Installation Prerequisites

The following sections describe the requirements for installing Cisco Prime Network Services Controller (Prime Network Services Controller) 3.0:

New and Changed Information

The following table describes information that has been added or changed since the initial release of this document.

Date	Revision	Location
February 14, 2014	Updated disk space requirements.	System Requirements, on page 2
	Updated information for upgrading from VNMC 2.1.	Upgrading to Prime Network Services Controller 3.0

System Requirements

Requirement	Description
Virtual Appliance	
Two Virtual CPUs	1.5 GHz
Memory	4 GB RAM

Disk Space	One of the following, depending on InterCloud functionality:
	
	• With InterCloud functionality, 220 GB on shared NFS or 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
VMware	
VMware vSphere	Release 5.x with VMware ESX or ESXi (English Only)
VMware vCenter	Release 5.x (English Only)
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	Either of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 9.0 or higher • Mozilla Firefox 11.0 or higher • Google Chrome 18.0 or higher[1]
Flash Player	Adobe Flash Player plugin 11.2 or higher

1 Before using Chrome with Prime Network Services Controller 3.0, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Prime Network Services Controller, on page 6.

Firewall Ports Requiring Access

The following Prime Network Services Controller ports require access.

Port	Description
80	HTTP
443	HTTPS
843	Adobe Flash

Ports to Access Amazon AWS

This table lists the port numbers you must enable to access the Amazon Web Services (AWS) public IP ranges listed at https://forums.aws.amazon.com/ann.jspa?annID=1701.

Protocol	Ports
TCP	22, 443, 3389, 6644, and 6646

Protocol	Ports
UDP	6644 and 6646

Cisco Nexus 1000V Series Switch Requirements

Requirement	Notes
General	
The procedures in this guide assume that the Cisco Nexus 1000V Series Switch (Nexus 1000V) is up and running, and that virtual machines (VMs) are installed.	—
VLANs	
Two VLANs configured on the Nexus 1000V uplink ports: • Service VLAN • HA VLAN	Neither VLAN needs to be the system VLAN.
Port Profiles	
One port profile configured on the Nexus 1000V for the service VLAN.	—

Information Required for Installation and Configuration

Required Information	Your Information
For Deploying the Prime Network Services Controller OVA	
Name	
Location of files	
Data store location	
Storage location, if more than one location is available	

Required Information	Your Information
Management port profile name for VM (Virtual Machine) management **Note** The management port profile is the same port profile that is used for the Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and is used for the Prime Network Services Controller management interface.	
IP Address	
Subnet Mask	
Gateway IP Address	
Domain Name	
DNS Server **Note** Access to a DNS server is required for Prime Network Services Controller to communicate with the Amazon Cloud Provider.	
Admin Password	
Shared secret password for communications between Prime Network Services Controller, Cisco Virtual Security Gateway (VSG), Cisco Adaptive Security Appliance 1000V (ASA 1000V), and VSM. (See Shared Secret Password Criteria, on page 5.)	
For Configuring VMware vCenter in Prime Network Services Controller	
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 channel. Passwords are designated as strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between Prime Network Services Controller, VSG, ASA 1000V, and VSM, adhere to the following criteria for setting valid, strong passwords:

- Do not include the following items in passwords:
    - These characters: & ' " ` ( ) < > | \ ; $

◦ Spaces

- Make sure your password contains the characteristics of strong passwords as described in the following table.

Strong passwords have:	Strong passwords do not have:
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive alphanumeric characters, such as abcd or 123. • 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 Prime Network Services Controller

To use Chrome with Prime Network Services Controller 3.0, 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.

Procedure

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 in to Prime Network Services Controller.