Discovering Devices With Prime Performance Manager

To generate reports, Prime Performance Manager must discover your network devices. Devices are commonly added to Prime Performance Manager by integrating it with other applications, then importing the application devices. Procedures for importing devices from other applications are provided in Chapter 4, "Importing Devices From Other Cisco Prime Applications."

You can also run device discovery from Prime Performance Manager. Use this discovery method when you have not imported devices from other applications, or want to add devices that aren't available in the other application. Before this can occur, you must create the credentials to allow Prime Performance Manager to connect to devices.

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

Device Discovery Requirements

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

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-performance-manager/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, from the Help menu choose **READMES and CLI Commands > Devices Info**.

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 credentials.

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

- The device identifier, such as IP address, DNS hostname, or other identifier.
- The credentials authorizing Prime Performance Manager to access the device.

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

In addition to these general requirements, some devices require special provisioning and setup. These requirements are described in the following topics:

- Data Center Discovery Requirements, page 5-13
- Small Cell Discovery Requirements, page 5-17
- Cisco CPT and ONS Discovery Requirements, page 5-18
- OpenStack Ceilometer Discovery Requirements, page 5-19
- Discovering Devices With Multiple Collectors, page 5-19
- Ceph Discovery Requirements, page 5-21
- KVM Discovery Requirements, page 5-21
- Cisco ME 4600 GPONs Discovery Requirements, page 5-23
- Cisco NAM Blade and Appliance Discovery Requirements, page 5-23

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 Device Credentials, page 5-3.
- Run discovery from Prime Performance Manager to acquire the gateways and units. See Running Device Discovery, page 5-11.

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.

Managing Device Credentials

You can run device discovery from Prime Performance Manager if you are not importing devices from another application or wish to add devices that are not in the imported application device inventory. Before you can run device discovery from Prime Performance Manager, 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 most Prime Performance Manager reports. However, many other protocols are supported to communicate with the many devices that Prime Performance Manager supports. Adding and managing device credentials are covered in the following topics:

Adding SNMP Device Credentials

Complete the following steps to add the SNMP credentials to communicate with network devices discovered by Prime Performance Manager. Complete this procedure if you run device discovery from Prime Performance Manager. You do not need to complete it if you imported devices from another application and do not wish to add devices not in the application imported device 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-9.

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. For example, 4000 is the Cisco Network Service Orchestrator default SNMP port. (To get the NSO SNMP port, log into NSO using **ncs_cli -u admin** and run the **show configuration snmp** command. The agent udp-port will point to the supported SNMP port number, which you must use for NSO device discovery.

  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 Device 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 Device Credentials, page 5-3, 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 Device 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 Device Credentials for Other Protocols

In addition to SNMP, Prime Performance Manager supports over twenty other device connection protocols including Telnet, SSH, HTTP, Data Center VMs, and many others. These credentials are added through the Network > Credentials Editor window.

In cases were multiple credentials are required, you complete the following procedure multiple times. 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 these reports, you would add an SSHv2 credential for Netconf and then add the Telnet credential, both on the same device.

To add device credentials for other connection protocols:

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

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

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

Step 4 In the Add Credentials Entry 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.
  - collectd_SSH—A daemon that collects, transfers, and stores performance data.
  - HTTP—HyperText Transfer Protocol.
  - HTTPS—Secure HTTP.
  - HTTP_BULK—Bulk statistics through HTTP.
  - WMI_HTTP—Windows Management Instrumentation over HTTP.
  - WMI_HTTPS—Windows Management Instrumentation HTTPS.
  - SMI_HTTPS—Storage Management Initiative over HTTPS.
  - ULS_HTTP—Allows Prime Performance Manager to perform Small Cell upload server HTTP credential verification including subsystem, username, password, and credential parameters. Beyond that, ULS_HTTP is identical to HTTP protocol.
  - vCenter_HTTPS—VMware vCenter server over HTTPS.
  - ESXi_HTTP—VMware ESXi embedded bare metal hypervisor over HTTP.
  - ESXi_HTTPS—VMware ESXi embedded bare metal hypervisor over HTTPS

Note When you define the credential for vCenter and ESXi devices, make sure the user account you use has the session privilege. For information, see Hypervisor Discovery Requirements, page 5-16.

