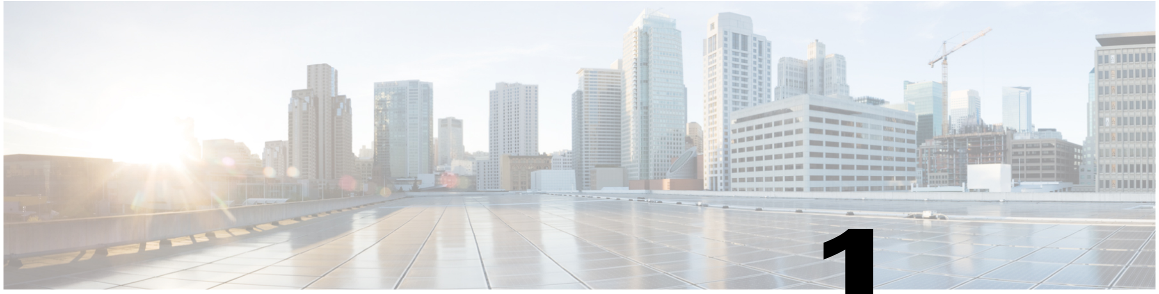
Cisco Prime Network Services Controller 3.0 Quick Start Guide

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

Text Part Number: OL-28178-01

CONTENTS



CHAPTER 1

Installation Prerequisites

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

New and Changed Information

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

Date	Revision	Location
February 14, 2014	Updated disk space requirements.	System Requirements, on page 2
	Updated information for upgrading from VNMC 2.1.	Upgrading to Prime Network Services Controller 3.0, on page 41

System Requirements

Requirement	Description
Virtual Appliance	
Two Virtual CPUs	1.5 GHz
Memory	4 GB RAM
Disk Space	One of the following, depending on InterCloud functionality: • With InterCloud functionality, 220 GB on shared NFS or SAN, and configured on two disks as follows: ◦ Disk 1—20 GB ◦ Disk 2—200 GB • Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: ◦ Disk 1—20 GB ◦ Disk 2—20 GB
Management Interface	One management network interface.
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
VMware	
VMware vSphere	Release 5.x with VMware ESX or ESXi (English Only)
VMware vCenter	Release 5.x (English Only)
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Web-Based GUI Client Requirements

Requirement	Description
Operating System	Either of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 9.0 or higher • Mozilla Firefox 11.0 or higher • Google Chrome 18.0 or higher[1]
Flash Player	Adobe Flash Player plugin 11.2 or higher

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

Firewall Ports Requiring Access

The following Prime Network Services Controller ports require access.

Port	Description
80	HTTP
443	HTTPS
843	Adobe Flash

Ports to Access Amazon AWS

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

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

Protocol	Ports
UDP	6644 and 6646

Cisco Nexus 1000V Series Switch Requirements

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

Information Required for Installation and Configuration

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

Required Information	Your Information
Management port profile name for VM (Virtual Machine) management **Note** The management port profile is the same port profile that is used for the Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and is used for the Prime Network Services Controller management interface.	
IP Address	
Subnet Mask	
Gateway IP Address	
Domain Name	
DNS Server **Note** Access to a DNS server is required for Prime Network Services Controller to communicate with the Amazon Cloud Provider.	
Admin Password	
Shared secret password for communications between Prime Network Services Controller, Cisco Virtual Security Gateway (VSG), Cisco Adaptive Security Appliance 1000V (ASA 1000V), and VSM. (See Shared Secret Password Criteria, on page 5.)	
For Configuring VMware vCenter in Prime Network Services Controller	
vCenter name	
Description	
Hostname or IP address	

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication channel. Passwords are designated as strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between Prime Network Services Controller, VSG, ASA 1000V, and VSM, adhere to the following criteria for setting valid, strong passwords:

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

    - Spaces

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

Strong passwords have:	Strong passwords do not have:
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive alphanumeric characters, such as abcd or 123. • Characters repeated three or more times, such as aaabbb. • A variation of the word Cisco, such as cisco, ocsic, or one that changes the capitalization of letters in the word Cisco. • The username, or the username in reverse. • A permutation of characters present in the username or Cisco.

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller 3.0, you must disable the Adobe Flash Players that are installed by default with Chrome.

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

Procedure

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

Step 2 Click **Details**.

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

Step 4 Download and install Adobe Flash Player version 11.6.602.180.

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

CHAPTER 2

Installing Prime Network Services Controller

This section includes the following topic:

Deploying the Prime Network Services Controller OVA

Before You Begin

- Set your keyboard to United States English before installing Prime Network Services Controller and using the VM console.
- Verify that the Prime Network Services Controller OVA image is available in the VMware vSphere Client.
- Make sure that all system requirements are met as specified in System Requirements, on page 2.
- Make sure that you have the information identified in Information Required for Installation and Configuration, on page 4.
- Configure Network Time Protocol (NTP) on all ESX and ESXi servers that run Prime Network Services Controller, ASA 1000V, VSG, VSM, and InterCloud images. For more information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and 5.0 hosts using the VMware vSphere Client" at http://kb.vmware.com/kb/0212069.

Procedure

Step 1 If you are installing Prime Network Services Controller on an ESXi 5.0 host, enable hardware-assisted virtualization by adding the property vhv.allow = TRUE to /etc/vmware/config.

Step 2 Use the VMware vSphere Client to log into the vCenter server.

Step 3 Choose the host on which to deploy the Prime Network Services Controller VM.

Step 4 From the File menu, choose **Deploy OVF Template**.

Step 5 In the Source screen, choose the Prime Network Services Controller OVA, then click **Next**.

