57
Upgrading VSE Manually	58
Upgrading VMware ESXi Hosts	60



CHAPTER 1

Overview

This chapter contains the following sections:

- [Information About Cisco Nexus 1000VE, on page 1](#)
- [Information About System Port Profiles and System VLANs, on page 4](#)
- [Installation Overview, on page 5](#)
- [Recommended Topologies, on page 6](#)

Information 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.

Information About the Cisco Nexus 1000VE 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.

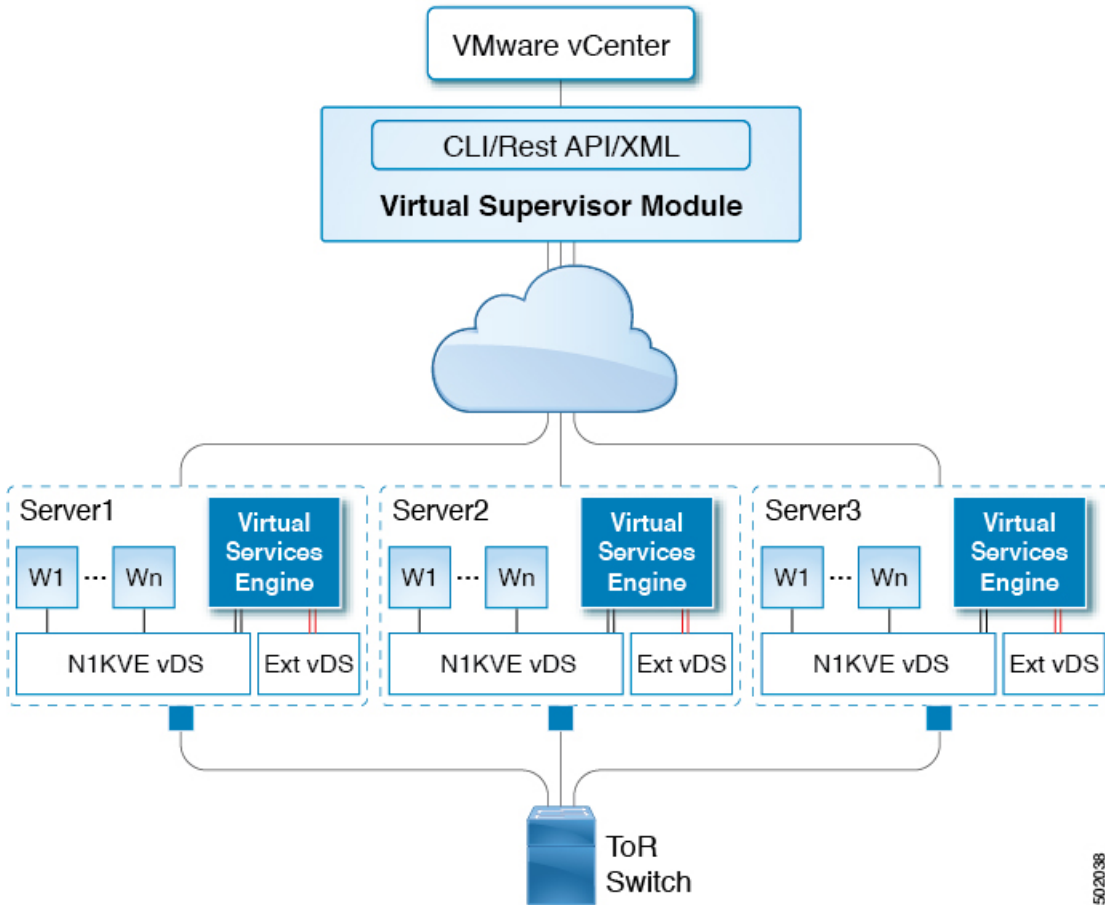
A single VSM can control up to 64 VSEs.

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.

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

Figure 1: Cisco Nexus 1000VE Architecture



Information About the 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.

Information 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*.

Information About System Port Profiles and System VLANs

System Port Profiles

System port profiles can establish and protect ports and VLANs that need to be configured before the VSE contacts the VSM.

When a server administrator adds a host to a DVS, its VSE must be able to contact the VSM. Because the ports and VLANs used for this communication are not yet in place, the VSM sends a minimal configuration, including the system port profiles and system VLANs, to vCenter Server, which then propagates it to the VSE.

When configuring a system port profile, you assign VLANs and designate them as system VLANs. The port profile becomes a system port profile and is included in the Cisco Nexus 1000VE opaque data. Interfaces that use the system port profile, which are members of one of the defined system VLANs, are automatically enabled and forward traffic when the VMware ESX starts even if the VSE does not have communication with the VSM. The critical host functions are enabled even if the VMware ESX host starts and cannot communicate with the VSM.



Caution VMkernel connectivity can be lost if you do not configure the relevant VLANs as system VLANs.

System VLANs

You must define a system VLAN in both the Ethernet and vEthernet port profiles to automatically enable a specific virtual interface to forward traffic outside the ESX host. If the system VLAN is configured only on the port profile for the virtual interface, the traffic is not forwarded outside the host. Conversely, if the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that needs that VLAN is not enabled by default and does not forward traffic.

The following ports must use system VLANs:

- Control and packet VLANs in the uplinks that communicate with the VSM.
- The Management VLAN in the uplinks and port profiles (that is, the Ethernet and vEthernet ports) and VMware kernel NICs used for VMware vCenter Server connectivity, Secure Shell (SSH), or Telnet connections.
- The VLAN that is used for remote storage access (iSCSI or NFS).



Note We recommend this to configure vmknics for management, NFS/iSCSI, and vMotion on the external VDS instead of the Nexus 1000VE.



Caution You must use system VLANs sparingly and only as described in this section. Only 32 system port profiles are supported.

After a system port profile has been applied to one or more ports, you can add more system VLANs, but you can only delete a system VLAN after you remove the port profile from service. This action prevents you from accidentally deleting a critical VLAN, such as a host management VLAN or a VSM storage VLAN.



Note One VLAN can be a system VLAN on one port and a regular VLAN on another port in the same ESX host.

Installation Overview

Information About Installing the Cisco Nexus 1000VE Manually

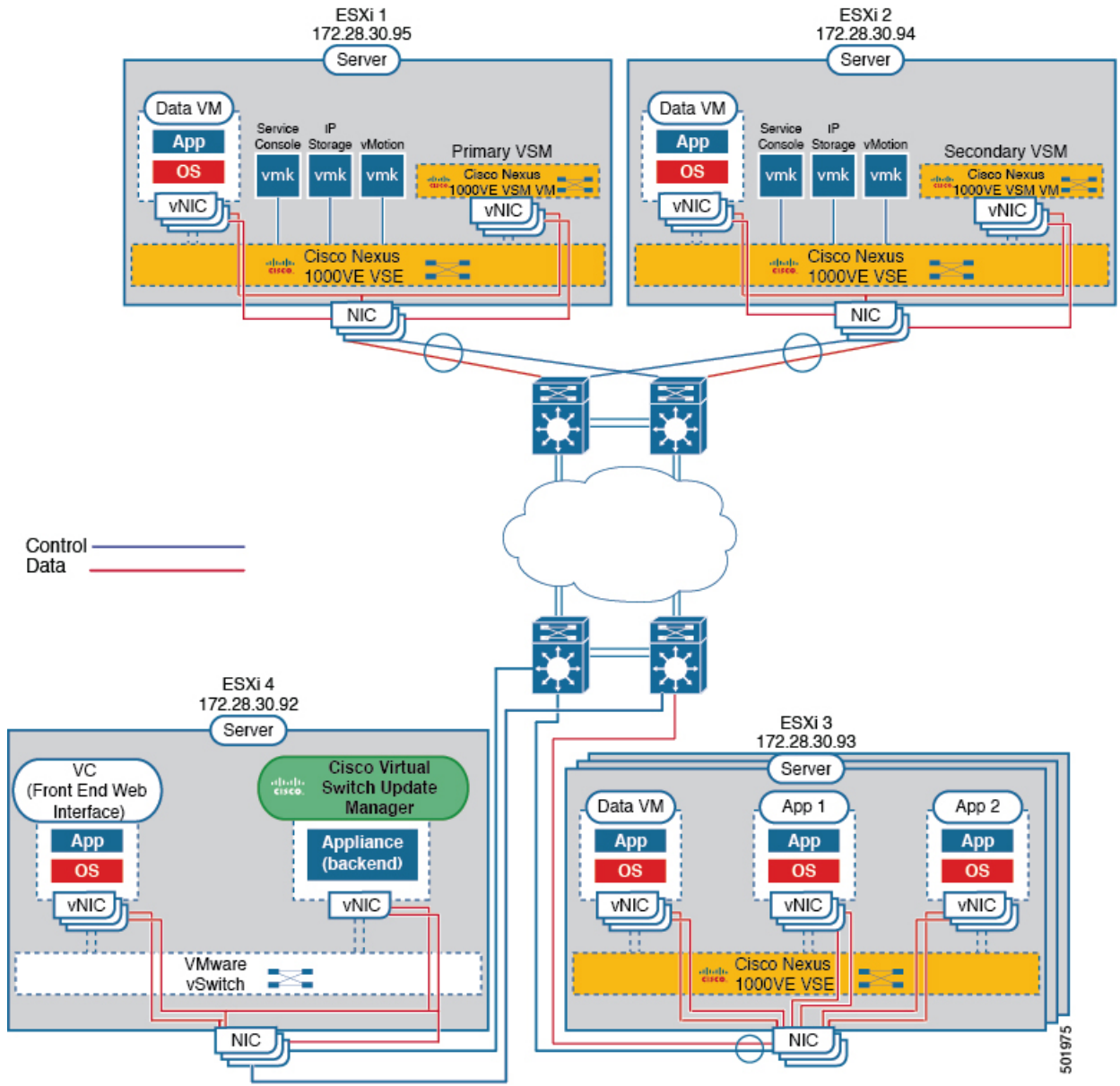
When you install the Cisco Nexus 1000VE manually, you download and install all of the necessary software. This installation method gives you the option of deploying Layer 3 connectivity between the VSM and VSEs. Layer 3 connectivity is the preferred method. For an example of the Layer 3 installation topology, see [Topology for Layer 3 Control Mode, on page 6](#).

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, on page 7](#)
- [Prerequisites for Installing the Cisco Nexus 1000VE, on page 7](#)
- [Guidelines and Limitations for Installing the Cisco Nexus 1000VE, on page 10](#)
- [Information Required for Installation, on page 12](#)
- [Verifying the Authenticity of the Cisco-Signed Image \(Optional\), on page 12](#)
- [Installing the Cisco Nexus 1000VE Software Using ISO or OVA Files, on page 13](#)

Supported VMware vSphere ESXi Hypervisor Versions

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

- 6.5a
- 6.0U3 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 6.0 U3 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 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 6](#).

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 VSMSs and there is no virtual channel (VC) connectivity on both VSMSs, the VSM that has the smaller number of modules is rebooted.
- If modules are attached to both VSMSs and one of the VSMSs 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 VSMSs 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 VSMSs have two modules attached or both VSMSs have no modules attached.

3. Last configuration change



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

- If both VSMSs 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.