  - 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 5-16

  - HyperV_HTTP—Microsoft HyperV server over HTTP.
  - HyperV_HTTPS—Microsoft HyperV server over HTTPS.
  - 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 7-27.

  - PNSC_HTTPS—Cisco Prime Network Services Controller secure HTTP connection.
  - GMOND_SOCKET—Ganglia Monitoring Daemon (gmond) socket.
  - AVI_HTTPS—AVI Networks load balancing device secure HTTP connection.

- 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 devices that are members of an Active Domain, you can enter the domain and username in the format *domain/username*.

Note For KVM_TLS, if SASL is enabled on the KVM device, add Simple Authentication Security Layer (SASL) credentials to the entry. SASL usernames typically have the SASL realm appended to it, such as user@hostname. If SASL is not enabled on the KVM device, you can leave the User Name and Password fields blank.

- 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.

Note For NSO, use the secondary username and password for the NSO NETCONF username and password.

Step 5 Click **OK**.

The new credential is added to the 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 User Name and Password entries. To change to the SSHv2 authentication keys:

a. In the Credentials Editor window Client Authentication Type field, and choose **Public Key**.

b. Click the Client Private Key field.

c. In the SSH Credentials for [hostname] dialog box, enter the private key file name and click **Import**.

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

e. Click **Generate Public Key**.

Step 7 In the new credential table row Actions column, click the **Test the Credential** tool.

A Testing Credentials for [*device name*] dialog box 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 Test Credentials for [*device name*] dialog box, click **Close**.

Step 9 If the credentials test succeeded, on the Credentials Editor toolbar, click the **Save Credentials Entries** 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 click the **Clear the Row** tool in the Action column to clear the row contents or click the **Delete** tool to delete the entire credential.

Note For Telnet/SSH credentials, verify the 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 device credentials for other protocols, you might want to run device discovery. See Chapter 5, "Discovering Devices With Prime Performance Manager," for procedures. You should also enable the reports for the devices whose credentials you added. see Chapter 7, "Managing Reports, Dashboards, and Views."

Credential Notes for Other Protocols

After you add credentials for other protocols, run device discovery, and enable the appropriate reports, review the following information:

- Default Credential—Prime Performance Manager includes a default *.*.*.* Telnet credential. The default values are from the XMP_PAL.properties file. You can edit XMP_PAL.properties to set new default credentials. If you change the default credentials in the GUI and save them, the edited credentials are saved to a credential file, not XMP_PAL.properties. Thereafter, the default credentials come from the credential file and not XMP_PAL.properties.
- Device Discovery—During device discovery, non-SNMP credentials of discovered devices are displayed in a table beneath the SNMP credentials. The device discovery search algorithm seeks an exact match first. If no exact match is found, the default entry is used for device access credential.
- Events—If a credential issue arises, a Credential Problem state event is displayed in the device summary indicating an issue accessing the device by its credential exists.
- 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.

Adding Credentials for Cisco CPT 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 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; only one 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, page 5-11), 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.

Securing Device Connections: SSH and SNMPv3

The security of device communication is maintained by specifying SSH and SNMPv3 authentication and encryption methods. Table 5-1 lists the security methods that are supported by each protocol.

Table 5-1 Supported Algorithms in SSHv1, SSHv2, and SNMPv3

Protocol	Supported Algorithms
SSHv1	Ciphers : des, 3des
SSHv2	Key exchange(kex): diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256 Ciphers: aes128-ctr, aes128-cbc, aes192-ctr, aes192-cbc, aes256-ctr, aes256-cbc, 3des-cbc MAC: hmac-sha1, hmac-sha2-256
SNMPv3	Auth: MD5, SHA Priv: 3des, des, aes128, aes192, aes256

Configuring vCenter and ESXi for Active Directory Authentication

To enhance VM troubleshooting, for example vCenter, ESXi, or other hosts with high CPU or memory utilization, 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 an HTTP or HTTPS credential check through its domain and username, not simply the username.

