Installing the Cisco Nexus 1000VE Software

This chapter contains the following sections:

Supported VMware vSphere ESXi Hypervisor Versions

Cisco Nexus 1000VE supports the following VMware vSphere ESXi Hypervisor 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 7 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 7 to reserve CPU and set the CPU reservation.

VSM Prerequisites

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

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

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

Table 2: HA Roles

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

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

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

VSE Prerequisites

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

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

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

Upstream Switch Prerequisites

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

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

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

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

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

end
```

Guidelines and Limitations for Installing the Cisco Nexus 1000VE

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

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

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

  The VSM reboot is based on the following conditions:

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

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

     - If both VSMs have the same number of modules, the software makes a selection that is based on the VC connectivity status.

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

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

     - If both VSMs have the same number of modules and no VC connectivity, the VSM with the latest configuration remains active and the other VSM is rebooted.
  4. Last active VSM
     - If the previous three conditions are not met, the VSM that became active most recently is rebooted.

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

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

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 1.
- 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)# svs connection vcenter65   // SVS Connection Name
N1KV-NG(config-svs-conn)# remote ip address 10.29.176.180 // vCenter IP Address
N1KV-NG(config-svs-conn)# vmware dvs datacenter-name TME-POD2 // Datacenter Name
N1KV-NG(config-svs-conn)# protocol vmware-vim
```

```
N1KV-NG(config-svs-conn)# register-plugin remote username administrator@vsphere.local
password Cisco123@ // vCenter administrator credentials
N1KV-NG(config-svs-conn)# connect
N1KV-NG(config-svs-conn)# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
N1KV-NG(config-svs-conn)# exit
N1KV-NG(config-svs)
```

Note The 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.