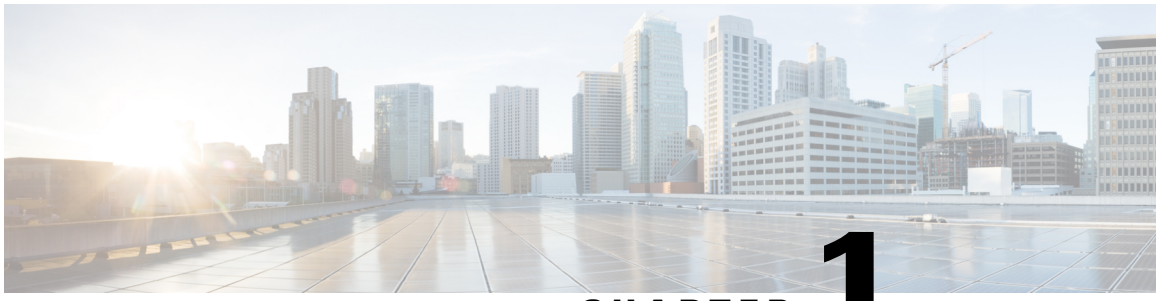
Cisco Prime Network Services Controller 3.4 Installation Guide

First Published: December 10, 2014

Last Modified: July 27, 2016

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

Installation Overview

This section contains the following topics:

Prime Network Services Controller Overview

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. Cisco Prime Network Services Controller simplifies operations with centralized, automated multidevice and policy management for Cisco network virtual services. For the latest Prime Network Services Controller release updates and overview, see the corresponding Prime Network Services Controller data sheet.

Cisco Prime Network Services Controller (Prime Network Services Controller) is the primary management element for Cisco Nexus 1000V (Nexus 1000V) switches and services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multitenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. Prime Network Services Controller is built on an information-model architecture in which each managed device is represented by its subcomponents (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall virtual security services.

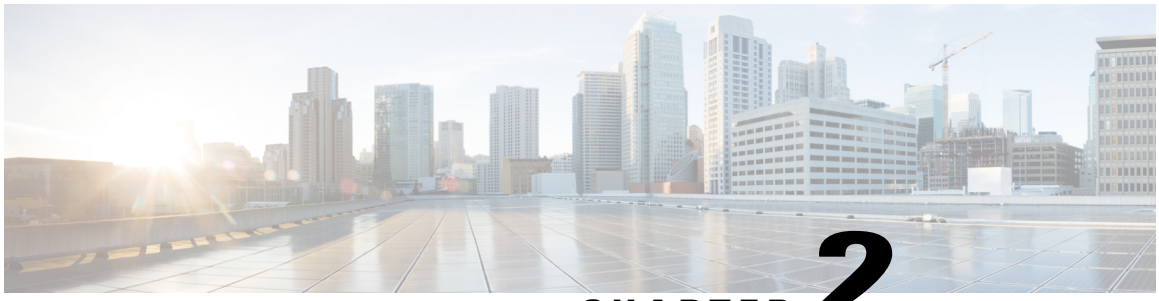
In addition, Prime Network Services Controller supports Cisco Cloud Services Router 1000V (CSR 1000V) edge routers, and Citrix NetScaler 1000V and Citrix NetScaler VPX load balancers. This combination of virtual services brings numerous possibilities to customers, enabling them to build virtual data centers with all of the required components to provide best-in-class cloud services.

Features and Benefits

The following table lists the features and benefits of using Prime Network Services Controller. For the latest Prime Network Services Controller release description and overview, see the latest Prime Network Services Controller data sheet and Release Notes.

Features	Description	Benefits
Multiple-Device Management	Prime Network Services Controller provides central management of installed VMs (edge routers, edge firewalls, compute firewalls, and load balancers) and Nexus 1000V.	Simplifies provisioning and troubleshooting in a scaled-out data center.
Load Balancing Profiles	An application network profile represents load balancer server farms and related features and attributes.	Simplifies provisioning, reduces administrative errors during load balancing policy changes, reduces audit complexities, and helps enable a highly scale-out data center environment.
Routing Profiles	A network profile represents edge router routing policies and related features and attributes.	Simplifies provisioning, reduces administrative errors during routing policy changes, reduces audit complexities, and helps enable a highly scale-out data center environment.
Security Profiles	A security profile represents the VSG or ASA 1000V security policy configuration in a profile (template).	Simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and helps enable a highly scaled-out data center environment.
Stateless Device Provisioning	The management agents in VSG and ASA 1000V are stateless, receiving information from Prime Network Services Controller.	• Enhances scalability. • Provides robust endpoint failure recovery without loss of configuration state.
Security Policy Management	Security policies are authored, edited, and provisioned centrally.	• Simplifies operation and management of security policies. • Helps ensure that security intent is accurately represented in the associated security policies.

Features	Description	Benefits
Context-Aware Security Policies	Prime Network Services Controller obtains virtual machine contexts from VMware vCenter.	Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure.
Support virtual services for DFA environments	Cisco Prime NSC obtains tenant information and allows virtual services to be added to DFA virtual overlay networks.	—
Dynamic Security Policy and Zone Provisioning	Prime Network Services Controller interacts with the Nexus 1000V VSM to bind the security profile to the corresponding Nexus 1000V port profile. When virtual machines are dynamically instantiated by server administrators and appropriate port profiles applied, their association with trust zones is also established.	Helps enable security profiles to stay aligned with rapid changes in the virtual data center.
Multi-Tenant (Scale-Out) Management	Prime Network Services Controller is designed to manage VSG and ASA 1000V security policies in a dense multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies.	Reduces administrative errors, helps ensure segregation of duties in administrative teams, and simplifies audit procedures.
Role-Based Access Control (RBAC)	RBAC simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures.	• Reduces administrative errors. • Enables detailed control of user privileges. • Simplifies auditing requirements.
XML-Based API	Prime Network Services Controller XML API allows external system management and orchestration tools to programmatically provision VSG and ASA 1000V.	• Allows the use of the best-in-class management software. • Offers transparent and scalable operation management.



CHAPTER 2

Installation Requirements

This section contains the following topics:

Requirements Overview

The following topics identify the primary requirements for installing and using Prime Network Services Controller.

System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 GB
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
Prime Network Services Controller Device Adapter	
Two virtual CPUs	1.8 GHz
Memory	2 GB RAM
Disk space	20 GB
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

Prime Network Services Controller is a multi-hypervisor virtual appliance that can be deployed on VMware vSphere, OpenStack KVM Hypervisor, or Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor).

- See the VMware Compatibility Guide to confirm that VMware supports your hardware platform.

- See the Windows Server Catalog to confirm that Microsoft Hyper-V supports your hardware platform.
- See the following links to confirm that OpenStack KVM supports your hardware platform:
  - OpenStack Compute and Image System Requirements
  - OpenStack for Cisco DFA Install Guide for Using the Cisco OpenStack Installer

Requirement	Description
VMware	
VMware vSphere	5.1, 5.5, and 6.0 with VMware ESXi (English only)
VMware vCenter	5.1, 5.5, and 6.0 (English only)
OpenStack KVM	
KVM Hypervisor	Ubuntu 12.04 LTS server, 64-bit
KVM Kernel	Version 3.2.0-52-generic
Cisco OpenStack Installer	Havana (Standalone mode only) Prime Network Services Controller 3.4 does not support Orchestrator mode.
Microsoft	
Microsoft Server	Microsoft Hyper-V Server 2012 R2 (Standard or Data Center)
Microsoft System Center Virtual Machine Manager (SCVMM)	Microsoft SCVMM 2012 R2

Note Prime Network Services Controller running as a virtual machine with version 3.4.1b and later can be hosted on VMware vSphere ESXi 6.0 hosts that are managed by VMware vCenter Server 6.0.

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Either of the following: • Microsoft Windows • Apple Mac OS

Requirement	Description
Browser	Any of the following: • Google Chrome 32.0 or later (recommended)[1] • Internet Explorer 10.0 or later • Mozilla Firefox 26.0 or later
Flash player	Adobe Flash Player plugin 11.9 or later

1 Before using Chrome with Prime Network Services Controller, you must disable Adobe Flash Player plugins that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Prime Network Services Controller, on page 11.

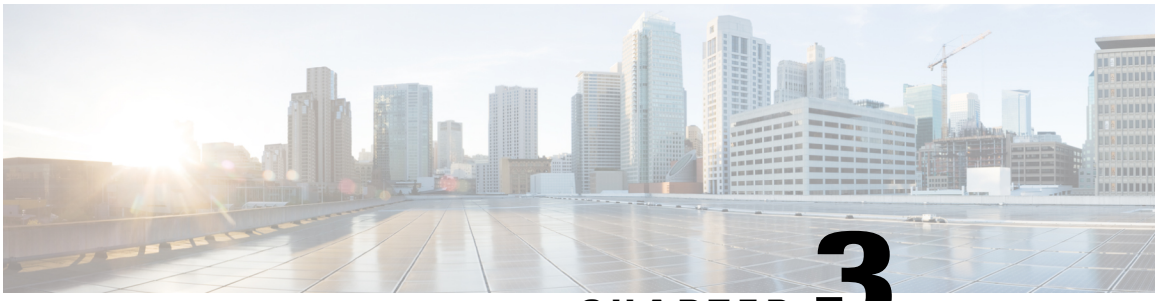
Firewall Ports Requiring Access

If Prime Network Services Controller is protected by a firewall, the following ports on the firewall must be open so that clients can contact Prime Network Services Controller.

Port	Description
22	TCP
80	HTTP
443	HTTPS
843	Adobe Flash

Cisco Nexus 1000V Series Switch Requirements

Category	Requirement
General	The Cisco Nexus 1000V Series Switch is operational and that virtual machines (VMs) are installed.
VLANs	The following VLANs are configured on the Cisco Nexus 1000V uplink ports: • Service VLAN • HA VLAN Neither VLAN needs to be the system VLAN.
Port profiles	One port profile is configured on the Cisco Nexus 1000V for the service VLAN.



CHAPTER 3

Preparing for the Installation

This section includes the following topics:

Information Required for Configuration and Installation

Before installation, collect the following information:

Required Information	Your Information/Notes
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management [2]	
VM / Instance name	
KVM flavor name	
KVM Instance Security Group	
VMware datastore location	
For Prime Network Services Controller Installation	

Required Information	Your Information/Notes
IP address For OpenStack environments, use the IP address that is assigned to the Prime Network Services Controller instance in OpenStack.	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria, on page 10.)	

2 The management port profile is the same port profile that is used for Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and used for the Prime Network Services Controller management interface.

Shared Secret Password Criteria

A shared secret password is a password that is known to only 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 special characters or spaces.
- Make sure your password contains the characteristics of strong passwords and avoids the characteristics of weak passwords as described in the following table:

Strong Passwords	Weak Passwords
• At least eight characters. • Contain characters from at least three of the following classes: lowercase letters, uppercase letters, and numbers.	• 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
- Es1955Ap

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.

Note Because Chrome automatically enables Adobe Flash Player plugins each time the system reboots, you must perform this procedure each time your client machine reboots.

Procedure

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

Step 2 Click **Details** to expand all the files associated with each plugin.

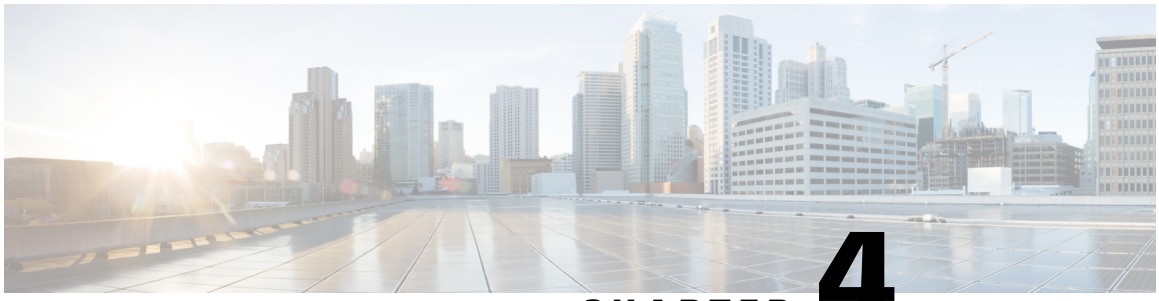
Step 3 Locate the Adobe Flash Player plugins, and disable each one.

Step 4 Download and install Adobe Flash Player plugin version 11.9 or higher.

Step 5 Close and reopen Chrome before logging in to Prime Network Services Controller.

PART I

Installing Prime Network Services Controller in VMware Environments



CHAPTER 4

Installing Prime Network Services Controller in VMware Environments

This section includes the following topics:

VMware Installation Overview

You can install Prime Network Services Controller on VMware by using either an ISO or an OVA image. The installation time varies from 10 to 20 minutes, depending on the host and the storage area network load.