Step 6 In the OVF Template Details screen, review the details of the Prime Network Services Controller template, then click **Next**.

Step 7 In the End User License Agreement screen, click **Accept**, then click **Next**.

Step 8 In the Name and Location screen, provide the required information, then click **Next**.

Step 9 In the Deployment Configuration screen, choose **Installer** from the Configuration drop-down list, then click **Next**.

Step 10 In the Datastore screen, select the data store for the VM, then click **Next**. The storage can be local or shared remote, such as NFS or SAN.

Step 11 In the Disk Format screen, click either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks, then click **Next**. The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

Note You can safely ignore the red text in the window.

Step 12 In the Network Mapping screen, select the management network port group for the VM, then click **Next**.

Step 13 In the Properties screen, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.

Note You can safely ignore the Prime Network Services Controller Restore fields.

Step 14 In the Ready to Complete screen, review the deployment settings, then click **Finish**.

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

A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 15 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 16 For ESXi 5.1 hosts, enable hardware-assisted virtualization by doing the following:

1. In the vSphere Client, right-click the Prime Network Services Controller VM, and choose **Upgrade Virtual Hardware**.
2. In the vSphere Web Client, right-click the Prime Network Services Controller VM, and choose **Configuration > Upgrade Virtual Hardware**.

VMware upgrades the virtual hardware to the latest supported version.

Step 17 Power on the Prime Network Services Controller VM.

Installing from an ISO Image

You can perform an installation using an ISO image.

Before You Begin

Make sure that all system requirements are met as specified in System Requirements, on page 2.

Procedure

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

Step 2 Open the VMware vSphere Client.

Step 3 Create a new virtual machine (VM) on the appropriate host as follows:

a) Enter the required information in the Configuration, Name and Location, and Storage screens.

b) In the Operating System screen, choose **Linux** and **Red Hat Enterprise Linux 5 64-bit**.

c) In the Network screen, choose a NIC.

Note A Single NIC is required for Prime Network Services Controller

d) In the Create a Disk Screen, provide the following information:

- Virtual Disk Size—Enter a minimum of 20 GB.
- Disk Provisioning—Choose **Thin or Thick Provisioning format**.

e) In the Ready to Complete Screen, review the information for accuracy and check the **Edit the Virtual Machine Settings Before Completion** check box.

f) In the Virtual Machine Properties dialog box, do the following:

1. In the Memory field, select **4 GB**.
2. In the Number of Virtual Sockets field, choose **2**.
3. Click **Add** to create a new hard disk with a minimum 200 GB disk size.
4. Click **OK** to create the new disk and to return to the Virtual Machine Properties dialog box.

g) In the Options tab, in the Boot Options field, choose **Force BIOS Setup**.

h) Click **Finish**.

Step 4 When the new VM is created, power it on.

Step 5 Mount the ISO to the VM CD ROM drive as follows:

1. Right-click the VM and choose **Open the VM Console**.
2. From the VM console, click **Connect/Disconnect CD/DVD Devices**.
3. Choose **CD/DVD Drive 1**.
4. Choose **Connect to ISO Image on Local Disk**.
5. Choose the **ISO image that you downloaded**.

Step 6 When prompted, enter the following information, then click **Next**:

- IP address
- Subnet mask
- Hostname
- Domain name
- Gateway IP address
- DNS server IP address

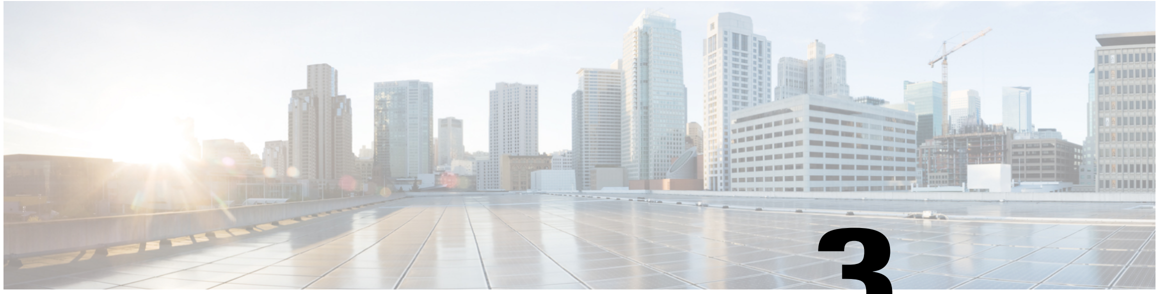
Step 7 In the Set Up NSC screen, enter the following information, then click **Next**:

- Admin password, and a confirming entry
- Shared secret password, and a confirming entry

Note Configuring a weak Shared secret at this stage will not create an error message, but the Shared secret will not be usable later.

Step 8 Confirm that the information is correct as displayed, then click **Next**.
Prime Network Services Controller is installed.

Step 9 When the installation is complete, reboot the VM.



CHAPTER 3

Configuring Prime Network Services Controller

This section includes the following topics:

Task 1—Configuring NTP

Before you perform any operations in Prime Network Services Controller system, configure Network Time Protocol (NTP) on Prime Network Services Controller, ASA 1000V, VSG, and VSM. NTP must be configured with a working NTP server. If you do not configure these items with a working NTP server, the following will occur:

- ASA 1000V, VSG, and VSM needs to be set up manually for time and date
- InterCloud functionality will not work because the AWS API requires the request time to be within a few seconds of the current time.

