Discovering Network Devices

To generate reports, Prime Performance Manager must discover your network devices. This is accomplished by importing the device inventory from Cisco Prime Network, running device discovery from Prime Performance Manager, or a combination of both. Before this can occur, the SNMP credentials to allow Prime Performance Manager to connect to devices must be created. (For Y.1371 SLA and Ethernet flow point QoS reports, Telnet or SSH credentials are required.)

The following topics tell you how to add the network devices that you want to monitor to Prime Performance Manager:

Device Discovery Requirements

Before you begin device discovery, review the devices Prime Performance Manager supports at:

http://www.cisco.com/en/US/products/ps11715/products_device_support_tables_list.html

In addition, the Prime Performance Manager Devices Readme lists the known devices and software versions that have been used by customers and in Cisco labs during testing and deployments. While these devices are not formally supported, informal experience indicates they can be used successfully with Prime Performance Manager. To access the Devices Readme, choose **Readmes and Commands** from the Help menu, then choose **Devices Readme**.

To produce network performance reports, Prime Performance Manager accesses the devices, determines the device type and installed hardware. It checks for provisioned functions and technologies and, based on the assigned polling frequencies, begins the reporting process. Before this can occur, devices must be discovered and assigned to units. The units connect to the devices using the required SNMP or Telnet and SSH credentials.

Device discovery is accomplished using any of the following methods:

- Import the device inventory from Cisco Prime Network. This can be done from the Prime Performance Manager GUI or by running the ppm inventoryimport command. For information, see:
  - Importing Devices From Prime Network, page 5-3
  - ppm inventoryimport, page B-36.)
- Import the device inventory from Cisco Prime Central. This requires you to integrate Prime Performance Manager with Prime Central. For information, see Integrating Prime Performance Manager with Prime Central, page 4-2
- Import the device inventory from Cisco Prime Network Services Controller. For information, see Integrating Prime Performance Manager With Prime Network Services Controller, page 4-9
- Run device discovery from Prime Performance Manager. This can be done from the Prime Performance Manager GUI or by running the ppm discover command. For information, see:
  - Prime Performance Manager Device Discovery, page 5-5
  - ppm discover, page B-24.)

To discover a device, you must have the following information:

- The device IP address or hostname.
- The credentials authorizing Prime Performance Manager to access the device. These include SNMP, Telnet, SSH, and many others.

Note If you are running only CSV-based reports, only the device IP address or hostname is required.

If you import the device inventory from Cisco Prime Network, Prime Performance Manager gets the device IP addresses and SNMP, Telnet, and SSH credentials from the Prime Network. If you run device discovery from Prime Performance Manager, you must add the credentials to Prime Performance Manager before you run the device discovery.

Discovering Gateways and Units

Reports can be generated for Prime Performance Manager gateways and units to help you monitor the gateway and unit server health and performance. To enable Prime Performance Manager gateway and unit reports, you must:

- Enable SNMP on the gateway and unit servers.
- Add the gateway and unit SNMP credentials. See Adding SNMP Credentials, page 5-6.
- Run discovery from Prime Performance Manager to acquire the gateways and units. See Running Device Discovery from Prime Performance Manager, page 5-13.

If you are importing devices from Prime Network, you have two options for adding the Prime Performance Manager gateways and units:

- To import Prime Network devices with strict synchronization enabled, acquire the gateways and unit in the Prime Network inventory before you perform the import. (The strict synchronization import option restricts the devices managed by Prime Performance Manager to those imported from Prime Network.)
- When importing the devices, do not enable strict synchronization. After the devices are imported, run device discovery from Prime Performance Manager to acquire the gateways and units.

Importing Devices From Prime Network

To import a Prime Network device inventory, Prime Performance Manager connects to the Prime Network gateway and retrieves the Prime Network device IP addresses, SNMP, Telnet, or SSH credentials, and HTTP/s for vCenter. If the Prime Network device has multiple credentials, for example, SNMP credentials and Telnet and HTTP credentials, those credentials will be downloaded. Prime Network devices are retrieved except devices whose Prime Network VNEs.

- Are in Maintenance investigation state.
- Are ICMP or cloud VNEs.
- Have a down admin status.

Note Prime Performance Manager can integrate with Prime Network 4.1, 4.0, 3.11, and 3.10.

Prime Performance Manager then connects to the devices and probes them for supported polling parameters. After the device connections are established and MIB profiles created, Prime Performance Manager maintains communication with the Prime Network gateway. If new Prime Network devices are added, Prime Performance Manager adds those devices. If a Prime Network device VNE goes into Maintenance state, Prime Performance Manager changes the device to unmanaged and stops polling. When the VNE state changes, Prime Performance Manager changes the device state back to managed and begins polling.

Strict Synchronization

Strict synchronization is a Prime Network import option that restricts Prime Performance Manager to Prime Network devices only. If strict synchronization is enabled, you cannot discover or manage devices that reside outside of Prime Network. Additionally, you cannot edit SNMP, Telnet, or SSH entries and you cannot edit device names. If strict synchronization is not enabled, all device discovery and SNMP, Telnet, or SSH device editing capabilities remain enabled. Strict synchronization is useful when you want a tight relationship between Prime Performance Manager and Prime Network to ensure all reports are Prime Network device reports.