To install Prime Network Services Controller on VMware, complete the following tasks:

Task	Comments
1. Configuring VMware for Prime Network Services Controller, on page 18	Required for ISO installations only.
2. Installing Prime Network Services Controller	Use the procedure appropriate for your environment: • Installing Prime Network Services Controller Using the ISO Image, on page 19 • Installing Prime Network Services Controller Using the OVA Image
3. Performing VMware Post-Installation Tasks	Required for all installations.

Installing Prime Network Services Controller Using the OVA Image

This procedure describes how to deploy the Prime Network Services Controller OVA image on VMware.

Before You Begin

- Set your keyboard to United States English.
- Confirm that the Prime Network Services Controller OVA image is available from the VMware vSphere Client.
- Make sure that all system requirements are met.
- Gather the information identified in Information Required for Configuration and Installation, on page 9.

Procedure

Step 1 Using the VMware vSphere Client, log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller VM.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the wizard, provide the information as described in the following table:

Screen	Action
Source	Choose the Prime Network Services Controller OVA.
OVF Template Details	Review the details.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Enter a name and choose a location for the template.
Deployment Configuration	Choose **Installer**.
Datastore	Select the data store for the VM. The storage can be local or shared remote, such as NFS or SAN.
Disk Format	Choose either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks.
Network Mapping	Choose the management network port group for the VM.
Properties Address any errors that are indicated in red colored text below a selection box. You can enter placeholder information as long as your entry meets the field requirements.	
A. IP Address	VM management IP address.

Screen	Action
B. IP Netmask	VM subnet mask.
C. Gateway	Gateway IP address.
D. DNS	• VM hostname • VM domain • DNS server IP address
E. NTP	NTP server IP address.
F. Operation Mode	• Standalone—Operates as a standalone VM. • Orchestrator—Integrates through an orchestrator with a northbound application. **Note** Prime Network Services Controller 3.4 does not support Orchestrator mode.
G. Passwords	• Administrator password • Shared secret password
H. Restore	You can safely ignore the Restore fields.
Ready to Complete	Review the deployment settings. **Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information for accuracy.

Step 5 Click **Finish**.
A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 7 Power on the Prime Network Services Controller VM.

Installing Prime Network Services Controller Using an ISO Image

To install Prime Network Services Controller in a VMware environment using an ISO image, complete the tasks described in the following topics:

1 Configuring VMware for Prime Network Services Controller, on page 18

2 Installing Prime Network Services Controller Using the ISO Image, on page 19

Configuring VMware for Prime Network Services Controller

Before you install Prime Network Services Controller on VMware using an ISO image, you must configure a VM for Prime Network Services Controller. This procedure describes how to configure the VM so that you can install Prime Network Services Controller on it.

Before You Begin

- Confirm that the system requirements have been met (see Requirements Overview, on page 5).
- Gather the information required for configuration as identified in Information Required for Configuration and Installation, on page 9.

Procedure

Step 1 Download a Prime Network Services Controller ISO image to your client machine.

Step 2 Open the VMware vSphere Client.

Step 3 Right-click the host on which to install the ISO image, and then choose **New Virtual Machine**.

Step 4 Create a new VM by providing the information as described in the following table:

Screen	Action
Configuration	Choose **Custom**.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the data store.
Virtual Machine Version	Choose **Version 8**.
Guest Operating System	Choose **Linux** and **Red Hat Enterprise Linux 5 (64-bit)**.
CPUs	Set the number of virtual sockets to **4**.
Memory	Set the memory to **4 GB**.
Network	**1** Set the number of NICs to **1**. A single NIC is required for Prime Network Services Controller. **2** Choose a NIC. **3** From the Adapter drop-down list, choose **E1000**. Prime Network Services Controller supports only E1000 adapters.
SCSI Controller	Choose **LSI Logic Parallel**.
Select a Disk	Choose **Create a new virtual disk**.

Screen	Action
Create a Disk	1 Disk Size—Enter a minimum of 20 GB. 2 Disk Provisioning—Choose **Thin Provision** or **Thick Provision**. 3 Location—Specify the location of the data store.
Advanced Options	Specify options as needed.

Step 5 In the Ready to Complete screen, review the information for accuracy, check the **Edit the Virtual Machine Settings Before Completion** check box, and then click **Continue**.

Step 6 In the Virtual Machine Properties dialog box in the Hardware tab, do the following:

a) Click **Memory** and in the Memory Size field, choose **4 GB**.
b) Click **CPUs** and in the Number of Virtual Sockets field, choose **4**.
c) Click **New Hard Disk** and then click **Add** to create a new hard disk. The disk requires a minimum of 20 GB.
d) After you supply the information in the Add Hardware Wizard, click **Finish** to create the new disk and to return to the Virtual Machine Properties dialog box.

Step 7 In the **Options** tab, choose **Boot Options**, check the **Force BIOS Setup** checkbox, and then click **Finish**.

Step 8 After the new VM is created, power it on.

Step 9 Mount the ISO to the VM CD ROM drive as follows:

a) Right-click the VM and choose **Open Console**.
b) From the VM console, click **Connect/Disconnect the CD/DVD Devices of the virtual machine**.
c) Choose **CD/DVD Drive 1**.
d) Choose **Connect to ISO Image on Local Disk**.
e) Choose the ISO image that you downloaded in Step 1.

What to Do Next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller Using the ISO Image, on page 19.

Installing Prime Network Services Controller Using the ISO Image

This procedure describes how to install the ISO image on a VM that has been configured for Prime Network Services Controller.

Before You Begin

Confirm the following items:

- All system requirements are met.
- You have the information identified in Information Required for Configuration and Installation, on page 9.

- You have configured the hypervisor for the Prime Network Services Controller installation procedure.
- A VM has been created for Prime Network Services Controller and has network access.
- You can access the VM console.

Procedure

Step 1 Open the VM console if it is not already open.
If you have just finished configuring the hypervisor, the Prime Network Services Controller installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Prime Network Services Controller VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Prime Network Services Controller is available in Standalone mode only.
- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore a previous Prime Network Services Controller installation.

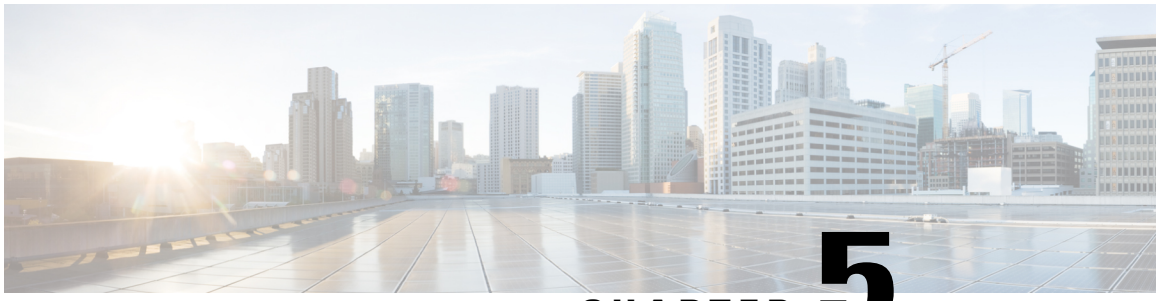
Step 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria, on page 10.

Note If you configure a weak shared secret password, no error message is generated during entry here, but the shared secret password is not usable when the VM is started during the installation process.

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**.
Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**.
Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.



CHAPTER 5

Performing VMware Post-Installation Tasks

This section contains the following topics:

Configuring NTP

Before performing any operations on the Prime Network Services Controller system, configure Network Time Protocol (NTP) on any of the following deployed VMs and Prime Network Services Controller:

- ASA 1000V
- Citrix NetScaler 1000V
- Citrix NetScaler VPX
- CSR 1000V
- VSG
- VSM

If you do not configure these items with NTP, they will not register with Prime Network Services Controller.

For information on configuring NTP, see the following topics:

- Configuring NTP on VMs, on page 21
- Configuring NTP in Prime Network Services Controller, on page 22

Configuring NTP on VMs

Configure NTP on VMs by using the information in the following table.

For this VM:	Do this:
ASA 1000V	(VMware only) Before you install ASA 1000V in Prime Network Services Controller, configure NTP on all ESX and ESXi servers that run ASA 1000V. For information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi hosts using the vSphere Client" at kb.vmware.com/kb/2012069. After installation, the ASA 1000V receives the Real Time Clock (RTC) value from the VMware ESX or ESXi host.
Citrix NetScaler 1000V	For information on setting NTP on Citrix NetScaler 1000V, see the Citrix NetScaler documentation.
Citrix NetScaler VPX	For information on setting NTP on Citrix NetScaler 1000V, see the Citrix NetScaler documentation.
CSR 1000V	For information on setting NTP on CSR 1000V, see the CSR 1000V documentation.
VSG	Configure the NTP server in the Prime Network Services Controller GUI as described in the Prime Network Services Controller User Guide, section "Configuring NTP."

VSM	Enter the following CLI command from the VSM console, where *x.x.x.x* is the NTP server IP address:
	`clock timezone zone-name offset-hours offset-minutes`
	`clock summer-time zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes`
	`ntp server x.x.x.x`

Configuring NTP in Prime Network Services Controller

Use this procedure to configure NTP in Prime Network Services Controller.

Procedure

Step 1 In your browser, enter **https://***ip-address* where *ip-address* is the Prime Network Services Controller IP address.

Step 2 In the Prime Network Services Controller login window, enter the username **admin** and the admin user password. This is the password that you set when installing Prime Network Services Controller.

Step 3 Set the time zone by doing the following:

a) Choose **Administration > System Profile > root > Profile > default** and click **Edit**.

b) In the General tab, choose the time zone in which the Prime Network Services Controller server resides.

c) Click **Save**.

Step 4 Add an external NTP server as the time source, as follows:

a) Choose **Administration > System Profile > root > Profile > default** and click **Edit**.
b) In the Policy tab, click **Add NTP Server**.
c) Enter the NTP server hostname or IP address and click **OK**.
d) Click **Save**.

Caution We recommend that you do not set the time zone after you add the NTP server.

Configuring Connectivity with VMware vCenter

After installing Prime Network Services Controller, configure Prime Network Services Controller so that it can communicate with the Virtual Machine Manager (VMM) for that hypervisor and the VMs that Prime Network Services Controller will manage. Prime Network Services Controller communicates with the VMM to perform the following actions on the VMs that it manages:

- Obtain the VM attributes that Prime Network Services Controller uses for VM management.
- Instantiate, start, stop, restart, or delete VMs.
- Map VM network interfaces.
- Instantiate and configure services on service VMs.

Establish connectivity between Prime Network Services Controller and VMware vCenter by performing the following tasks:

1 Exporting the vCenter Extension File, on page 23
2 Registering the vCenter Extension Plugin in vCenter, on page 24
3 Configuring Connectivity with vCenter, on page 24

Exporting the vCenter Extension File

The first step in configuring connectivity with VMware vCenter is exporting the vCenter extension file.

Before You Begin

If you use Internet Explorer, do one of the following to ensure that you can download the extension file:

- Open Internet Explorer in Administrator mode.
- After starting Internet Explorer, choose **Tools > Internet Options > Security**, and uncheck the **Enable Protected Mode** check box.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > VM Managers > VM Managers**.

Step 2 In the VM Managers pane, click **Export vCenter Extension**.

Step 3 Save the vCenter extension file in a directory that the vSphere Client can access because you will need to register the vCenter extension plug-in from within the vSphere Client (see Registering the vCenter Extension Plugin in vCenter, on page 24).

Step 4 Open the XML extension file to confirm that the content is available.

Registering the vCenter Extension Plugin in vCenter

Register the vCenter extension plugin so that you can create a VMM. The VMM enables Prime Network Services Controller to communicate with vCenter and the VMs that Prime Network Services Controller manages.

Procedure

Step 1 Log in to the VMware vSphere Client server with the VMs that Prime Network Services Controller will manage.

Step 2 In the vSphere Client, choose **Plug-ins > Manage Plug-ins**.

Step 3 Right-click the window background and choose **New Plug-in**.

Tip Scroll down and right-click near the bottom of the window to view the New Plug-in option.

Step 4 Browse to the vCenter extension file that you previously exported and click **Register Plug-in**.
The vCenter Register Plug-in window appears, displaying a security warning.

Step 5 In the security warning message box, click **Ignore**.

Note If desired, you can install this certificate for further integration with Public Key Infrastructure (PKI) and Kerberos facilities.

A progress indicator shows the task status.

Step 6 When the success message is displayed, click **OK**, and then click **Close**.

Configuring Connectivity with vCenter

After registering the vCenter extension plug-in with vCenter, configure Prime Network Services Controller so that it can communicate with the VMM for the hypervisor and the VMs that Prime Network Services Controller will manage.