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.SV5.1.1.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.SV5.1.1.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:

-
- Step 1** Copy the following files to a directory on the Linux machine:
- Nexus1000v.5.2.1.SV5.1.2.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.
- ```
Nexus1000v.5.2.1.SV5.1.2.zip
```
- Step 4** Check the output. If the validation is successful, the following message displays:
- ```
Authenticity of Cisco-signed image Nexus1000v.5.2.1.SV5.1.2.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.

- 
- 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)# svcs 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 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:

### SUMMARY STEPS

1. Right click the port group and select Edit Settings option from the pop-up menu.
2. In the Outside trunk Edit Settings window, click Security.
3. 3. In the Security page, do the following:.

### DETAILED STEPS

- 
- 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, on page 17](#)
- [Installing the Cisco Nexus 1000VE Manager vCenter Plugin, on page 18](#)
- [Retrieving HTTPS SHA1 Thumbprint, on page 21](#)
- [Installing VSE Using the N1KVE Manager vCenter Plugin, on page 21](#)
- [Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin, on page 23](#)

## Cisco Nexus 1000VE Manager vCenter Plugin Software Requirements

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



**Note** Cisco Nexus 1000VE vCenter Plugin is a Flex based plugin and appears only on vSphere Web Client (FLEX).

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

| Platform               | Recommended Release                                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware vCenter         | <ul style="list-style-type: none"><li>• 6.0 Linux Appliance</li><li>• 6.5 Linux Appliance</li><li>• 6.0 U3 Windows</li><li>• 6.5 Windows</li><li>• 6.7 U1 Linux Appliance</li><li>• 6.7 U1 Windows</li></ul> |
| Cisco Nexus 1000VE VSM | 5.2(1)SV5(1.2)                                                                                                                                                                                               |




---

**Note** If you are upgrading VMware vCenter from version 6.0 that has Cisco Plugin installed to VMware vCenter version 6.5, a warning message appears indicating that non-VMware distributed switch will not be supported in future VMware vSphere releases. Press **Ok** to continue normal upgrade process.

---




---

**Note** VMware vCenter version 6.7GA is not supported by the plugin. Currently, only VMware vCenter version 6.7U1 is validated to work with the migration plugin.

---

## 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 separate Plugin versions available for vCenter 6.0 and vCenter 6.5 or 6.7. Please download 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_v2.py` script to a python environment where `pymomi` 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 18
- [Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2](#), on page 20

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

**Step 1** Download the `deploy_n1kve_plugin_v2.py` python script from `https://<N1KVE-VSM-IP>/` to the Python environment.

**Example:**

**Step 2** Run the Python script, `deploy_n1kve_plugin_v2.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 to vCenter 6.0 and 6.5/6.7. Please provide respective file path depending upon your vCenter version.
  - If vCenter can reach Cisco Nexus 1000VE VSM over HTTP/HTTPS, then provide the URL similar to  
`https://<N1KVE-VSM-IP>/vcplugin/n1kve-vcenter6.X-plugin-1.0.2.zip`
  - 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.

```
$ python deploy_n1kve_plugin_v2.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: 10.126.129.211
vCenter Username: administrator@vsphere.local
Password:
Plugin zip file URL: http://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.2.zip
Select one of the following:-
1. Windows VCenter
2. VCenter Server Appliance
Enter 1 or 2
Choice: 2
Root password:
...
...
...

Connecting to the vCenter 10.126.129.211...
Fetching service instance content ...
Checking the API version ...
Checking if any version of the plugin is already present ...
Similar plugin found. Uninstalling it ...

Installing the plugin ...

The plugin information was successfully installed on the vCenter 10.126.129.211
```

```
--- 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...

Please restart vsphere-client service

**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. The Cisco Nexus 1000VE Manager icon is added under **Operations and Policies** section on the **Home** tab. This allows you to manage your Nexus 1000VE.

**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

---

**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:

```
<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>1.0.2</version>
 <server>
 <url>https://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.2.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>
</extension>
<client>
 <version>1.0.2</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-1.0.2.zip</url>
</client>
<lastHeartbeatTime>2019-05-16T00:00:00Z</lastHeartbeatTime>
<shownInSolutionManager>>false</shownInSolutionManager>
</extension>
```

- Step 6** Click **Invoke method** to register the plugin with the VMware vCenter. You must log out and log in again into the VMware vCenter in order 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 instructions so retrieve 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 instructions so retrieve 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 N1KVE Manager vCenter Plugin

Complete these steps to install VSE using N1KVE Manager vCenter plugin. You can also use the migrate option available on the N1KVE Manager vCenter plugin to install VSEs and to migrate the configuration from all existing Nexus 1000V instances. For more information see, [Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin](#), on page 23.

### Before you begin

- Ensure that you have configured a static IP pool or DHCP server in the VMware vCenter.

- Ensure that VSM is already deployed.

- 
- 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.
- Step 3** On the **Getting Started** tab, click [Create new content library](#).
- Step 4** In the **New Content Library** dialog box, do the following:
- 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
  - Click **Next**.
  - On the **Configure content library** page, verify that the default option, **Local content library** is selected
  - Click **Next**.
  - On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.
  - Click **Next**.
  - On the **Ready to complete** page, click **Finish**.
  - On the **Navigator** tab, select the new content library that you just created
  - On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box
  - 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**.
  - In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.
  - On the **Select referenced files** dialog box, click **Ok**.
  - On the **New Content Library – Import Library Item** dialog-box, click **Ok**.
  - 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**.

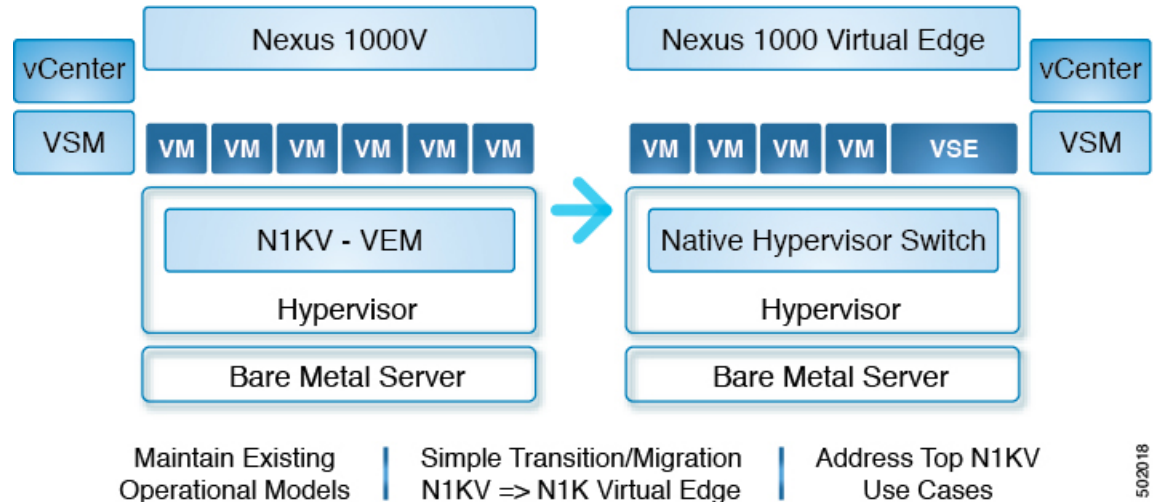
You can check the installation progress in the **Recent Tasks** tab at the bottom of VMware vCenter.

## Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin

This section explains about how you can migrate from Cisco Nexus 1000V to Nexus 1000VE. Migrating from Nexus 1000V to Nexus 1000VE involves use of Nexus 1000VE Manager vCenter plugin. The plugin provides easy migration with minimal disruption during the transition.

### Migration Work Flow

The following figure shows hypothetical view of Cisco Nexus 1000V to Cisco Nexus 1000VE migration.



Migration work flow is broadly classified into two steps:

- Configuration Migration: Migrate all the relevant configurations, filtering out unsupported or not applicable configurations from Cisco Nexus 1000V VSM to Cisco Nexus 1000VE VSM.
- Host Migration
  - Bring up the Cisco Nexus 1000VE VSE VM and other relevant vDS with port groups to which it is attached to
  - Migrate all the Virtual Machine ports from Cisco Nexus 1000V DVS to Cisco Nexus 1000VE vDS.
  - Migrate the VMKernel ports and Physical NICs that are part of Cisco Nexus 1000V DVS to corresponding vDS(s) at Cisco Nexus 1000VE.

## Prerequisites for Migrating Cisco VSG, Cisco PNSC, and Cisco Nexus 1000V to Nexus 1000VE Environment

Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE has the following prerequisites:

- You have downloaded and imported the Cisco Nexus 1000VE VSE OVF package to VMware vCenter Content Library.
- Cisco Nexus 1000VE VSM is running and available.
- Cisco Nexus 1000VE VSM is registered to vCenter and corresponding VDS is created and configured. Use the **show svcs connections** command to verify the connection status between Cisco Nexus 1000VE VSM and vCenter. Login to vCenter to verify whether Cisco Nexus 1000VE VDS is created or not.
- You have configured Cisco Nexus 1000V and Cisco Nexus 1000VE vDS as part of the same datacenter in VMware vCenter.
- Ensure that Cisco Nexus 1000V and Cisco Nexus 1000VE VSM do not use the same SVS Domain ID.
- Ensure that SSH is enabled for both both Cisco Nexus 1000V and Cisco Nexus 1000VE VSMs before migration.
- Cisco Nexus 1000VE VSE instance is a Virtual Machine deployed one per ESXi host that is installed through Cisco Nexus 1000VE Manager. First adapter of every VSE VM is reserved for management and it needs an IP address obtained either through Static IP Pool mapped to a port group or from a DHCP server running externally.

For more information about how to configure Static IP pools, see VMware documentation at: [Configuring IP Pools](#).

- Ensure that the IP address allocated to VSE VM through Static IP pool or DHCP server is reachable from Cisco Nexus 1000VE VSM management. You need to define the correct IP Pool with all free (unused) IP addresses. Incorrect IP pool configuration does not invoke error messages. You can detect duplicate IP address using the Linux command **arping -D ip\_address**.
- You have configured different vmknics for Nexus 1000V specific services (for example, ERSPAN/VSG) and VMware specific services (for example, vMotion) before migration.
- You have deployed the same number of new VSGs for Nexus 1000VE as configured in Cisco Nexus 1000V before starting the migration process.

One needs to deploy as many new VSGs as configured in Nexus1000v before migration.

- Ensure that the management IP address, data IP address, and the HA id of the Cisco Nexus 1000VE VSG is different from that configured in the VSG of the Cisco Nexus1000v.
- Ensure that the vmknics used for the communication between the Cisco Nexus1000v Vpath and Cisco VSG have the vMotion service disabled.
- For Nexus1000VE VSG, ensure that that vservice node is configured with adjacency I3 in Nexus 1000VE VSM while editing the migration config window during migration process. This is because adjacency I2 is not supported.
- .vservice node adjacency I3 configuration has no changes to Nexus1000VE , all the related configurations of Nexus1000V will work.

- Ensure that you configure the license and switch edition (either essential or advanced ) on Cisco Nexus 1000VE VSM before migration.

## Usage Guidelines and Limitations

Follow these usage guidelines and limitations while migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE:

- If a VSE management port-group is on VMware vSwitch, then the management port group with same name should be configured on all the Physical hosts that are chosen for installation or migration.
- Currently, it is not possible to change the management IP address of N1KVE-VSE after deployment. Please contact Cisco TAC support to allow access to root for changing the management IP address of VSE.
- Cisco Nexus 1000VE supports only ESXi version 6.0 and above. If any Hosts exists with previous version of ESXi in Cisco Nexus 1000V, its recommended to upgrade the same to ESXi version 6.0 and above to be a candidate for migration.
- Cisco Nexus 1000VE does not support multiple uplink port-profiles for a single VSE. However, each VSE can potentially use a different uplink port-profile.

We recommend that you create a new single uplink port-profile, by merging all the currently in-use uplink port-profile configurations including the VLANs, channel-group and policies. Do not move the PNICS manually and let the Cisco Nexus 1000VE Manager move all the PNICS as part of migration process using the newly created uplink port-profile.



---

**Note** Make sure to do the necessary configurations at the upstream switch ports attached to the PNICS to avoid disruption in traffic.

---

- Only the hosts that are using a common uplink ethernet port-profile on Cisco Nexus 1000VE can be migrated as a batch.
- Only the supported and applicable configurations are migrated from Nexus 1000V VSM to Cisco Nexus 1000VE VSM. The Nexus 1000VE manger migration plugin tool filters out the unsupported and not applicable configurations.
- The Nexus 1000VE Manager Plugin is not supported for use on a vCenter using the same Platform Service Controller (PSC) as other vCenters.
- Ensure that the Management Port Group name is unique.
- You cannot migrate single port-channel to multiple port-channel configuration.
- You can install or uninstall or migrate up to five Hosts at a time using the N1KVE Manager vCenter plugin.
- When migrating using the migration plugin, make sure the number of ports does not use the scale limit of 45000, after which there can be issues on adding the hosts to Nexus 1000VE.
- Only one Nexus 1000VE vDS is supported per datacenter in vCenter Server.
- Expect some packet drops during the migration process. The migration process is not hit-less.