For information on configuring NTP, see the following topics:

- Configuring NTP in VMs, on page 14
- Configuring Prime Network Services Controller, on page 14

Configuring NTP in VMs

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

For this VM:	**Do this:**
ASA 1000V	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 4.1 and ESXi 5.0 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.
InterCloud Extender VM	Configure the NTP server in the Prime Network Services Controller GUI by choosing **InterCloud Management > InterCloud Policies > Device Profiles**. You can add the NTP server to the existing default device profile or create a new device profile with the required NTP server.
InterCloud Switch VM	When instantiating the InterCloud extender and InterCloud switch in Prime Network Services Controller using the InterCloud Link Wizard, select the correct device profile (with an NTP server configured) in the wizard to use for that instantiation.
VSG	Enter the following CLI command from the VSG console, where *x.x.x.x* is the NTP server IP address. `ntp server x.x.x.x`
VSM	Enter the following CLI command from the VSM console, where *x.x.x.x* is the NTP server IP address. `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://***server-ip-address* where *server-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 deploying the Prime Network Services Controller OVA (see Step 12 in Deploying the Prime Network Services Controller OVA, on page 9).

Step 3 Set the time zone by doing the following:

a) Choose **Administration** > **System Profile** > **root** > **System Profile** > **default**.
b) In the General tab, select the time zone.
c) Click **Save**.

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

a) Choose **Administration** > **System Profile** > **root** > **System Profile** > **default**.
b) In the Policy tab, select **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.

Task 2—Configuring Prime Network Services Controller Connectivity with vCenter

After you deploy the Prime Network Services Controller OVA, you need to establish connectivity with VMware vCenter by:

1. Downloading the vCenter Extension File, on page 15
2. Registering the vCenter Extension Plug-in in vCenter, on page 16
3. Configuring vCenter in Prime Network Services Controller VM Manager, on page 16

Downloading the vCenter Extension File

The first step in setting up vCenter connectivity is to download the vCenter extension file.

Before You Begin

- Make sure you have the information identified in Information Required for Installation and Configuration, on page 4.
- 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 **Administration** > **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 Plug-in in vCenter, on page 16).

Registering the vCenter Extension Plug-in in vCenter

Registering the vCenter Extension plug-in enables you to create a VM Manager in Prime Network Services Controller and connect to VMs.

Before You Begin

Make sure you have the information identified in Information Required for Installation and Configuration, on page 4.

Procedure

Step 1 From the VMware vSphere Client, log into the vCenter server that you want to manage by using Prime Network Services Controller.

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 You might need to scroll down and right-click near the bottom of the window to view the New Plug-in option.

Step 4 Browse to the Prime Network Services Controller vCenter extension file that you previously downloaded 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**.
A progress indicator shows the task status.

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

Configuring vCenter in Prime Network Services Controller VM Manager

Configuring a VM Manager in Prime Network Services Controller enables you to connect directly to VMs.

Procedure

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

Step 2 In the VM Managers pane, click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, enter the required information for vCenter, then click **OK**.
A successfully added VM manager is displayed with the following information:

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

Task 3—Registering VMs with Prime Network Services Controller

Registering VMs with Prime Network Services Controller ensures that Prime Network Services Controller recognizes and can communicate with the VMs. The VMs that must be registered are:

- ASA 1000V
- VSG
- VSM

Before You Begin

- Configure NTP on all ESX and ESXi servers that run VMs. For more information, see Task 1—Configuring NTP, on page 13.
- Deploy the VMs using the VMware vSphere Client.
- 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 VMware vSphere Client, choose **Home** > **Inventory** > **Hosts and Clusters**.

Step 2 Navigate to the newly deployed (and powered on) VM.

Step 3 Click the **Console** tab to access the CLI.

Step 4 In the CLI, register each VM as follows, depending on the type of VM:

- For ASA 1000V VMs, configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
vm-name> 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
```

- For VSG VMs, configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
vm-name> enable
Password:
vm-name# configure terminal
vm-name(config)# vnm-policy-agent
vm-name(config-vnmc-policy-agent)# registration-ip n.n.n.n
vm-name(config-vnmc-policy-agent)# shared-secret MySharedSecret
```

