Cisco Prime Network Services Controller 3.5.1b Installation Guide

First Published: 2020-06-29

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. simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services. For the latest release updates and overview, see the corresponding data sheet.

Cisco Prime Network Services Controller is the primary management element for Cisco Nexus 1000VE Switches and Services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000VE 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.

Cisco 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. 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 security services.

Note Starting with Cisco PNSC Release 3.4.2a, Cisco Adaptive Security Appliance (ASA 1000V), Cisco Cloud Services Router (CSR), Citrix NetScaler VPX, Citrix NetScaler, and KVM Hypervisor, and Microsoft HyperV platforms are not supported.

Hypervisor Support

The Prime Network Services Controller platform supports multiple VM Managers through their APIs and through tight integration with Nexus 1000VE Virtual Supervisor Modules (VSMs) and Virtual Ethernet Modules (VEMs).

Cisco Dynamic Fabric Automation Integration Support

Cisco Dynamic Fabric Automation (DFA) delivers fabric optimization, management, and automation capabilities under Cisco Unified Fabric. Prime Network Services Controller plays a critical role in the Cisco DFA solution with L4-7 services integration. Prime Network Services Controller integrates with Cisco Data Center Network Manager (DCNM) to support the managed resources and services in a VMware vSphere environment.

Consistent and Efficient Security Policies

Prime Network Services Controller uses security profiles for template-based configuration of security policies. A security profile is a collection of security policy sets and integrated policies and rules that can be predefined and applied on demand at the time of virtual machine instantiation. This profile-based approach significantly simplifies authoring, deployment, and management of security policies, including dense multi-tenant environments, while enhancing deployment agility and scaling. Security profiles also help reduce administrative errors and simplify audits.

The XML API for Prime Network Services Controller facilitates integration with northbound network provisioning tools for programmatic network and security provisioning and management of Cisco VSG (VSG) and ASA 1000V. The option of programmatic control of those virtual appliances can greatly simplify operational processes and reduce infrastructure management costs.

Nondisruptive Administration Model

By providing visual and programmatic controls, Prime Network Services Controller can enable the security operations team to author and manage security policies for virtualized infrastructure and enhance collaboration with the server and network operations teams. This nondisruptive administration model helps ensure administrative segregation of duties to reduce errors and simplify regulatory compliance and auditing:

- Security administrators can author and manage security profiles and manage VSG instances. Security profiles are referenced in Nexus 1000VE port profiles.
- Network administrators can author and manage port profiles, and manage Nexus 1000VE switches. Port profiles with referenced security profiles are available in VMware vCenter through the Nexus 1000VE VSM programmatic interface with VMware vCenter.
- Server administrators can select an appropriate port profile in VMware vCenter when instantiating a virtual machine.

Efficient Management for Easier Scalability

Prime Network Services Controller implements an information-model architecture in which each managed device, such as VSG or Cisco ASA 1000V, is represented by the device's object-information model. This model-based architecture helps enable the use of:

- Stateless managed devices—Security policies (security templates) and object configurations are abstracted into a centralized repository and used as templates against any virtual device type.
- Dynamic device allocation—A centralized resource management function manages pools of devices that are commissioned (deployed) in service and a pool of devices that are available for commissioning. This approach simplifies large-scale deployments because managed devices can be preinstantiated and then configured on demand, and devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools.
- Scalable management—A distributed management-plane function is implemented using an embedded agent on each managed device that helps enable greater scalability.

Features and Benefits

The following table lists the features and benefits of using .

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. **Note** Citrix NetScaler VPX, CSR 1000V and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Starting with Cisco PNSC release 3.4.2a, only Cisco VSG is supported.	Simplifies provisioning and troubleshooting in a scaled-out data center.
Security Profiles	A security profile represents the VSG 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 are stateless, receiving information from .	• 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.
Context-Aware Security Policies	obtains virtual machine contexts from VMware vCenter.	Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure.