Deleting Device Credentials for Other Protocols

Complete the following steps to delete other connection protocol device 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 **Credentials Editor**.

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

Step 4 On the Credential Editor toolbar, click **Delete Selected Credential Entry**.

Step 5 When finished, on the Credential Editor toolbar, click **Save Credentials Entries**.

Running Device Discovery

Before you run device discovery from Prime Performance Manager, you must add the credentials for all the devices you want to discover. Procedures are provided in Managing Device Credentials, page 5-3. Before you begin device discovery, you will need one of the following:

- A list of IP addresses, address ranges, subnets, Classless Inter-Domain Routing (CIDR) blocks, or DNS hostnames that you want Prime Performance Manager to use for discovery, or
- 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 Network Discovery window displays the following areas:

- Discovery Seeds—Displays the seed files, if they exist, containing the address information you want Prime Performance Manager to use for device discovery. It also displays the unit to which the discovered addresses will be assigned.
- SNMP Parameters—The SNMP credentials that will be used to connect to devices. See Adding SNMP Device Credentials, page 5-3.
- Other Credentials—Device credentials for other protocols are displayed. See Adding Device Credentials for Other Protocols, page 5-6, for a list of all supported protocols.

Step 3 If you want to run device discovery from a saved seed file, continue with Step 4. If you have no saved seed files, or want to run device discovery with a new one, complete the following steps:

a. In the IP Address, Address Range, Subnet, CIDR, or DNS hostname field, enter an IP address or address range, subnet, CIDR block, or DNS host name. Examples:

- 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. By default, Prime Performance Manager assigns units to discovered devices automatically. If you want to specify the unit, assign it in the Unit field.

Note You generally should allow Prime Performance Manager to allocate discovered devices to the units. Never use this field to reassign a device. To change a device-to-unit assignment, see Changing a Device-to-Unit Assignment, page 13-8.

c. Click **Add**. The device address or range is added as a seed entry.

d. Repeat Steps a through c until all information covering the devices you want to discover are added. (Should you wish to remove the address or range, select it and click **Delete**.

e. To save the individual seed entries as a seed file, on the toolbar click **Save Seeds**.

f. In the Save As dialog box, enter the following:

- Filename—Enter the file name. Spaces are not permitted.
- New Folder—(optional) If you want to place the seed file in a new folder, click **New Folder** and enter the new folder name.
- Make this my preferred Startup—(optional) Check if you want this seed file to appear by default whenever you run device discovery.

g. Click **OK**.

Prime Performance Manager saves the seed entries, closes the dialog box, and returns to the Network Discovery window. Device address information from the seed file is displayed in the Seed Devices File pane. SNMP and other protocol credentials for each seed device are shown in the SNMP Parameters and Other Credentials areas.

h. Continue with Step 5.

Step 4 To load a device from a saved seed file:

a. From the Network Discovery 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.

c. If needed, you can make the selected seed file you preferred startup file by clicking **Make This My Preferred Startup**

d. Click **OK**.

Step 5 When you are ready to start device discovery, on the Network Discovery toolbar, 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 9-2 on page 9-3.) 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 6 To view the devices that Prime Performance Manager discovered, from the Navigation menu, choose **Devices**. (See Displaying Device Information at the Network Level, page 9-2 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 or other communications required protocol 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 7 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 Discovery Requirements