- For enterprise VSM VMs, configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
vm-name> enable
Password:
vm-name# configure terminal
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
```

Task 4—Verifying VM Registration in Prime Network Services Controller

This procedure enables you to verify that the required VMs are registered with Prime Network Services Controller.

Before You Begin

- Make sure you have the information identified in Information Required for Installation and Configuration, on page 4.
- Confirm the following:

For this device:	Confirm that:
ASA 1000V	• The ASA 1000V is installed. • NTP is set up on the ASA 1000V. • The Prime Network Services Controller policy agent status is correct on the ASA 1000V. • The ASA 1000V is registered to Prime Network Services Controller.
VSG	• The VSG is installed. • NTP is set up on the VSG. • The Prime Network Services Controller policy agent status is correct on the VSG. • The VSG is registered to Prime Network Services Controller.
VSM	• The VSM is registered to Prime Network Services Controller. • NTP is set up on the VSM. • The VSG and ASA 1000V port profiles are configured on the VSM. • The Prime Network Services Controller policy agent status is correct on the VSM.

For more information, see the following topics:

- Task 1—Configuring NTP, on page 13
- Task 3—Registering VMs with Prime Network Services Controller, on page 17

Procedure

Step 1 In Prime Network Services Controller, choose **Administration > Service Registry > Clients**.

Step 2 Confirm that the table in the Clients window contains *registered* in the Oper State column for the ASA 1000V, VSG, and VSM entries.

Task 5—Configuring a Tenant

Tenants are entities (such as businesses, agencies, or institutions) whose data and processes are hosted on VMs in a virtual data center. To provide firewall security for each tenant, you must first configure the tenant in Prime Network Services Controller.

Procedure

Step 1 Choose **Tenant Management > root**.

Step 2 In the upper-right corner of the Tenant Management Root pane, click **Create Tenant**.

Step 3 In the Create Tenant dialog box, enter a name and brief description for the tenant, then click **OK**.
The newly created tenant is listed in the navigation pane under root.

Task 6—Configuring a Service Profile

A profile is a collection of policies. By creating a profile and then applying that profile to one or more objects (such as a data interface for an ASA 1000V or a VSM port profile), you can ensure that those objects have consistent policies.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root >** *tenant* **> Compute Firewall > Compute Security Profiles** where *tenant* is the required tenant.

Step 2 In the General tab, click **Add Compute Security Profile.**

Step 3 In the Add Compute Security Profile dialog box, enter a name and description for the security profile, then click **OK**.

Task 7—Configuring a Device Profile

Device profiles enable you to apply multiple policies to one or more devices and ensure policy consistency across devices that use the same profile.

Procedure

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > *tenant* > **Device Profiles** where *tenant* is the required tenant.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, enter a name and description for the device profile, then click **OK**.

Task 8—Configuring a Compute Firewall

A compute firewall is a logical virtual entity in Prime Network Services Controller that contains the device profile that you assign to a VSG VM. Any device policies that are in the Prime Network Services Controller device profile are applied to the assigned VSG. After the policy has been applied to the VSG, the Config State status changes from *not-applied* to *applying*, and then to *applied*.

Procedure

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

Step 2 In the General tab, click **Add Compute**.

Step 3 In the Add Compute Firewall dialog box, enter the information described in the following table, then click **OK**.

Field	Description
Name	Compute firewall name, consisting of 1 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved.
Description	Brief description of the compute firewall.
Firewall Settings	
Device Profile	To apply a device profile: **1** Click **Select**. **2** In the Select Device Profile dialog box, choose the device profile, then click **OK**
Management Hostname	VSG hostname.
Data IP Address	VSG data IP address (*not* the management IP address).

Field	Description
Data IP Subnet	VSG subnet mask.

Task 9—Assigning a Compute Firewall to a VSG

After you configure a compute firewall in Prime Network Services Controller, you can assign it to a VSG so that the device policies in the specified device profile are applied to the VSG.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 Right-click the selected compute firewall, and choose **Assign VSG.**

Step 3 In the Assign VSG dialog box, from the VSG Management IP drop-down list, choose the VSG IP address, then click **OK**.
As the configuration is applied to the VSG, the Config State status changes from *not-applied* to *applying*, and then to *applied*.

Task 10—Configuring an Edge Firewall

Prime Network Services Controller provides support for virtual edge firewalls, such as ASA 1000V instances. After you add a virtual edge firewall, you can:

- Create and configure service policies.
- Create and configure edge device profile and edge security profiles for the edge firewalls.
- Apply the required profiles to the edge firewall and an outside edge firewall interface.

Procedure

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

Step 2 In the General tab, click **Add Edge Firewall**.

Step 3 In the Add Edge Firewall dialog box, provide the information described Add Edge Firewall Dialog Box, on page 23.

Step 4 Add one inside and one outside data interface to the edge firewall as follows:

1. Click **Add Data Interface**.

The Add Data Interface dialog box is displayed.

2 Add one inside data interface by using the information described in Add Data Interface Dialog Box, on page 23, then click **OK**.

3 Add one outside data interface by using the same information, then click **OK**.

Step 5 Click **OK** in the open dialog boxes.

Field Descriptions

Add Edge Firewall Dialog Box

Field	Description
Name	Edge firewall name.
Description	Brief description of the edge firewall.
HA Mode	High Availability (HA) role of the edge firewall: HA or standalone.
Device Profile	To apply a device profile: 1 Click **Select**. 2 In the Select Device Profile dialog box, choose the desired profile and click **OK**.
Edge Device Profile	To apply an edge device profile: 1 Click **Select**. 2 In the Select Edge Device Profile dialog box, choose the desired profile, then click **OK**.

Add Data Interface Dialog Box

Field	Description
Name	Interface name.
Description	Brief interface description.
Role	Whether the interface is for inside or outside communications.

Field	Description
DHCP	(Outside interfaces only) Check the **Enable DHCP** check box to enable DHCP on the interface.
Primary IP Address	IP address for this interface.
Secondary IP Address	(High availability mode only) Secondary IP address for this interface.
Subnet Mask	Mask to apply to the IP address.
Edge Security Profile	(Outside interfaces only) To apply an edge security profile: **1** Click **Select**. **2** In the Select Edge Security Profile dialog box, choose the desired profile, then click **OK**.
VLAN	(Inside interfaces only) VLAN to use for a service path if the device is running in Layer 2 mode.

Task 11—Assigning an Edge Firewall to an ASA 1000V Instance

Assigning an edge firewall to an ASA 1000V instance places the ASA 1000V in service with the associated policies and profiles.

Procedure

Step 1 Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Edge Firewalls** > *edge-firewall*. The Prime Network Services Controller GUI displays the newly added edge firewall and the following information:

- Configuration state
- Association state
- Pool assignment
- Faults tab