To import Prime Network devices, you need the following Prime Network gateway information:

- IP address or hostname
- Port
- Prime Network administrator or configurator username and password. The user must have a device scope set for all network elements.

Complete the following steps to import the device inventory from Cisco Prime Network using the Prime Performance Manager GUI. (For information on importing Prime Network devices using the CLI, see ppm inventoryimport, page B-36.) This procedure requires a Level 5 (administrator) user level.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Prime Network Integration**.

Step 3 In the Prime Network window, enter the following information:

- Host Name or IP Address—Enter the Prime Network gateway hostname or IP address.
- Port—Enter the Prime Network gateway port. The default Cisco Prime Network web services port is 9003. The Port field accepts values from 1 to 65535.
- Unsecured Port—Indicates the port entered in the Port field is an unsecure port intended for BQL debugging.

- User Name (Admin User Level)—Enter the Prime Network gateway administrator or configurator username.
- Password—Enter the Prime Network user password.
- Strict Sync—Check this box if you want Prime Performance Manager to monitor only Prime Network devices. If you check Strict Sync, Prime Performance Manager cannot connect to devices that have not been added to Prime Network first, and certain functionality is disabled, including the Network menu Discovery option and the ability to edit SNMP, Telnet, and SSH entries.

Step 4 From the Prime Network Integration toolbar, click the **Prime Network Integration Setup** tool.

The Prime Network device inventory import proceeds.

Note If Prime Performance Manager finds duplicate device custom names, an error is issued.

Step 5 After it completes, from the Network menu, choose **Devices** to review the devices that were added. For information about the displayed device properties, see **Displaying Device Properties at the Network Level, page 8-3.**

Step 6 To display information about the last Prime Network inventory synchronization, on the Administration Prime Network Integration window toolbar, click **Last Inventory Import Info**.

The date and time and status of the last inventory import is displayed.

Updating the Prime Network Device Inventory

Complete the following steps to update the Prime Network device inventory after you complete the "Importing Devices From Prime Network" procedure on page 5-3.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Prime Network Integration**.

Step 3 In the Administration Prime Network Integration window, choose **Import Inventory** on the toolbar.

The device inventory is updated.

Note Should Prime Network VNE IP addresses change from the first discovery to the next, Prime Performance Manager will update the device IP address with no loss of report information.

Prime Performance Manager Device Discovery

Importing devices from Prime Network is the most common method for adding devices to Prime Performance Manager, particularly if Prime Performance Manager is integrated with the Prime suite. (For information, see Importing Devices From Prime Network, page 5-3.)

You can also run device discovery from Prime Performance Manager. Use this discovery method when:

- You are not running Prime Network or do not wish to enable reports on Prime Network devices.
- You imported Prime Network devices but want to add devices that are not in the Prime Network inventory.

Before you run device discovery from Prime Performance Manager, you must add the device credentials. Credential management and device discovery are covered in the following topics:

- Managing Device Credentials, page 5-5.
- Running Device Discovery from Prime Performance Manager, page 5-13

Managing Device Credentials

You can run device discovery from Prime Performance Manager if you are not importing devices from Prime Network or wish to add devices that are not in the Prime Network inventory. Before you can do this, however, you must add the device credentials (or edit the credentials through the Edit Device Credentials dialog) so Prime Performance Manager can communicate with the device.

SNMP is the primary protocol used by Prime Performance Manager for device communication for nearly all Prime Performance Manager reports. For some reports, such as SLS 1731 reports, other communication methods are used, including Telnet and SSH. Adding and managing device credentials are covered in the following topics:

- Adding SNMP Credentials, page 5-6
- Editing SNMP Credentials, page 5-7
- Deleting SNMP Credentials, page 5-8
- Adding Telnet and SSH Credentials, page 5-8
- Deleting Telnet and SSH Credentials, page 5-11
- Telnet and SSH Credential Notes, page 5-11
- Adding Credentials for Cisco Carrier Packet Transport Devices, page 5-12

Adding SNMP Credentials

Complete the following steps to add the SNMP credentials to communicate with network devices discovered by Prime Performance Manager. This procedure is required if you run device discovery from Prime Performance Manager. You do not need to perform it if you imported devices from Prime Network and do not wish to add devices not in the Prime Network inventory.

Note You can enter an SNMP v2 community string and an SNMP v3 username and authentication password. If you specify both for the same device, Prime Performance Manager will try the SNMP v3 username and authentication password first. If this fails, Prime Performance Manager will try the SNMP v2 community string. Subsequent polls will try the SNMP v3 credentials and if it fails, try the SNMP v2. This provides a retry mechanism for failed SNMP v3 credentials.

Note To add SNMP credentials using the CLI, see ppm addsnmpcomm, page B-6.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 From the SNMP Editor toolbar, click the **Add a New SNMP Entry** tool.