Features	Description	Benefits
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	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	is designed to manage VSG 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	XML API allows external system management and orchestration tools to programmatically provision VSG .	• Allows the use of the best-in-class management software. • Offers transparent and scalable operation management.

Note Citrix NetScaler VPX, CSR 1000V, and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Hypervisors Openstack KVM and Microsoft HyperV are supported in PNSC releases up to 3.4.1d.

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

Requirement	Description
Disk space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 GB • 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

Hypervisor Requirements

Prime Network Services Controller is a multi-hypervisor virtual appliance that can be deployed on VMware vSphere.

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

Requirement	Description
VMware	
VMware vSphere	6.5.0, 6.7 U1, 6.7 U2, 6.7 U3
VMware vCenter	6.5 U2, 6.7 U1, 6.7 U2, 6.7 U3

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Either of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following: • Mozilla Firefox 26.0 or later (recommended) • Google Chrome 32.0 or later • Internet Explorer 10.0 or later
Flash player	Adobe Flash Player plugin 11.9 or later

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/SSH
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.

Category	Requirement
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, on page 9
- Shared Secret Password Criteria, on page 10
- Configuring Chrome for Use with Prime Network Services Controller, on page 11

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 [1]	
VM name	
VMware datastore Location	
For Prime Network Services Controller Installation	
IP address	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	

Required Information	Your Information/Notes
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria, on page 10.)	

[1] 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 , VSG, 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.

SUMMARY STEPS

1. In the Chrome URL field, enter **chrome://plugins**.
2. Click **Details** to expand all the files associated with each plugin.
3. Locate the Adobe Flash Player plugins, and disable each one.
4. Download and install Adobe Flash Player plugin version 11.9 or higher.
5. Close and reopen Chrome before logging in to Prime Network Services Controller.

DETAILED STEPS

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, on page 15
- Installing Prime Network Services Controller Using the OVA Image, on page 15
- Installing Prime Network Services Controller Using an ISO Image, on page 17

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 PNSC	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.

SUMMARY STEPS

1. Using the VMware vSphere Client, log in to the vCenter server.
2. Choose the host on which to deploy the Prime Network Services Controller VM.
3. Right-click **Host** and select **Deploy OVF Template** from the Pop-up menu.
4. In the wizard, provide the information as described in the following table:
5. Click **Finish**.
6. After Prime Network Services Controller is successfully deployed, click **Close**.
7. Power on the Prime Network Services Controller VM.

DETAILED STEPS

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 Right-click **Host** and select **Deploy OVF Template** from the Pop-up menu.

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.	

Screen	Action
A. IP Address	VM management IP address.
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 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:

Configuring VMware for Prime Network Services Controller

Before you install Prime Network Services Controller (PNSC) 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 and gather the information required for configuration. See *Preparing for Imstallation* chapter.

Step 1 Download a Prime Network Services Controller ISO image to your client machine. In case of vSphere 6.5 and greater, upload the PNSC ISO image to datastore.

Step 2 Open the VMware vSphere Client (for version 5.5 or 6.0) or Web client (version 6.5a).

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	• Set the number of NICs to **1**. A single NIC is required for Prime Network Services Controller. • Choose a NIC. • 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**.
Create a Disk	**a.** Disk Size—Enter a minimum of 20 GB. **b.** Disk Provisioning—Choose Thin Provision or Thick Provision. **c.** Location—Specify the location of the data store.
Advanced Options	Specify options as needed.

Step 5 For VMware vSphere version 5.5 and 6.0, 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. Create an additional hard disk with 200 GB memory with thin provisioning. For VMware vSphere 6.5 webclient, choose the **Network** and **ISO disk** from the datastore and select the **Connect** check box.

e. 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.

f. For VMware vSphere 6.5 webclient, choose the Network for the VM. For the Image choose your uploaded ISO disk from datastore.

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

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

Step 9 For VMware vSphere 5.5 and 6.0, 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/Dsiconnect 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.

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.