- Layer 2 adjacency between vpath(VSE) and VSG is not supported
- IPv6 is not supported for VSM and VSE.
- Fully Qualified Domain Name (DNS) is not supported for VSE and VSM.
- Virtual Ethernet trunk mode is not supported on Nexus 1000VE.
- You can migrate upto 8 PNICS per Host that are part of Nexus 1000V VEM to Nexus 1000VE External vDS for LACP port-channel. Note that LACP does not run natively on Nexus 1000VE VSE or VSM.

## Unsupported Features

Cisco Nexus 1000VE Release 5.2(1)SV5(1.2) does not support the following features:

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

## Compatibility Matrix - Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Environment

Following table lists the minimum software versions required for various component to migrate from Nexus 1000V to Nexus 1000VE environment.

**Table 4: Compatibility Matrix**

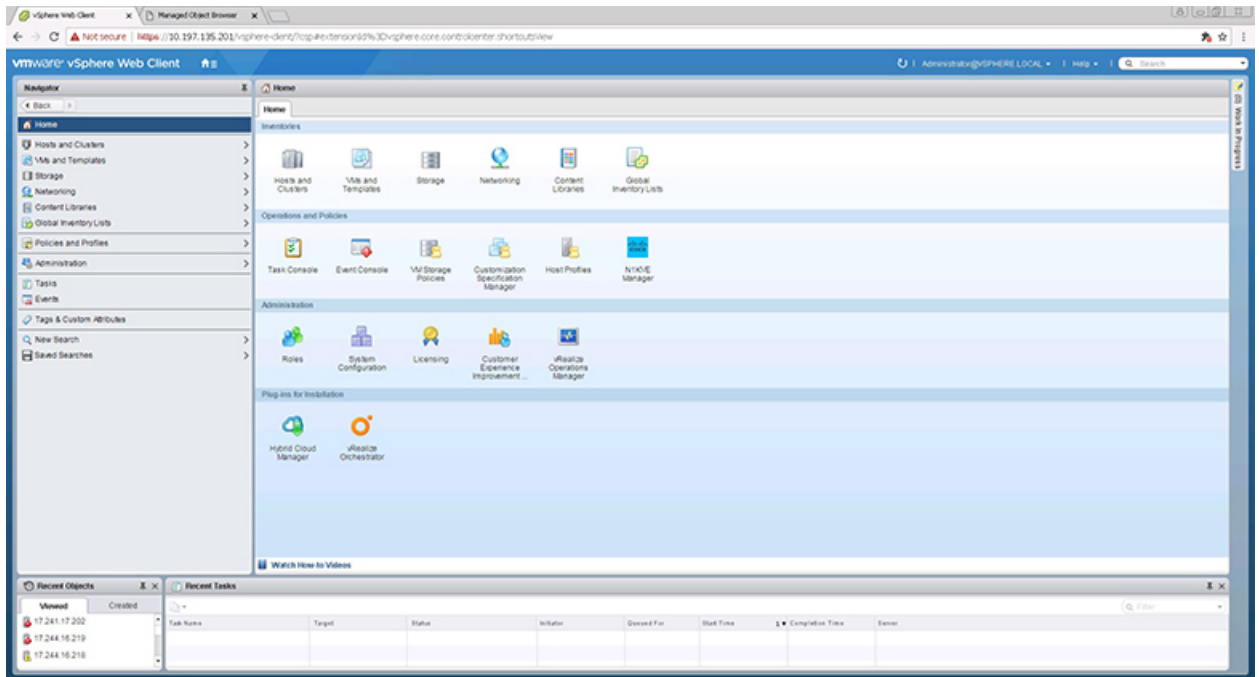
Cisco Nexus 1000V Version	Cisco VSG Version	Cisco PNSC Version	VMware ESXi Version
5.2(1)SV3(3.1)	VSG 2.2.2	<ul style="list-style-type: none"> <li>• PNSC 3.4.2c</li> <li>• PNSC 3.4.2d</li> </ul>	6.5a and 6.0
5.2(1)SV3(4.1)	VSG 2.2.2	<ul style="list-style-type: none"> <li>• PNSC 3.4.2c</li> <li>• PNSC 3.4.2d</li> </ul>	6.5a and 6.0



# Migrating ESX Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1KVE Manager vCenter Plugin

Follow these steps to migrate a ESX host from Cisco Nexus 1000V to Cisco Nexus 1000VE platform. If you have a VSG in your environment, see [Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment, on page 37](#).

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



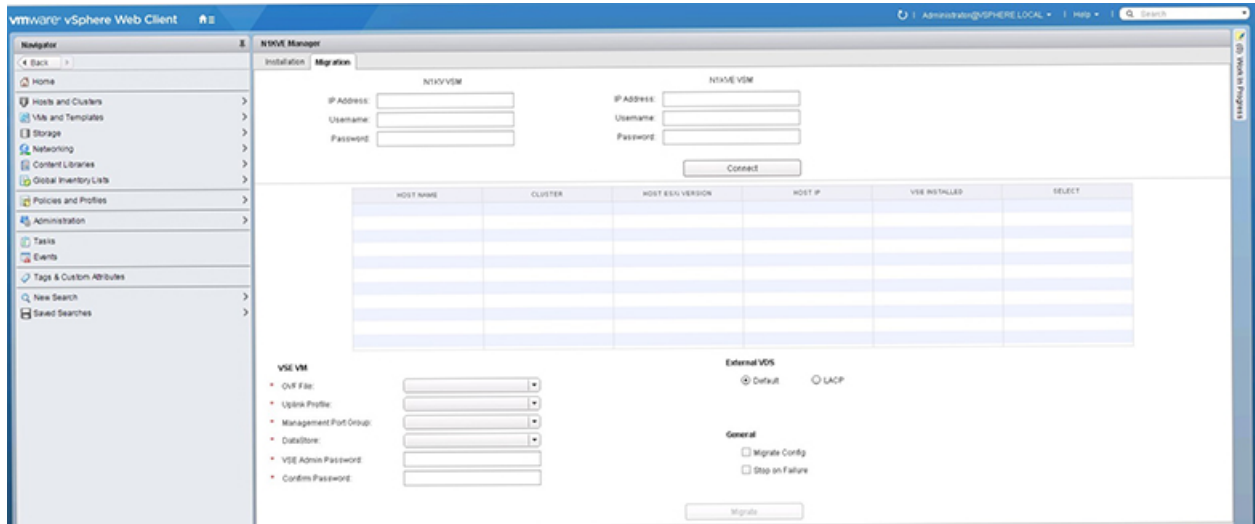
**Step 2** On the **Home** tab, under the **Operations and Policies** section, click the **Nexus 1000VE Manager (N1KVE)** icon.

**Step 3** Enter the VMware vCenter password to login into N1KVE Manager.

**Step 4** On the **N1KVE Manager** Window, click the **Migration** tab and enter the following details:

- NIKV VSM
  - IP address: IP address of NIKV VSM
  - Username: User name for NIKV VSM
  - Password: Password for NIKV VSM
- NIKVE VSM
  - IP address: IP address of NIKVE VSM
  - Username: User name for NIKVE VSM
  - Password: Password for NIKVE VSM

**Step 5** Click **Connect**. All the hosts attached to legacy N1KV that are eligible for migration are listed on the **Migration** tab.



**Step 6** Select a host to migrate. It's recommended to choose at a maximum of 5 hosts for migration at a time.

**Step 7** Select the Nexus 1000VE VSE OVF file from the **OVF File** drop-down list.

**Step 8** Select a port profile to migrate from the **Uplink Port Profile** drop-down list.

**Step 9** Select a management port group from the **Management Port Group** drop-down list.

**Step 10** Select deployment location for the Nexus 1000VE VSE from the **DataStore** drop-down list. If you select Auto, location for VSE VM is chosen randomly by the vCenter.

**Step 11** Enter a new password and confirm the password in the VSE Admin Password and Confirm Password text-fields.

**Step 12** Select applicable port channel type configured in the Nexus 1000V under External VDS.

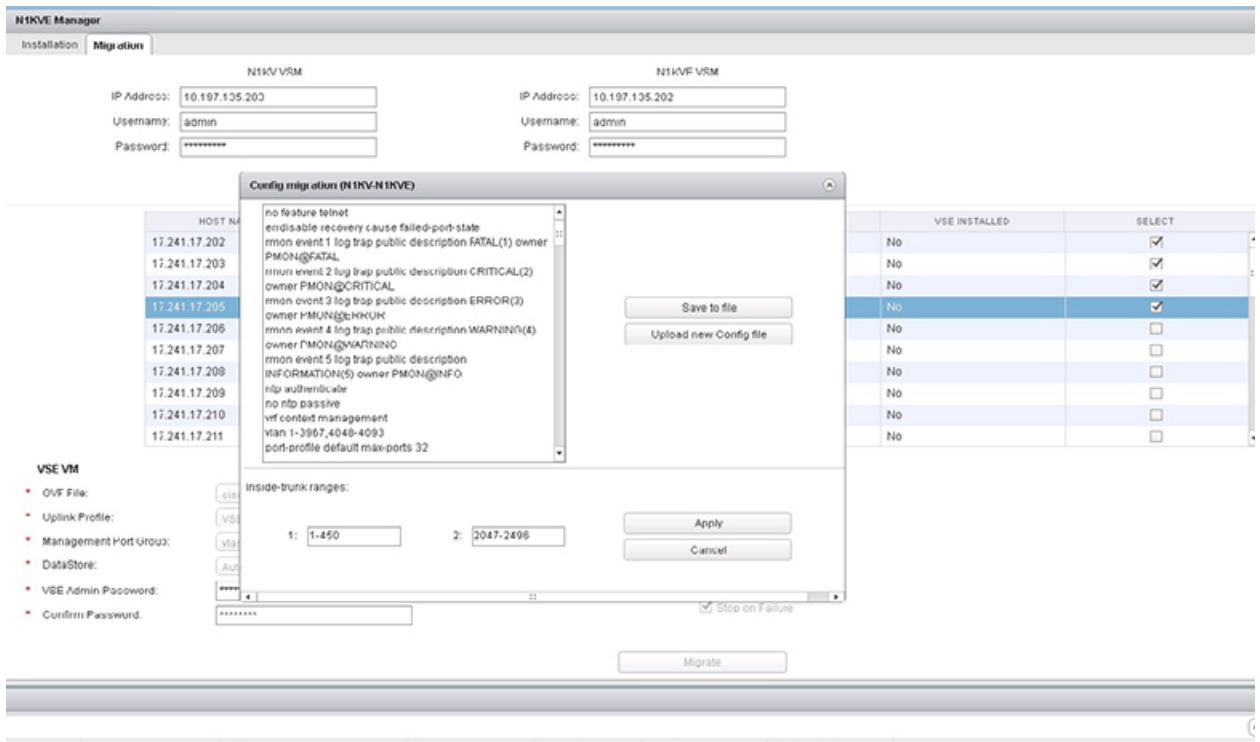
**Step 13** Select **Migrate Config** option. You must select this option while migrating hosts for the first time. For the subsequent host migrations to Cisco Nexus 1000VE, select this option if you want to migrate the latest/modified configuration from the Cisco Nexus 1000V VSM. Else uncheck this option.

**Step 14** Select **Stop on Failure** option. This is enabled by default.

**Step 15** Click **Migrate** to initiate the migration process.

**Step 16** Click **Yes** in the Migrate Configuration dialog box. The Config Migration dialog box appears with filtered configuration from the Cisco Nexus 1000V VSM instance. In the **Config Migration** dialog box, please remove the port-profiles that belong to VEM VMkernel adapters, so that those adapters will not be considered for migration.

Figure 3:



You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Config migration from N1KV to N1KVE) in the Recent Tasks tab.

- Step 17** (Optional) If you want to save this configuration for future reference, click Save to file.
- Step 18** (Optional) To select a different configuration (text file format only), click Upload new Config file.
- Step 19** Under Inside-trunk ranges section, the two text fields show the range of ports required (Calculated dynamically by the tool for each cluster). You can change these ranges. For more information about Inside-trunk ranges, see Install Guide.
- Step 20** Click **Apply** to start the migration process.
- Step 21** Once the configuration migration is completed, a new dialog box appears for host migration. Click Yes in the Migrate Host to N1KVE dialog box. The migration process starts. You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Migration from N1KV to N1KVE) in the Recent Tasks tab.
- Step 22** Check the status of VEM using the **vem status** command on the ESXi host.