Procedure

Step 1 Choose **Resource Management > VM Managers > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, enter the following information and then click **OK**:

- Name—VMM name.
- Description—VMM description.
- Hostname / IP Address—Hostname or IP address of the VMM.
- Port Number—Port number to use for communications.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- VMware vCenter version.

Enabling Enhanced Scale for Managing Protected VMs Only

By default, Prime Network Services Controller discovers all VMs on Nexus 1000V switches whether or not a tenant or another organization is configured on the VM vNIC. This procedure describes how to configure Prime Network Services Controller so that it discovers *only* those VMs with a tenant or another organization configured on a vNIC.

Note If you enable this option, VMs that are protected but powered off will not be managed by Prime Network Services Controller.

Before You Begin

Obtain the Prime Network Services Controller debug plugin nsc-dplug.3.4.*n.x*.bin. If you need assistance in locating this file, contact the Cisco Technical Assistance Center.

You can contact the TAC over the phone or via the Web:

- Regional phone numbers are available at http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html#numbers.
- To use the Web, go to http://www.cisco.com/cisco/web/support/index.html.

Procedure

Step 1 Install the Prime Network Services Controller debug plugin and access the root shell.
For information on installing the debug plugin, contact the Cisco TAC.

Step 2 In the root shell, do the following:

a) Using SSH, connect to Prime Network Services Controller and log in as the admin user.

b) Enter the following commands:

```
# connect local-mgmt
(local-mgmt)# update bootflash:/nsc-dplug.x.x.x.x.bin
(local-mgmt)# run sudo bash
```

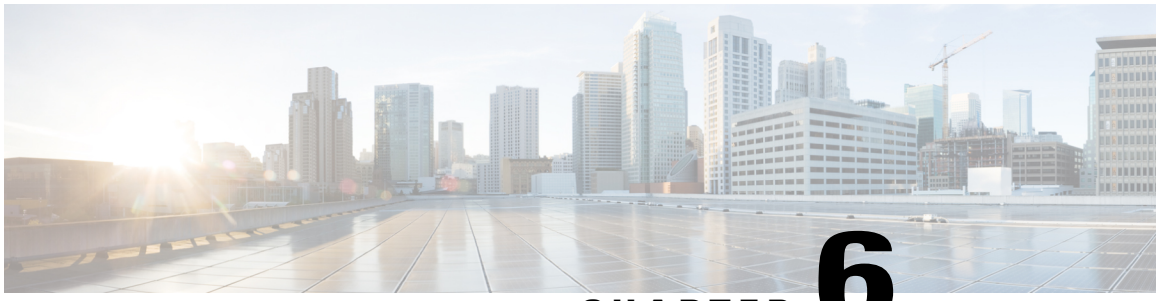
Step 3 Using a vi editor, open /opt/cisco/sam.config for editing.

Step 4 In the custom section of the file, add the following entry:

```
skipNonTenantVms=true
```

Step 5 Save the file and exit the editor.

Step 6 Enter **exit** and then enter **service restart**.



CHAPTER 6

Registering Service VMs Installed on VMware

This section contains the following topics:

Registering Service VMs on VMware

Registering service VMs with Prime Network Services Controller ensures that Prime Network Services Controller recognizes and can communicate with the VMs.

The following topics describe how to register Cisco and third-party VMs that are deployed on VMware with Prime Network Services Controller:

- For Cisco service VMs, see Registering Cisco VMs Deployed on VMware, on page 27.
- For third-party service VMs, see Registering Third-Party VMs in VMware, on page 28.

Registering Cisco VMs Deployed on VMware

This procedure describes how to register ASA 1000V and VSM VMs that have been installed directly on the hypervisor. Cisco VMs that are instantiated on a hypervisor through Prime Network Services Controller are automatically registered with Prime Network Services Controller upon instantiation.

You do not need to register a VSG that is installed directly on the hypervisor. The deployment procedure automatically registers the VM with Prime Network Services Controller.

Before You Begin

- Configure NTP on the required hypervisor.
- Install the required Cisco VMs on the hypervisor.

- Confirm that each Cisco VM is deployed and powered on.
- Make sure that a network path exists between each VM management IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 In the hypervisor, navigate to the VM to be registered with Prime Network Services Controller.

Step 2 Open a console window for the VM.

Step 3 In the CLI, register the VM as follows:

- ASA 1000V

```
enable
Password:
vm-name# configure terminal
vm-name(config)# vnmc policy-agent
vm-name(config-vnmc-policy-agent)# registration host n.n.n.n
vm-name(config-vnmc-policy-agent)# shared-secret MySharedSecret
vm-name(config-vnmc-policy-agent)# copy running-config startup-config
```

- VSM (Version 5.2(1)SV3(1.1) and higher)

```
vm-name# configure terminal
vm-name(config)# nsc-policy-agent
vm-name(config-nsc-policy-agent)# registration-ip n.n.n.n
vm-name(config-nsc-policy-agent)# shared-secret MySharedSecret
vm-name(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.n.n.n.bin
vm-name(config-nsc-policy-agent)# copy running-config startup-config
```

- VSM (Versions prior to 5.2(1)SV3(1.1))

```
vm-name# configure
vm-name(config)# vnm-policy-agent
vm-name(config-vnm-policy-agent)# registration-ip n.n.n.n
vm-name(config-vnm-policy-agent)# shared-secret MySharedSecret
vm-name(config-vnm-policy-agent)# policy-agent-image bootflash:
vnmc-vsgpa.n.n.n.bin
vm-name(config-vnm-policy-agent)# copy running-config startup-config
```

Registering Third-Party VMs in VMware

To register third-party VMs in Prime Network Services Controller, install the Prime Network Services Controller Device Adapter before deploying and registering the third-party VMs.

The following table identifies the tasks and related topics for deploying a Citrix NetScaler load balancer on VMware and registering the load balancer with Prime Network Services Controller:

Task	Comments
1. Install Prime Network Services Controller Device Adapter.	See Deploying the Prime Network Services Controller Device Adapter on VMware, on page 29.
2. (Optional) Configure licensing for the Citrix NetScaler load balancer.	See Configuring Load Balancer Licenses, on page 31.
3. Deploy a Citrix NetScaler load balancer.	Deploy the Citrix NetScaler load balancer VM in VMware. For more information, see the following URLs: • Citrix product documentation at http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html. • Citrix licensing information at http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10-1/ns-initial-config-using-ftu-wizard-tsk.html.
4. Register the Citrix NetScaler load balancer with Prime Network Services Controller.	See Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller, on page 33.

Deploying the Prime Network Services Controller Device Adapter on VMware

The Prime Network Services Controller Device Adapter enables third-party VMs (such as Citrix NetScaler load balancers) to register with Prime Network Services Controller.

This procedure installs the Prime Network Services Controller Device Adapter on a VMware host using an OVA image. For information on how to deploy a VM using an ISO image, see the VMware documentation.

The following guidelines apply when deploying the Prime Network Services Controller Device Adapter:

- Prime Network Services Controller Device Adapter must be installed before you can deploy and register third-party service nodes, such as Citrix NetScaler load balancers.
- Adding or editing policies from the Prime Network Services Controller Device Adapter is not supported. All configuration must be performed using the Prime Network Services Controller GUI.
- You need to install the Prime Network Services Controller Device Adapter only once for each Prime Network Services Controller instance.
- If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Before You Begin

Confirm that a network path exists between the Prime Network Services Controller Device Adapter IP address and the Prime Network Services Controller management IP address.

Procedure

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

Step 2 Choose the host on which to deploy the Prime Network Services Controller Device Adapter.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the wizard, provide the required information as described in the following table:

Screen	Action
Source	Navigate to and choose the nsc-device-adapter.3.4.1*x*.ova file.
OVF Template Details	Review the details of the Prime Network Services Controller Device Adapter template.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Specify a name and location for the VM. The name must begin with a letter.
Storage	Choose the data store for the VM.
Disk Format	Choose the required format.
Network Mapping	Choose the management network port group for the VM.
Properties	Provide the following information: • VM IP address, subnet mask, and gateway IP address. • DNS server and NTP server IP addresses. • IP address for the Prime Network Services Controller server. • Password and shared secret password for access to the VM.
Ready to Complete	Review the deployment settings for accuracy.

Step 5 Click **Finish**.

Step 6 After the deployment is complete, power up the VM.
You can monitor the progress of the deployment by opening the VM console.

Step 7 Confirm that the Prime Network Services Controller Device Adapter VM is successfully registered with Prime Network Services Controller by logging in to the Prime Network Services Controller server and choosing **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM that you deployed.

Configuring Load Balancer Licenses

Prime Network Services Controller enables you to import bundled Citrix NetScaler load balancer licenses and prepare those licenses for assigning to load balancers. For more information, see the following topics:

- Citrix Load Balancer Bundled Licenses, on page 31
- Importing and Configuring Load Balancer Licenses, on page 32

Citrix Load Balancer Bundled Licenses

A Citrix NetScaler load balancer license bundle is a compressed file (with .zip extension) that contains:

- One or more license files with the extension .lic.
- A license.xml file.

To view a sample license.xml file, see Example license.xml File, on page 31.

The following conditions apply to license bundles:

- All license files in the bundle must be from the same vendor and for a single platform. For the current release, the only supported vendor/platform combinations are *Citrix* and *VPX* or *NS1000V*.
- All license files in the bundle must be of the same license category. For example, they must have same feature level (such as Standard or Premium) and throughput level (such as 10 or 1000).
- You must import the license bundle before instantiating the load balancer.
- You can import multiple license bundles, but the bundles cannot contain files with the same host ID or the same filename as an existing file.
- You cannot delete a license if it is assigned to a load balancer service device.

Example license.xml File

```
xml version="1.0" encoding="UTF-8"
<LicenseBundle>
  <Vendor>vendor-name</Vendor>
  <Platform>platform-type</Platform>
  <LicenseCategory>
     <FeatureLevel>feature-level</FeatureLevel>
     <ThroughputLevel>throughput-level</ThroughputLevel>
     <Licenses>
         <License file="license1.lic">
            <HostId>host1-id</HostId>
         <License file="license2.lic">
            <HostId>host2-id</HostId>
     </Licenses>
  </LicenseCategory>
</LicenseBundle>
```

License XML Tag	Description	Example
Vendor	Vendor from whom the licenses were obtained.	Citrix
Platform	Platform for which the licences can be used.	VPX

License XML Tag	Description	Example
LicenseCategory	License category based on feature and throughput level.	
—FeatureLevel	Feature level of the licenses in the bundle.	Standard
—ThroughputLevel	Throughput level of the licenses in the bundle.	10
Licenses	Licenses in the bundle.	
—License file	License filename.	"GID_6087fdd1_1435dda300b__6e02.lic"
—HostId	Host ID of the device for which the license was issued.	005056a91f72

Importing and Configuring Load Balancer Licenses

This topic describes how to import bundled Citrix NetScaler load balancer licenses and prepare those licenses for assignment to load balancers.

Before You Begin

- Generate and download a license bundle for the required type of Citrix NetScaler load balancer. For more information, see:
  - Citrix Load Balancer Bundled Licenses, on page 31
  - http://support.citrix.com/article/CTX122426
- Confirm the license category that has been purchased. For more information about the available license categories for Citrix NetScaler load balancers, see http://support.citrix.com/article/CTX122426.

Procedure

Step 1 Choose **Resource Management >Managed Resources > root** or **root >** *tenant*.

Note If licenses are imported at root, all tenants below root can use the license. For more granular control, import licenses at the tenant level or lower.

Step 2 In the License tab, click **Import License Bundle**.

Step 3 Enter the import details, and then click **OK**. To check the import status, view the Recent Jobs window. After the import completes, the bundle is displayed in the table with a success status.

Step 4 Under the Feature License per platform area, choose the device and the license category.

Step 5 Click **Edit** to view the different licenses available for that category. You can also look at this table at a later time to see which licenses are assigned to instantiated load balancers.

Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller

After a Citrix NetScaler load balancer VM starts, you can register it with Prime Network Services Controller.

Before You Begin

- Deploy a Citrix NetScaler load balancer VM in the hypervisor. For more information, see:
  - For OpenStack, see Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack, on page 63.
  - For VMware, see Citrix product documentation at http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html.
- Create a tenant in Prime Network Services Controller if one does not exist.
- Configure a virtual server profile in Prime Network Services Controller.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, from the **Active** drop-down list, choose **Add Load Balancer**.

Step 3 In the Add Load Balancer wizard, provide the following information:

a) In the Properties screen, enter a name and hostname for the load balancer.

b) In the Service Device screen, choose **Register** and provide the following information:

- IP address
- Subnet mask
- Gateway IP address
- Device type
- Version
- Access credentials

c) In the Interfaces screen, add a data interface.

d) In the Virtual Server screen, add a virtual IP address and select the virtual server profile to use.

e) In the Summary screen, review the information for accuracy, and then click **Finish**.