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

- Cisco ASA 1000v
- Cisco ASA 5500
- Cisco Nexus 9000 Series
- Cisco Nexus 7000 Series
- Cisco Nexus 6000 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 FIC 6400
- 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 vCenter Server
- ESXi hypervisor
- 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
- Cisco vNAM
- Ceph
- NetApp Storage
- AVI Load Balancer
- Cisco IOS XRv Router
- Cisco Web Security Appliance (WSA)
- Cisco Next Generation Intrusion Prevention System (NGIPS)
- Cisco Email Security Appliance (ESAV)
- Cisco Open Virtual Switch (OVS)
- Cisco Network Service Orchestrator
- Cisco Integrated Services Routers (ISR)

Prime Performance Manager also supports the following Windows OSs as data center hypervisor VM hosts:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

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 5-15
- Hypervisor Discovery Requirements, page 5-16
- Xen and KVM TLS Discovery Requirements, page 5-16

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 physical switch framework. The VDC runs as a separate logical entity within the switch. It maintains its own unique set of running software processes, has its own configuration, and is managed by a separate administrator. A Nexus can be configured with four VDCs, each appearing as a separate device.

Prime Performance Manager polls each VDC separately. This means you must add all VDC management IP addresses and credentials to 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 virtualized hypervisor devices including Hyper-V, Xen, KVM and ESXi. For VMware hypervisors, Prime Performance Manager uses the virtualization API, libvirt. This API requires a user with a session privilege.

Following procedures in the vSphere documentation (https://www.vmware.com/support/pubs/), complete the following steps:

Step 1 Log into VMware vSphere ESXi or vCenter.

Step 2 Create a new user role cloned from the vSphere default read-only role.

Step 3 Assign the new role the Sessions privileges.

Step 4 Add permission to vSphere ESXi or vCenter with an individual or group of vSphere recognized users and assign them the newly created role.

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 the libvirt website. For Prime Performance Manager servers, install the cyrus-sasl-md5 library to support SASL authentication.

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

cyrus-sasl-md5 is also required to support SASL authentication (if you sign your certificates using md5, which is the default). You can create TLS certificates using an older hashing algorithm, but installing the md5 package on Prime Performance Manager is easier.

UCS Server Discovery Requirements

Prime Performance Manager uses the Cisco Unified Computing System (UCS) Manager XML API for UCS discovery. The UCS XML is a programmatic interface to the Cisco UCS. The API accepts XML documents through HTTP or HTTPS. Therefore, to discover UCS servers, add its credentials using HTTP or HTTPS to Prime Performance Manager. See the "Adding Device Credentials for Other Protocols" procedure on page 5-6. To test the UCS credentials, you must configure the SNMP read community.

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

Note For UCS C-Series with CIMC 1.6 or later, you must configure the SNMP Community with the HTTP/HTTPS credential on the CIMC port.

Small Cell Discovery Requirements

Prime Performance Manager supports the following small cell devices:

- RMS Central Node
- RMS Serving Node
- RMS Upload Server
- 3G and 4G 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 Radio Access Network (RAN) Management System (RMS) upload server find utility is 4.4.2 or higher. If not, upgrade it.

Step 3 Enable the SNMP service on the RMS Central Node, Serving Nodes, and Upload Servers.

- 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 RMS Central Nodes and Serving Nodes and upload servers, add and test the following credentials to verify the credential connectivity. See Adding SNMP Device Credentials, page 5-3.

- SNMP—SNMP credentials must be configured for each PMG and upload server.
- SSH—SSH credentials must be configured for each PMG and upload server.

Step 5 For PMG performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway in etc/csvPull/system/pmg-perf.properties.

Step 6 For upload server performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway in etc/csvPull/system/uls-perf.properties.

Step 7 For BAC RDU and DPE reports, verify the parameters are correctly configured on the Prime Performance Manager gateway:

etc/bacStats/system/bac-rdu-perf.properties

etc/bacStats/system/bac-dpe-perf.properties

etc/csvPull/system/rdu-kpi.properties

etc/csvPull/systemdpe-kpi.properties

Step 8 For Device Command and Control (DCC) UI reports, verify that the settings in the gateway etc/csvPull/system/dccui-stats.properties file are consistent with the DCC UI configuration. The gateway synchronizes the file to all units. If settings are inconsistent, make the appropriate changes. For information, see Setting Up DCC UI Reports, page 8-46.