#### Example:

```
[root@localhost:~] vem status
```

```
VEM modules are loaded
```

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
vSwitch0	5012	44	128	1500	vmnic4
DVS Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
NG-vsm-231	5012	15	1024	9000	
DVS Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
n1kve-outside-vds-DC-2	5012	8	512	1500	vmnic6,vmnic5

```
VEM Agent (vemdpa) is running
```

**Step 23** If the VEM is in running state, stop the VEM process using the **vem stop** command or **kill** command.

**Example:**

```
[root@localhost:~] vem stop
stopDpa
VEM SWiSCSI is already stopped
Terminating DPA watchdog and DPA (PID 74416 74657 74658)
watchdog-vemdpa: Terminating watchdog process with PID 74408
[root@localhost:~]
```

**Step 24** Remove the VIB using the **esxcli software vib remove --vibName=vib name --maintenance-mode** command.

**Example:**

```
[root@localhost:~] esxcli software vib list | grep cisco
cisco-vem-v522-esx 5.2.1.3.4.1a.0-6.5.1 Cisco PartnerSupported
2019-05-17
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli software vib remove --vibName=cisco-vem-v522-esx --maintenance-mode
Removal Result
 Message: Operation finished successfully.
 Reboot Required: false
 VIBs Installed:
 VIBs Removed: Cisco_bootbank_cisco-vem-v522-esx_5.2.1.3.4.1a.0-6.5.1
 VIBs Skipped:
[root@localhost:~]
```

## Verifying the Host Migration

Login to Cisco Nexus 1000VE VSM and use the **show** commands to check whether the selected host migrated successfully to Cisco Nexus 1000VE.

Sample output for **show module** command.

```
testing-158# show module
Mod Ports Module-Type Model Status
--- -
1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby
3 1022 Virtual Service Engine NA ok
4 1022 Virtual Service Engine NA ok
5 1022 Virtual Service Engine NA other

Mod Sw Hw
--- -
1 5.2(1)SV5(1.2) 0.0
2 5.2(1)SV5(1.2) 0.0
3 5.2(1)SV5(1.2) NA
4 5.2(1)SV5(1.2) NA
5 5.2(1)SV5(1.2) NA

Mod Server-IP Server-UUID Server-Name
--- -
1 16.1.0.103 NA NA
2 16.1.0.103 NA NA
3 16.2.0.100 422CF071-5E7D-6A1F-7630-C995EA58966A localhost.localdomain
4 16.2.0.101 422CDE9E-D950-1923-FD2C-161304F3ACEC localhost.localdomain
5 16.2.0.102 422C4B49-4A2D-2863-5A0B-305089F8ED75 localhost.localdomain
```

```

Mod VSE-IP Host-IP
--- -
3 16.2.0.100 10.197.128.87
4 16.2.0.101 10.197.128.92
5 16.2.0.102 10.197.128.91

```

```

* this terminal session
testing-158#

```

Sample output for **show interface brief** command.

```
testing-158# show interface brief
```

```

Port VRF Status IP Address Speed MTU

mgmt0 -- up 16.1.0.103 1000 1500

```

```

Ethernet VLAN Type Mode Status Reason Speed Port
Interface

Eth3/1 1 eth trunk up none 10G
Eth4/1 1 eth trunk up none 10G
Eth5/1 1 eth trunk up none 10G

```

```

Vethernet VLAN/ Type Mode Status Reason MTU Module
Segment

Veth1 1602 virt access up none 1500 4
Veth2 1602 virt access up none 1500 4
Veth3 1602 virt access up none 1500 5
Veth4 1602 virt access up none 1500 5

```

```

Port VRF Status IP Address Speed MTU

control0 -- up -- 1000 1500

```

NOTE : \* Denotes ports on modules which are currently offline on VSM

Sample output for **show interface virtual** command.

```
testing-158# show interface virtual
```

```

Port Adapter Owner Mod Host

Veth1 Net Adapter 1 vm14 4 localhost.localdomain
Veth2 Net Adapter 1 vm12 4 localhost.localdomain
Veth3 Net Adapter 1 vm13 5 localhost.localdomain
Veth4 Net Adapter 1 vm11 5 localhost.localdomain
testing-158#

```

Sample output for **show running-config** command.

```
testing-158# show running-config
```

```

!Command: show running-config
!Time: Fri Jun 22 09:43:04 2012

```

```

version 5.2(1)SV5(1.2)
svs switch edition advanced

```

```
hostname testing-158
```

```

no feature telnet
feature tacacs+
feature cts
feature port-profile-roles
feature vtracker

logging level aaa 5
logging level cdp 6
logging level radius 5
logging level tacacs 5
logging level monitor 6
username admin password 5 1yhU5WlBH$sKPYWegaDsCpfTH6R8hAM1 role network-admin
username admin keypair generate rsa
username dcnm password 5 ! role network-admin
username visinoc password 5 ! role network-admin

banner motd #Nexus 1000v Switch
#

ip domain-lookup
ip host testing-158 16.1.0.103
aaa group server radius aaa-private-sg
logging event link-status default
errdisable recovery cause failed-port-state
ip access-list test
 statistics per-entry
 10 permit icmp 16.2.0.111/32 16.2.0.112/32
 11 permit icmp 16.2.0.112/32 16.2.0.111/32
 12 deny icmp 17.1.1.1/32 12.2.2.2/32
 13 permit tcp any any
 14 permit ip any any
vse 3
 host id 422CF071-5E7D-6A1F-7630-C995EA58966A
vse 4
 host id 422CDE9E-D950-1923-FD2C-161304F3ACEC
vse 5
 host id 422C4B49-4A2D-2863-5A0B-305089F8ED75
snmp-server user admin network-admin auth md5 0x9f18743a6a8510da4b020aae147549fa priv
0x9f18743a6a8510da4b020aae147549fa localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp authenticate
no ntp passive

vrf context management
 ip route 0.0.0.0/0 16.1.0.1
vlan 1,1601-1650
vlan 1604
 name CVT2.0_BAN_Primary
vlan 1605
 name CVT2.0_BAN_Isolated
vlan 1606
 name FT_Logging

port-channel load-balance ethernet source-mac
port-profile default max-ports 64
port-profile default port-binding static
port-profile type vethernet 103-1640
 switchport mode access
 switchport access vlan 1640

```

```

no shutdown
max-ports 32
state enabled
vmware port-group
port-profile type vethernet 103-1641
switchport mode access
switchport access vlan 1641
no shutdown
max-ports 32
state enabled
vmware port-group
port-profile type ethernet Unused_Or_Quarantine_Uplink
shutdown
description Port-group created for Nexus 1000V internal usage. Do not use.
state enabled
vmware port-group
port-profile type vethernet Unused_Or_Quarantine_Veth
shutdown
max-ports 32
description Port-group created for Nexus 1000V internal usage. Do not use.
state enabled
vmware port-group
port-profile type vethernet inside-trunk1
switchport mode trunk
switchport trunk allowed vlan 1-50
no shutdown
max-ports 32
description Port-group created for Nexus 1000V internal usage. Do not use.
state enabled
vmware port-group
port-profile type ethernet outside-trunk
switchport mode trunk
switchport trunk allowed vlan 1-3967,4048-4093
no shutdown
description Port-group created for Nexus 1000V internal usage. Do not use.
state enabled
vmware port-group
port-profile type vethernet inside-trunk2
switchport mode trunk
switchport trunk allowed vlan 2047-2096
no shutdown
max-ports 32
description Port-group created for Nexus 1000V internal usage. Do not use.
state enabled
vmware port-group
port-profile type vethernet l3-control
switchport mode access
switchport access vlan 1602
no shutdown
capability l3control
state enabled
vmware port-group
port-profile type vethernet MGMT_vMotion
switchport mode access
switchport access vlan 3800
no shutdown
state enabled
vmware port-group
port-profile type ethernet Mgmt-Uplinks
switchport mode trunk
switchport trunk allowed vlan 3000
mtu 9000
no shutdown
state enabled

```

```

 vmware port-group
port-profile type ethernet Cust-Uplinks
 switchport mode trunk
 switchport trunk allowed vlan 2,41,45,54,145,518,541,545,554,980-981
 switchport trunk allowed vlan add 983-984,3018
 mtu 9000
 no shutdown
 state enabled
 vmware port-group
port-profile type ethernet vKernel-Uplinks
 switchport mode trunk
 switchport trunk allowed vlan 3800-3801
 mtu 9000
 no shutdown
 state enabled
 vmware port-group
port-profile type vethernet GLB_LanA_VLAN_45
 switchport mode access
 switchport access vlan 45
 no shutdown
 state enabled
 vmware port-group
port-profile type vethernet GLB_BAN_VLAN_545
 switchport mode access
 switchport access vlan 545
 no shutdown
 max-ports 128
 state enabled
 vmware port-group
port-profile type vethernet GLB_TestDev_VLAN_145
 switchport mode access
 switchport access vlan 145
 no shutdown
 state enabled
 vmware port-group
port-profile type vethernet v2
 switchport mode access
 switchport access vlan 2
 no shutdown
 max-ports 8
 description VM on vlan 2
 state enabled
 vmware port-group SDC_Backup-2
port-profile type vethernet VPS_ESXMGMT_VLAN_983
 switchport mode access
 switchport access vlan 983
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet LCV_LanA_VLAN_54
 switchport mode access
 switchport access vlan 54
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet VPS_OVMMGMT_VLAN_984
 switchport mode access
 switchport access vlan 984
 no shutdown
 max-ports 16
 state enabled
 vmware port-group

```



```
port-profile type vethernet DAI_LanA_VLAN_41
 switchport mode access
 switchport access vlan 41
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet DAI_BAN_VLAN_541
 switchport mode access
 switchport access vlan 541
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet LCV_BAN_VLAN_554
 switchport mode access
 switchport access vlan 554
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet ONE_SANMgmt_981
 switchport mode access
 switchport access vlan 981
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet ONE_SDCOPS_980
 switchport mode access
 switchport access vlan 980
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet SON_BAN_VLAN_518
 switchport mode access
 switchport access vlan 518
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet SON_OVMMGMT_VLAN_3018
 switchport mode access
 switchport access vlan 3018
 no shutdown
 max-ports 16
 state enabled
 vmware port-group
port-profile type vethernet GLB_L2Only_Heartbeat_47
 switchport mode access
 switchport access vlan 47
 no shutdown
 max-ports 16
 state enabled
 vmware port-group GLB_Heartbeat_VLAN_47
port-profile type ethernet uplink2
 switchport mode trunk
 switchport trunk allowed vlan 1,1601-1650
 no shutdown
 system vlan 1601-1650
 state enabled
 vmware port-group
port-profile type vethernet vm1-pp
```

```

switchport mode access
switchport access vlan 1602
ip port access-group test in
ip port access-group test out
no shutdown
max-ports 1024
system vlan 1602
state enabled
vmware port-group
port-profile type vethernet vm2-pp
switchport mode access
switchport access vlan 1607
no shutdown
max-ports 1024
state enabled
vmware port-group

system storage-loss log time 60
system inter-sup-heartbeat time 15
track network-state
track network-state interval 3

interface mgmt0
ip address 16.1.0.103/24

interface Vethernet1
inherit port-profile vml-pp
description vm14, Net Adapter 1
vmware dvport 0 dvs switch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
vmware vm mac 0050.56AC.DCA4

interface Vethernet2
inherit port-profile vml-pp
description vm12, Net Adapter 1
vmware dvport 0 dvs switch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
vmware vm mac 0050.56AC.2DAB

interface Vethernet3
inherit port-profile vml-pp
description vm13, Net Adapter 1
vmware dvport 0 dvs switch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
vmware vm mac 0050.56AC.10E0

interface Vethernet4
inherit port-profile vml-pp
description vm11, Net Adapter 1
vmware dvport 0 dvs switch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
vmware vm mac 0050.56AC.72D7

interface Ethernet3/1
inherit port-profile uplink2

interface Ethernet4/1
inherit port-profile uplink2

interface Ethernet5/1
inherit port-profile uplink2
line console
line vty
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SV5.1.0.228.bin sup-1
boot system bootflash:/n1000v-dk9.5.2.1.SV5.1.0.228.bin sup-1
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SV5.1.0.228.bin sup-2
boot system bootflash:/n1000v-dk9.5.2.1.SV5.1.0.228.bin sup-2

