Installing Cisco Prime Network Services Controller

This chapter contains the following sections:

Information About the Cisco Prime NSC

The Cisco Prime Network Services Controller (Cisco Prime NSC) 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 Prime NSC 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	1.5 GHz for each virtual CPU
Memory	4 GB RAM

Requirement	Description
Disk Space	One of the following, depending on InterCloud functionality: • With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows: ◦ Disk 1: 20 GB ◦ Disk 2: 200 GB • 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
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix **Note** You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php.
VMware	
VMware vSphere	ESXi 5.0, 5.1, and 5.5
VMware vCenter	Release 5.5 (5.1 vCenter supports host version upto 5.1)
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: • Microsoft Windows • Apple Mac OS
Browser	Any of the following browsers: • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher **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 Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco Prime NSC, on page 5.
Flash Player	Adobe Flash Player plugin 11.2 or higher

Firewall Ports Requiring Access

Requirement	Description
80	HTTP/TCP
443	HTTPS
843	Adobe Flash

Information Required for Installation and Configuration

Information Type	Your Information
For Deploying the Cisco Prime NSC OVA	
Name	
Location of files	
Datastore location	
Storage location, if more than one location is available	
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 Prime NSC management interface.	
IP address	
Subnet mask	
Gateway IP address	
Domain name	
DNS server	
NTP server	
Admin password	
Shared secret password for communications between the Cisco Prime NSC, Cisco VSG, and VSM.	
For Configuring VMware vCenter in Cisco Prime NSC	
vCenter 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 Prime NSC, 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 following characteristics:

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

Configuring Chrome for Use with Cisco Prime NSC

To use Chrome with Cisco Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome.

Note You must perform this procedure each time your client machine reboots. Chrome automatically enables the Adobe Flash Players when the system on which it is running reboots.

Step 1 In the Chrome URL field, enter chrome://plugins.

Step 2 Click **Details**.

Step 3 Locate the Adobe Flash Player plugins, and disable each one.

Step 4 Download and install Adobe Flash Player version 11.6.602.180.

Step 5 Close and reopen Chrome before logging into the Cisco Prime NSC

ESXi Server Requirement

You must set the clock to the correct time on all ESXi servers that will run Cisco Prime NSC, ASA 1000V instances, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco Prime NSC CA certificate that is created when the Cisco Prime NSC VM is deployed might have an invalid time stamp. An invalid time stamp can prevent you from successfully registering ASA 1000V instances to the Cisco Prime NSC.

After you set the clock to the correct time on all ESXi servers that run the Cisco Prime NSC, you can, as an option, set the clock on the Cisco Prime NSC 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

You can deploy the Cisco Prime NSC OVA, resulting in a Cisco Prime NSC VM.

Before You Begin

- Set your keyboard to United States English before installing the Cisco Prime NSC and using the VM console.
- Verify that the Cisco Prime NSC OVA image is available in the vSphere client.
- Make sure that all system requirements are met as recommended in Cisco Prime NSC System Requirements, on page 1.
- Make sure you have the information identified as in Information Required for Installation and Configuration.

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

Step 1 Use the VMware vSphere Client to log into the vCenter server.

Step 2 Choose the host on which to deploy the Cisco Prime NSC VM.

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

Step 4 In the **Source** window, choose the Cisco Prime NSC OVA, then click **Next**.

Step 5 In the **OVF Template Details** window, review the details of the Cisco Prime NSC template, and then click **Next**.

Step 6 In the **End User License Agreement** window, click **Accept** after reviewing the End User License Agreement, and then click **Next**.

Step 7 In the **Name and Location** window, provide the required information, and then click **Next**.
The name can contain up to 80 characters and must be unique within the inventory folder.

Step 8 In the **Deployment Configuration** window, choose **Installer** from the Configuration drop-down list, then click **Next**.

Step 9 In the **Datastore** window, select the data store for the VM, and then click **Next**.

Note The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN). If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.

Step 10 In the **Disk Format** window, click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks, and then click **Next**.
The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

Step 11 In the **Network Mapping** window, select the management network port group for the VM, then click **Next**.

Step 12 In the **Properties** window, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.

Note You can safely ignore the Cisco Prime NSC Restore fields.

Note For choosing the shared secret password, follow the guidelines given in Shared Secret Password Criteria, on page 5.

Step 13 In the **Ready to Complete** window, review the deployment settings information, and then click **Finish**.

Caution Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information.

A progress indicator shows the task progress until Cisco Prime NSC is deployed.

Step 14 After Cisco Prime NSC is successfully deployed, click **Close**.