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**. For vSphere 6.5a Webclient, you need to power off the VM and edit the configuration to uncheck the **Connect** check box for ISO disk and then power on the VM again to complete the 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:

- VSG
- VSM

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

Note NTP service does not come up on the terminal when PNSC is upgraded from the previous releases to Release 3.4.1d or later. To access the NTP service, you need to re-login into the same terminal or start a new terminal.

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:
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."

For this VM:	Do this:

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.

SUMMARY STEPS

1. In your browser, enter **https://***ip-address* where *ip-address* is the Prime Network Services Controller IP address.
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.
3. Set the time zone by doing the following:
4. Add an external NTP server as the time source, as follows:

DETAILED STEPS

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

Establish connectivity between 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

Note You need to export and Register the VMware vCenter Extension plugin for VMware vCenter releases 5.5 and 6.0. For VMware vCenter release 6.5 onward, plugin registration is automated and you need to enter VMware vCenter Administrator Credentials while adding VM Manager.

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.

SUMMARY STEPS

1. In , choose **Resource Management** > **VM Managers** > **VM Managers**.
2. In the VM Managers pane, click **Export vCenter Extension**.
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).
4. Open the XML extension file to confirm that the content is available.

DETAILED STEPS

Step 1 In , 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

Registering the vCenter extension plug-in enables you to create a VM Manager in Prime Network Services Controller and communicate with the vCenter VMM and the VMs that Prime Network Services Controller manages.

SUMMARY STEPS

1. From the VMware vSphere Client, log in to the vCenter server that you want to manage by using Prime Network Services Controller.
2. In the vSphere Client, choose **Plug-ins** > **Manage Plug-ins**.
3. Right-click the window background and choose **New Plug-in**.
4. Browse to the Prime Network Services Controller vCenter extension file that you previously exported and click **Register Plug-in**.
5. In the security warning message box, click **Ignore**.
6. When the success message is displayed, click **OK**, and then click **Close**.

DETAILED STEPS

Step 1 From the VMware vSphere Client, log in to 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 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 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 you register the vCenter extension plug-in in vCenter, you can configure connectivity with vCenter in Prime Network Services Controller.

SUMMARY STEPS

1. Choose **Resource Management** > **VM Managers** > **VM Managers**, and then click **Add VM Manager**.
2. In the Add VM Manager dialog box, enter the following information and then click **OK**:

DETAILED STEPS

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.
- For VMware vCenter release 6.5, choose **vCenter 6.5 and greater** check box and enter vSphere vCenter Administrator credentials.

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.3.5.*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.

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.

Registering Cisco VMs Deployed on VMware

This procedure describes how to register 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.

SUMMARY STEPS

1. In the hypervisor, navigate to the VM to be registered with Prime Network Services Controller.
2. Open a console window for the VM.
3. In the CLI, register the VM as follows:

DETAILED STEPS

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:

- 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
```

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.

SUMMARY STEPS

1. Choose **Policy Management** > **Service Policies** > **root** > **Policies** > **Service Path**.
2. In the General tab, choose the default service path and then click **Delete**.

DETAILED STEPS

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**.

Note Instead of service path configurations from PNSC GUI, use vservice node configurations from VSM CLI to use Cisco Virtual Security Gateway. For deployment configurations, see the Cisco Virtual Security Gateway Deployment Guide. Use the Cisco VSG-L2 adjacent and Cisco VSG-L3 adjacent configurations.

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 29
- Troubleshooting Devices and Services, on page 31

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 29
- Updating Nexus 1000V Services After Changing the Prime Network Services Controller IP Address, on page 30

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.

SUMMARY STEPS

1. For each VSM registered with Prime Network Services Controller:
2. For each VSG registered with Prime Network Services Controller:

DETAILED STEPS

Step 1 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 2 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.3.5.*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.

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.3.5.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.

Troubleshooting Devices and Services

You can use to troubleshoot faults associated with managed devices and services.

SUMMARY STEPS

1. Choose **Resource Management** > **Managed Resources** > **root** > *tenant*.
2. In the Network Services tab, choose the required service or device, and then click **Edit**.
3. In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.
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**.

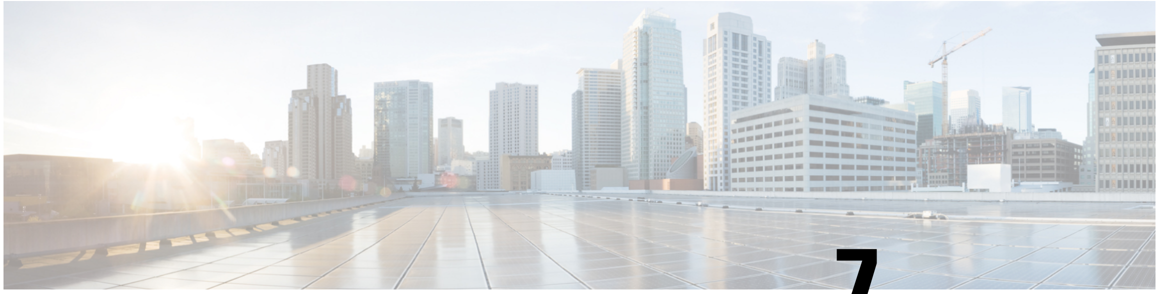
DETAILED STEPS

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 3.5.1b 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 3.5.1b.

The following tables show the supported upgrade paths for Prime Network Services Controller. Upgrading to Prime Network Services Controller 3.5.1b is supported only in VMware environments.

Table 1: Supported Upgrade Paths for Prime Network Services Controller 3.5.1b

Hypervisor	**Supported Upgrade Versions**	
	Standalone Mode	**Orchestrator Mode**
VMware	3.2, 3.2.2a, 3.2.2b, 3.4.1c, 3.4.1d, 3.4.2a, 3.4.2b, 3.4.2c, 3.5.1a, 3.5.1b	Not applicable

To upgrade from VNMC 2.x to Prime Network Services Controller 3.5.1b, 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 3.5.1b.
- Exporting from VNMC 1.x or 2.x and importing to Prime Network Services Controller 3.5.1b.

To upgrade to Prime Network Services Controller 3.5.1b, confirm that you meet the following requirement:

- 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.

Note For more information on PNSC upgrade matrix, see the *Cisco Prime Network Services Controller Release Notes* at http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_services_controller/3-4-2b/release-notes/b_CiscoPrimeNetworkServicesController-3-4-2-ReleaseNotes.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 35.
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 , on page 37.
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: Mozilla Firefox (recommended browser), Internet Explorer, and Chrome.

Migrating Classic PNSC (Release 3.4.2x) to NG PNSC (Release 3.5.1x)

To upgrade classic PNSC (release 3.4.2x) to next generation PNSC (release 3.5.1x), follow the instructions provided in Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment section.

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.

SUMMARY STEPS

1. Using the console, log in to Prime Network Services Controller as admin.
2. Enter system mode:
3. Create a full-state backup file:
4. When prompted, enter the required password.
5. At the `/system/backup*` prompt, enter:
6. Log in to the SCP server, and make sure that */file* exists and that the file size is not zero (0).

DETAILED STEPS

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).

PNSC Environment Upgrade Matrix and Path

This section lists the compatibility information and upgrade path for Cisco PNSC versions.

Table 2: PNSC Upgrade Path

Initial Version	Intermediate State(s)	Final Version
2.0.3	2.1 to 3.0.2g to 3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
2.1	3.0.2 to 3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
3.0.2	3.2.2a to 3.4.1d to 3.5.1a	3.5.1b
3.2.1d	3.4.1d to 3.5.1a	3.5.1b
3.2.2b	3.4.1d to 3.5.1a	3.5.1b
3.4.1b	3.4.1d to 3.5.1a	3.5.1b
3.4.1c	3.4.1d to 3.5.1a	3.5.1b
3.4.1d	3.5.1a	3.5.1b
3.4.2a	3.5.1a	3.5.1b
3.4.2b	3.4.2d	3.5.1b
3.4.2c	3.5.1a	3.5.1b
3.4.2d	N/A	3.5.1b
3.5.1a	N/A	3.5.1b

Upgrading to Prime Network Services Controller

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

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.

Note For more information on PNSC upgrade matrix, see the *Cisco Prime Network Services Controller Release Notes* at http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_services_controller/3-4-2b/release-notes/b_CiscoPrimeNetworkServicesController-3-4-2-ReleaseNotes.html.

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 35.
- Prime Network Services Controller 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 .

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 image from a remote file server:

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

Step 5 Upgrade to Prime Network Services Controller :