Deleting the Default Service Path

By default, Prime Network Services Controller includes a service path for use with the automatic instantiation of network services. This service path can cause issues if it is used by a port profile. As a result, we recommend that you remove the default service path from Prime Network Services Controller.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > Service Path**.

Step 2 In the General tab, choose the default service path and then click **Delete**.

Managing Service VMs and the Device Adapter

The following topics can help troubleshoot issues that you might encounter with the Prime Network Services Controller Device Adapter and service VMs:

- Prime Network Services Controller IP Address Change, on page 34
- Updating Device Adapter Properties, on page 36
- Device Adapter Not Reachable, on page 37
- Troubleshooting Devices and Services, on page 38

Prime Network Services Controller IP Address Change

If you change the management IP address of Prime Network Services Controller, configure service VMs that were previously registered with Prime Network Services Controller so that they can continue to communicate with Prime Network Services Controller. See the following topics for more information:

- Reregistering Service VMs, on page 34
- Updating Nexus 1000V Services After Changing the Prime Network Services Controller IP Address, on page 35

Reregistering Service VMs

After changing the Prime Network Services Controller management IP address, you must register service VMs with the new IP address as follows.

Before You Begin

Confirm the following:

- Each Cisco VM is deployed and powered on.
- A network path exists between each VM management IP address and the new Prime Network Services Controller management IP address.

Procedure

Step 1 For each ASA 1000V registered with Prime Network Services Controller:

a) Disable the policy agent by entering the following commands:

```
asa# configure terminal
asa(config)# no vnmc policy-agent
```

b) Enable the policy agent and register the ASA 1000V with the new Prime Network Services Controller IP address as shown in Registering Cisco VMs Deployed on VMware, on page 27.

Step 2 For each VSM registered with Prime Network Services Controller:

a) Uninstall the policy agent by entering the following commands:

```
vsm# config
vsm(config)# xxx-policy-agent
vsm(config-policy-agent)# no policy-agent-image
```

where *xxx*-policy-agent is either vnm-policy-agent or nsc-policy-agent, depending on the VSM version.

b) Reinstall the policy agent and register the VSM with the new Prime Network Services Controller IP address as shown in Registering Cisco VMs Deployed on VMware, on page 27.

Step 3 For each VSG registered with Prime Network Services Controller:

a) Uninstall the policy agent by entering the following commands:

```
vsg# config
vsg(config)# vnm-policy-agent
vsg(config-policy-agent)# no policy-agent-image
```

b) Reinstall the policy agent and register the VSG with the new Prime Network Services Controller IP address by entering the following commands:

```
vsg# configure terminal
vsg(config)# vnm-policy-agent
vsg(config-vnmc-policy-agent)# registration-ip n.n.n.n
vsg(config-vnmc-policy-agent)# shared-secret MySharedSecret
vsg(config-vnmc-policy-agent)# policy-agent-image
bootflash:xxxx-vsgpa.n.n.n.bin
vsg(config-vnmc-policy-agent)# copy running-config startup-config
```

The name of the policy agent image (vnmc-vsgpa.*n.n.n*.bin or nsc-vsgpa.*n.n.n*.bin) depends on whether you are using VMware or Hyper-V Hypervisor.

Updating Nexus 1000V Services After Changing the Prime Network Services Controller IP Address

If you change the IP address of the Prime Network Services Controller server, you must update vsm-service as follows so that Prime Network Services Controller can maintain communications with Nexus 1000V switches.

Before You Begin

Obtain the Prime Network Services Controller debug plugin nsc-dplug.3.4.*n.x*.bin. If you need assistance in locating this file, contact the Cisco Technical Assistance Center.

You can contact the TAC over the phone or via the Web:

- Regional phone numbers are available at http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html#numbers.
- To use the Web, go to http://www.cisco.com/cisco/web/support/index.html.

Procedure

Step 1 Log in to Prime Network Services Controller via the console.

Step 2 Stop the pmon services by entering the following commands:

```
# connect local-mgmt
(local-mgmt)# service stop
```

Step 3 Load the Prime Network Services Controller debug plugin:

```
(local-mgmt)# update bootflash:/nsc-dplug.3.4.n.x.bin
```

A $ prompt is displayed when the **update bootflash** command is complete.

Step 4 Delete the database for the vsm-service:

```
$ sudo bash
# rm /opt/cisco/vsm-service/db/flash/dme.db
```

Step 5 Restart pmon services:

```
# connect local-mgmt
(local-mgmt)# service start
```

Step 6 Use the Prime Network Services Controller XML API to identify and delete the stale extpolClient object for vsm-service.
For more information, see the Cisco Prime Network Services Controller XML API Guide.

Updating Device Adapter Properties

If you enter incorrect information when deploying the Prime Network Services Controller Device Adapter, it will not be able to register with Prime Network Services Controller. For example, if you enter an incorrect IP address or shared secret password when deploying the OVF, the Device Adapter cannot register with Prime Network Services Controller. If this occurs, use the following procedure to correct the situation.

Procedure

Step 1 In the hypervisor, stop the Device Adapter VM.

Step 2 Navigate to the OVF settings in the hypervisor and update the properties as required.

Step 3 Restart the Device Adapter.
The Device Adapter registers with Prime Network Services Controller.

Device Adapter Not Reachable

Certain circumstances, such as loss of network connectivity, can cause Prime Network Services Controller and the Prime Network Services Controller Device Adapter (Device Adapter) to lose communication with each other. If this occurs, use the instructions in this topic to recover communications.

First, determine whether or not Prime Network Services Controller and the Device Adapter can communicate with each other. To do this, log in to the Prime Network Services Controller GUI and choose **Administration > Service Registry**. The Device Adapter should be displayed with two entries: managed-endpoint and mgmt-controller. If both entries are in *lost-visibility* state, it indicates that Prime Network Services Controller and the Device Adapter have not been able to communicate with each other for an extended period of time. If Prime Network Services Controller and the Device Adapter can resume communication with each other automatically, they will recover from the lost-visibility state.

If communication with the endpoint cannot be reestablished, you can remove the managed endpoints that are in lost-visibility state. **However, do not remove the managed endpoint for the Device Adapter.** Instead, replace the Device Adapter VM by using the same host information (hostname, access credentials, and management IP address) as the Device Adapter VM that is in lost-visibility state.

By removing the existing VM and recreating the Device Adapter VM with the same host information, Prime Network Services Controller will recognize the new Device Adapter VM as a replacement for the previous Device Adapter VM. In addition, the new Device Adapter VM will assume management of any third-party devices that the previous Device Adapter VM managed.

Scenario 1

In this scenario, Prime Network Services Controller is deployed with the Device Adapter.

1. Prime Network Services Controller deploys three load balancers (lb1, lb2, and lb3) that are managed by Adapter1.
2. Adapter 1 becomes unavailable.
3. The administrator does not remove the managed-endpoint for Adapter1.
4. The administrator removes the Adapter1 VM and recreates it by using the same host information as that for the original Device Adapter.
5. Prime Network Services Controller recovers connectivity and recognizes the new Device Adapter VM as a replacement for the previous Adapter1.
6. The new Adapter1 assumes management of the existing service nodes. In addition, Prime Network Services Controller will deploy new service nodes (such as lb4) that are assigned to the new Adapter1.

Note The new Adapter1 might attempt to reapply the configuration to the existing service nodes (lb1, lb2, and lb3). If this occurs, Prime Network Services Controller might update the configuration state for these service nodes to *failed-to-apply*. If this occurs, reboot the service nodes to display the correct configuration state.

Scenario 2

In this scenario, a new Device Adapter has different host information than the original Device Adapter.

If the new Device Adapter VM has different host information, such as a different management IP address or hostname, Prime Network Services Controller might not recognize it as a replacement for the existing VM. All existing service nodes that were managed by the original Device Adapter VM will continue to run, but in headless mode. Any additional configuration changes that are made to those service nodes by using Prime Network Services Controller will not be applied. In addition, because Prime Network Services Controller does not recognize the new Device Adapter VM as the replacement for the previous Device Adapter VM, subsequent deployments will fail because they cannot be assigned to the original Device Adapter.

As in the previous scenario, Prime Network Services Controller is deployed with Device Adapter (Adapater1).

1. Prime Network Services Controller deploys three load balancers (lb1, lb2, and lb3).
2. Adapter1 enters lost-visibility state.
3. The administrator does not remove the managed-endpoint for Adapter1.
4. The administrator deploys a new Device Adapter VM (Adapter2) with a management IP address that is different from the management IP address for Adapter1.
5. Prime Network Services Controller does not recognize Adapter2 as a replacement for Adapter1 and instead considers it a new instance of the Device Adapter.
6. All services (lb1, lb2, and lb3) that were managed by Adapter1 continue to run, but in headless mode; that is, any attempt by Prime Network Services Controller to change the configuration for those services fails.
7. Additional deployments, such as lb4, might be assigned to Adapter1 for management and will therefore fail to complete deployment.

Note If you delete the managed-endpoint for the Device Adapter before replacing the Device Adapter VM, Prime Network Services Controller will not recognize the new Device Adapter VM as a replacement for the original Device Adapter VM. Instead, you will encounter the behavior described in this scenario.

Troubleshooting Devices and Services

You can use Prime Network Services Controller to troubleshoot faults associated with managed devices and services.

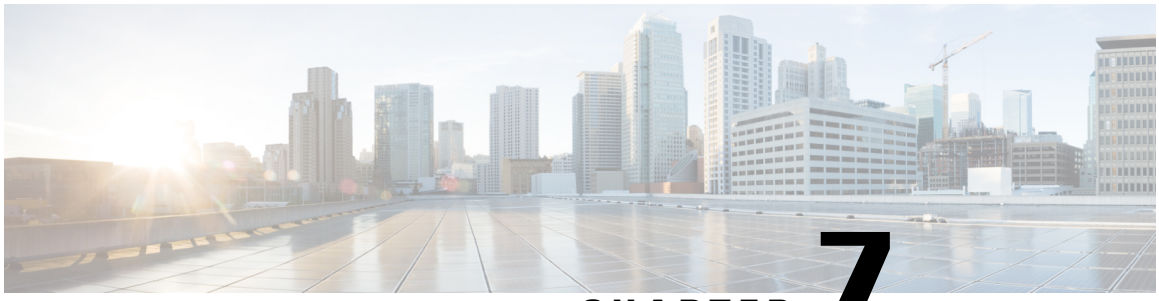
Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose the required service or device, and then click **Edit**.

Step 3 In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.

Step 4 In the Faults tab, review the displayed faults. To view additional information about a fault, double-click the entry, or choose the entry and then click **Properties**.



CHAPTER 7

Upgrading Prime Network Services Controller

This section includes the following topics:

Upgrading Overview

Note Prime Network Services Controller 3.4 does not support InterCloud functionality. If you upgrade from a previous version of Prime Network Services Controller with InterCloud objects, the upgrade procedure will detect those objects and stop the upgrade process. You must delete all InterCloud objects before you can upgrade to 3.4.

The following table shows the supported upgrade paths for Prime Network Services Controller 3.4. Upgrading to Prime Network Services Controller 3.4 is supported only in VMware environments.

Table 1: Supported Upgrade Paths for Prime Network Services Controller 3.4

Hypervisor	Supported Upgrade Versions	
	Standalone Mode	Orchestrator Mode
VMware	3.2, 3.2.2a, 3.2.2b	Not applicable
OpenStack KVM	—	—
Hyper-V Hypervisor	—	—

To upgrade from VNMC 2.x to Prime Network Services Controller 3.4, you must first upgrade to one of the supported upgrade versions.

The following scenarios are not supported:

- Backing up from VNMC 1.x or 2.x and restoring to Prime Network Services Controller 3.4.
- Exporting from VNMC 1.x or 2.x and importing to Prime Network Services Controller 3.4.

To upgrade to Prime Network Services Controller 3.4, confirm that you meet the following requirements:

1. If you are upgrading from VNMC 2.1, ensure that the VNMC 2.1 is deployed in a single disk. The upgrade will fail if the VNMC 2.1 deployment spans more than one disk.
2. If you are upgrading from VNMC 2.0 or 2.1, first upgrade to Prime Network Services Controller 3.2, 3.2.2, or 3.2.2b—See the applicable *Cisco Prime Network Services Controller Quick Start Guide* at http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html.

Upgrade Workflow

The following table identifies the tasks in sequence for a smooth upgrade.

