Administrator Setup Tasks

The Cisco Prime Infrastructure administrator should plan on completing several initial setup tasks soon after the product is installed.

Related Topics

- Setting Up Operations Center
- Required Software Versions and Configurations
- Configuring Data Sources for Prime Infrastructure With Assurance
- Enabling Medianet NetFlow
- Enabling NetFlow and Flexible NetFlow
- Deploying Network Analysis Modules (NAMs)
- Installing Prime Infrastructure Patches

Setting Up Operations Center

Prime Infrastructure Operations Center is a licensed feature that allows you to manage multiple instances of Prime Infrastructure from a single instance. Before you can use Operations Center, you must first:

1. Activate your Operations Center license on the Prime Infrastructure server that will host Operations Center.
2. Enable single sign-on (SSO) on each of the Prime Infrastructure instances that you will manage using Operations Center.
3. Add the Prime Infrastructure instances to Operations Center.
4. (Optional) Disable the personal and global idle-user timeouts for Operations Center and all of its managed instances.
5. (Optional) Configure remote AAA using TACACS+ or RADIUS servers for Operations Center and all of its managed instances,

The Related Topics explain how to complete each of these tasks.

Related Topics

- Before You Begin Setting Up Operations Center
- Activating Your Operations Center License
- Enabling SSO for Operations Center

- Troubleshooting Operations Center SSO Issues
- Adding Prime Infrastructure Instances to Operations Center
- Disabling Idle User Timeouts for Operations Center
- Enabling AAA for Operations Center
- Operations Center Next Steps

Before You Begin Setting Up Operations Center

Before setting up Operations Center:

- Verify that the DNS entry for the Prime Infrastructure server that will host the Operations Center matches the host name configured on that server. For example: Running the commands **nslookup *ipaddress*** and **hostname** on the Prime Infrastructure server that will host the Operations Center should yield the same output.
- Ensure that all users who will access network information using Operations Center have both NBI Read and NBI Write access privileges. You can do this by editing these users' profiles to make them members of the "NBI Read" and "NBI Write" User Groups (see "Changing User Group Memberships" in Related Topics).
- By default, the maximum SSO login sessions for one user is five in Operation Center. This is also applicable for instances. Hence, ensure that the number of Active SSO Sessions does not exceed five, else the managed instances will go to unreachable state.
- Ensure that Prime Infrastructure is upgraded from 2.2.X to 3.0 before upgrading the Operations Center. Inline upgrading is also available for Operations Center.

Related Topics

- Setting Up Operations Center
- Changing User Group Memberships

Activating Your Operations Center License

Operations Center does not have a separate installation procedure. After you have installed Prime Infrastructure, you enable Operations Center by activating an Operations Center license on that installed server instance. The number of Prime Infrastructure instances you can manage using Operations Center depends on the license you have purchased.

Operations Center requires a **Cluster Base** License File and **Incremental** License File. For details, see the *Cisco Prime Infrastructure Ordering and Licensing Guide* (in Related Topics).

Step 1 Select **Administration > Licenses and Software Updates > Licenses**. The Licenses Summary page displays.

Step 2 From the left-hand navigation menu, select **Files > License Files**. The License Files page displays.

Step 3 Click **Add**. The Add a License File dialog box displays.

Step 4 Click **Choose File**.

Step 5 Navigate to your license file, select it, and then click **Open**.

Step 6 Click **OK**. Your license should now be listed in the Licenses > License Files page.

Step 7 Log out of Prime Infrastructure and then log back in. The login page that appears should display "Cisco Prime Infrastructure Operations Center", which indicates the license has been applied.

Related Topics

- Setting Up Operations Center
- *Cisco Prime Infrastructure Ordering and Licensing Guide*

Enabling SSO for Operations Center

Complete the following procedure as many times as needed to enable SSO:

1. First: On the Prime Infrastructure server that will host Operations Center. This server must act as the SSO server.
2. Then: On all the other Prime Infrastructure servers that the Operations Center will manage. These servers must act as the SSO clients.

For additional help, see the related topic, "Troubleshooting Operations Center SSO Issues".

Please note that you can configure more than one SSO server for Prime Infrastructure. However, the first SSO server you configure will always act as the system SSO server until it fails. In that case, authentication will fall back to the second SSO server, and so on.

Step 1 Select **Administration > Users > Users, Roles & AAA**. The AAA Mode Settings page displays.