```

```
monitor session 1 type erspan-source
cts device tracking
cts interface delete-hold 60
cts sxp node-id interface mgmt0
svs-domain
 domain id 103
 control vlan 1
 packet vlan 1
 svl mode L3 interface mgmt0
 switch-guid 8329b603-ee69-419a-82f6-b1d373df3643
 enable l3sec
vse-dvs
 outside-trunk vlan 1-4094
 inside-trunk 1 tag 1-50
 inside-trunk 2 tag 2047-2096
svs connection vc
 protocol vmware-vim
 remote ip address 10.197.128.76 port 80 vrf management
 transport type ipv4
 vmware dvs uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76" datacenter-name DC - 2
 max-ports 12000
 vmware dvs-version 5.0.0
 connect
vservice global type vsg
 no tcp state-checks invalid-ack
 no tcp state-checks seq-past-window
 no tcp state-checks window-variation
 no bypass asa-traffic
 no l3-frag
vservice global
 idle-timeout
 tcp 30
 udp 4
 icmp 4
 layer-3 4
 layer-2 2
nsc-policy-agent
 registration-ip 0.0.0.0
 shared-secret *****
 log-level

testing-158#
```

## Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment

To migrate Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment, complete the following tasks:

- [Registering Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC, on page 38](#)
- [Creating Firewall Object for Nexus 1000VE VSG on PNSC, on page 39](#)
- [Migrating Cisco VSG and Cisco PNSC with ESXi Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1kVE Manager vCenter Plugin, on page 39](#)
- [Verifying vService Nodes, on page 43](#)
- [Upgrading PNSC, on page 44](#)

- [Verifying Cisco PNSC Upgrade, on page 46](#)
- [Re-registering Cisco Nexus 1000VE VSM PA AND VSG PA, on page 46](#)

## Registering Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC

Complete these steps to register Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC:

**Step 1** Log in to VSM and use **registration-ip** command to register VSM to PNSC.

**Example:**

```
NG_VSM# conf
Enter configuration commands, one per line. End with CNTL/Z.
NG_VSM(config)# nsc-policy-agent
NG_VSM(config-nsc-policy-agent)# registration-ip 1.1.1.1 // pnc ip address
NG_VSM(config-nsc-policy-agent)# shared-secret password
NG_VSM(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.3a.bin
NG_VSM(config-nsc-policy-agent)# end
NG_VSM# copy r s
[#####] 100%
Copy complete, now saving to disk (please wait)...
NG_VSM#
```

**Step 2** Verify whether VSM registration to PNSC was successful.

**Example:**

```
NG_VSM # sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
```

**Step 3** Deploy as many new VSG(s) as configured in the classic Nexus 1000V for Nexus1000VE.

**Step 4** Log in to VSG and use **registration-ip** command to register VSG to PNSC.

**Example:**

```
vsg# conf
WARNING: This device is managed by Prime Network Services Controller. Changing configuration using
CLI is not recommended.
vsg(config)# nsc-policy-agent
vsg(config-nsc-policy-agent)# registration-ip 1.1.1.1 // pnc ip address
vsg(config-nsc-policy-agent)# shared-secret password
vsg(config-nsc-policy-agent)# policy-agent-image bootflash:nsc-vsgpa.2.1.3i.bin
vsg(config-nsc-policy-agent)# end
vsg# copy r s
[#####] 100%
Copy complete, now saving to disk (please wait)...
vsg#
```

**Step 5** Deploy as many new VSG(s) as configured in classic Nexus 1000V for Nexus1000VE.

**Step 6** Verify whether VSG registration to PNSC was successful.

**Example:**

```
vsg# sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
```

## Creating Firewall Object for Nexus 1000VE VSG on PNSC

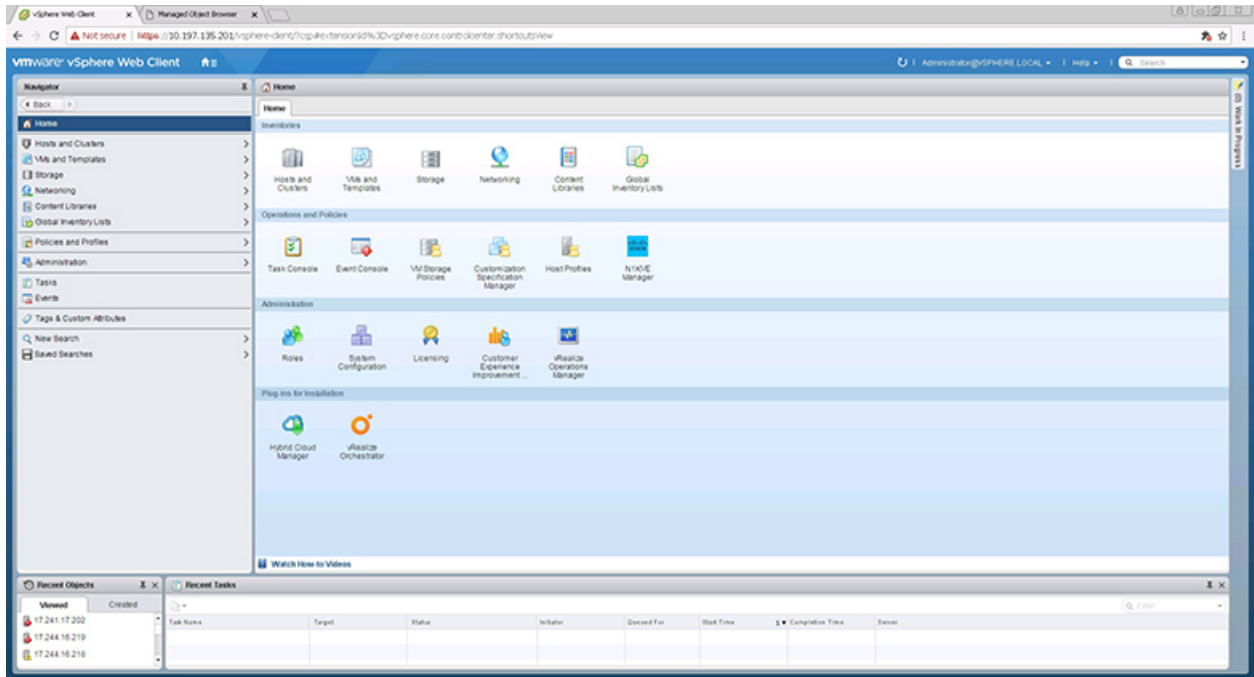
You need to create a firewall object for Nexus 1000VE VSG with different data IP on Cisco PNSC.

- 
- Step 1** Log in to Cisco PNSC GUI.
- Step 2** Navigate to **Resource Management > Managed Resources** and under the **root** navigation pane, select a tenant to deploy the firewall. **Compute Firewall**.
- Step 3** On the tenant page, click **Network Services** and from the **Action** drop-down list click **Add Compute Firewall**.
- Step 4** In the **Create** dialog-box, enter the name and description for the firewall and click **Next**.
- Step 5** On the **Select Service Device** page, select **Assign VSG** option.
- Step 6** From the **VSG Device** drop-down list, select IP address of N1KVE VSG registered in the previous task.
- Step 7** Click **Next**.
- Step 8** In the **Configure Data Interface** page, enter the following details:
- Data IP Address (should be different from data IP address assigned to VSG under classic Nexus 1000V environment)
  - Subnet Mask
  - VLAN
- Step 9** Click **Next**.
- Step 10** On the **Summary** page, review the configurations and click **Finish** to create a VSG firewall object.
- 

## Migrating Cisco VSG and Cisco PNSC with ESXi Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1kVE Manager vCenter Plugin

Follow these steps to migrate Cisco VSG and Cisco PNSC with ESXi Host (VEM) from Cisco Nexus 1000V to Cisco Nexus 1000VE environment using N1KVE Manager.

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



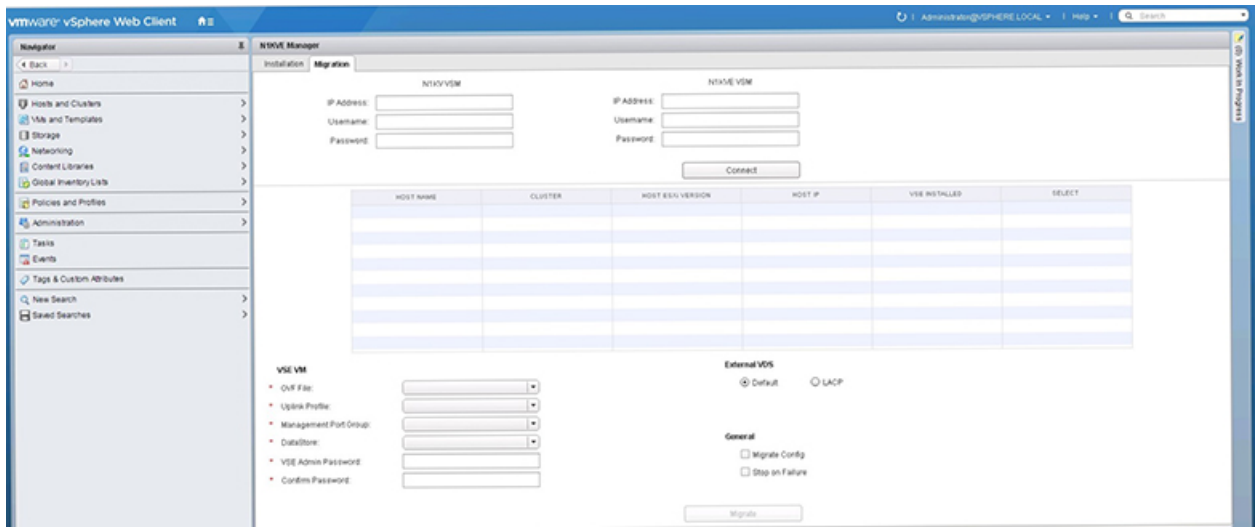
**Step 2** On the **Home** tab, under the **Operations and Policies** section, click the **N1KVE Manager** icon.