Task	Notes
1. Perform a full-state backup of Prime Network Services Controller using the Secure Copy (SCP) protocol.	See Backing Up Data, on page 41.
2. Stop the Prime Network Services Controller Device Adapter VM.	Do not delete this VM yet. You can delete it after you verify that the upgrade is successful and that you do not need to restore the previous version.
3. Upgrade Prime Network Services Controller by using the CLI **update bootflash** command.	See Upgrading to Prime Network Services Controller 3.4, on page 42.
4. Using the new Prime Network Services Controller Device Adapter version, deploy a new Prime Network Services Controller Device Adapter VM and power it up.	When configuring the new Prime Network Services Controller Device Adapter VM, use the same host information (hostname, access credentials, and management IP address) as the previous version.
5. Verify that Prime Network Services Controller has been successfully upgraded.	1. In the console, enter the **show version** command to confirm that the new version is installed. 2. Log in to the Prime Network Services Controller GUI and confirm that the service nodes are registered.
6. Delete the previous Prime Network Services Controller Device Adapter VM.	After verifying that the service nodes are registered, you can delete this VM.

After upgrading Prime Network Services Controller:

- Allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.
- Allow approximately five minutes for each service node to register with Prime Network Services Controller.
- If you see the previous version of Prime Network Services Controller in your browser, clear the browser cache and history, and restart the browser. This applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Backing Up Data

Back up Prime Network Services Controller before upgrading to a new version.

Adhere to the following conventions when backing up Prime Network Services Controller:

- Temporarily disable the Cisco Security Agent (CSA) on the remote file server.
- Do not use TFTP to back up data.
- Do not perform a backup while the system is importing images.
- Access the CLI through the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

```
create backup scp://user@host/file full-state enabled
```

where:

- *user* is the username.
- *host* is the system name.
- */file* is the full path and name of the backup file.

Step 4 When prompted, enter the required password.

Step 5 At the `/system/backup*` prompt, enter:

```
commit-buffer
```

Step 6 Log in to the SCP server, and make sure that */file* exists and that the file size is not zero (0).

Upgrading to Prime Network Services Controller 3.4

Note Prime Network Services Controller 3.4 does not support InterCloud functionality. If you upgrade from a previous version of Prime Network Services Controller with InterCloud objects, the upgrade procedure will detect those objects and stop the upgrade process. You must delete all InterCloud objects before you can upgrade to 3.4.

After you back up the data for your existing Prime Network Services Controller installation, you can upgrade to Prime Network Services Controller 3.4.

Adhere to the following guidelines when upgrading Prime Network Services Controller:

- Do not use TFTP to update data.
- Do not access the GUI during the upgrade process.
- Use the console to access the CLI instead of SSH. If the SSH session should disconnect, you will not be able to access the VM.

Before You Begin

Confirm the following:

- You have backed up your current system for recovery purposes, if needed. For more information, see Backing Up Data, on page 41.
- Prime Network Services Controller 3.4 has two virtual disks with the following configuration:
  - Disk 1—20 GB
  - Disk 2—200 GB

  If you do not have two disks configured, you will not be able to upgrade to 3.4.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 (Optional) Check the current version of the Prime Network Services Controller software:

```
show version
```

Step 4 Download the Prime Network Services Controller 3.4 image from a remote file server:

```
copy scp://imageURLtoBinFile bootflash:/
```

Step 5 Upgrade to Prime Network Services Controller 3.4:

```
update bootflash:/nsc.3.4.1x.bin
```

where *nsc.3.4.1x.bin* is the image name.

Step 6 Restart the server:

```
service restart
```

Step 7 (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 8 (Optional) Verify that the Prime Network Services Controller software version has been updated:

```
show version
```

Step 9 To confirm that Prime Network Services Controller is fully accessible after the upgrade, log in to the GUI. If your browser displays the previous version instead of the upgraded version, clear the browser cache and browsing history, and restart the browser.

Step 10 If you have changed the server hostname or fully qualified domain name (FQDN), reconfigure Prime Network Services Controller connectivity with the VMM.

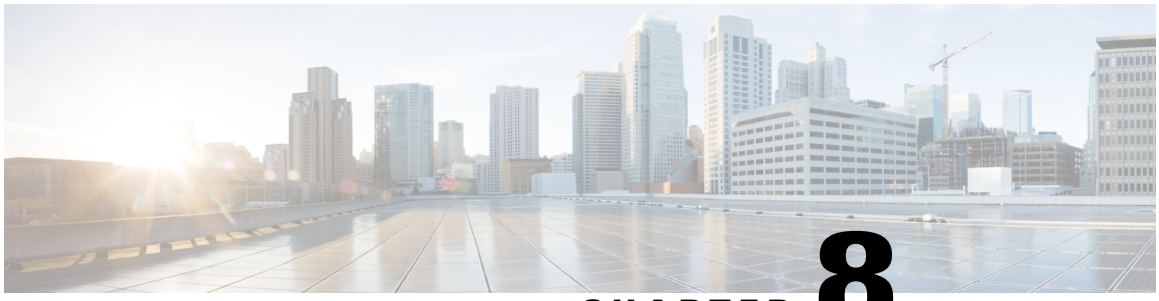
Note You must perform this step before attempting any enterprise VM-related operations.

For more information, see the topic appropriate for your environment:

- Configuring Connectivity with VMware vCenter, on page 23
- Configuring Connectivity with OpenStack KVM, on page 54
- Configuring Connectivity with Microsoft SCVMM, on page 73

PART II

Installing Prime Network Services Controller in OpenStack Environments



CHAPTER 8

Installing Prime Network Services Controller in OpenStack KVM Environments

This section includes the following topics:

OpenStack Installation Overview

You install Prime Network Services Controller on OpenStack by using the ISO image. The installation time varies from 10 to 20 minutes depending on the host and the storage area network load.

To install Prime Network Services Controller on OpenStack, complete the tasks described in the following topics:

1. Configuring OpenStack for Prime Network Services Controller, on page 47
2. Installing Prime Network Services Controller on OpenStack KVM, on page 49
3. Performing OpenStack KVM Post-Installation Tasks

Configuring OpenStack for Prime Network Services Controller

To prepare OpenStack for installing Prime Network Services Controller using the Cisco OpenStack Installer (COI), you must create a flavor, import an image, and launch an instance. This procedure describes how to complete these tasks.

Before You Begin

In OpenStack:

- Confirm that you have met the requirements in Requirements Overview, on page 5. OpenStack Havana is required for Prime Network Services Controller 3.4 functionality.

Note Although you can install Prime Network Services Controller 3.4 on OpenStack Grizzly, you will not have access to 3.4 functionality unless you use OpenStack Havana.

- Gather the information required for configuration as identified in Information Required for Configuration and Installation, on page 9.
- Confirm that you have admin privileges.
- Confirm that the Cinder service is up and running.
- Create a project on which to install Prime Network Services Controller.
- Create a Cinder volume with the size of 20 GB.
- Configure a security group that allows TCP, UDP, and ICMP traffic with Prime Network Services Controller.

  For information on how to configure these items, see the OpenStack documentation at docs.openstack.org.

Procedure

Step 1 In the OpenStack Dashboard, choose **Admin > Flavors**, and then click **Create Flavor**.

Step 2 In the Create Flavor dialog box, enter the following information, and then click **Create Flavor**:

- Name—Flavor name.
- vCPUs—Enter **4**.
- RAM MB—Enter **4096**.
- Root Disk—Enter **20 GB**.
- Ephemeral Disk—Enter **20 GB**.
- Swap Disk—Enter **400 MB**.

Step 3 Choose **Admin > Images**, and then click **Create An Image**.

Step 4 In the Create An Image dialog box, provide the following information, and then click **Create Image**:

- Name—Enter an image name.
- Image Source—Specify the image source.
- Image File—Use this field if the image is available on your local system.
- Format—Choose **ISO - Optical Disk Image**.
- Public—Check the check box to make the image available to all users with access to the current project.
- Protected—Check the check box to ensure that only users with permission can delete the image.

After the image has been created, it appears in the Images table at **Admin > Images** or **Project >** *project* **> Manage Compute > Images & Snapshots**.

Step 5 Choose **Project >** *project* **> Manage Compute > Volumes**, and click **Create Volume**.

Step 6 In the Create Volume dialog box, add a volume with the size of 20 GB, and click **Create Volume**.

Step 7 At the command line, enter the following command to launch the Prime Network Services Controller instance:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 8 In the OpenStack GUI, choose **Project >** *project* **> Manage Compute > Instances**.

Step 9 In the Instances pane, note the IP address of the launched instance.

Step 10 Click the instance and choose **More > Console** to start the Prime Network Services Controller installation procedure.

What to Do Next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller on OpenStack KVM, on page 49.

Installing Prime Network Services Controller on OpenStack KVM

This procedure describes how to install the ISO image on a VM that has been configured for Prime Network Services Controller.

Before You Begin

Confirm the following items:

- All system requirements are met.
- You have the information identified in Information Required for Configuration and Installation, on page 9.
- You have configured the hypervisor for the Prime Network Services Controller installation procedure.
- A VM has been created for Prime Network Services Controller and has network access.
- You can access the VM console.
- You have the IP address for the instance launched in OpenStack.

Procedure

Step 1 Open the VM console if it is not already open.

If you have just finished configuring the hypervisor, the Prime Network Services Controller installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Prime Network Services Controller VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Prime Network Services Controller is available in Standalone mode only.
- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore a previous Prime Network Services Controller installation.

Step 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria, on page 10.

Note If you configure a weak shared secret password, no error message is generated during entry here, but the shared secret password is not usable when the VM is started during the installation process.

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**.
Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**.
Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.

Rebooting Prime Network Services Controller from OpenStack

If you reboot a Prime Network Services Controller instance from the OpenStack Horizon UI, the reboot operation fails and the console contains a message stating that no bootable image can be found. This situation occurs for instances that were created using an ISO image, such as Prime Network Services Controller.

In OpenStack, the first time an instance is created by using an ISO image and rebooted, the root device name is set to /dev/hda. After the instance is created, the bootable image is located on vda. However, with the implementation of hard and soft reboot options in OpenStack, the disk definitions change. As a result, a bootable image cannot be found for the Prime Network Services Controller instance.

To reboot Prime Network Services Controller in OpenStack, use either of the following procedures:

- Rebooting Prime Network Services Controller Without an Image, on page 51
- Rebooting Prime Network Services Controller by Changing the Disk Files, on page 51

Rebooting Prime Network Services Controller Without an Image

Use this procedure to reboot a Prime Network Services Controller instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org/.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—0 GB (no ephemeral disk)

Step 2 Using either the Horizon GUI or the CLI, create one volume (vda) for Prime Network Services Controller and one volume (vdb) for storing imported images.
To use the CLI, enter the following commands:

```
cinder create --display-name vda-name 20
cinder create --display-name vdb-name 200
```

Step 3 Using the CLI, boot the instance and install Prime Network Services Controller as follows:

a) Enter the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=vda-id:::0 --block-device-mapping
vdc=vdb-id:::0 pnsc-image-name
```

b) When prompted to reboot after the installation, click **Stop**.

Step 4 Terminate the instance created in Step 3 to remove the instance while retaining the required two volumes.

Step 5 To boot the Prime Network Services Controller instance, enter the **boot** command without the `--image` parameter and using the correct volume IDs:

```
nova boot --flavor=flavor-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vda=vda-id:::0 --block-device-mapping
vdb=vdb-id:::0 pnsc-image-name
```

Rebooting Prime Network Services Controller by Changing the Disk Files

Use this procedure to reboot a Prime Network Services Controller instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—20 GB

The ephemeral disk will act as the Prime Network Services Controller system disk.

Step 2 Using either the Horizon UI or the CLI, create one volume (vdb) for storing imported images.
To use the CLI, enter the following command:

```
cinder create --display-name vdb-name 200
```

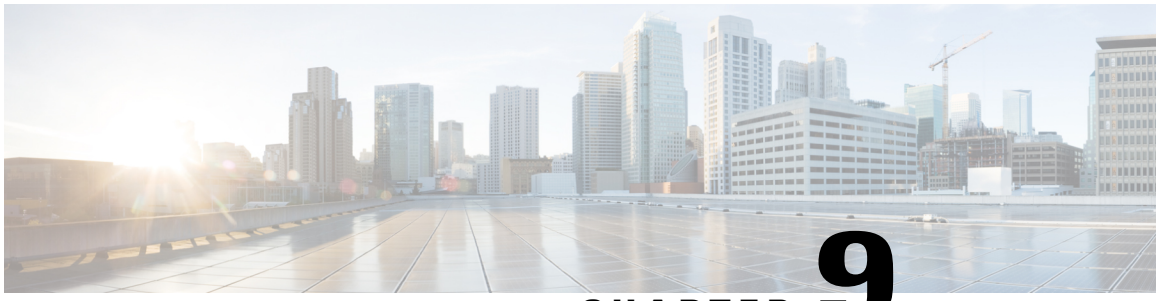
Step 3 Using the CLI, boot the instance and install Prime Network Services Controller by entering the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 4 When prompted, disconnect from the media source and click **Reboot**.
Prime Network Services Controller is then installed on the VM.

Step 5 Change the disk files by entering the following commands:

```
mv /var/lib/nova/instance-uuid/disk /var/lib/nova/instance-uuid/disk.tmp
ln -s /var/lib/nova/instance-uuid/disk.local
/var/lib/nova/instance-uuid/disk
```



CHAPTER 9

Performing OpenStack KVM Post-Installation Tasks

This section contains the following topics:

Removing Anti-Spoofing Rules for CSR 1000V Data Interfaces

For hosts running OVS-based OpenStack, a situation exists that affects all devices with routing functionality, such as CSR 1000V VMs.

In this situation, the OVS Quantum plugin enters anti-spoofing entries for each vNIC of the VM. For each vNIC interface, two iptables entries must be removed to enable ANY-ANY routing for CSR 1000V VM services.

Perform the following procedure:

- On the compute node on which the CSR 1000V VM is running.
- Each time a CSR 1000V VM is migrated to another compute node.

Procedure

Step 1 Display iptables entries by entering the following command:

```
iptables -L --line-numbers
```

The output should resemble the following:

```
Chain quantum-openvswi-oc43a12ff-e (2 references)
Chain quantum-openvswi-oc4ea12ff-e (2 references)
num  target  prot  opt source        destination
1    DROP     all  --  anywhere      anywhere     MAC ! FA:16:3E:16:6E:EE
2    RETURN   udp  --  anywhere      anywhere     udp spt:bootpc dpt:bootps
3    DROP     all  -- !193.1.1.6     anywhere
```

```
4    DROP     udp  --  anywhere      anywhere     udp spt:bootps dpt:bootpc
5     DROP      all  --  anywhere       anywhere      state INVALID
6    RETURN   all  --  anywhere      anywhere     state RELATED,ESTABLISHED
7     RETURN    all  --  anywhere       anywhere
8     quantum-openvswi-sg-fallback  all  --  anywhere    anywhere
```

Step 2 In the output, locate the iptable rule chains that contain the CSR 1000V data interface IP address and MAC address.
In the example, DROP rules 1 and 3 are for a CSR 1000V with the MAC address FA:16:3E:16:6E:EE and the IP address 193.1.1.6.

Step 3 Remove the first DROP rule by entering the following command:
iptables -D *chain-name rule-num*

Step 4 Enter the following command to refresh the list of rules:
iptables -L --line-numbers

Note Entering this command after removing an entry helps ensure that you delete the correct entry with the next command.

Step 5 In the output, identify the next rule to be deleted, and repeat Steps 3 and 4.

Configuring Connectivity with OpenStack KVM

After installing Prime Network Services Controller, configure Prime Network Services Controller so that it can communicate with the Virtual Machine Manager (VMM) for that hypervisor and the VMs that Prime Network Services Controller will manage. Prime Network Services Controller communicates with the VMM to perform the following actions on the VMs that it manages:

- Obtain the VM attributes that Prime Network Services Controller uses for VM management.
- Instantiate, start, stop, restart, or delete VMs.
- Map VM network interfaces.
- Instantiate and configure services on service VMs.

Before You Begin

Obtain the OpenStack admin or superuser username and password for OpenStack access.

Procedure

Step 1 Choose **Resource Management > VM Managers**, and then click **Add VM Manager**.

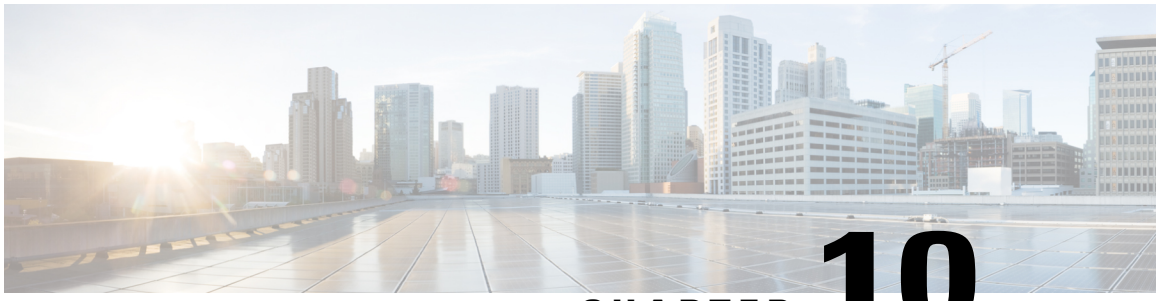
Step 2 In the Add VM Manager dialog box, add the required information as described in the following table, and then click **OK**.

Field	Description
Name	VMM name.
Description	VMM description.

Field	Description
Service Tenant	Name of the OpenStack project that can be used for network services and the management network. **Note** This feature is not supported in Prime Network Services Controller 3.4.
Hostname / IP Address	Hostname or IP address of the OpenStack controller.
Secure	Check the check box to use HTTPS for connections between Prime Network Services Controller and OpenStack. Prime Network Services Controller uses HTTPS for communications with OpenStack by default. Uncheck the check box to use HTTP for connections between Prime Network Services Controller and OpenStack.
Domain Name / Username	OpenStack admin or superuser username.
Password	OpenStack admin or superuser password.
Port Number	Port number of the Keystone service running on the OpenStack controller.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.



CHAPTER 10

Registering Service VMs Installed on OpenStack

This section contains the following topics:

Registering Service VMs in OpenStack

Registering service VMs with Prime Network Services Controller ensures that Prime Network Services Controller recognizes and can communicate with the VMs.

See the following topics for information on how to register Cisco and third-party VMs that are deployed on OpenStack with Prime Network Services Controller:

- For Cisco service VMs, see Registering Cisco VMs Deployed on OpenStack KVM, on page 57.
- For third-party service VMs, see Registering Third-Party VMs, on page 58.

Registering Cisco VMs Deployed on OpenStack KVM

This procedure describes how to register CSR 1000V VMs with Prime Network Services Controller. This procedure applies only to those edge routers that have been installed directly on the hypervisor. Edge routers that are instantiated on the hypervisor by using Prime Network Services Controller are automatically registered with Prime Network Services Controller upon instantiation.

Before You Begin

- Complete the tasks described in Performing OpenStack KVM Post-Installation Tasks, on page 53.
- Install the CSR 1000V VM on the hypervisor.
- Confirm that the VM is installed and powered on.
- Make sure that a network path exists between the VM management IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 On OpenStack, configure the edge router so that it supports remote management by Prime Network Services Controller.
For more information, see the Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide.

Step 2 In OpenStack, navigate to the edge router VM to be registered with Prime Network Services Controller.

Step 3 Open a console window for the VM.

Step 4 In the CLI, register the edge router VM by entering the following commands:

```
Router> enable
Router# configure terminal
Router(config)# remote-management
Router(config-remote-mgmt)# pnsc host n.n.n.n local-port number
shared-secret string
Router(config-remote-mgmt)# end
Router# show remote-management status
```

Registering Third-Party VMs

Registering third-party VMs that are installed on OpenStack with Prime Network Services Controller involves installing the Prime Network Services Controller Device Adapter on OpenStack and then instantiating and registering the third-party VMs with Prime Network Services Controller.

Complete the following tasks to instantiate a Citrix NetScaler load balancer on OpenStack and register the load balancer with Prime Network Services Controller.

Task	Related Topic
1. Confirm that the prerequisites are met.	Prerequisites for Citrix NetScaler Load Balancers on OpenStack, on page 59
2. Install Prime Network Services Controller Device Adapter.	Installing the Prime Network Services Controller Device Adapter on OpenStack, on page 59
3. Configure OpenStack.	Configuring OpenStack for Citrix NetScaler Load Balancers, on page 62
4. Instantiate a Citrix NetScaler load balancer.	Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack, on page 63
5. Register the Citrix NetScaler instance with Prime Network Services Controller.	Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller, on page 64

Prerequisites for Citrix NetScaler Load Balancers on OpenStack

The following table lists the prerequisites for instantiating Citrix NetScaler load balancers on OpenStack and registering the load balancers with Prime Network Services Controller.

Requirement	Notes
Prime Network Services Controller has been installed and is accessible from OpenStack.	See the following topics: • Configuring OpenStack for Prime Network Services Controller, on page 47 • Installing Prime Network Services Controller on OpenStack KVM, on page 49
A project has been created in OpenStack.	• The project name in OpenStack must be the same as the tenant name in Prime Network Services Controller when you register the Citrix NetScaler load balancer. • The member list for the project includes a superuser admin with the admin role. For information on how to add an admin user to the member list and assign the admin role, see the OpenStack documentation at docs.openstack.org.
The network requirements are met.	• Two vNICs are available: one for management and one for data. • The management interface is in the same subnet as Prime Network Services Controller.

Installing the Prime Network Services Controller Device Adapter on OpenStack

The Prime Network Services Controller Device Adapter enables third-party VMs (such as Citrix NetScaler load balancers) to register with Prime Network Services Controller.

The following guidelines apply when deploying the Prime Network Services Controller Device Adapter:

- Prime Network Services Controller Device Adapter must be installed before you can deploy and register third-party service nodes, such as Citrix NetScaler load balancers.
- Adding or editing policies from the Prime Network Services Controller Device Adapter is not supported. All configuration must be performed using the Prime Network Services Controller GUI.
- You need to install the Prime Network Services Controller Device Adapter only once for each Prime Network Services Controller instance.

- If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Before You Begin

- Confirm that Prime Network Services Controller is running and accessible from OpenStack.
- In OpenStack, create a security group that allows TCP, UDP, and ICMP traffic from Prime Network Services Controller.

For more information about OpenStack, see docs.openstack.org.

Procedure

Step 1 In the OpenStack Dashboard, choose **Admin > Flavors**, and click **Create Flavor**.

Step 2 In the Create Flavor dialog box, provide the following information, and then click **Create Flavor**:

- Name—Enter a flavor name.
- vCPUs—Enter **2**.
- RAM MB—Enter **2048**.
- Root Disk GB—Enter **20**.
- Ephemeral Disk GB—Enter **20**.

Step 3 Choose **Admin > Images**, and click **Create An Image**.

Step 4 In the Create An Image dialog box, specify the following information for the Prime Network Services Controller Device Adapter image (nsc-device-adapter.3.4.1*x*.iso), and click **Create Image**:

- Name—Enter an image name.
- Description—Enter a description as desired.
- Image Source—Indicate whether the image is available at a remote location or is on a local system.
- Image Location—Specify the remote location of the image.
- Image File—Choose an image that is available on your local system.
- Format—Choose **ISO - Optical Disk Image**.
- Minimum Disk (GB)—Leave blank.
- Minimum RAM (MB)—Leave blank.
- Public—Check the check box to make the image available to all users with access to the current project.
- Protected—Check the check box to ensure that only users with permission can delete the image.

After the image has been created, it appears in the Images table at **Admin > Images** or **Project >** *project* **> Manage Compute > Images & Snapshots**.

Step 5 In the Images table, choose the Prime Network Services Controller Device Adapter image, and click **Launch**.

Step 6 In the Launch Instance dialog box, provide the required information in the following tabs:

Tab	Description
Details	Provide the following information: • Availability zone for the instance to use • Instance name • Flavor to use to create the instance • Number of instances to create • Whether the instance will boot from an image, snapshot, or volume • The image, snapshot, or volume to use.
Access & Security	Choose the security group that was created as part of the prerequisites.
Networking	Choose the network to use for the Prime Network Services Controller Device Adapter vNIC. Prime Network Services Controller Device Adapter requires one vNIC.

Step 7 Click **Launch**.

Step 8 In the Instances pane, note the IP address of the launched instance.

Step 9 Click the Prime Network Services Controller Device Adapter instance and open the console.
The Network Configuration screen is displayed.

Step 10 In the Network Devices area, click **Edit**.

Step 11 In the Edit Interface dialog box, enter the IP address and netmask for the Prime Network Services Controller Device Adapter instance. The IP address is the one noted in Step 8.

Step 12 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 13 In the Administrative Access screen, enter the Prime Network Services Controller IP address, admin password, and shared secret password.

Step 14 In the Summary screen, confirm that the information is accurate, and then click **Next**.

Step 15 When prompted, click **Reboot**.
The Prime Network Services Controller Device Adapter is then installed.

Step 16 Confirm that the Prime Network Services Controller Device Adapter is registered with Prime Network Services Controller by logging into the Prime Network Services Controller GUI and choosing **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM.

Configuring OpenStack for Citrix NetScaler Load Balancers

This procedure describes how to configure OpenStack so that you can instantiate a Citrix NetScaler load balancer. The procedure involves:

- Creating an initialization shell script.
- Creating a flavor.
- Uploading a Citrix NetScaler load balancer image.
- Creating the required subnet.

For more information about OpenStack and the commands included in this procedure, see the OpenStack documentation at docs.openstack.org.

Before You Begin

Confirm the following:

- The prerequisites have been met as described in Prerequisites for Citrix NetScaler Load Balancers on OpenStack, on page 59.
- The Prime Network Services Controller Device Adapter has been installed on OpenStack and is registered with Prime Network Services Controller. For more information, see Installing the Prime Network Services Controller Device Adapter on OpenStack, on page 59.

Procedure

Step 1 In OpenStack, create an initialization shell script as follows:

a) Open an SSH session on the OpenStack controller.

b) Create an initialization shell script that contains env variables for the default admin user and the project name.

Note If needed, you can download a shell script from OpenStack using the OpenStack Horizon UI. The path is *tenant* > **Access & Security > API Access > Download OpenStack RC File**.

c) Run the shell script.

Step 2 In the OpenStack dashboard, create a flavor with the following attributes:

- vCPU—2
- RAM—4096 MB
- Root Disk—0 MB
- Ephemeral Disk—0 MB
- Swap Disk—0 MB

Step 3 Upload a Citrix NetScaler load balancer image using the following command:

Note We recommend that you do not use the OpenStack dashboard to import the image.

