Installing the Cisco Prime Network Services Controller

This chapter contains the following sections:

Information About the Cisco Prime NSC

The Cisco Prime Network Services Controller (Cisco PNSC) is a virtual appliance that provides centralized device and security policy management for Cisco virtual services. Designed to support enterprise and multiple-tenant cloud deployments, the Cisco PNSC provides transparent, seamless, and scalable management for securing virtualized data center and cloud environments.

Installation Requirements

Cisco Prime NSC System Requirements

Requirement	Description
Virtual Appliance	
Four virtual CPUs	1.8 GHz each
Memory	Minimum 4 GB RAM, recommended 4 GB RAM
Disk space	Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: • Disk 1: 20 GB • Disk 2: 20 GB

Requirement	Description
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor
Microsoft Hyper-V	
Microsoft SCVMM 2016 R2	
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Any of the following: • Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 9.0 • Mozilla Firefox 23.0 • Chrome 29.0 **Note** If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco PNSC.
Flash Player	Adobe Flash Player plugin (Version 11.2 or higher)

Note	Before you can use Chrome with Prime NSC 3.2, you must first disable the Adobe Flash Players that are installed by default with Chrome.

Firewall Ports Requiring Access

Requirement	Description
80	HTTP/TCP
443	HTTP
843	TCP

Cisco Nexus 1000V Series Switch Requirements

Requirement	Notes
General	
The procedures in this guide assume that the Cisco Nexus 1000V Series switch is up and running, and that endpoint Virtual Machines (VMs) are installed.	—
Port Profiles	
One port profile configured on the Cisco Nexus 1000V Series Switch for the service VLAN.	—

Information Required for Installation and Configuration

Information Type	Your Information
For Deploying the Cisco PNSC ISO	
Name	
ISO file location	
Storage location	
Management port profile name for VM management **Note** The management port profile is the same port profile that is used for VSM. The port profile is configured in VSM and is used for the Cisco PNSC management interface.	

Information Type	Your Information
IP address	
Subnet mask	
Gateway IP address	
Domain name	
DNS server	
Admin password	
Shared secret password for communications between the Cisco PNSC, Cisco VSG, and VSM.	
For Configuring Microsoft Hyper-V in Cisco PNSC	
HyperV name	
Description	
Hostname or IP address	

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication. Passwords are designated strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between the Cisco PNSC, Cisco VSG, and VSM, adhere to the following criteria for setting valid, strong passwords:

Do not include the following items in passwords:

- Characters: & ' " ` ( ) < > | \ ; $

- Spaces

Create strong passwords based on the characteristics in this table:

Table 1: Characteristics of Strong Passwords

Strong passwords have...	Strong passwords do not have...
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive characters, such as *abcd*. • Characters repeated three or more times, such as *aaabbb*. • A variation of the word Cisco, such as *cisco*, *ocsic*, or one that changes the capitalization of letters in the word *Cisco*. • The username or the username in reverse. • A permutation of characters present in the username or *Cisco*.

Examples of strong passwords are:

- If2CoM18

- 2004AsdfLkj30

- Cb1955S21

Microsoft Hyper-V Server Requirement

You must set the clock to the correct time on all the Microsoft Hyper-V servers that will run Cisco PNSC, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco PNSC CA certificate that is created when the Cisco PNSC VM is deployed might have an invalid time stamp.

After you set the clock to the correct time on all the Hyper-V servers that run the Cisco PNSC, you can, as an option, set the clock on the Cisco PNSC as follows:

- If you set the clock manually, be sure to enter the correct time zone as a Coordinated Universal Time (UTC) offset.

- If you set the clock by synchronizing with the Network Time Protocol (NTP), you can select the UTC time zone.

Installing Cisco Prime NSC

Before you begin

- Verify that the Hyper-V host on which to deploy the Cisco PNSC VM is available in SCVMM.

- Copy the Cisco PNSC ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose **Library > Library Servers**, right-click the library location, and then refresh.

- Set your keyboard to United State English before installing the Cisco PNSC and using the VM console.

• There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

Step 1 Launch the SCVMM.

Step 2 Choose the Hyper-V host on which to deploy the Cisco PNSC VM.

Step 3 Right-click the Hyper-V host and choose **Create Virtual Machine**.

Step 4 In the **Create Virtual Machine** wizard, from the **Select Source** screen, choose the **Create the new virtual machine with a blank virtual hard disk** radio button, then click **Next.**

Step 5 In the **Specify Virtual Machine Identity** screen, provide the required information, then click **Next.**

Step 6 In the **Configure Hardware** screen, do the following:

   a) From General, do the following:

      • Choose **Processor** and choose the number of processors.

      • Choose **Memory** and choose the required memory value. You will need a minimum 4 GB of memory for Prime NSC.

   b) From **Bus Configuration > IDE Devices**, do the following:

      • Choose **Hard Disk**, enter the required size of the hard disk. You will need a minimum of 20 GB of hard disk.

      • Choose **Virtual DVD Drive**, check the **Existing ISO image file** radio button, and browse to choose theCisco PNSC 3.4 ISO image file.

   c) Choose **Network Adapters > Network Adapter 1**, check the **Connect to a VM Network** radio button, and browse to choose a VM Network.

   d) Click **Next.**

Step 7 In the **Select Destination** screen, do the following:

   a) Check the **Place the virtual machine on a host** radio button.

   b) Choose **All hosts** from the **Destination** drop-down list.

   c) Click **Next.**

Step 8 In the **Select Host** screen, choose the destination, then click **Next.**

Step 9 In the **Configure Settings** screen, review the virtual machine settings, then click **Next.**

Step 10 In the **Add properties** screen, choose the **Red Hat Enterprise Linux 5 (64 bit)** operating system, then click **Next.**

Step 11 In the **Summary** screen, do the following:

   a) Verify the settings.

   b) Check the **Start the virtual machine after deploying it** check box.

   c) Click **Create.**

   The job Create virtual machine starts. You can see the status of this job in The Recent Jobs window. Ensure that the job completes without any errors.

Step 12 After the virtual machine is successfully created, right-click the new Virtual Machine (vnmc21-perf in this case) and choose **Connect or View > Connect Via Console**.

Step 13 Launch the console and install Cisco PNSC.

Note   Before the final Cisco PNSC installation step, before you reboot, launch Microsoft SCVMM again, right-click the Virtual machine (vnmc21-hyperv in this case), and choose **Properties > Hardware Configuration > Bus Configuration > Virtual DVD Drive > no media** so that Cisco PNSC does not use the ISO image at boot time.

Step 14   After Cisco PNSC is successfully deployed, click **Close** and power on the Cisco PNSC VM.