Note Before you begin collecting AP data, review and modify, if needed, the APSTATS_BACK_PERIOD setting in /properties/APStats.properties. This setting controls how far back Prime Performance Manager should retrieve data files. The default is 259200 seconds, or three days. If a large backlog has accrued before the first report polling cycle, you can change this setting to retrieve more backlog data. For more information, see Setting Up AP Reports, page 8-41

Step 9 Add the ULS to a ULS redundancy group, for example:

```
/opt/CSCOppm-gw/bin/ppmManageULSRedundancy.sh set SampleRedundancyGroup 10.74.125.205
```

Step 10 For Cisco Prime Network Registrar (PNR) Caching/Recursive Domain Name System (CDNS) performance log reports, verify that the settings in the gateway etc/bacStats/system/PNR-CDNS.properties file are consistent with the CDNS configuration. The gateway synchronizes the file to all units. If settings are inconsistent, make the appropriate changes. For information, see Setting Up DCC UI Reports, page 8-46.

Step 11 Restart Prime Performance Manager. See Restarting Gateways and Units, page 2-5.

Step 12 Enable the small cell reports, located in the Small Cell Statistics report category. For information on enabling reports, see Customizing Individual Report Settings, page 7-27.

Note The TR-069 Session Utilization report assumes the default SSL port is in use on the RMS serving device BAC-DPE component. If the default SSL port is changed on the BAC-DPE serving device, the TR-069 Session Utilization report will not display accurate information.

Cisco CPT and ONS Discovery Requirements

Cisco Carrier Packet Transport (CPT) devices are ordinarily added through Cisco Prime Network. If you add them through Prime Performance Manager device discovery, the requirements depend on the CPT release:

- Releases before Release 9.7—Define two devices, one for each CPT card, for example, 1.1.1.1@4 and 1.1.1.1@5.
- Release 9.7—Define one 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.

Prime Performance Manager supports Optical Networking Service (ONS) and CPT devices through HTTP bulk statistics residing on the device side. Prime Performance Manager can access the devices through HTTP(s) using PAL or HTTPClient.

Prime Performance Manager supports the following performance management (PM) parameters:

- Optical Transport Network (OTN) /G.709 PM statistics for a client or Dense Wavelength Division Management (DWDM) line (ONS and CPT)
- FEC PM (ONS and CPT)
- Ethernet statistics for PT systems (CPT only)

Supported gateway network element (GNE) and end network element (ENE) SNMP credentials include:

- SNMP Community: the SNMP Community is specified in the SNMP editor.
- Add GNE device IP with a public community entry.
- Add ENE device IP with the community, <GNE IP>@public.

Table 5-2 lists the Telnet and SSH credentials for ONS and CPT devices.

Table 5-2 Telnet and SSH Credentials for ONS and CPT Devices

Parameters	GNE	ENE
IP Address	GNE device IP	ENE device IP
Port	80	80
Username	GNE user name	ENE user name
Password	GNE user password	ENE user password
Subsystem	n/a	<GNE IP>@1080
Protocol	HTTP_BULK	HTTP_BULK

To discover ONS and CPT devices, enter the following:

- GNEs—Enter the GNE device IP address.
- ENEs—Enter <ENE device IP>@<GNE device IP>.

OpenStack Ceilometer Discovery Requirements

OpenStack Ceilometers provide points of contact for billing systems to acquire the measurements needed for customer billing across OpenStack core components.

To discover Ceilometers, complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 and enter the following information:

- Device—Enter the OpenStack identity administration URL.
- Connection Protocol—Choose **HTTP** or **HTTPS**.
- Port—The default port is 35357.
- Subsystem—Enter **identity**.
- User Name—The username format is TenantName\Username

After entering the Ceilometer credentials, you can complete discovery following normal device discovery procedures. For information, see Managing Device Credentials, page 5-3 procedure.