```
# glance image-create --name image-name
--disk-format raw --container-format=bare --is-public=true
--file=/home/localadmin/images/image-name.raw
```

Your entry might resemble the following:

```
# glance image-create --name NSVPX-KVM-10.1-120.13 --disk-format raw --container-format=bare
 --is-public=true --file=/home/localadmin/images/NSVPX-KVM-10.1-120.13_nc.raw
```

Step 4 After the image is uploaded, note the UUID of the image. Use the UUID instead of the image name to ensure that a unique value is specified.

Tip If you need to obtain the UUID later, enter the following command:

```
# glance image-list | grep NSVPX*
```

Step 5 Create a private subnet by entering the following command. The Citrix NetScaler data interface must be in a different subnet than the management interface.

```
# quantum net-create SubnetName
```

Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack

This procedure describes how to instantiate a Citrix NetScaler VPX load balancer in OpenStack.

For more information about OpenStack and the commands included in this procedure, see the OpenStack documentation at docs.openstack.org.

Before You Begin

- Make sure that you have configured OpenStack as described in Configuring OpenStack for Citrix NetScaler Load Balancers, on page 62.
- Confirm that anti-spoofing has been disabled on OpenStack. For information on disabling anti-spoofing in OpenStack, see Removing Anti-Spoofing Rules for CSR 1000V Data Interfaces, on page 53. If you do not disable anti-spoofing in OpenStack, service VMs will not work.

Procedure

Step 1 Obtain the following UUIDs:

- The subnet created in Configuring OpenStack for Citrix NetScaler Load Balancers, on page 62.
- The network labeled "external."

Step 2 Enter the following command to create the Citrix NetScaler instance:

```
# nova boot --flavor=flavorID --image=imageID
--security-groups=securityGroup --nic net-id=netID1,
v4-fixed-ip=ipAddress1--nic net-id=netID2
,v4-fixed-ip=ipAddress2 vmName
```

For example, your command might resemble the following:

```
# nova boot --flavor=99 --image=4c5716cd-eef9-4947-8bce-d2d1432d5ccd
--security-groups=open_network
--nic net-id=645683e7-0b66-4c96-8f71-0edee35f1408,v4-fixed-ip=172.25.117.220
--nic net-id=39f7b506-b7f5-4bcd-b475-0e49b21da759,v4-fixed-ip=10.11.25.10 m-vpx-220
```

Note The two net-id values are different; be sure to enter the correct UUIDs.

Step 3 Note the IP address assignments. You must use the same IP address later in this procedure when you configure the load balancer.

Step 4 After the load balancer instance starts, access the instance console by clicking **Instances** in the dashboard and then choosing the **Console** tab.

Step 5 After the instance boots and the console displays a State UP message, press **Enter** twice to obtain the login prompt.

Step 6 Log in to the Citrix NetScaler load balancer.

Step 7 At the command prompt, enter **shell**.

Step 8 In the shell, enter the following command:

```
root@ns# vi /nsconfig/na.conf
```

Step 9 Modify the na.conf file as follows:

a) Update the IPAddress line so that the IP address is the same as the management IP address that you used to boot the load balancer instance in Step 2.

b) Update the route information that is a few lines below the IPAddress line.

Step 10 Save the file and exit the editor.

Step 11 Reboot the load balancer instance.

Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller

After a Citrix NetScaler load balancer VM starts, you can register it with Prime Network Services Controller.

Before You Begin

- Deploy a Citrix NetScaler load balancer VM in the hypervisor. For more information, see:
  - For OpenStack, see Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack, on page 63.
  - For VMware, see Citrix product documentation at http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html.
- Create a tenant in Prime Network Services Controller if one does not exist.
- Configure a virtual server profile in Prime Network Services Controller.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, from the **Active** drop-down list, choose **Add Load Balancer**.

Step 3 In the Add Load Balancer wizard, provide the following information:

a) In the Properties screen, enter a name and hostname for the load balancer.

b) In the Service Device screen, choose **Register** and provide the following information:

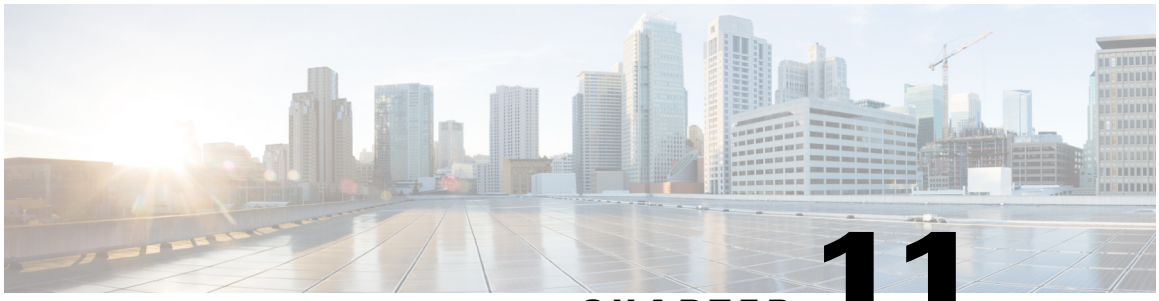
- IP address

- Subnet mask
- Gateway IP address
- Device type
- Version
- Access credentials

c) In the Interfaces screen, add a data interface.
d) In the Virtual Server screen, add a virtual IP address and select the virtual server profile to use.
e) In the Summary screen, review the information for accuracy, and then click **Finish**.

PART III

Installing Prime Network Services Controller in Hyper-V Hypervisor Environments



CHAPTER 11

Installing Prime Network Services Controller in Hyper-V Hypervisor Environments

This section contains the following topics:

Hyper-V Hypervisor Installation Overview

You install Prime Network Services Controller on Hyper-V Hypervisor by using an ISO image. The installation time varies from 10 to 20 minutes depending on the host and the storage area network load.

To install Prime Network Services Controller on Hyper-V Hypervisor, complete the tasks described in the following topics:

1. Configuring Hyper-V Hypervisor for Prime Network Services Controller, on page 69
2. Installing Prime Network Services Controller on Hyper-V Hypervisor, on page 71
3. Performing Hyper-V Hypervisor Post-Installation Tasks, on page 73

Configuring Hyper-V Hypervisor for Prime Network Services Controller

Before you can install Prime Network Services Controller on Hyper-V Hypervisor, you must create a VM. This procedure describes how to create a VM for Prime Network Services Controller.

Before You Begin

- Confirm that you have met the requirements described in Requirements Overview, on page 5.
- Gather the information required for preinstallation configuration as described in Information Required for Configuration and Installation, on page 9.

- Verify that the Hyper-V Hypervisor host on which you are going to deploy the Prime Network Services Controller VM is available in the System Center Virtual Machine Manager (SCVMM).
- Copy the Prime Network Services Controller 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 click **Refresh**.

Procedure

Step 1 Launch the SCVMM.

Step 2 Right-click the Hyper-V Hypervisor host on which to deploy the Prime Network Services Controller VM, and choose **Create Virtual Machine**.

Step 3 In the Create Virtual Machine wizard, provide the information as described in the following table:

Screen	Action
Select Source	Click **Create the new virtual machine with a blank virtual hard disk**.
Specify Virtual Machine Identity	Enter the VM name.
Configure Hardware	**1** In the Hardware Profile field, choose **Default**. **2** From General: **a** Choose **Processor** and set the number of processors to **4**. **b** Choose **Memory** and set the VM memory to **4 GB**. **3** From **Bus Configuration > IDE Devices**: **a** Choose **Hard Disk** and enter **20 GB**. **b** Choose **Virtual DVD Drive**, click **Existing ISO image file**, and choose the Prime Network Services Controller ISO image. **4** Choose **Network Adapters > Network Adapter 1**, click **Connect to a VM Network**, and choose a VM network. **5** Choose **Network Adapters > MAC Address > Static**, and enter a static MAC address from the SCVMM MAC address pool. **Note** Using dynamic MAC address assignment can result in a loss of network connectivity if the VM is migrated.
Select Destination	**1** Click **Place the virtual machine on a host**. **2** From the Destination drop-down list, choose **All hosts**.
Select Host	Choose the destination.
Configure Settings	Review the VM settings.
Select Networks	Confirm that the correct virtual switch is specified.

Screen	Action
Add Properties	Choose **64-bit edition of Windows Server 2012**.
Summary	1 Confirm that the settings are correct. 2 Check the **Start the virtual machine after deploying** check box. 3 Click **Create**.

The Jobs window displays the status of the VM being created. Verify that the job completes successfully.

Step 4 After the VM is successfully created, right-click it and choose **Connect or View > Connect Via Console**.

Step 5 Launch the console to start the Prime Network Services Controller installation procedure.

What to Do Next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller on Hyper-V Hypervisor, on page 71.

Installing Prime Network Services Controller on Hyper-V Hypervisor

This procedure describes how to install the ISO image on a VM that has been configured for Prime Network Services Controller.

Before You Begin

Confirm the following items:

- All system requirements are met.
- You have the information identified in Information Required for Configuration and Installation, on page 9.
- You have configured the hypervisor for the Prime Network Services Controller installation procedure.
- A VM has been created for Prime Network Services Controller and has network access.
- You can access the VM console.

Procedure

Step 1 Open the VM console if it is not already open.

If you have just finished configuring the hypervisor, the Prime Network Services Controller installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Prime Network Services Controller VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Prime Network Services Controller is available in Standalone mode only.
- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore a previous Prime Network Services Controller installation.

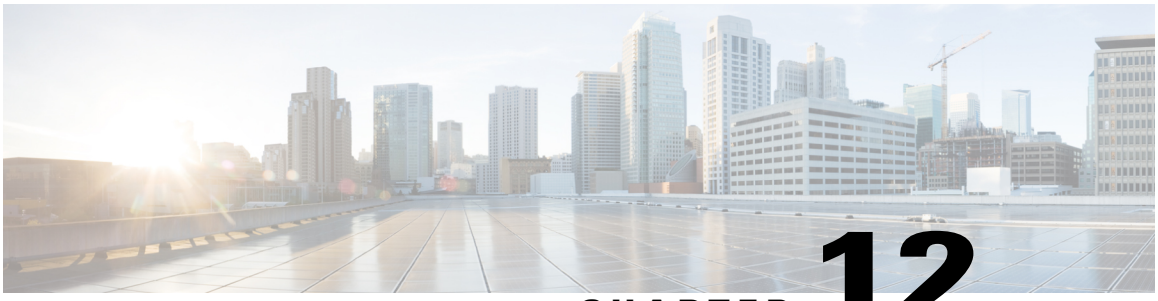
Step 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria, on page 10.

Note If you configure a weak shared secret password, no error message is generated during entry here, but the shared secret password is not usable when the VM is started during the installation process.

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**.
Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**.
Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.



CHAPTER 12

Performing Hyper-V Hypervisor Post-Installation Tasks

This section contains the following topics:

Performing Hyper-V Hypervisor Post-Installation Tasks

After you install Prime Network Services Controller on Hyper-V Hypervisor, complete the following tasks to ensure that Prime Network Services Controller can communicate with Hyper-V Hypervisor and the VMs that Prime Network Services Controller will manage.

Task	Related Topic
1. Configure NTP on VMs and Prime Network Services Controller.	Configuring NTP, on page 21
2. Configure communications with Prime Network Services Controller.	Configuring Connectivity with Microsoft SCVMM, on page 73
3. Register Cisco service VMs with Prime Network Services Controller.	Registering Cisco VMs Installed on Hyper-V Hypervisor, on page 74

Configuring Connectivity with Microsoft SCVMM

Use this procedure to configure Prime Network Services Controller connectivity with Microsoft SCVMM (SCVMM).

Before You Begin

- Confirm that you have the username and password for SCVMM access.
- Install Microsoft Service Provider Framework (SPF) so that Prime Network Services Controller can communicate with SCVMM. For more information, see http://technet.microsoft.com/en-us/library/jj642895.aspx.
- Confirm that SPF is installed correctly and functional in SCVMM by connecting to https://spf_host_ip:8090/SC2012R2/VMM/Microsoft.Management.Odata.Svc.

Procedure

Step 1 Choose **Resource Management > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, provide the information described in the following table, and then click **OK**:

Field	Description
Name	VMM name.
Description	VMM description.
Hostname / IP Address	Hostname or IP address of the VMM.
Domain Name / Username	Domain or username for SCVMM access.
Password	Password for SCVMM access.
Port Number	Port to use for communications.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- SCVMM version.

Registering Cisco VMs Installed on Hyper-V Hypervisor

This topic describes how to register the following Cisco VMs on Hyper-V Hypervisor with Prime Network Services Controller. This topic applies only to those Cisco VMs that have been installed directly on the hypervisor. Cisco VMs that are instantiated on a hypervisor through Prime Network Services Controller are automatically registered with Prime Network Services Controller upon instantiation.

- VSG

- VSM

Before You Begin

- Configure NTP on the required hypervisor.
- Install the required Cisco VMs on the hypervisor.
- Confirm that each Cisco VM is deployed and powered on.
- Make sure that a network path exists between each VM management IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 In the hypervisor, navigate to the VM to be registered with Prime Network Services Controller.

Step 2 Open a console window for the VM.

Step 3 In the CLI, register the VM as follows.

- VSG VM

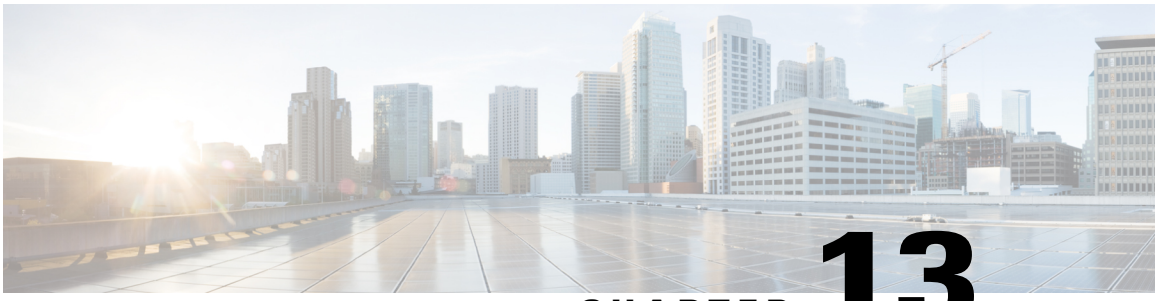
```
vm-name# configure
vm-name(config)# nsc-policy-agent
vm-name(config-nsc-policy-agent)# registration-ip n.n.n.n
vm-name(config-nsc-policy-agent)# shared-secret MySharedSecret
vm-name(config-nsc-policy-agent)# policy-agent-image
bootflash:vnmc-vsgpa.n.n.n.bin
vm-name(config-nsc-policy-agent)# exit
vm-name(config)# copy running-config startup-config
vm-name(config)# exit
vm-name# show nsc-pa status
```

- VSM VM