Step 2 In the General tab, right-click the required edge firewall and choose **Assign ASA 1000V**.

Step 3 In the Assign ASA 1000V dialog box, choose the required ASA 1000V instance from the ASA 1000V Management IP drop-down list, then click **OK**.

The Prime Network Services Controller GUI displays the newly added edge firewall and the following information:

- Faults associated with firewall

- Edge Security Profiles tab (to view associated edge security profiles configured in VSM)
- ASA 1000V instance information:
    - Service ID
    - Management IP address
    - HA role
    - Association state
    - Reachability

Step 4 To access more ASA 1000V instance properties, task details, faults, or events, click **Task** in the ASA 1000V Details area.

Task 12—Creating an Edge Security Profile

Edge security profiles include the policies and policy sets that you choose to ensure security for your edge firewalls.

Procedure

Step 1 Choose **Policy Management** > **Service Profiles** > **root** > *tenant* > **Edge Firewall** > **Edge Security Profiles**.

Step 2 In the General Tab, click **Add Edge Security Profile**.

Step 3 In the Add Edge Security Profile dialog box, do the following:

a) In the General tab, enter a name and description for the Edge Security Profile.
b) In the Ingress tab, choose a policy set from the Ingress Policy Set drop-down list.
c) In the Egress tab, choose a policy set from the Egress Policy Set drop-down list.

Note To add an ACL Policy set, click **Add ACL Policy Set** and follow the instructions in Task 13—Configuring Access Rules, on page 29.

Step 4 In the NAT tab, either select an existing NAT policy set or add a new policy set, as follows:

a) Click **Add NAT Policy Set**.
b) In the Add NAT Policy Set dialog box, enter the information as described in Add NAT Policy Set Dialog Box, on page 26.
c) To add a NAT policy, click **Add NAT Policy** and enter the information as described in Add NAT Policy Dialog Box, on page 26.
d) To add a rule to the NAT policy, click **Add Rule** and enter the information as described in Add NAT Policy Rule Dialog Box, on page 27.
e) To add a rule condition, click Add Rule Condition and enter the information as described in Add Condition Dialog Box, on page 29.

Note For information on the VPN and Advanced tabs, see the online help.

Step 5 Click **OK** in the open dialog boxes.

Field Descriptions

Add NAT Policy Set Dialog Box

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Whether the administrative state of the policy set is enabled or disabled.
Policies Area	
Add NAT Policy	Adds a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Add NAT Policy Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Rule Table	
Add Rule	Adds a rule to the current policy.
Name	Rule name.

Field	Description
Source Condition	Source attributes that must be matched for the current policy to apply.
Destination Condition	Destination attributes that must be matched for the current policy to apply.
Protocol	Protocols to which the policy applies.
Action	Whether the NAT translation is static or dynamic.
Source IP Pool	Translated address pool for a source IP address match condition.
Source Port Pool	Translated address pool for a source port match condition.
Source IP PAT Pool	Translated address pool for a source port address translation (PAT) match condition.
Destination IP Pool	Translated address pool for a destination IP address match condition.
Destination Port Pool	Translated address pool for a destination port match condition.

Add NAT Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Original Packet Match Conditions	
Source Match Conditions	Source attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.

Field	Description
Destination Match Conditions	Destination attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.
Protocol	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
NAT Action Table	
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.
Translated Address	Identify a translated address pool for each original packet match condition from the following options: • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group. The Source IP PAT Pool option is available only if you choose dynamic translation. Click **Add Object Group** to add object groups for the translation actions.

Field	Description
NAT Options	Check and uncheck the check boxes as required: • Enable Bidirectional—Check the check box for connections to be initiated bidirectionally; that is, both to and from the host. Available only for static address translation. • Enable DNS—Check the check box to enable DNS for NAT. • Enable Round Robin IP—Check the check box to allocate IP addresses on a round-robin basis. Available only for dynamic address translation. • Disable Proxy ARP—Check the check box to disable proxy ARP. Available only for static address translation.

Add Condition Dialog Box

Field	Description
Attribute Type	Attribute type for this condition. The available types depend on the type of policy that is being configured. For example, the attribute types available for an ACL policy differ from those available for a NAT policy.
Expression	
Attribute Name	Attribute names. The attributes that are available depend on the hypervisor that you are using.
Operator	Available operators to apply to the attribute. Depending upon the operator you choose, different information is required in the **Attribute Value** field.
Attribute Value	Attribute value. The information required depends upon the attribute name and operator.

Task 13—Configuring Access Rules

Access rules in Prime Network Services Controller permit or deny traffic based on the following items:

- Protocol
- Source IP address or network

- Destination IP address or network
- (Optional) Source and destination ports

Procedure

Step 1 Choose **Policy Management** > **Service Policies** > **root** > *tenant* > **Policies** > **ACL** > **ACL Policy Sets**.

Step 2 In the General tab, click **Add ACL Policy Set**.

Step 3 In the Add ACL Policy Set Dialog Box, enter a name and description for the policy set.

Step 4 To use an existing ACL policy, select the policy in the Available list and move it to the Assigned list.

Step 5 To add an ACL policy:

1. Click **Add ACL Policy**.
2. In the Add ACL Policy dialog box, enter a name and description for the policy, then click **Add Rule**.
3. In the Add ACL Policy Rule dialog box, enter the information as described in Add ACL Policy Rule Dialog Box, then click **OK**.

Step 6 Click **OK** in the open dialog boxes.
The Prime Network Services Controller window is refreshed, and the ACL Policy Sets table contains the new policy set.

Field Descriptions

Add ACL Policy Rule Dialog Box

Field	Description
Name	Rule name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	Brief rule description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).

Field	Description
Action to Take	1 Click the action to take if the rule conditions are met: • **Drop—**Drops traffic or denies access. • **Permit—**Forwards traffic or allows access. • **Reset—**Resets the connection. 2 Check the **Log** check box to enable logging.
Condition Match Criteria	Do one of the following: • Click **match-all** for the ACL Policy Rule to match all the conditions (AND). • Click **match-any** for the ACL Policy Rule to match any one condition (OR).
Src-Dest-Service Tab A rule can have a service condition or a protocol condition, but not both.	
Source Conditions	1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.
Destination Conditions	1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.

Field	Description
Service	1 Click **Add**. 2 Enter the required values for following: • Operator • Protocol • Port 3 Click **OK**.
Protocol Tab	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: 1 Uncheck the **Any** check box. 2 From the **Operator** drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. 3 In the Value fields, specify the protocol, object group, or range.
Ether Type Tab	Specify the encapsulated protocols to be examined for this rule: 1 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Greater than, Less than, Member, Not Member, In range, or Not in range. 2 In the Value fields, specify the hexadecimal value, object group, or hexadecimal range.