Step 4 In the Add New SNMP Entry dialog box, enter the following information:

- IP Address Range or Hostname—Enter the device IP address or DNS name, or range of devices. An asterisk (*) indicates a wildcard value.
- SNMP Version—Enter the SNMP version used to poll the device: 1, 2c, or 3. Version 1 and 2c require a Read Community string. Version 3 requires a username, at a minimum.
- Read Community—Enter the SNMP community name that the device uses for read access to the information maintained by the SNMP agent on the device.
- Max Table Varbind—SNMP requests (Get, GetNext, GetBulk) can get multiple variables (varbinds) in a single request. All devices do not support the same number of varbinds per request; some devices behave abnormally if too many varbinds are included in a single request.

  Use this parameter only at the direction of Cisco support to manually reduce the number of SNMP varbinds that Prime Performance Manager polls in one request. For performance, Prime Performance Manager normally polls for multiple varbinds per request. Because of a combination of factors including platform, IOS version, device config, and others, some devices do not support the number of variables that can be contained in a single request, so Max Table Varbind can be used to manually reduce the number of variables in one request. It should only be specified when a problem occurs with a given device. Problems are normally determined by reviewing packet captures, interpreting the request and responses for adherence to protocol standards.
- Port—Allows you to specify an alternate device port for SNMP polling. By default, Prime Performance Manager uses Port 161, unless another port is entered here.

  Note The alternate device port is not supported if Prime Performance Manager is integrated with Prime Network.
- User Name (v3)—Enter the username (SNMP v3).
- Authentication Protocol (v3)—Enter the authentication protocol (SNMP v3):

  - md5—Uses the Hash-based Message Authentication Code (HMAC) MD5 algorithm for authentication
  - sha—Uses the HMAC SHA algorithm for authentication
- Authentication Password (v3)—Enter the authentication password (SNMP v3),
- Privacy Protocol (v3)—Enter the privacy protocol (SNMP v3):
  - 3des—Uses Data Encryption Standard (DES) v3.
  - des—Uses the Data Encryption Standard (DES).
  - aes128—Uses Advanced Encryption Standard (AES) 128-bit encryption.
- Privacy Password (v3)—Enter the privacy password (SNMP v3).

Step 5 Click **OK**.

Step 6 Repeat Steps 3–5 until all SNMP credentials are added.

Step 7 On the SNMP Editor toolbar, click **Save All SNMP Entries**.

Editing SNMP Credentials

SNMP credentials are required for communication with devices that are discovered by Prime Performance Manager. If you need to edit the SNMP credentials:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 In the SNMP table, edit any of the following SNMP parameters. See Adding SNMP Credentials, page 5-6, for parameter descriptions.

- IP Address Range or Hostname
- Read Community
- Max Table Varbind
- Port
- Username (v3)
- Authentication Protocol (v3):
  - md5
  - sha
- Authentication Password (v3)
- Privacy Protocol(v3):
  - 3des
  - des
  - aes128
- Privacy Password (v3)

Step 4 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Deleting SNMP Credentials

Complete the following steps to delete the SNMP credentials from Prime Performance Manager.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 Select the SNMP credential table row(s) that you want to remove by checking the box(es) on the far left column.

Step 4 On the Network SNMP Editor toolbar, click **Delete Selected SNMP Entries**.

Step 5 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Adding Telnet and SSH Credentials

Y.1731 Ethernet performance monitoring reports can be enabled on devices running IOS and IOS-XR, and Ethernet flow point QoS reports can be enabled on devices running IOS-XR. If you plan to run Y.1731 reports, you must add the Telnet or SSH device credentials to Prime Performance Manager.

Note To add multiple credentials to a device, complete the following procedure once for each credential. For example, the Cisco Nexus 7000 BGP VRF Messages and BGP Neighbor Messages reports require Netconf, while the MPLS Traffic Engineering Tunnel report requires Telnet. To enable all reports, add an SSHv2 credential for Netconf and a Telnet credential to the same device or set of devices.

To add the Telnet or SSH credentials:

Step 1 Log into the Prime Performance Manager GUI as the administrator user.

Step 2 From the Network menu, choose **Telnet/SSH Editor**.

Step 3 In the Device Credentials Editor toolbar, click the **Add New Telnet/SSH Entry** tool.

Step 4 In the Add a Credential dialog box, enter the following:

- Device—Enter the device hostname or IP address.
- Connection Protocol—Choose the protocol to be used to communicate with device:
  - Telnet—Telnet.
  - SSHv1—SSH Version 1.
  - SSHv2—SSH Version 2.
  - WSMA_SSH—Web Services Management Agent over SSHv2. WSMA is an infrastructure framework that allows external applications to monitor and control Cisco devices. WSMA uses transports such as SSH, HTTP, and HTTPS to access a set of Web Services agents residing on the Cisco device.
  - Collected_SSH—A daemon that collects, transfers, and stores performance data.
  - vCenter_HTTPS—VMWare vCenter server over HTTPS.
  - ESXi_HTTPS—VMWare ESXi embedded bare metal hypervisor over HTTPS.
  - ESXi_HTTP—VMWare ESXi embedded bare metal hypervisor over HTTP.

Note When you define the Telnet/SSH credential for vCenter and ESXi devices, make sure the user account you use has the session privilege. For information, see Hypervisor Discovery Requirements, page 5-17.