Step 2 In the AAA Mode field, select the **Local** radio button and then click **Save**.

Step 3 From the left-hand navigation menu, click **SSO Servers** to open the SSO Servers page.

Step 4 Choose **Select a Command > Add SSO Server > Go**. The Add SSO Servers page displays.

Step 5 Enter the following information:

- **IP Address**: Enter either the IP address of the server on which you activated your Operations Center license (i.e., Operations Center IP).

  Note that you must be consistent in specifying either the IP address or the Domain Name across all of the Operations Center clients (that is, the managed instances of Prime Infrastructure) that you add to the SSO server. This is because the browser cookies that provide the Single Sign-On functionality are stored in the browser according to either the IP address or the Domain Name given here.
- **DNS Name**: DNS name of the server on which you activated the license. Enter the DNS name only when the forward and reverse DNS lookups are the same. Otherwise setup SSO with the Server IP Address.
- **Port**: The port used to log in to the SSO server. By default, port 443 is set. Do not change this value.
- **Retries**: The number of retries to attempt when logging into the SSO server. By default, this value is set to 1.
- **Certificate Type**: Select the type of SSL/TLS certificate that the SSO server uses. Select from either Self-Signed Certificate or Certificate Authority (CA) certificate type.

When you are finished, click **Save**. The server should now be listed on the Add SSO Servers page.

Step 6 From the left-hand navigation menu, select **AAA Mode Settings** to reopen the AAA Mode Settings page.

Step 7 Click the **SSO** radio button (if it is not already selected) and then click **Save**.

Step 8 After enabling SSO, log out of the instance of Prime Infrastructure on which you enabled SSO and then log back in.

On the login page for the Operations Center instance, you will see “Cisco Operations Center [SSO]”. After you log in, the product title displayed at the top of the page will be “Cisco Prime Infrastructure Operations Center”.

On the login page for each of the managed instances, you will see “Cisco Operations Center [SSO]”. After you log in, the product title will be “Cisco Prime Infrastructure”.

Related Topics

- Setting Up Operations Center
- Troubleshooting Operations Center SSO Issues

Troubleshooting Operations Center SSO Issues

As explained in “Enabling SSO for Operations Center”, you must enable single sign-on (SSO) such that the Operations Center server acts as the SSO server and the managed instances of Prime Infrastructure act as SSO clients. Here are some common SSO setup pitfalls and how you can avoid them:

- There are different ways to add the SSO server to the SSO client. Each requires a different level of DNS set up. If you are using:
  - Self-signed setting: This requires both forward and reverse DNS lookup of the SSO server from the SSO client. This means that if you take the Fully Qualified Domain Name (FQDN) of the SSO server and resolve it using DNS, you can take the resulting IP address, do a reverse lookup, and get the original FQDN.
  - CA-signed setting with IP addresses: Neither reverse nor forward DNS mappings are required.
  - CA-signed setting with domain names: Only forward DNS mapping (domain name to IP address) is needed.
- If you are using the self-signed setting: Verify that the DNS entry for the Prime Infrastructure server that will host the Operations Center matches the host name configured on that server. To do this, run **nslookup *ip-address,*** replacing ***ip-address*** with the IP address of your Operations Center server. Then log in to the admin console of the Operations Center server and run the **show running-config** command. Ensure that the output of these two commands matches.
- If you are using the self-signed setting: Access the Operations Center server using a browser and check that Common Name (CN) of the certificate matches the FQDN of the Operations Center server. The steps to follow vary with the browser you are using. For example, using Chrome:
  a. Click on the lock icon displayed at the far left in the browser’s URL box.
  b. Select **Certificate Information**.
  c. Expand the **Details** field to view the Common Name of the certificate. It must match the correct FQDN of the server. If the two do not match, the Prime Infrastructure administrator must regenerate the SSO certificate.
- When configuring SSO, leave the “Certificate Type” as “CA”. This will result in fewer checks to verify the certificate on the SSO client side
- Ensure that the SSO Server and clients are all added consistently. For example, use either the IP address or FQDN across all instances. Don’t mix and match these.

Once SSO is configured you can check to see if it is working as expected by logging in to Operations Center (the SSO server) and opening a new browser tab to access one of the Prime Infrastructure instances (an SSO client). SSO should automatically log you into the Prime Infrastructure instance automatically, without requiring you to re-authenticate.