Discovering Devices With Multiple Collectors

Prime Performance Manager uses SNMP as the primary protocol to discover a device and assign the device type based on the base sysObjectID value. However, some devices might have multiple collectors including SNMP, Ceilometers, Cisco UCS Manager (UCSM), Storage Management Initiative (SMI), Windows Management Instrumentation (WMI), hypervisors ESIx, Xen, Hyper-V, and KVM, and the

gmond and collectd daemons, For devices containing multiple collectors, you can control the collector Prime Performance Manager uses to access the device. For example, if you are discovering a server that provides data through collectd, you might not want to enable SNMP collectors for the device.

To specify the collector Prime Performance Manager uses to discover a device with multiple collectors:

Step 1 Log into the Prime Performance Manager gateway server as the root user.

Step 2 Navigate to the following directory: /opt/CSCOppm-gw/properties/.

Step 3 With a text editor, open Server.properties and set the MULTI_COLLECTOR_ENABLED flag to true.

Step 4 Save your change.

Step 5 Reboot the gateway. See Restarting Gateways and Units, page 2-5.

Step 6 Repeat Steps 2 through 5 on each unit connected to the gateway.

Step 7 After the gateway and unit reboots are complete, log into the Prime Performance Manager gateway GUI.

Step 8 Verify credentials are added for all collectors contained on the device you want to manage. For information, see the following topics:

- Adding SNMP Device Credentials, page 5-3
- Adding Device Credentials for Other Protocols, page 5-6

Step 9 From the Network menu, choose **Discovery**.

Step 10 In the Network Discovery window IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the IP address of the device containing multiple collectors that you want to manage.

Step 11 Click **Add**.

Step 12 In the Collector Parameters area, select each discovery type that reside on the device and click **Add**. Available types include:

- SNMP
- Ceilometer
- collectd
- WMI
- UCSM
- SMI
- Hypervisor (includes ESXi, KVM, Hyper-V, Xen, and vCenter)
- gmond
- AVI
- UCS-CIMC
- Openstack

Step 13 Under Selected Discovery Types, choose the type you want Prime Performance Manager to use for device discovery and click **Raise** until it is at the top. For example, if you choose Ceilometer + SNMP, the device will be discovered as Ceilometer device. If you choose SNMP + Ceilometer, the device will be discovered as a Linux device.

Step 14 On the Network Discovery toolbar, click **Discover Network**.

Step 15 Wait a few minutes for the discovery to complete and data collected, then, from the Network menu, choose **Devices**.

Step 16 Verify the device is displayed on the Network Devices list.

Step 17 Should you wish to change or remove the primary collector:

a. Select the device.

b. From the Actions menu, choose **Edit Discovery Type**.

c. In the Edit Discovery Type dialog box, add or remove the discovery types making sure the discovery type you want Prime Performance Manager to use as the primary discovery type is at the top of Selected Discovery Types list.

d. Click **Save**.

Ceph Discovery Requirements

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 the Ceph device credentials for which you want to gather performance statistics. A Ceph cluster consists of one or more Monitors, one or more Object Storage Daemons (OSDs) and, optionally, 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.

To gather performance statistics from Ceph clusters install the Ceph plugin, which you can get from https://github.com/collectd/collectd. The plugin provided on this site is the only one that is supported.

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 displayed in the Prime Performance Manager Network Devices window will be “Collectd base directory does not exist.”

Define Ceph device credentials in the Credentials Editor using collectd_SSH as the connection protocol and the Ceph device IP, username, password. See Adding Device Credentials for Other Protocols, page 5-6. Device discovery is the same as any other device. Enter the Ceph device IP address entered in the Credentials Editor. See Running Device Discovery, page 5-11.

KVM Discovery Requirements

Kernel-based Virtual Machine (KVM) is a virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.