  - XEN_TLS—XEN hypervisor over Transport Layer Security (TLS) protocol.
  - KVM_TLS—Linux Kernal-based Virtual Machine (KVM) over TLS.

Note XEN_TLS and KVM_TLS have discovery requirements. See XEN and KVM TLS Discovery Requirements, page 5-17

  - HyperV_HTTPS—Microsoft HyperV server over HTTPS.
  - HyperV_HTTP—Microsoft HyperV server over HTTP.
  - JMX—Java Management Extensions. Collects statistics from Java processes running on various servers.

Note JMX reports are not enabled by default. After adding the JMX credential, you will need to enable the reports. For information, see Customizing Individual Report Settings, page 7-24.

  - PNSC_HTTPS—Cisco Prime Network Services Controller secure HTTP connection.
  - GMOND_SOCKET—Ganglia Monitoring Daemon (gmond) socket.

- Port—The device port to be used by the transport protocol chosen in the Protocol field.
- Sub System—The subsystem used by transport protocol. If the subsystem is defined on the device, enter it here. A blank string is the default subsystem for SSH. The default subsystem for WSMA is “wsma”.

Note To poll the Cisco Nexus 7000 through its XML management interface using Network Configuration Protocol (NETCONF), enter **netconf** in the Sub System field. Using the XML interface allows you to generate Border Gateway Protocol (BGP) reports.

- User Name—Enter the device login username.

Note For vCenter and ESXi that are member of an Active Domain, you can enter the domain and username in the format *domain/username*.

- Password—Enter the password for the login user.
- Secondary Login Type—Indicates how the secondary user and password should be processed:
  - Enable—Executes the Cisco IOS enable command, which provides Prime Performance Manager privileged EXEC level (Level 15) access to the device.
  - Second Login—Executes the login command to log into the device using the secondary username and password. If you choose this option, the secondary user must have privileged EXEC access to the device,

Note Secondary Login Type is only available for Telnet or SSH connections.

- Secondary User Name—Enter the secondary username.
- Secondary User Password—Enter the secondary user password.

Step 5 Click **OK**.

The new credential is added to the Telnet/SSH credential table.

Step 6 If you entered an SSHv2 or HTTPS credential and want to use the SSHv2 key authentication, complete the following steps. Otherwise, continue with Step 7. By default, Prime Performance Manager authenticates itself to the device using the the User Name and Password entries. To change to the SSHv2 authentication keys:

a. In the Network Telnet/SSH Editor window Client Authentication Type field, and choose **Public Key**.

b. In the SSH Credentials dialog box, enter the private key file name and click **Import**.

c. Enter the the public key file name and click **Import**.

d. Click **Generate Public Key**.

Step 7 Test the credential:

a. In the new credential table row Actions column, click the **Test the Credential** tool.

A Testing Credentials for [*device name*] window appears. If Prime Performance Manager succeeded in connecting to the device with the credentials you entered, the following is displayed:

```
****Starting Credentials Test****
Connection test successfully!
****Test Completed****
```

If Prime Performance Manager could not connect to the device, an error is displayed, for example:

```
****Starting Credentials Test****
Exception while connecting to device!
****Test Completed****
```

Step 8 In the Testing Credentials window, click **Close**.

Step 9 If the credentials test succeeded, on the Device Credentials Editor toolbar, click the **Save All Credentials** tool to save the new credential.

If the credentials test failed, verify the credentials with your network administrator and check network connectivity. You can update the credential and run the test again until it succeeds. Additionally, you can:

- From the Actions column, click the **Clear the Row** tool to clear the row contents or click the **Delete this Credential** tool to delete the entire credential.
- From the Device Credentials Editor toolbar, click the **Reload Credentials from the Server** tool to reload all the Telnet and SSH credentials.

Note Verify the Telnet/SSH credential has permission to execute the CLI terminal length 0 and terminal width 0, or Prime Performance Manager might not be able to collect data from the CLI.

After you add the Telnet and SSH credentials, you might want to perform the following tasks:

- Run device discovery. See Chapter 5, "Discovering Network Devices," for procedures.

- Enable the Y.1731 and Ethernet Flow Point reports: from the Performance menu, choose **Reports**, click the **Report Status** tab, enable the **IP SLA: Y.1731** and **IP QoS: Transport and Availability** reports. For more information, see Chapter 7, "Managing Reports, Dashboards, and Views."

Deleting Telnet and SSH Credentials

Complete the following steps to delete the Telnet/SSH credentials from Prime Performance Manager.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Telnet/SSH Editor**.

Step 3 Select the Telnet/SSH credential table row(s) that you want to remove by checking the box(es) on the far left column.

Step 4 On the Network Telnet/SSH Editor toolbar, click **Delete Selected Telnet/SSH Entries**.

Step 5 When finished, on the Telnet/SSH Editor toolbar, click **Save All Telnet/SSH Entries**.