If you are still having Operations Center SSO login and connection issues:

1. Download and examine related Prime Infrastructure logs and, where necessary, use enhanced logging to check for errors and timeouts (for details, see the related topics “Downloading and Emailing Error Logs” and “Changing Logging Options to Enhance Troubleshooting”). Be sure to look at the log files from both Operations Center (the SSO server) and the managed instances (SSO clients) of Prime Infrastructure. Log files of special interest to SSO and Operations Center are:
   - xmpNbiFw.log
   - xmpNbifwPerformance.log: Look at the response times for APIs dispatched from Operations Center to the managed instances.
   - cas.log
   - ncs-*.log
   - XmpUserMgmtRbac.log
   - usermgmt.log:
2. Adjust the values for cluster.timeout and cluster.connectionTimeout in the file /opt/CSCOlumos/conf/cluster.properties. These two properties have the following defaults:
   - cluster.timeout=40000: This is the timeout (in milliseconds) for all the requests dispatched from Operations Center.
   - cluster.connectionTimeout=5000: This is the timeout used when Operations Center tries to establish initial connections with the managed instances.

   If there is a high latency between Operations Center and the managed instances having connection issues, increasing these timeout limits can help.

   When you are finished changing these values, restart the Operations Center using the commands explained in “Restarting Prime Infrastructure” (see Related Topics).

Related Topics

- Enabling SSO for Operations Center
- Setting Up Operations Center
- Downloading and Emailing Error Logs
- Changing Logging Options to Enhance Troubleshooting
- Restarting Prime Infrastructure

Adding Prime Infrastructure Instances to Operations Center

Once you have configured SSO on Operations Center and the other Prime Infrastructure instances, you must add each of the Prime Infrastructure managed instances to Operations Center.

Prime Infrastructure 3.0 instances can be managed only in Prime Operations Center. Support for Prime Infrastructure 2.2.X (N-1 Version) instances will be provided in later releases.

Step 1 Log in to Prime Infrastructure Operations Center.

Step 2 Select **Monitor > Manage and Monitor Servers**.

Step 3 Click **Add**.

Step 4 Enter the IP address and port number of the instance of Prime Infrastructure that you want to manage using Operations Center. You may also enter an alias for the server. Then click **OK**.

By default, port 443 is set. Do not change this value.

Step 5 Repeat these steps to add other Prime Infrastructure servers, up to the license limit.

Related Topics

- Setting Up Operations Center

Disabling Idle User Timeouts for Operations Center

Be default, Prime Infrastructure automatically signs out all users whose sessions stay idle for too long. This feature is enabled by default to preserve network bandwidth and Prime Infrastructure processing cycles for active use.

This feature can be annoying for Operations Center users, who will typically have sessions opened not only with Operations Center, but with one or more of the instances of Prime Infrastructure that Operations Center is managing. Idleness in one of these sessions can force a global idle-user timeout for all the sessions, resulting in a sudden logout without warning.

To avoid this inconvenience, Prime Infrastructure administrators must:

1. Disable the global idle user timeout feature, as explained in “Changing the Global Idle Timeout” in Related Topics. Note that the administrator must disable this feature *separately*, on *each* of the Prime Infrastructure managed instances that Operations Center manages.
2. Instruct Operations Center users to disable the user-specific idle-user timeout feature for the Prime Infrastructure managed instances they access, as explained in “Changing Your Idle User Timeout” in Related Topics. Note that each Prime Infrastructure user must disable this feature *separately*, on *each* of the Prime Infrastructure managed instances they access.

Related Topics

- Setting Up Operations Center
- Changing the Global Idle Timeout
- Changing Your Idle User Timeout

Enabling AAA for Operations Center

Operation Center supports local authentication as well as remote AAA using TACACS+ and RADIUS servers. Using remote AAA is optional, but if you want to use it, you must first add a TACACS+ or RADIUS server to Operations Center. Follow this workflow:

1. On the Operations Center instance of Prime Infrastructure, add one or more TACACS+ or RADIUS servers to provide AAA services. For details, see “Adding TACACS+ Servers” or “Adding RADIUS Servers” in related topics. Remember that the shared secret configured on the TACACS+ or RADIUS server must match the shared secret you enter when adding this AAA server to Operations Center.
2. Set the AAA mode on the Operation Center instance, as explained in “Setting the AAA Mode”

Related Topics

- Setting Up Operations Center
- Adding TACACS+ Servers
- Adding RADIUS Servers
- Setting the AAA Mode

Operations Center Next Steps

When you have completed the setup tasks, you are ready to use Operations Center. See “Monitoring Multiple Prime Infrastructure Instances” for typical tasks you perform when using Operations Center.