Time Range Tab	
To apply the rule all the time	Check the **Always** check box.
To apply the rule for a specific time range	1 Uncheck the **Always** check box. 2 Check the **Range** check box. 3 In the Absolute Start Time fields, provide the start date and time. 4 In the Absolute End Time fields, provide the end date and time.

Field	Description
To apply the rule based on membership in an object group	1 Uncheck the **Always** check box. 2 Check the **Pattern** check box. 3 From the Operator drop-down list, choose **member (Member of)**. 4 Do any of the following : • From the **Select Object Group** drop-down list, choose an existing object group. • Click **Add Object Group** to create a new object group. • Click the Resolved Object Group link to review or modify the specified object group.
To apply the rule on a periodic basis, with the frequency you specify	1 Uncheck the **Always** check box. 2 Check the **Pattern** check box. 3 From the Operator drop-down list, choose **range (In range)**. 4 In the Begin fields: 1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range. 2 Choose the beginning hour and minute, and AM or PM. 5 In the End fields: 1 From the End drop-down list, choose the ending day of the week or frequency. 2 Choose the ending hour and minute, and AM or PM. **Note** If you choose a frequency from the Begin drop-down list, choose the same frequency from the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.

Field	Description
Advanced Tab	Specify any source port attributes that must be matched for the current policy to apply: 1 Click **Add**. 2 Provide the required information in the following fields, and then click **OK**: • Attribute Name • Operator • Attribute Value

Task 14—Enabling Logging

Configuring and enabling a syslog policy for a VSG or ASA 1000V element ensures that you receive syslog messages for the severities that you specify. For example, depending on the syslog policy, you could receive syslog messages notifying you that a firewall rule has been invoked and that a permit or deny action has been taken.

Logging enables you to monitor traffic, troubleshoot issues, and verify that devices are configured and operating properly.

You can configure and enable syslog policies for VSG or ASA 1000V elements by doing either or both of the following:

- Enabling Policy-Engine Logging in a Monitor Session, on page 34
- Enabling Global Policy-Engine Logging

Enabling Policy-Engine Logging in a Monitor Session

Configuring a syslog policy enables you to specify the level of syslog messages to log and where to log the messages.

Procedure

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Syslog**.

Step 2 In the Syslog table, select **default**, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.

Step 4 In the Syslog Policy table, select the primary server type, then click **Edit**.

Step 5 In the Edit Syslog Client dialog box, provide the following information, then click **OK** in the open dialog boxes:

- Hostname/IP Address—Enter the syslog server IP address or hostname.

- Severity—Choose **Information (6)**.
- Admin State—Choose **Enabled**.

Enabling Global Policy-Engine Logging

Prime Network Services Controller enables you to set system-wide logging for the policy engine.

Procedure

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles** > **default**.

Step 2 In the Device Profiles pane, click the **Policies** tab.

Step 3 In the Policy Engine Logging area at the lower-right of the Policies tab, click **Enabled**, and then click **Save**.

CHAPTER 4

Troubleshooting Prime Network Services Controller Installation and Configuration

This section includes the following topics:

Overview

The Prime Network Services Controller interface provides links to browser windows that enable you to examine policy and configuration errors that prevent the successful application of a policy, or to review the faults and events associated with successfully applied policies and configurations. This feature also enables you to examine the faults associated with a compute or edge firewall.

Examining Faults and Errors for Edge Firewalls

Prime Network Services Controller enables you to view faults and configuration errors for edge firewalls.

Before You Begin

Assign the edge firewall to an ASA 1000V instance.

Procedure

Step 1 Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Edge Firewalls** > *edge-firewall*.

Step 2 In the General tab, in the States area, click **View Configuration Faults**.

Step 3 In the Fault Table window that appears in a new browser window, click the required tab:

- Faults—Includes fault severity, affected object, cause, last transition, acknowledgment state, type, and description.

- Events—Includes identifier, affected object, user, time stamp, cause, and description.
- Warnings—Includes affected object, scope, and description.

Step 4 To view additional information about an entry, select the entry, then click **Properties**.

Note You can also double-click an entry to view the fault or event details.

Step 5 To view updated information in the main window, click **Refresh Now**.

Examining Faults and Errors for Compute Firewalls

Prime Network Services Controller enables you to examine faults and configuration errors for compute firewalls.

Before You Begin

Assign the compute firewall to a VSG instance.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the General tab, in the States area, click **View Configuration Faults**.
The Fault Table is displayed in a new browser window, and includes the fault severity, affected object, cause, last transition, acknowledgment state, type, and description.

Step 3 To view additional information about an entry, double-click the entry, or select the entry and then click **Properties**.

CHAPTER 5

Upgrading and Patching Prime Network Services Controller

This section includes the following topics:

Overview

Note

- Use the following upgrade procedure when you upgrade to a newer Prime Network Services Controller version. For Prime Network Services Controller 3.0, the only supported upgrade paths are from Cisco Virtual Network Management Center (VNMC) 2.0 or 2.1 to Prime Network Services Controller 3.0.
- If are upgrading from VNMC 2.1, the VNMC 2.1 deployment must span only one disk. If it spans more than a single disk, you cannot upgrade to Prime Network Services Controller 3.0.

The following scenarios are not supported:

- Backing up from VNMC 2.0 or 2.1 and restoring to Prime Network Services Controller 3.0.
- Exporting from VNMC 2.0 or 2.1 and importing to Prime Network Services Controller 3.0.

To upgrade from VNMC 2.0 or 2.1 to Prime Network Services Controller 3.0, perform the following tasks:

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. Perform a full-state backup of VNMC 2.x by using Secure Copy (SCP) protocol—See Backing Up Data, on page 40.

3 Upgrade to Prime Network Services Controller 3.0 by using the CLI **update bootflash** command—See Upgrading to Prime Network Services Controller 3.0, on page 41.

Note After you upgrade to Prime Network Services Controller 3.0, you might see the previous version in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Backing Up Data

You can use either of the following methods to back up data before upgrading Prime Network Services Controller:

- To use the CLI, continue with this topic.
- To use the GUI, see Backing Up Prime Network Services Controller, on page 46.

We recommend that you *not* perform a backup when any of the following tasks are running on the system:

- Image import
- Migration of a VM to the cloud
- Deployment of an InterCloud Switch
- Creation of an InterCloud link

Note Temporarily disable the Cisco Security Agent (CSA) on the remote file server.

Note Do not use TFTP to back up data.

Procedure

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

Note We recommend that you access the CLI via the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