Telnet and SSH Credential Notes

After adding the Telnet and SSH credentials, running device discovery, and enabling the Y.1731 and Ethernet Flow Point reports, review the following information:

- Default Credential—Prime Performance Manager includes a default *.*.*.* Telnet credential. The default values are from XMP_PAL.properties file. You can edit XMP_PAL.properties to set new initial default credential. If you change the default credentials in the web GUI and save it, your new default credentials will be saved to credential file instead of property file, which means now the default credentials are from credential file.
- Device Discovery—During device discovery, the Telnet and SSH credentials of discovered devices are displayed in a table beneath the SNMP credentials. The Telnet and SSH search algorithm seeks an exact match first. If no exact match is found, the default entry is used for device Telnet/SSH access credential.
- Events—If a Telnet or SSH credential issue arises, a Credential Problem state event is displayed in the device summary indicating an issue accessing the device by its Telnet or SSH credential exists.
- Reports—Only the Y.1731 SLA and Ethernet Flow Point reports require Telnet or SSH credentials. All other reports use SNMP polling.
- Prime Network Integration—When you import device credentials from Prime Network, the protocol credential, including Telnet, SSH_v1 and SSH_v2, are imported with the SNMP credentials. vCenter HTTP/s is also imported from the Prime Network UCS cluster VNE. For protocols not supported by Prime Performance Manager, the default protocol, Telnet, is used and relevant information is logged.

Tip To view detailed information about a device inventory import, click the question mark icon in Prime Performance Manager toolbar.

- Commands—Telnet and SSH credentials can be managed using the following commands:
  - ppm addcreds—Adds the Telnet and SSH credentials to access the device. See ppm addcreds, page B-6.

- ppm showcreds—Shows the Telnet or SSH credential configured for a device. See ppm setpctrapdestination, page B-70.
- ppm deletecreds—Deletes the Telnet or SSH credential from the device. See ppm deletecreds, page B-20.
- ppm xmlpoll—Retrieves the device XML output. See ppm xmlpoll, page B-93.

Adding Credentials for Cisco Carrier Packet Transport Devices

Adding credentials for Cisco Carrier Packet Transport (CPT) devices requires a few additional steps because the CPT chassis has a control card and two or more line cards. One line card runs the Cisco IOS image. The CPT control card controls access to the line cards.

To Prime Performance Manager, the control card and the line card running the Cisco IOS image appear as a separate devices that use the same IP address for management. Performance statistics reside on both the control card and the line card running the Cisco IOS image. To gather both sets of statistics using the same IP address, you must complete the following steps so that Prime Performance Manager can reach the line card with the Cisco IOS image through the control card (a process called SNMP relay):

Step 1 Set up a community string for the CPT 200 chassis and card. Card discovery utilizes SNMP relay, so one community string is used for both the chassis and the card. The community string is specified as follows:

```
ppm addsnmpcomm -i [ ipaddress ]  -c public
```

Step 2 Set up Telnet credentials for the chassis and card. This is a single row specified as follows:

```
ppm addcreds -i [ ipaddress ] -u CISCO15 -r Telnet -o 23
```

The credentials database is keyed by IP address, so only a single entry can exist. Chassis access is controlled by this entry. Access to the card uses the entry credentials, but Prime Performance Manager dynamically determines the port. The port is generated internally as '2000 + slot number'.

Step 3 Run device discovery to discover the CPT chassis and card using either the GUI (see Running Device Discovery from Prime Performance Manager, page 5-13), or the command line:

```
ppm discover [ipaddress ipaddress@2
```

The '@2' tells Prime Performance Manager the card is reachable through SNMP relay using the specified IP address. The device name is suffixed with the slot#. If the IP address is resolvable to a device name, the name will have the slot number appended accordingly. For example:

```
ipaddress@2
devicename@2
```

Step 4 Verify that the CPT devices are discovered in the GUI and device details are displayed including state, IOS version, description, device type, and other details.

Step 5 Verify that reports are generated based on the device capabilities.

Configuring vCenter and ESXi for Active Directory Authentication

To enhance troubleshooting of VM machines, such as vCenter, ESXi, or other hosts where high CPU or memory utilization is displayed, you can configure vCenter and ESXi for Active Directory. For devices, such as vCenter, which have Windows authentication based on Active Directory, Prime Performance Manager provides the device Telnet credential check through its domain and username, not simply the username.

Running Device Discovery from Prime Performance Manager

Device discovery is accomplished either by importing devices from Prime Network (see Importing Devices From Prime Network, page 5-3), or by running device discovery from Prime Performance Manager.

To run device discovery from Prime Performance Manager you enter IP addresses, address ranges, subnets, DNS hostnames, then launch discovery. The collection of addresses used for device discovery can be saved as device seed files for future use.

Before you begin device discovery, you will need:

- A list of IP addresses, address ranges, and subnets that you want Prime Performance Manager to use for discovery.
- A device seed file containing the IP addresses, address ranges, and subnets that you want Prime Performance Manager to use for discovery. If you are running discovery for the first time, you will enter the IP addresses manually, after which you can create the seed file for later use.

To run discovery from Prime Performance Manager:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Discovery**.

The Discover Network window appears. Window areas include:

- Discovery Seeds—Displays the seed files containing the address information you want Prime Performance Manager to use for device discovery.
- SNMP Parameters—The SNMP parameters that will be used to connect to devices. See Adding SNMP Credentials, page 5-6.
- Telnet/SSH Parameters—The Telnet/SSH parameters that will be used to connect to devices if you will run Y.1731 or Ethernet flow point reports. See Adding Telnet and SSH Credentials, page 5-8.