**Step 3** Enter the VMware vCenter password to login into N1KVE Manager.

**Step 4** On the **N1KVE Manager** window, click the **Migration** tab and enter the following details:

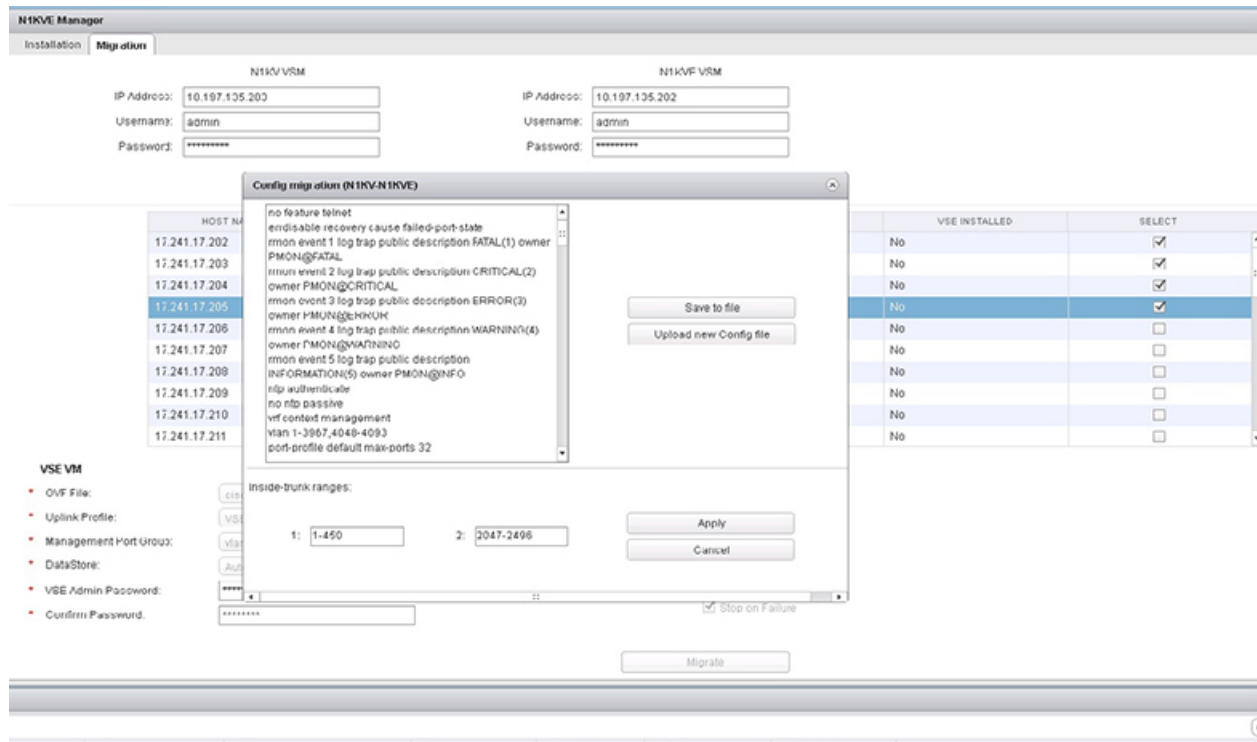
- NIKV VSM
  - IP address: IP address of NIKV VSM
  - Username: User name for NIKV VSM
  - Password: Password for NIKV VSM
- NIKVE VSM
  - IP address: IP address of NIKVE VSM
  - Username: User name for NIKVE VSM
  - Password: Password for NIKVE VSM

**Step 5** Click **Connect**. All the hosts attached to legacy N1KV that are eligible for migration are listed on the **Migration** tab.



- Step 6** Select a host to migrate. Choose a maximum of 4 hosts for migration at a time.
- Step 7** Select the Nexus 1000VE VSE OVF file from the **OVF File** drop-down list.
- Step 8** Select a port profile to migrate from the **Uplink Port Profile** drop-down list.
- Step 9** Select a management port group from the **Management Port Group** drop-down list.
- Step 10** Select deployment location for the Nexus 1000VE VSE from the **DataStore** drop-down list. If you select **Auto**, location for VSE VM is chosen randomly by the VMware vCenter.
- Step 11** Enter a new password and confirm the password in the **VSE Admin Password** and **Confirm Password** text-fields.
- Step 12** Select applicable port channel type configured in the Nexus 1000V under **External VDS**.
- Step 13** Select **Migrate Config** option. You must select this option while migrating hosts for the first time. For the subsequent host migrations to Cisco Nexus 1000VE, select this option if you want to migrate the latest configuration from the Cisco Nexus 1000V VSM.
- Step 14** Ensure that the **Stop on Failure** option is selected.
- Step 15** Click **Migrate** to initiate the migration process.
- Step 16** Click **Yes** in the **Migrate Configuration** dialog box.
- Step 17** The **Config Migration** dialog box appears with filtered configurations from the Cisco Nexus 1000V VSM instance. Edit the vservice node ip address of each VSG configured to reflect the new VSGs deployed. If adjacency I2 configuration is present, replace it with adjacency I3. To prevent migration of the port-profiles that belong to VEM VMKernel adapters, remove the port-profiles from the list.

Figure 4: N1kVE Manager



**Note** You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Config migration from N1kV to N1kVE) in the Recent Tasks tab.

- Step 18** (Optional) If you want to save this configuration for future reference, click **Save** to file.
- Step 19** (Optional) To select a different configuration (text file format only), click **Upload new Config file**.
- Step 20** Under **Inside-trunk ranges** section, the two text fields show the range of ports required (Calculated dynamically by the tool for each cluster). You can change these ranges.
- Step 21** Click **Apply** to start the migration process.
- Step 22** Once the configuration migration is completed, a new dialog box appears for host migration. Click **Yes** in the **Migrate Host to N1kVE** dialog box. The migration process starts. You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Migration from N1kV to N1kVE) in the Recent Tasks tab.
- Step 23** Once the migration is successful, upgrade **Cisco PNSC** to version 3.5.1a.
- Step 24** Check the status of VEM using the **vem status** command on the ESXi host.

**Example:**

```
[root@localhost:~] vem status
```

```
VEM modules are loaded
```

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
vSwitch0	5012	44	128	1500	vmnic4
DVS Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
NG-vsm-231	5012	15	1024	9000	
DVS Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
n1kve-outside-vds-DC-2	5012	8	512	1500	vmnic6,vmnic5



VEM Agent (vemdpa) is running

**Step 25** If the VEM is in running state, stop the VEM process using the **vem stop** command or **kill** command.

**Example:**

```
[root@localhost:~] vem stop
stopDpa
VEM SWiSCSI is already stopped
Terminating DPA watchdog and DPA (PID 74416 74657 74658)
watchdog-vemdpa: Terminating watchdog process with PID 74408
[root@localhost:~]
```

**Step 26** Remove the VIB using the **esxcli software vib remove --vibName=vib name --maintenance-mode** command.

**Example:**

```
[root@localhost:~] esxcli software vib list | grep cisco
cisco-vem-v522-esx 5.2.1.3.4.1a.0-6.5.1 Cisco PartnerSupported
2019-05-17
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli software vib remove --vibName=cisco-vem-v522-esx --maintenance-mode
Removal Result
 Message: Operation finished successfully.
 Reboot Required: false
 VIBs Installed:
 VIBs Removed: Cisco_bootbank_cisco-vem-v522-esx_5.2.1.3.4.1a.0-6.5.1
 VIBs Skipped:
[root@localhost:~]
```

---

On successful migration, Cisco PNSC is attached to Cisco Nexus 1000VE VSM and Cisco VSG.




---

**Note** All the VM information on PNSC is lost during the migration process and traffic loss occurs for rules with VM attributes. To restore the traffic, you need to upgrade PNSC to 3.5.1a and re-register the VSM and VSG PAs after the migration process is completed.

---

## Verifying vService Nodes

Log into Cisco Nexus 1000VE VSM and verify that the vService nodes are in **Alive** state.

---

Log in to Cisco Nexus 1000VE VSM and use **show vservice node brief** and **ping vservice node** commands to verify that the vservice nodes are in **Alive** state.

**Example:**

```
NG_VSM# sh vservice node brief

 Node Information

ID Name Type IP-Address Mode MTU State Module
1 VSG_T1 vsg 192.168.163.240 13 NA Alive 3,4,5,

NG_VSM#
NG_VSM#
```

```

NG_VSM# ping vservice node all src-module all
ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=0 timeout=1-sec
 module(usec) : 3(284) 4(579) 5(527)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=1 timeout=1-sec
 module(usec) : 3(415) 4(628) 5(676)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=2 timeout=1-sec
 module(usec) : 3(400) 4(580) 5(693)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=3 timeout=1-sec
 module(usec) : 3(478) 4(556) 5(553)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=4 timeout=1-sec
 module(usec) : 3(384) 4(540) 5(664)

NG_VSM#

```

---

## Upgrading PNSC

You need to upgrade PNSC after you have migrated PNSC from Nexus 1000V environment to Nexus 1000VE environment.

### Before you begin

- You are logged in to the CLI in EXEC mode.
  - You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
  - You must have the Cisco PNSC Release 3.5.1a downloaded.
- 

- Step 1** `nsc# connect local-mgmt`  
Places you in local management mode.
- Step 2** (Optional) `nsc (local-mgmt)# show version`  
Displays the version information for the Cisco PNSC software.
- Step 3** (Optional) `nsc (local-mgmt)# copy scp://user@example-server-ip/example-dir/filename bootflash:/`  
Copies the Cisco PNSC software file to the VM.
- Step 4** `nsc (local-mgmt)# dir bootflash:/`  
Verifies that the desired file is copied in the directory.
- Step 5** `nsc (local-mgmt)# update bootflash:/filename`  
Begins the update of the Cisco PNSC software.
- Step 6** (Optional) `nsc (local-mgmt)# service status`  
Allows you to verify that the server is operating as desired.
- Step 7** (Optional) `nsc (local-mgmt)# show version`

Allows you to verify that the Cisco PNSC software version is updated.

**Note** After you upgrade to Cisco PNSC Release 3.5.1a, you might see the previous version of Cisco PNSC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

**Note** For detailed information about Upgrading PNSC, see [Upgrading Prime Network Services Controller](#).

### Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco PNSC:

```
nsc(local-mgmt)# show version

Name Package Version GUI

core Base System 3.4(2d) 3.4(2d) service-reg
Service Registry 3.4(2d) 3.4(2d) policy-mgr
Policy Manager 3.4(2d) 3.4(2d) resource-mgr
Resource Manager 3.4(2d) 3.4(2d) vm-mgr
VM manager 3.4(2d) none vsm-service
VSM Service 3.4(2d) none cloudprovider-mgr
Cloud Provider Mgr 3.4(2d) none
localhost(local-mgmt)#
```

The following example shows how to copy the Cisco PNSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.5.1a.bin bootflash:/
Enter password:
100% 143MB 11.9MB/s 00:12
```

The following example shows how to see the directory information for Cisco PNSC:

```
nsc(local-mgmt)# dir bootflash:/

1.1G Dec 05 00:57 nsc.3.5.1a.bin

Usage for bootflash://

6359716 KB used
10889320 KB free
18187836 KB total
```

The following example shows how to start the update for the Cisco PNSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.5.1a.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
Press enter to continue or Ctrl-c to exit.
```

## Verifying Cisco PNSC Upgrade

After migrating and upgrading Cisco PNSC in Cisco Nexus 1000VE environment, you can verify whether the PNSC upgrade was successful.

To verify the latest PNSC version, use the **show version** command.

### Example:

```
localhost# show version
```

Name	Package	Version	GUI
core	Base System	3.5(1a)	3.5(1a)
service-reg	Service Registry	3.5(1a)	3.5(1a)
policy-mgr	Policy Manager	3.5(1a)	3.5(1a)
resource-mgr	Resource Manager	3.5(1a)	3.5(1a)
vm-mgr	VM manager	3.5(1a)	none
vsm-service	VSM Service	3.5(1a)	none
cloudprovider-mgr	Cloud Provider Mgr	3.5(1a)	none

```
localhost#
```

## Re-registering Cisco Nexus 1000VE VSM PA AND VSG PA

You need to re-register Cisco Nexus 1000VE VSM PA and Cisco VSG PA to restore the traffic

**Step 1** Log in to Cisco Nexus 1000VE VSM and re-register the VSM PA.

### Example:

```
NG_VSM# conf
Enter configuration commands, one per line. End with CNTL/Z.
NG_VSM(config)# nsc-policy-agent
NG_VSM(config-nsc-policy-agent)# no policy-agent-image
NG_VSM(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.3a.bin
NG_VSM(config-nsc-policy-agent)# end
NG_VSM# copy r s
[#####] 100%
Copy complete, now saving to disk (please wait)...
NG_VSM#
```

**Step 2** Verify whether the VSM PA registration process was successful.

### Example:

```
NG_VSM # sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
NG_VSM#
```

**Step 3** Log in to Cisco VSG and re-register the VSG PA.

### Example:

```

firewall# conf
WARNING: This device is managed by Prime Network Services Controller. Changing configuration using
CLI is not recommended.
firewall(config)# nsc-policy-agent
firewall(config-nsc-policy-agent)# no policy-agent-image
firewall(config-nsc-policy-agent)# policy-agent-image bootflash:nsc-vsgpa.2.1.3i.bin
firewall(config-nsc-policy-agent)# end
firewall# copy r s
[#####] 100%
Copy complete, now saving to disk (please wait)...
firewall#