```
vm-name# configure terminal
vm-name(config)# nsc-policy-agent
vm-name(config-nsc-policy-agent)# registration-ip n.n.n.n
vm-name(config-nsc-policy-agent)# shared-secret MySharedSecret
vm-name(config-nsc-policy-agent)# policy-agent-image
bootflash:vsmpa.n.n.n.bin
vm-name(config-nsc-policy-agent)# copy running-config startup-config
```

PART IV

Managing Prime Network Services Controller



CHAPTER 13

Prime Network Services Controller Administrative Tasks

This section contains the following topics:

Initial Prime Network Services Controller Configuration

After installing Prime Network Services Controller, perform the following tasks to configure Prime Network Services Controller for use.

Task	Description
1. Configure Prime Network Services Controller connectivity with the hypervisor VM Manager.	Required only if you did not perform this task as part of the post-installation activities.
2. Verify service VM registration.	Confirms that service VMs that were deployed directly on the hypervisor are registered with Prime Network Services Controller.
3. Create user roles.	Configures user roles and privileges.
4. Configure authentication.	Configures LDAP providers and identifies a primary authentication service.
5. Create a trusted point.	Configures trusted points for LDAP over SSL.
6. Configure default system profiles and policies.	Configures the default Prime Network Services Controller system profile.

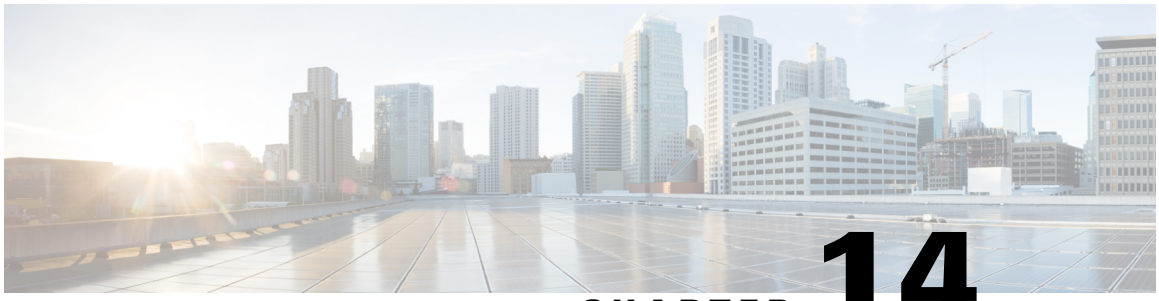
For more information on these tasks, see the Cisco Prime Network Services Controller User Guide or the online help.

Ongoing Administrative Activities

The following tasks are performed regularly as a part of ongoing administrative activities for Prime Network Services Controller.

Task	Description
Configure tenants.	Add tenants and subordinate organizations for resource and service allocation.
Configure service policies and profiles.	Configure access and security-related policies for access to resources.
Configure device policies and profiles.	Configure device-specific policies and profiles.
Add and configure resources.	Add and configure resources and services for each tenant or organization.
Import images.	Import images for service instantiation.

For more information on these tasks, see the Cisco Prime Network Services Controller User Guide or the online help.



CHAPTER 14

Backing Up and Restoring Prime Network Services Controller

This section contains the following topics:

Backing Up and Restoring Overview

Note

- We recommend that you use backup and restore as a disaster recovery mechanism. To migrate configuration data from one Prime Network Services Controller server to another use export and import operations.
- If you import a configuration from another Prime Network Services Controller instance, your current session will end. Log in again to continue.

For more information, see "Configuring Administrative Operations" in the Cisco Prime Network Services Controller User Guide.

Prime Network Services Controller enables you to back up and restore data for the same Prime Network Services Controller version. That is, the following backup and restore operations are supported:

- Backing up VNMC 2.1 and restoring to VNMC 2.1.
- Backing up Prime Network Services Controller 3.4 and restoring to Prime Network Services Controller 3.4.

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.4) is not supported.

After you restore Prime Network Services Controller, we recommend that you allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.

Note Do not use TFTP for backup and restore operations.

The following topics describe how to back up and restore data for Prime Network Services Controller:

- Workflow for Backing Up and Restoring Prime Network Services Controller, on page 82
- Restoring the Previous Version, on page 83

Workflow for Backing Up and Restoring Prime Network Services Controller

Prime Network Services Controller enables you to perform a backup using either the GUI or the CLI. You can back up and restore data for the same Prime Network Services Controller version. Backing up one version and restoring to another (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.4) is not supported.

We recommend the following:

- Do not perform a backup while the system is importing images.
- Use backup and restore as a disaster recovery mechanism.

The following table identifies the tasks associated with backing up and restoring Prime Network Services Controller and provides related information. This workflow assumes that Prime Network Services Controller is up and running and that service VMs are registered with Prime Network Services Controller.

Task	Notes
1. Back up Prime Network Services Controller.	You can back up Prime Network Services Controller using either the CLI or the GUI: • Using the CLI—See Backing Up Data, on page 41. • Using the GUI—See the online help or the "Configuring Administrative Operations" section in the Cisco Prime Network Services Controller User Guide.
2. In the hypervisor, power off and then delete the Prime Network Services Controller Device Adapter VM.	You will create a new Device Adapter instance after restoring Prime Network Services Controller.
3. Restore Prime Network Services Controller.	See Restoring the Previous Version, on page 83.

Task	Notes
4. Create a new instance of the Prime Network Services Controller Device Adapter.	When instantiating the Device Adapter: • Use the Device Adapter version that is the same as the version of Prime Network Services Controller that you are restoring. • Use the same host information (hostname, access credentials, and management IP address) that was used before you powered off the Device Adapter. For more information, see: • Deploying the Prime Network Services Controller Device Adapter on VMware, on page 29 • Installing the Prime Network Services Controller Device Adapter on OpenStack, on page 59
5. Clear the browser cache and log into the Prime Network Services Controller GUI.	Clearing the browser cache ensures that you do not see outdated information for Prime Network Services Controller.
6. Confirm that the service VMs and Device Adapter are registered with the restored Prime Network Services Controller and in running state.	• Service VMs—Choose **Resource Management > Managed Resources > root >** *tenant* and, in the Network Services tab, confirm that the service VMs are in Running state. • Device Adapter—Choose **Administration > Service Registry > Providers** and confirm that the Providers table includes managed endpoint and mgmt-controller entries for the Device Adapter. **Note** There might be a short delay before the Device Adapter is registered with Prime Network Services Controller. This is expected behavior and is not an issue if the service VMs are in Running state.

Restoring the Previous Version

Note

- Do not use TFTP to update data.
- Access the CLI through the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Before You Begin

Temporarily disable the CSA on the remote file server.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 (Optional) Check the current version of Prime Network Services Controller:

```
show version
```

Step 4 Download the required image from a remote file server:

```
copy scp://imageURLtoBinFile bootflash:/
```

Step 5 Enter the **update** command:

```
update bootflash:/ force
```

Step 6 Restore the previous version:

```
restore scp://user@host-ip-address/tmp/backup-file.tgz
```

where:

- *user* is the username for accessing the remote host.
- *host-ip-address* is the IP address of the remote host with the backup file.
- */tmp/backup-file.tgz* is the path and filename for the backup file.

Step 7 Restart the server:

```
service restart
```

Step 8 (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 9 (Optional) Verify that the Prime Network Services Controller software version has been restored:

```
show version
```

Step 10 Allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.

Step 11 To confirm that Prime Network Services Controller is fully accessible, log in via the GUI.

What to Do Next

Perform the post-restoration tasks described in Post-Restoration Tasks, on page 85.

Post-Restoration Tasks

After you successfully restore Prime Network Services Controller, complete the following tasks to reestablish the previous environment:

1 Updating VM Managers, on page 85

2 Reimporting Images, on page 85

Updating VM Managers

You must update any configured VM Managers after you upgrade or restore Prime Network Services Controller.

Procedure

Step 1 Choose **Resource Management > VM Managers**.

Step 2 Delete any stale VM Manager entries.

Reimporting Images

Prime Network Services Controller does not restore images that were previously imported. After you restore Prime Network Services Controller, complete the following procedure to reimport any required images.

Note Although you can upgrade a device out-of-band, doing so can disrupt traffic for standalone service nodes.

Before You Begin

Restore Prime Network Services Controller as described in Restoring the Previous Version, on page 83.

Procedure

Step 1 Log in to the Prime Network Services Controller GUI.

Step 2 Choose **Resource Management > Resources > Images**.

Step 3 For each image that you want to reimport, note the image properties, such as its name, operating system, and version. You can delete images that you no longer use or need.

Tip To find the original location of the image, right-click the item and choose **Edit** or **Properties**. The dialog box includes the location and name of the source file.

Step 4 After noting the details, delete each image from Prime Network Services Controller.

Step 5 Reimport the images using the information that you collected in Step 3.

Related Documentation

Prime Network Services Controller

The Prime Network Services Controller documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-services-controller/tsd-products-support-series-home.html

Cisco Intercloud Fabric Documentation

The Cisco Intercloud Fabric documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/security/asa-1000v-cloud-firewall/tsd-products-support-series-home.html

Cisco Cloud Services Router 1000V Documentation

The Cisco Cloud Services Router 1000V (CSR 1000V) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/tsd-products-support-series-home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-1000v-switch-vmware-vsphere/tsd-products-support-series-home.html

Cisco Prime Data Center Network Manager Documentation

The Cisco Prime Data Center Network Manager (DCNM) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/tsd-products-support-series-home.html

Cisco Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway (VSG) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/switches/virtual-security-gateway/tsd-products-support-series-home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.