Step 3 Load a device seed file:

To load a seed file from saved files:

a. From the Discover Network toolbar, click **Load Seeds**.

The Load File dialog box displays the following information and options:

- Folder icon—Click this icon to go up one folder in the directory structure.
- Type—Indicates whether the item in the table is a file or a folder.
- Name—Seed file or folder name.
- Last Modified—Date and time the seed file or folder was last modified.
- Size (bytes)—Size of the seed file or folder, in bytes.

b. Choose a seed file. To make it your preferred startup file, click **Make This My Preferred Startup**.

c. If needed, you can:

- Modify file names by entering the new name in the Name column
- Delete files by selecting them and clicking **Delete**.

d. Click **OK**.

Prime Performance Manager saves any changes you made, closes the dialog box, and returns to the Discovery Network window. Device address information from the seed file is displayed in the Seed Devices File pane. SNMP and Telnet/SSH parameters for each seed device is shown in the SNMP and Telnet/SSH areas.

To create a seed file:

a. Enter an IP address, IP address range, IP address/subnet, CIDR subnet, or DNS hostname in the IP address field. Example inputs include:

- IP Address: 111.222.333.555
- Address Range: 111.222.333.555-800
- CIDR: 111.222.333.555/24 or 111.222.333.555/255.255.255.0
- DNS Hostname: abc_router

b. Click **Add**. The device address or range is added to the seed file.

c. Repeat Steps a and b until you have all device address information added to the file. (Should you wish to remove the address or range, select it and click **Delete**.

Step 4 After all devices are added to the seed file, click **Save Seeds** from the Discover Network toolbar.

Step 5 In the Save File dialog box:

a. If you want to create a new directory for the file, click **New Folder**, enter the folder name, then click **OK**. Alternatively, click **Go Up One Folder** to navigate to a directory above the current one.

b. Enter the file name, then click **OK**. The new file is saved and automatically loaded into the Seed Devices File pane.

Step 6 When you are ready to start device discovery, click **Discover Network**.

- The Discover Network tool changes to Stop Discovery.
- A Discovery In Progress message appears in the title bar of all Prime Performance Manager client windows.

The Network Devices summary window appears. (For Network Devices parameter descriptions, see Table 8-2 on page 8-3.) Devices requested for discovery will display the status, Waiting and the status reason, For Unit. As the unit completes the initial device discovery, the status changes to the detected device status, which is usually Active with status reason, None.

The time required to complete device discovery depends on multiple factors including number of devices, device types, the number of enabled reports, and network latency.

Step 7 To view the devices that Prime Performance Manager discovered, from the Navigation menu, choose **Devices**. (See Displaying Device Information at the Network Level, page 8-2 for information about displayed device parameters.) By default, discovered devices are sorted by alarm severity. If you suspect that Prime Performance Manager did not discover all of the devices, verify that:

- Prime Performance Manager server can ping the devices.
- SNMP is enabled on the devices.

- Prime Performance Manager is configured with the correct SNMP community name.

If you suspect that Prime Performance Manager did not discover all the devices, run the device discovery again.

Step 8 To view information about the last discovery, click **Last Discovery Info** on the Network Discovery toolbar. The date and time of the last discovery and discovery status is displayed.

Data Center Device Support

Prime Performance Manager supports the following devices used for data centers.

- Cisco ASA 1000v
- Cisco ASA 5500
- Cisco Nexus 7000 Series
- Cisco Nexus 5000 Series
- Cisco Nexus 3000 Series
- Cisco Nexus 2000 Series
- Cisco ACE20/30
- Cisco ACE 4710
- Cisco Nexus 1000v
- Cisco Nexus 1010
- Cisco UCS FIC 6100
- Cisco UCS FIC 6200
- Cisco UCS 5100
- Cisco UCS 2100 (IO Module)
- Cisco UCS B-series
- Cisco UCS C-series
- Cisco MDS 9100
- Cisco MDS 9200
- Cisco MDS 9500
- Cisco ME 1200 and 4600 Series
- Cisco Catalyst 6000, 6500 and 7600 Series Firewall Service Module
- VMWare
- Kernal-Based Virtual Machine (KVM)
- Xen
- Hyper-V
- Cisco ASA 5500 cluster
- Cisco Nexus 9000 Series
- Cisco ASR cluster and 9Kv

- Citrix NetScaler VPX and SDX Virtual Appliance Family
- Cisco Virtual Security Gateway
- Cisco CSR 1Kv
- Ceph

Some data center devices or device modes require you to perform special steps to enable Prime Performance Manager support. These are described in the following topics:

- Discovering Nexus Switches in VDC Mode, page 5-16
- Hypervisor Discovery Requirements, page 5-17
- XEN and KVM TLS Discovery Requirements, page 5-17

Discovering Nexus Switches in VDC Mode

The Cisco Nexus operating system, Cisco NX-OS, supports virtual device contexts (VDCs). VDCs allow Cisco Nexus 7000 data center switches to be virtualized at the device level. Each configured VDC presents itself as a unique device to connected users within the framework of that physical switch. The VDC runs as a separate logical entity within the switch, maintaining its own unique set of running software processes, having its own configuration, and being managed by a separate administrator. A Nexus can be configured with four VDCs. Each context appears as a device.