```

**Step 4** Verify whether the VSG PA registration process was successful.

**Example:**

```

firewall# sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
firewall#

```

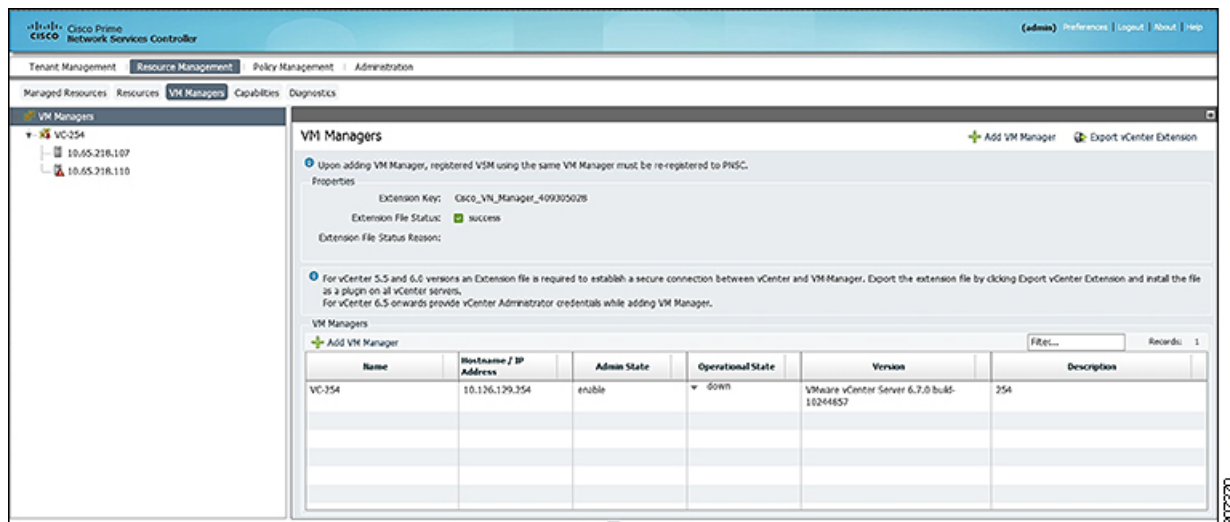
## Registering PNSC with VMware vCenter Version 6.7(U1)

Cisco PNSC is currently not supported on VMware vCenter version 6.7(U1). To enable support for Cisco PNSC on VMware vCenter version 6.7(U1), complete these steps:

**Step 1** Log into Cisco Prime Network Services Controller.

**Step 2** Click **Resource Management > VM Managers**.

**Figure 5: Cisco Prime Network Services Controller - Resource Management**



**Step 3** In the **VM Managers** pane, click **Export vCenter Extension** to create a VMware vCenter configuration backup.

**Step 4** In the **Save As** dialog box, navigate to the location where you want to save the configuration backup file and click **Save** to save the backup file in XML file format.

**Step 5** Open the configuration backup file using an XML editor.

**Step 6** Locate the **Key** tag in the backup file and copy the **Key** tag content. For example, Cisco\_VN\_Manager\_1935748790.

**Figure 6: Configuration Backup XML**



```

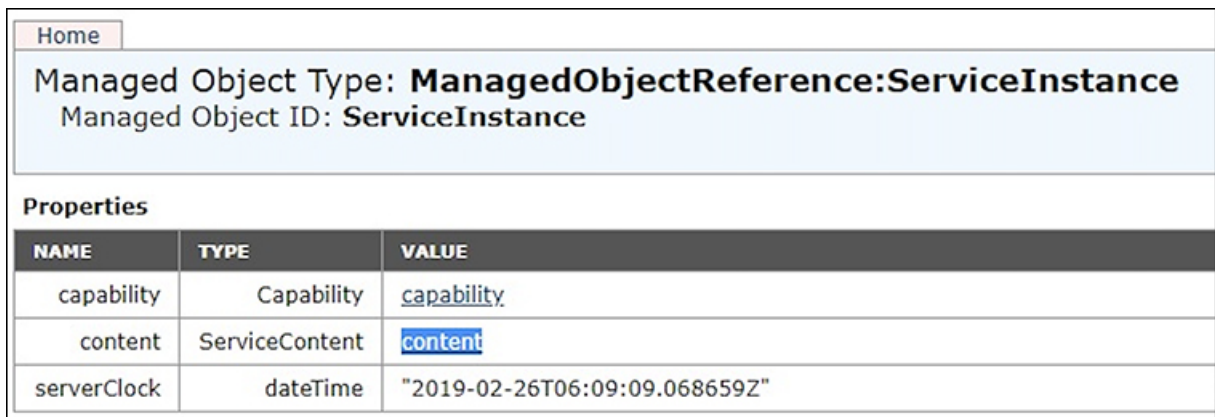
1 <extensionData>
2 <obj xmlns="urn:vim25" versionId="uber" xsi:type="Extension" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3 <description>
4 <label></label>
5 <summary></summary>
6 </description>
7 <key>Cisco_VN_Manager_409305028</key>
8 <version>1.0.0</version>
9 <subjectName>/CN=localhost.localdomain</subjectName>
10 <server>
11 <url></url>
12 <description>
13 <label></label>
14 <summary></summary>
15 </description>
16 <company>Cisco Systems Inc.</company>

```

**Step 7** Log into VMware vCenter Managed Objects page with vCenter IP address using Google Chrome. For example, [http://<vCenter\\_IP\\_Address>/mob](http://<vCenter_IP_Address>/mob).

**Step 8** In the VMware vCenter Managed Objects page, Click **Content** under the **Properties** section.

**Figure 7: VMware vCenter Managed Objects**

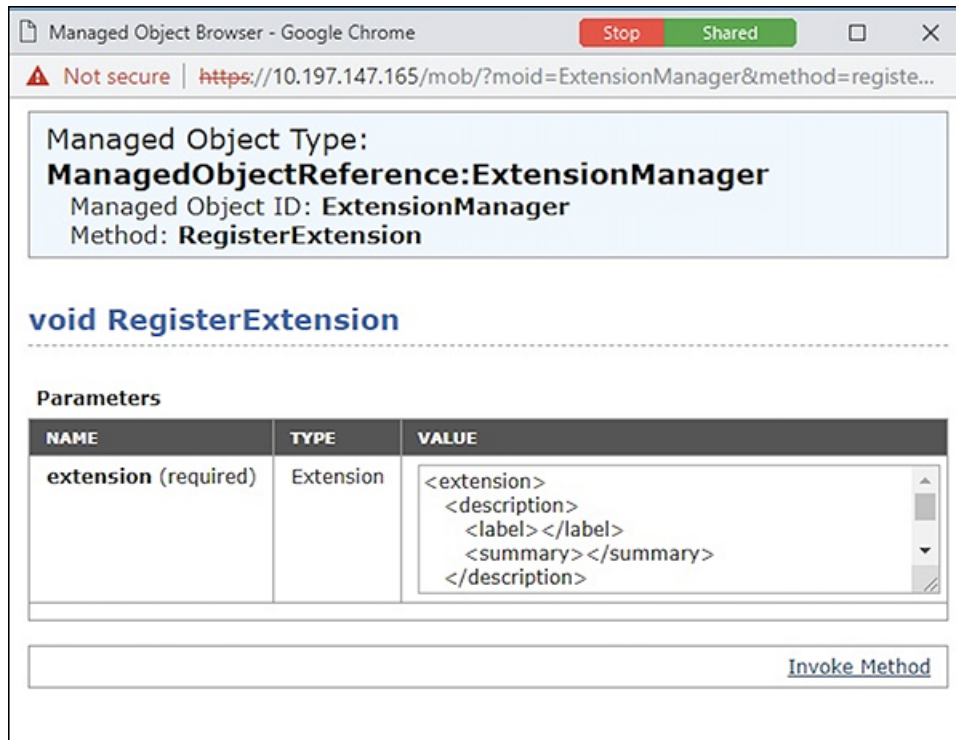


Home		
Managed Object Type: <b>ManagedObjectReference:ServiceInstance</b>		
Managed Object ID: <b>ServiceInstance</b>		
Properties		
NAME	TYPE	VALUE
capability	Capability	<a href="#">capability</a>
content	ServiceContent	<a href="#">content</a>
serverClock	dateTime	"2019-02-26T06:09:09.068659Z"

**Step 9** In the **ServiceContent** page, under the **Properties** section, click **ExtensionManager**.

**Step 10** In the **ManagedObjectReference: ExtensionManager** page, under the **Methods** section, click **RegisterExtension**.

Figure 8: Managed Object Browser



307374

- Step 11** In the **Managed Object Browser** dialog box, replace the content in **VALUE** text-field with the content listed below and replace the content for Key tag with the value copied from the configuration backup file.

**Example:**

```
<extension>
 <description>
 <label></label>
 <summary></summary>
 </description>
 <key>Cisco_VN_Manager_1935748790</key>
 <company></company>
 <type></type>
 <version>1.0.0</version>
 <subjectName></subjectName>
 <server>
 <url></url>
 <description>
 <label></label>
 <summary></summary>
 </description>
 <company></company>
 <type></type>
 <adminEmail>string</adminEmail>
 <serverThumbprint></serverThumbprint>
 </server>
 <client>
 <version>1.0.0</version>
 <description>
 <label></label>
 <summary></summary>
 </description>
```

```

 <company></company>
 <type></type>
 <url></url>
 </client>
 <resourceList>
 <locale></locale>
 <module></module>
 <data>
 <key></key>
 <value></value>
 </data>
 </resourceList>
 <lastHeartbeatTime>1970-01-01T00:00:00Z</lastHeartbeatTime>
 <healthInfo>
 <url></url>
 </healthInfo>
 <extendedProductInfo>
 </extendedProductInfo>
 <shownInSolutionManager>>false</shownInSolutionManager>
</extension>

```

**Step 12** Click **Invoke Method**. Ensure that the **Method Invocation Result** is void.

**Step 13** Close the **Managed Object Browser** dialog box.

**Step 14** Under the **Methods** section, click **SetExtensionCertificate**.

**Step 15** In the new dialog box, complete the following steps to configure certificate information:

- Enter the key value, the key copied from the configuration backup file, for **extensionKey** field. For example, Cisco\_VN\_Manager\_1935748790.
- Copy the certificate information from the configuration backup file. Ensure that all the content including the content for begin certificate and end certificate is copied.