```
create backup scp://user@host/file fullstate 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 into the SCP server, and make sure that */file* exists and that the file size is not zero (0).

Upgrading to Prime Network Services Controller 3.0

After you back up the VNMC 2.x data, you can upgrade to Prime Network Services Controller 3.0.

Caution To save a state for recovery purposes, perform a backup before beginning the upgrade. For more information, see Backing Up Data, on page 40.

Note

- Do not use TFTP to update data.
- Do not access the GUI during the upgrade process.

Before You Begin

- Ensure that Prime Network Services Controller can access a DNS server. If a DNS server is not accessible, Prime Network Services Controller will not be able to access the Amazon Cloud Provider.
- If you are upgrading from VNMC 2.1, the VNMC 2.1 deployment must span only one disk. If it spans more than a single disk, you cannot upgrade to Prime Network Services Controller 3.0.
- Prime Network Services Controller 3.0 requires 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 3.0.
- Ensure the VNMC 2.1 deployed using ISO images are on a single disk. If the VNMC deployment is on 2 or more disks, you will not be able to upgrade to 3.0.

Procedure

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

Note We recommend that you access the CLI via the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

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 3.0 image from a remote file server:

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

Step 5 Upgrade to Prime Network Services Controller 3.0:

```
update bootflash:/nsc.3.0.0.XXXX.bin
```

where *nsc.3.0.0.XXXX.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 via 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.

Patching Prime Network Services Controller

Use the CLI to apply the patch.

Procedure

Step 1 As user admin, log into the Prime Network Services Controller system to be patched:

```
ssh admin@server-ip-address
```

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 Update the bootflash:

```
update bootflash:/nsc.3.0.0.XXXX.bin
```

where *nsc.3.0.0.XXXX.bin* is the name of the patch file.

Step 4 Restart the Prime Network Services Controller services:

```
service restart
```

Step 5 Verify that all services are running:

```
service status
```

Step 6 To verify that the patch was applied, check the update history:

```
show update-history
```

CHAPTER 6

Backing Up and Restoring Prime Network Services Controller

This section includes the following topics:

Note For information about exporting or importing, see the Cisco Prime Network Services Controller 3.0 User Guide.

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, see the Cisco Prime Network Services Controller 3.0 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 2.0 and restoring to VNMC 2.0.
- Backing up Prime Network Services Controller 3.0 and restoring to Prime Network Services Controller 3.0.

Backing up one version and restoring to another version (such as backing up VNMC 2.0 and restoring to Prime Network Services Controller 3.0) is not supported.

Note Do not use TFTP for backup and restore operations.

The following topics describe how to back up data and restore data for Prime Network Services Controller 3.0:

- Backing Up Prime Network Services Controller, on page 46
- Restoring the Previous Version, on page 46

Backing Up 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 2.0 and restoring to Prime Network Services Controller 3.0) is not supported.

We recommend the following:

- That you do not perform a backup when any of the following tasks are running on the system:
    - Image import
    - Migration of a VM to the cloud
    - Deployment of an InterCloud Switch
    - Creation of an InterCloud link
- That you use backup and restore as a disaster recovery mechanism. To save a state for recovery purposes, perform a backup via the GUI or CLI, using one of the following methods:
    - CLI—See Backing Up Data, on page 40.
    - GUI—See the Cisco Prime Network Services Controller 3.0 User Guide.

Restoring the Previous Version

Note Do not use TFTP to update data.

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.

Note We recommend that you access the CLI via the console instead of SSH. If the SSH session should disconnect, you will not be able to access the VM.

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:/nsc.3.0.0.XXXX.bin 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 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 47.

Post-Restoration Tasks

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

- Update VM Managers—See Updating VM Managers, on page 48.
- Reimport InterCloud and VM images—See Reimporting InterCloud and VM Images, on page 48.
- Verify InterCloud status—See Verifying InterCloud Status, on page 49.

Updating VM Managers

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

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Managers**.

Step 2 For existing vCenters that you wish to retain, reimport the vCenter Extension plugin. For more information, see the Cisco Prime Network Services Controller 3.0 User Guide.

Step 3 Check and delete any stale VM Manager entries.

Reimporting InterCloud and VM Images

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

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 46.