Prime Performance Manager polls the VDC separately. This means you must enter all VDC management IP addresses and credentials, including SNMP and Telnet/SSH, into Prime Performance Manager so that Prime Performance Manager can poll the statistics and inventory data for the Data Center view.

To discover Nexus VDCs:

Step 1 Log into the Cisco Nexus switch as the administrator user. Refer to the Cisco Nexus user documentation for login procedures.

Step 2 Following instructions in the Cisco Nexus user documentation, create the VDCs under the default VDC instance, for example:

```
ppm7000a(config)# vdc ?
  <WORD>             Create a new vdc
```

Step 3 Allocate the interfaces to the VDCs under the default VDC instance, for example:

```
ppm7000a(config-vdc)# allocate interface ethernet 1/37-48
```

Step 4 Switch to the new VDC and initialize the VDC configuration following the Nexus wizard:

- admin username/password,
- snmp RO/RW credential,
- Mgmt 0 IP address (for Prime Performance Manager polling),
- Mgmt vrf route gateway, and so on

For example:

```
ppm7000a# switchto vdc ?
  ppm7000a  VDC number 1
  vdc2      VDC number 2
  vdc3      VDC number 3
  vdc4      VDC number 4
```

In the following Cisco Nexus VDC configuration example, the access VDC is managed through the 192.168.119.53 address. This address is used as the seed during Prime Performance Manager device discovery.

```
telnet ppm70002
vdc Access id 2
  allocate interface Ethernet1/1-8
vdc Agg id 3
  allocate interface Ethernet1/9-16
vdc Core id 4
  allocate interface Ethernet1/17-24
switchto vdc access
config
vrf context management
  ip route 0.0.0.0/0 192.168.119.1
vlan 622
  name Management
username admin password 5 $1$rvdiuLA.$8j5arfEmxh1Bw7YtTNHCr/  role vdc-admin
snmp-server community SMFtest123 group vdc-operator
interface mgmt0
   ip address 192.168.119.53/25
```

Hypervisor Discovery Requirements

Prime Performance Manager can discover a variety of virtualized hypervisor devices including Hyper-V, Xen, KVM and EXSi. For VMWare hypervisors, Prime Performance Manager uses the virtualization API, libvirt. This API requires a user with a session privilege. In VMWare:

1. Create a role named "***".
2. Create a user on the Windows machine where VCenter is installed and assign that user the role, “Clone of read-only.”
3. Give the user the session privilege.

XEN and KVM TLS Discovery Requirements

XEN TLS and KVM TLS hypervisors require libvirtd 0.9.13 or above to be enabled on the hypervisor. For security, use TLS+SASL for authentication. More details can be found in libvirt website. For the Prime Performance Manager server, install library cyrus-sasl to support SASL authentication.

In addition to TLS elements, you must install some dependency libraries on the Prime Performance Manager server for hypervisor reports including libgcrypt, libintl and libiconv. For Solaris, make sure the 64 ELF libraries are used because 32 ELF is default library type.

UCS Server Discovery Requirements

Prime Performance Manager uses the Cisco UCS Manager XML API for UCS discovery. The UCS XML is a programmatic interface to the Cisco Unified Computing System. The API accepts XML documents through HTTP or HTTPS. Therefore, to discover UCS servers, add its credentials using HTTP or HTTPS in the “Adding Telnet and SSH Credentials” procedure on page 5-8. To test the UCS credentials, you must configure the SNMP read community.

If you import UCS servers through Cisco Prime Network, Prime Performance Manager automatically configures the SNMP and HTTP or HTTPS credentials for UCS devices.

Note For UCS C-Series with CIMC 1.5 or later, The SNMP Community must be configured along with HTTP/HTTPS credential on the CIMC port.

Small Cell Device Support

Prime Performance Manager supports the following small cell devices:

- Cisco Provisioning and Management Gateway (PMG)
- Log Upload Server (LUS)
- 3G access points (APs)

To prepare Prime Performance Manager for small cell support:

Step 1 Verify that Network Time Protocol (NTP) is synchronized between the Prime Performance Manager unit and the small cell devices.

Step 2 Verify the LUS find utility is 4.4.2 or higher. If not, upgrade it.

Step 3 Enable the SNMP service on the PMGs and LUS.

- Configure the SNMP community; grant read access to the Prime Performance Manager unit.
- If you need to monitor system resources such as CPU, MEM, IO, or DISK, configure the SNMP agent to enable the related management information bases (MIBs).

Step 4 Before discovering the PMGs and LUS, add and test the following credentials to verify the credential connectivity. See Adding SNMP Credentials, page 5-6.

- SNMP—SNMP credentials must be configured for each PMG and LUS.
- SSH—SSH credentials must be configured for each PMG and LUS.
- HTTP—HTTP credentials must be configured for LUS only. The subsystem field must be configured correctly. See the note in Step 7.