**Example:**

```

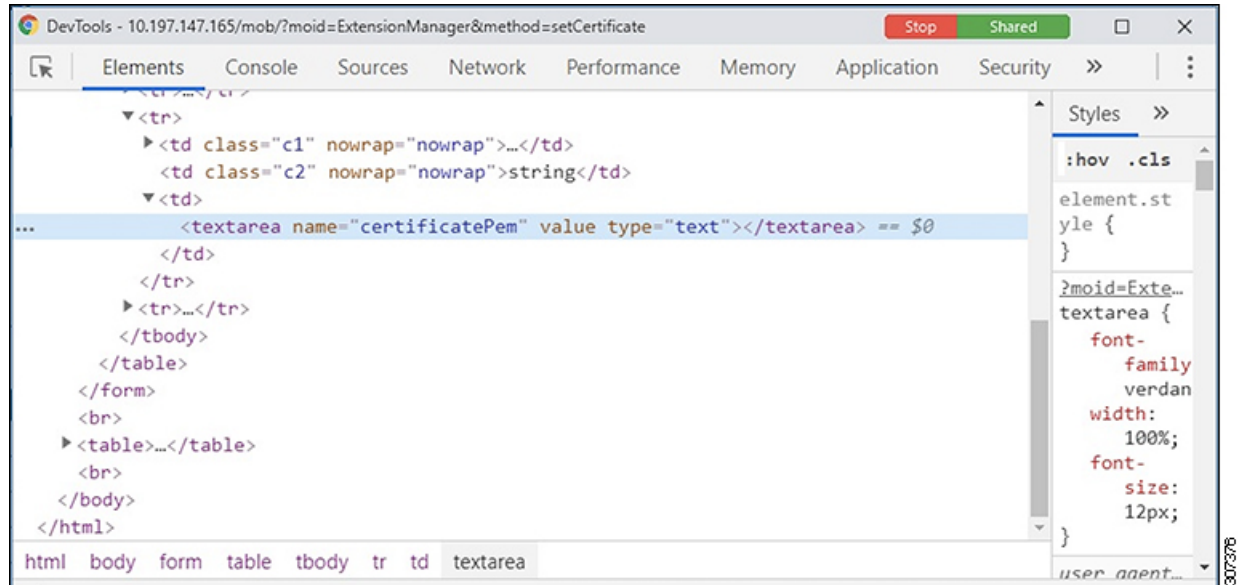
-----BEGIN CERTIFICATE-----
MIIDRTCAi2gAwIBAgIJALzYESXqSzCiMA0GCSqGSIb3DQEBBQUAMCAxHjAcBgNV
BAMTFWxvY2FsaG9zdC5sb2NhbGRvbWVpbjAeFw0xOTAzMTUwMzQ1MTFaFw0yOTAz
MTIwMzQ1MTFaMCAxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWVpbjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANEvtFkU1VyIlo1ze4U+Z+KHDx/p
qC2gz1jcuYi4YOWL4AkWjo11ur6mfM8Pro7YID9DgB2Yq9KQrSVBTheJAjytrie3
GGeHJc6Y/S9U/P9i4qIs2aswg3ZiFqEB/qb1ghbMRSbmdLFqLmrd141LjL85NA/f
Fpf3V0K+trx0ZKmQluYealGjB+mUgzHRUK0OhWqenF+BgsMxTz0yPFqhcFYFvrki
gQw00LRu5CpgreN044QOmeGD9BpMy0021N9Y/d7tAjKjTXUoSwc45Ynvg/eD4028
T8cX912+NNsd8WtFtv97Jmk4UoEmK2IYpk0k+vBjdyovvh/LsBfVSxXqUMUCAwEA
AaOBgTB/MB0GA1UdDgQWBBSHJohMLfT2hzAfMnKjSZAKLZAATzBQBGNVHSMESTBH
gBShJohMLfT2hzAfMnKjSZAKLZAAT6EkpCIwIDEeMBwGA1UEAxMVbG9jYWxob3N0
LmxxvY2FsZG9tYXlucG9tYXlucG9tYXlucG9tYXlucG9tYXlucG9tYXlucG9tYXluc
AQUFAAOCAQEAL8JdJZbWcIvqR/05sgCCbtMcg8RTMYto9x28f5muxrYadu46sFv/
Zo7ae/ZmcTC5mqWZiis4vmPB1hdwFrFCLX64saTMFydETOehLsKsQ2+2JWL5squx
u0FXWoQrlznnr7FF2WNshhHmgQSUN3F5a21U/57jp5d1fyyiF0vJzC7FrYSWU0F6
n4TqJ39vCgRwwWDH9VEaJM92HgiKUSHQ+zLzSoKkPYFz3mqZNKIHY1Eum6Fy5neB
yxMYfGyV+sJDwgd7rgCpQvY5rhx1csRQWqSqeFHAzG30Lx7HO0r0rRHqx4BK601o
9UOZtzJq53gplcetN7e2n+uRG2GE9ukDPA==
-----END CERTIFICATE-----

```

- The default form has a one line input field for **certificatePem**, you need to change this into a multiline field. Right-click the field for **certificatePem** and from the pop-up menu, select **Inspect** to open the **DevTools** Google Chrome window.
- In the **DevTools** window, change the table data (<td>) type from input to textarea. Close the **DevTools** window.



Figure 9: DevTools Utility for Google Chrome



- e) In the **Managed Object Browser** dialog box, paste the certificate information in the **certificatePem** text area.
- f) Close the dialog box to complete the PNSC registration with VMware vCenter.





## CHAPTER 4

# Upgrading the Cisco Nexus 1000V

---

This chapter contains the following sections:

- [Pre-requisites and Usage Guidelines, on page 53](#)
- [Upgrading Nexus 1000VE Virtual Supervisor Module, on page 53](#)
- [Upgrading VMWare vCenter Server, on page 55](#)
- [Upgrading Cisco Nexus 1000VE Manager vCenter Plugin, on page 56](#)
- [Upgrading VMware ESXi Hosts, on page 60](#)

## Pre-requisites and Usage Guidelines

Follow these prerequisites and usage guidelines before upgrading Cisco Nexus 1000VE from Release 5.2(1)SV5(1.1) to 5.2(1)SV5(1.2):

- Ensure that the current Nexus 1000VE, release 5.2(1)SV5(1.1) instance is up and running in the existing setup.
- Cisco Nexus 1000VE release 5.2(1)SV5(1.2) 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.
- In-Service Software Upgrade (ISSU) is not supported while upgrading to Cisco Nexus 1000VE release 5.2(1)SV5(1.2). There is service disruption during upgrade process. Make sure that you have sufficient maintenance window before proceeding with the upgrade process.

## Upgrading Nexus 1000VE Virtual Supervisor Module

To upgrade Cisco Nexus 1000VE Virtual Supervisor Module (VSM), complete the following steps in sequence:

- 
- Step 1** Log into Cisco.com, and navigate to [Software download](#) page.
  - Step 2** Download and copy the kickstart image (n1000v-dk9-kickstart.5.2.1.SV5.1.2.bin) and system image (n1000v-dk9.5.2.1.SV5.1.2.bin) to VSM `bootflash:` directory.
  - Step 3** Log into Nexus 1000VE switch with administrator credentials.
  - Step 4** Set the boot variable for VSM in global configuration mode.

**Note** You may ignore the warning messages while changing the boot parameters to new version.

**Example:**

```
N1KVE-VSM#
N1KVE-VSM#terminal monitor
N1KVE-VSM#configure terminal
N1KVE-VSM(config)#boot kickstart bootflash:n1000v-dk9-kickstart.5.2.1.SV5.1.2.bin
Performing image verification and compatibility check, please wait.
Note: system and kickstart bootvars are pointing to incompatible images

N1KVE-VSM(config)# boot system bootflash:n1000v-dk9.5.2.1.SV5.1.2.bin
Performing image verification and compatibility check, please wait.

N1KVE-VSM(config)#end
N1KVE-VSM#copy running-config startup-config
```

**Note** For VSM HA setup, wait for approximately 5 minutes for the new kickstart and system images to copy to the standby VSM automatically.

**Step 5** Reload the configuration with updates using the **reload** command.

**Example:**

```
N1KVE-VSM# reload
```

**Note** It takes few minutes for VSM to reload with the updated Cisco Nexus 1000VE 5.2(1)SV5(1.2) version.

**Step 6** Verify the VSM upgrade in the configuration using the **show** commands.

**Example:**

```
N1KVE-VSM# show version | include version
kickstart: version 5.2(1)SV5(1.2)
system: version 5.2(1)SV5(1.2)

N1KVE-VSM# show module 1-2
Mod Ports Module-Type Model Status

1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby

Mod Sw Hw

1 5.2(1)SV5(1.2) 0.0
2 5.2(1)SV5(1.2) 0.0

Mod Server-IP Server-UUID Server-Name

1 XXX.XXX.XXX.XXX NA NA
2 XXX.XXX.XXX.XXX NA NA

Mod VSE-IP Host-IP

* this terminal session

N1KVE-VSM# show svcs connections

connection XXXX_XXXX:
hostname: -
ip address: XXX.XXX.XXX.XXX
ipv6 address: -
```

```

remote port: 80
transport type: ipv4
vrf: management
protocol: vmware-vim https
certificate: default
datacenter name: XXX
admin:
max-ports: 12000
extension key: any
DVS uuid: xx xx xx xx xx xx xx xx-xx xx xx xx xx xx xx xx
dvs version: 5.0.0
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 6.5.0 build-xxxxxxx
vc-uuid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
ssl-cert: self-signed or not authenticated

```

## Upgrading VMWare vCenter Server

Complete these steps to upgrade VMware vCenter Server to v6.7 version:

- Step 1** 1. Change the default DVS version on Cisco N1KVE VSM before upgrading vCenter. Use the **vmware dvs-version dvs\_value** command to change the default DVS version:

**Example:**

```

N1KVE-VSM#terminal monitor
N1KVE-VSM#configure terminal
N1KVE-VSM(config)#svs connection connection-name
N1KVE-VSM(config)#vmware dvs-version 6.0.0
N1KVE-VSM(config)#no connect
N1KVE-VSM(config)#connect
N1KVE-VSM(config)#end
N1KVE-VSM#show svs connection
connection XXXX_XXXX:
hostname: -
ip address: XXX.XXX.XXX.XXX
ipv6 address: -
remote port: 80
transport type: ipv4
vrf: management
protocol: vmware-vim https
certificate: default
datacenter name: XXX
admin:
max-ports: 12000
extension key: any
DVS uuid: xx xx xx xx xx xx xx xx-xx xx xx xx xx xx xx xx
dvs version: 6.0.0
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 6.5.0 build-70242859
vc-uuid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
ssl-cert: self-signed or not authenticated

```

**Step 2** Upgrade VMware vCenter to version 6.7. For more information, refer to [VMware documentation](#).

**Step 3** Verify whether the svcs connection is established with the upgraded VMware vCenter on Cisco Nexus 1000VE VSM. Use the **svcs connection** and **svcs domain** commands.

**Example:**

```
N1KVE-VSM#show svcs connection

connection XXXX_XXXX:
hostname: -
ip address: XXX.XXX.XXX.XXX
ipv6 address: -
remote port: 80
transport type: ipv4
vrf: management
protocol: vmware-vim https
certificate: default
datacenter name: XXX
admin:
max-ports: 12000
extension key: any
DVS uuid: xx xx xx xx xx xx xx xx-xx xx xx xx xx xx xx xx
dvs version: 6.0.0
config status: Enabled
operational status: Connected
sync status: Complete
version: VMware vCenter Server 6.7.0 build-10244857
vc-uuid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
ssl-cert: self-signed or not authenticated
```

**Step 4** If the SVCS connection is not in a connected state, Use the **no connect** and **connect** command to establish connection with upgraded VMware vCenter.

**Example:**

```
N1KVE-VSM# no connect
N1KVE-VSM# connect
```

## Upgrading Cisco Nexus 1000VE Manager vCenter Plugin

Before you begin upgrading Cisco Nexus 1000VE Manager vCenter plugin, ensure that you have:

- Downloaded and installed the Cisco N1KVE Plugin installation script (`deploy_n1kve_plugin_v2.py`) and Cisco N1KVE Plugin (`n1kve-vcenter-plugin-1.0.2.zip`) from Nexus 1000VE VSM (<https://<VSM-IP>>).

You can install the Cisco Nexus 1000VE Manager vCenter plugin using two methods:

- Upgrading VSE using Cisco Nexus 1000VE Manager vCenter Plugin
- Manually Upgrading VSE



**Note** You may choose one of the methods to upgrade VSEs. However, we recommend to use the first method, Cisco Nexus 1000VE Manager vCenter Plugin to upgrade VSEs.

## 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(1.2) is installed on vCenter.

- 
- Step 1** Download the new VSE images, cisco-vse-5.2.1.SV5.1.2.ovf and cisco-vse-5.2.1.SV5.1.2-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:
- 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
  - Click **Next**.
  - On the **Configure content library** page, verify that the default option, Local content library is selected.
  - Click **Next**.
  - On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.
  - Click **Next**.
  - On the **Ready to complete** page, click **Finish**.
  - On the **Navigator** tab, select the new content library that you just created.
  - On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box.
  - 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**.
  - In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.
  - On the **Select referenced files** dialog box, click **Ok**.
  - On the **New Content Library – Import Library Item** dialog-box, click **Ok**.
  - 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(1.2) 0.0
2 5.2(1)SV5(1.2) 0.0
5 5.2(1)SV5(1.2) NA
6 5.2(1)SV5(1.2) 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.

- Step 1** Download the new VSE image, cisco-vse-5.2.1.SV5.1.2.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:
- Browse over **Hosts and Clusters** tab and Select a Host.
  - Select the VSE Virtual Machine, under the Host. Typically the VSE VMs are named as "N1KVE\_VSE\_<HOST\_IP\_ADDRESS>".
  - Right-click the VSE and select to **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** 4. 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 entry of VSE.

**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.SV5.1.2.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 svcs 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 IP static IP setting.
  - Network 1 Netmas : Subnet mask for VSE adapter.
  - Uplink Port-profile: Provide the outside-trunk. Use the show running-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(1.2) 0.0
2 5.2(1)SV5(1.2) 0.0
5 5.2(1)SV5(1.2) NA
6 5.2(1)SV5(1.2) 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 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/>