Procedure

Step 1 Log into the Prime Network Services Controller GUI.

Step 2 Review the imported images in the following screens:

- VM Images—Choose **InterCloud Management > Enterprise > VM Images**.
- Infrastructure Images—Choose **InterCloud Management > InterCloud Link > Infrastructure Images**.
- InterCloud Agent Images—Choose **InterCloud Management > InterCloud Link > InterCloud Agent Images**.

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

Note To find the original location of the image, right-click the image and choose **Edit**. The Edit 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.

Verifying InterCloud Status

When a backup is performed, InterCloud-related tasks might be running but not completed. When the system is restored, Prime Network Services Controller starts the tasks from the point at which it was backed up. The following steps enable you to verify the status of InterCloud-related objects after you restore the system.

If a task fails for any reason, we recommend that you abort, terminate, or undeploy the task as appropriate, and then restart the task.

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 46.

Procedure

Step 1 Choose **InterCloud Management** > **InterCloud Link** > **Provider Accounts** and confirm that the provider accounts are valid.

Step 2 Choose **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc* > *intercloud-link* and review the link status:

- If an InterCloud link was deployed in the backed-up system, but is no longer deployed:

  1. Choose **Administration** > **Service Registry** > **Clients**.
  2. If the Oper State column contains *lost-visibility*, wait approximately 10 minutes to see if visibility is regained. If visibility is not regained after 10 minutes, continue with the next steps.
  3. In VMware vCenter, verify that the InterCloud Extender exists in the VM placement detail. The path in VMware is *vm-manager* > *datacenter* > *cluster/host* > *extender-vm* > **Edit** > **Placement**.
  4. In VMware vCenter, verify that the InterCloud Switch exists on the public cloud. The path in VMware is *vm-manager* > *datacenter* > *cluster/host* > *switch-vm* > **Edit** > **General**.
  5. If the InterCloud Extender or InterCloud Switch does not exist, undeploy and then delete the link.

- If an InterCloud link was being deployed when the system was backed up and completed deployment after the backup, Prime Network Services Controller will attempt to deploy the link from the point at which the system was backed up. In this situation, do either of the following, as appropriate:

  - Because the InterCloud Extender and InterCloud Switch exist in the network, you can wait to see if the link will be deployed within a few minutes.
  - If the InterCloud link deployment task displays an error, undeploy the link and redeploy it.

Step 3 Choose **InterCloud Management** > **Public Cloud VPCs** > *vpc* > **VMs** and review cloud VM status:

- If a cloud VM was deployed and existed in the backed-up system but was deleted due to VM termination after the system backup:

  1 In the list of cloud VMs, obtain the cloud instance ID.

  2 Check the public cloud for the selected cloud instance.

  3 If the VM instance does not exist on the cloud, you can delete the VM.

- If a user created a cloud VM instance after the backup, the restored system will not have a record of it. There is no way to recover the cloud VM instance. You will need to create a new cloud VM.
- If a cloud VM was being instantiated when the system was backed up and completed deployment after the backup, Prime Network Services Controller will start the VM instantiation task from the point at which the system was backed up. In this situation, do either of the following, as appropriate:
  - Wait for a while to see if the cloud VM will be instantiated.
  - If the instantiation fails for any reason, terminate the VM instantiation process, and initiate a new cloud VM instantiation.

Step 4 Reconcile the InterCloud Switch and cloud VM public IP addresses.
If the InterCloud Switch and cloud VM public IP addresses are changed after the backup, you need to restore the IP addresses manually. This situation can occur if the InterCloud Switch or cloud VM is rebooted after the backup. To reconcile the IP addresses:

1 If the InterCloud Switch is in lost-visibility state (**Administration** > **Service Registry** > **Clients**), reboot the InterCloud Switch by choosing **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc* > *intercloud-link* > **InterCloud Switch Tab** > *intercloud-switch* > **Reboot**.

2 If the cloud VM tunnel is not *up* (**InterCloud Management** > **Public Cloud** > **VPCs** > *vpc* > **VMs**), reboot the cloud VM.

Step 5 Reconcile the InterCloud link and cloud VM that were created after the backup on Prime Network Services Controller, as follows:

a) For InterCloud links that were created after the backup, do the following:

1 Remove the InterCloud Extender in vCenter.

2 Remove the InterCloud Switch in Amazon Web Services (AWS).

3 Remove the cloud VMs from AWS.

b) For Intercloud links that were deleted after the backup, perform the following steps in the Prime Network Services Controller GUI:

1 Terminate the cloud VMs by choosing **InterCloud Management** > **InterCloud Link** > **VPCs** > **VMs tab** > *cloud-vm* > **Terminate**.

2 Undeploy the InterCloud link by choosing **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc* > *intercloud-link* > **Undelploy**.

3 Delete the InterCloud link by choosing **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc* > *intercloud-link* > **Delete**.

CHAPTER 7

Additional Information

This section includes the following topics:

Related Documentation

Cisco Virtual Network Management Center

The following Prime Network Services Controller documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- *Cisco Prime Network Controller 3.0 Documentation Overview*
- *Cisco Prime Network Controller 3.0 Release Notes*
- *Cisco Prime Network Controller 3.0 Quick Start Guide*
- *Cisco Prime Network Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Controller 3.0 User Guide*
- *Cisco Prime Network Controller 3.0 XML API Reference Guide*
- *Open Source Used in Cisco Prime Network Controller 3.0*

Cisco ASA 1000V Documentation

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

http://www.cisco.com/en/US/products/ps12233/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/en/US/products/ps11208/tsd_products_support_model_home.html

Cisco Nexus 1000V Series Switch Documentation

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

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/en/US/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.