Step 5 For PMG performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway:

- etc/csvPull/system/pmg-perf.properties
- etc/csvstats/system/pmg-perf.properties

Step 6 For LUS performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway:

- etc/csvPull/system/lus-perf.properties
- etc/csvstats/system/lus-perf.properties

Step 7 For AP reports, configure the fileDirectory property in etc/apStats/system/RMS-LUS.properties.

Note The fileDirectory should match the HTTP credentials subsystem.fileDirectory = /opt/CSCOppm-gw/apache/share/htdocs/help/apStats /opt/CSCOppm-gw/apache/share/htdocs/ is Apache's root directory, strip that, we get subsystem -> help/apStats

Step 8 On the Prime Performance Manager unit, modify properties/BulkStats.properties according to the requirement. The default value is 15 seconds. For example, to change it to 60 seconds, enter:

```
DIR_MONITOR_REFRESH_INTERVAL=60
```

Step 9 Restart Prime Performance Manager. See Restarting Gateways and Units, page 2-5.

Step 10 Enable the following small cell reports. For information on enabling reports, see Customizing Individual Report Settings, page 7-24.

- Small Cell Statistics > RMS
  - PMG
  - LUS
  - AP
  - RMS System
- PPM System
  - AP Stats Metrics
- RMS System

Cisco Carrier Packet Transport Support

Cisco Carrier Packet Transport (CPT) devices are ordinarily added through Cisco Prime Network. If you add them through Prime Performance Manager device discovery, requirements differ depending on the CPT release. For releases before Release 9.7, you must define two devices, one for each CPT card, for example, 1.1.1.1@4 and 1.1.1.1@5. For Release 9.7, you only need to define a single device. The CPT will route the SNMP request to the active card, for example, 1.1.1.1@2.

Ports 2000 and 2004 are for Telnet access to CPT cards. Prime Performance Manager does not support dynamic Telnet routing. It accesses the cards through Port 2000 plus the slot number.

Openstack Ceilometer Support

OpenStack ceilometer provides a point of contact for billing systems to acquire the measurements needed for customer billing across OpenStack core components.

To discover OpenStack ceilometer, complete the Telnet/SSH credential procedure. See Telnet and SSH Credential Notes, page 5-11 for more details and enter the following information:

Step 1 For IP address and port, enter the OpenStack identity administration URL.

Step 2 Choose **HTTP/HTTPS** as the connection protocol.

Step 3 For username, the format is TenantName\Username.

Step 4 The default port is 35357.

Step 5 The subsystem is identity.

Step 6 After entering the ceilometer credentials, you can complete discovery following normal device discovery procedures. For information, see Prime Performance Manager Device Discovery, page 5-5 procedure.

Ceph Device Support

Ceph is a distributed object store and file system designed to provide performance, reliability and scalability. Ceph runs on commodity hardware in the Linux kernel. To discover Ceph devices, add Ceph device credentials from which you want to gather performance statistics. A Ceph cluster consists of one or more Monitors, one or more Object Storage Daemons (OSDs) and a Metadata Server (MDS).

Monitors provide basic availability statistics for the cluster: number of Monitors, OSDs, MDSs, their availabilities and statuses. OSDs are the main performance statistics provider. They provide I/O, latency, disk utilization, and other performance statistics.

Note Prime Performance Manager does not gather statistics from MDS devices.

Prime Performance Manager uses a specific collectd package to gather performance statistics from Ceph clusters. The package can be found at https://github.com/crdc-ppm/collectd. Some default JSON parsing libraries do not support 64-bit integers. Without the correct JSON library, statistics with numbers greater than 2,147,483,647 are incorrectly parsed.

Because Prime Performance Manager gathers collectd data through RRD files, install collectd with the RRDTool plugin enabled. The collectd.conf file must have an RRDTool entry that specifies the data directory (DataDir) where the RRD files are stored.

Prime Performance Manager defines the COLLECTD_BASE_DIR . It assumes collectd stores RRD files as /var/lib/collectd. As long as the collectd.conf file DataDir definition matches this directory, Prime Performance Manager will collect data from collectd. If the Ceph device does not have COLLECTD_BASE_DIR, the Ceph device status in Network Devices window will be “Collectd base directory does not exist.”

Define Ceph device credentials in the Telnet/SSH Editor using collectd_SSH as the connection protocol and the Ceph device IP, username, password. See Adding Telnet and SSH Credentials, page 5-8. Device discovery is the same as any other device. Enter the Ceph device IP address entered in the Telnet/SSH Editor. See Running Device Discovery from Prime Performance Manager, page 5-13.

Cisco ME 4600 Gigabit Passive Optical Network Support

If you are discovering Cisco ME 4600 Series devices Gigabit-capable Passive Optional Networks (GPONs), you must disable the following reports before you discover the ME 4600 Optical Line Terminal (OLT) devices. Reports that you must disable include:

- IP Protocols > ICMP v4/v6
- Resources > IP Address
- Transport Statistics > PE-CE Interface >
  - PE-CE IPv4 Interface
  - PPE-CE IPv6 Interface

See gponPtin.notes for additional ME 4600 device implementation notes.