KVM allows you to run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc. The KVM kernel component is included in mainline Linux, as of 2.6.20.

To monitor KVM devices with Prime Performance Manager, you can use the kvmTLSConfigScript located in /opt/CSCOppm-gw/samples/kvmTLSConfiguration, to configure the Transport Layer Security (TLS) and optionally, Simple Authentication and Security Layer (SASL) on libvirt for KVM devices. Ubuntu is the only supported Linux distribution for this script. Puppet files are included to make multiple KVM device configurations easier. Puppet installs all required packages. However, if you run the script manually, the following packages are required to configure TLS authentication:

- libvirt-bin
- gnutls-bin
- policycoreutils

To configure SASL authentication, the following packages are required:

- cyrus-sasl-md5
- sasl2-bin
- expect

Sample execution of the script looks like the following:

```
.../kvmTLSConfigScript off false false
```

or:

```
.../kvmTLSConfigScript on false true user password novaUser novaPassword
```

kvmTLSConfigScript takes the following parameters:

- sasl (on|off, default=off)—Configure SASL for libvirt
- overwrite_certs (true|false, default=false)—If TLS certs already exist, overwrite?
- sasl_nova_compute (true|false, default=false)—If Openstack Nova-compute is installed on this device, whether to create a nova user if SASL is enabled. Nova-compute won't be able to authenticate without a special authentication file for the nova SASL user.
- sasl_user—User to create for SASL authentication.
- sasl_pw—Password for the sasl_user
- nova_user (default=nova@$HOST—(only valid if sasl_nova_compute=true) User to create as the Openstack Nova-compute user for SASL
- nova_pw (default=nova—(only valid if sasl_nova_compute=true)—Password for nova_user.

If you are using puppet, specify these parameters and the IP addresses/hostnames of the KVM devices in the site.pp file. A sample site.pp file is included in this directory. Your site.pp file should be placed in /etc/puppet/manifests/site.pp on the puppet master node. The necessary puppet class files are provided here in the classes directory. Place these in /etc/puppet/manifests/classes/ on the puppet master node. Finally, place the script itself at: /etc/puppet/modules/kvmTLSConfig/files/kvmTLSConfigScript.

Avi Networks Discovery Requirements

Avi Networks Load Balancer provides the health and availability reports for Controller, Service Engine, Virtual Services, Pool, Members and Throughput and connection-related statistics.

To discover AVI devices, complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 and enter the following information:

- Device—Enter the AVI identity administration URL.
- Connection Protocol—Choose **AVI_HTTPS**.
- Port—The default port is 443.

After entering the AVI credentials, complete the "Running Device Discovery" procedure on page 5-11 and select **AVI** from the available discovery types. For information about device credentials, see Managing Device Credentials, page 5-3.

Cisco ME 4600 GPONs Discovery Requirements

If you are discovering Cisco ME 4600 Series devices Gigabit Passive Optional Networks (GPONs), 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.

Cisco NAM Blade and Appliance Discovery Requirements

Prime Performance Manager supports the collection of data from the following Cisco Network Analysis Module (NAM) blades and appliances:

- Cisco Network Analysis Module Blades
  - Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1)
  - Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)
  - Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2)
- Cisco Prime Network Analysis Module Appliances
  - Cisco NAM 2000 Series Appliances
- Cisco Prime Network Analysis Module Virtual Blades
  - Cisco Prime Network Analysis Module for ISR G2 SRE
  - Cisco Prime Network Analysis Module for Nexus 1100 Series
  - Cisco Prime Network Analysis Module for WAAS Virtual Blade (VB)
- Cisco Prime Network Analysis Module Virtual Appliances
  - Cisco Prime Virtual Network Analysis Module (vNAM)

NAM support requires the following:

- Timing must be synchronized between the Prime Performance Manager gateway and the device where the Cisco NAM blade or appliance is installed.

- SNMP must be enabled on the device hosting the Cisco NAM blade or appliance.