```
update bootflash:/
```

where 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.

Synchronizing PNSC system clock with Network Time Protocol Server

After the PNSC upgrade is complete, to synchronize the PNSC system clock with the configured Network Time Protocol (NTP) server, perform the the following steps.

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

Step 2 Connect to **policy-mgr**:

```
localhost#connect policy-mgr
```

Step 3 Create an NTP server host `127.127.1.0`.

a) `localhost(policy-mgr)# scope org`

b) `localhost(policy-mgr) /org # scope deviceprofile default`

c) `localhost(policy-mgr) /org/deviceprofile # create ntp-server 127.127.1.0`

d) `localhost(policy-mgr) /org/deviceprofile* # commit`

Step 4 Delete the NTP server host which you created in the previous step.

a) `localhost(policy-mgr) /org/deviceprofile # delete ntp-server 127.127.1.0`

b) `localhost(policy-mgr) /org/deviceprofile* # commit`

c) `localhost(policy-mgr) /org/deviceprofile # exit`

d) `localhost(policy-mgr) /org # exit`

e) `localhost(policy-mgr)# exit`

Step 5 Verify if the NTP server host has been deleted.

```
localhost(local-mgmt)# sh ntp peer status
```

Only the NTP configured server/servers will be displayed.

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
bgl11-row1-dc-n .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

PART II

Managing Prime Network Services Controller

CHAPTER 8

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 9

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 3.5.x and restoring to Prime Network Services Controller 3.5.x.

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.5.x) 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 46
- Restoring the Previous Version, on page 47

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) 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 35. • 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 47.

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 PNSC Device Adapter on VMware* • *Installing the PNSC Device Adapter on OpenStack*
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.

SUMMARY STEPS

1. Using the console, log in to Prime Network Services Controller as admin.
2. Connect to local-mgmt:
3. (Optional) Check the current version of Prime Network Services Controller:
4. Download the required image from a remote file server:
5. Enter the **update** command:
6. Restore the previous version:
7. Restart the server:
8. (Optional) Confirm that the Prime Network Services Controller server is operating as desired:
9. (Optional) Verify that the Prime Network Services Controller software version has been restored:
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.
11. To confirm that Prime Network Services Controller is fully accessible, log in via the GUI.

DETAILED STEPS

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 49.

Post-Restoration Tasks

After you successfully restore , complete the following tasks to reestablish the previous environment:

1. Updating VM Managers, on page 49
2. Reimporting Images, on page 50

Updating VM Managers

You must update any configured VM Managers after you upgrade or restore .

SUMMARY STEPS

1. Choose **Resource Management** > **VM Managers**.
2. Delete any stale VM Manager entries.

DETAILED STEPS

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 47.

SUMMARY STEPS

1. Log in to the Prime Network Services Controller GUI.
2. Choose **Resource Management** > **Resources** > **Images**.
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.
4. After noting the details, delete each image from Prime Network Services Controller.
5. Reimport the images using the information that you collected in Step 3.

DETAILED STEPS

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 Nexus 1000VE Series Switch Documentation

The Cisco Nexus 1000VE documentation is available on Cisco.com at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-1000ve/series.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

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.