Related Topics

- Monitoring Multiple Prime Infrastructure Instances
- Setting Up Operations Center

Required Software Versions and Configurations

To work with Prime Infrastructure, your devices must run at least the minimum required software versions shown in the list of supported devices. You can access this list using the Prime Infrastructure user interface: Choose **Help > Supported Devices**.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as explained in the related topics.

Related Topics

- Configuring SNMP
- Configuring NTP

Configuring SNMP

To ensure that Prime Infrastructure can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using Prime Infrastructure.
- Configure these same devices to send SNMP notifications to the Prime Infrastructure server.

Use the following Cisco IOS configuration commands to set read/write and read-only community strings on an SNMP device:

```
admin(config)# snmp-server community private RW
admin(config)# snmp-server community public RW
```

where ***private*** and ***public*** are the community strings you want to set.

After you set the community strings, you can specify that device notifications be sent as traps to the Prime Infrastructure server using the following Cisco IOS global configuration command on each SNMP device:

```
admin(config)# snmp-server host Host traps version community
notification-type
```

where:

- ***Host*** is the IP address of the Prime Infrastructure server.
- ***version*** is the version of SNMP that is used to send the traps.
- ***community*** is the community string sent to the server with the notification operation.
- ***notification-type*** is the type of trap to send.

You may need to control bandwidth usage and the amount of trap information being sent to the Prime Infrastructure server using additional commands.

For more information on configuring SNMP, see:

- The snmp-server community and snmp-server host commands in the *Cisco IOS Network Management Command Reference*.
- The "Configuring SNMP Support" section and the list of notification-type values in the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*.

If you are planning on implementing IPSec tunneling between your devices and the Prime Infrastructure server, be advised that you will not receive syslogs transmitted from those devices to the Prime Infrastructure server after implementing IPSec tunneling because IPSec does not support free-form syslogs. However, IPSec does support SNMP traps. To continue getting SNMP notifications of any kind from these devices, you need to configure your devices to send SNMP traps to the Prime Infrastructure server.

Configuring NTP

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Prime Infrastructure server. This includes all Prime Infrastructure-related servers: Any remote FTP servers that you use for Prime Infrastructure backups, secondary Prime Infrastructure high-availability servers, the Prime Infrastructure Plug and Play Gateway, VMware vCenter and the ESX virtual machine, and so on.

You specify the default and secondary NTP servers during Prime Infrastructure server installation. You can also use Prime Infrastructure's **ntp server** command to add to or change the list of NTP servers after installation. For details, see the section Connecting Via CLI in this Guide and the section on the **ntp server** command in the *Command Reference Guide for Cisco Prime Infrastructure*. Note that Prime Infrastructure cannot be configured as an NTP server; it acts as an NTP client only.

Failure to manage NTP synchronization across your network can result in anomalous results in Prime Infrastructure. Management of network time accuracy is an extensive subject that involves the organization's network architecture, and is outside the scope of this Guide. For more information on this topic, see (for example) the Cisco White Paper *Network Time Protocol: Best Practices*.

Configuring Data Sources for Prime Infrastructure With Assurance

If you are licensing the Prime Infrastructure Assurance features, you must complete pre-installation tasks so that Assurance can monitor your network interfaces and services. See Supported Assurance Data Sources for information about these tasks.

Supported Assurance Data Sources

Prime Infrastructure with Assurance needs to collect data from your network devices using the exported data sources shown in Table 2-1. For each source, the table shows the devices that support this form of export, and the minimum version of Cisco IOS or other software that must be running on the device to export the data.

Use Table 2-1 to verify that your network devices and their software are compatible with the type of data sources Prime Infrastructure uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum*. Your devices can run any later version of the same software or Cisco IOS release train.

You may also need to make changes to ensure that Prime Infrastructure can collect data using SNMP, as explained in Configuring SNMP.

Configuring Assurance Data Sources

Before installing Prime Infrastructure, you should enable the supported devices shown in Table 2-1 to provide Prime Infrastructure with fault, application, and performance data, and ensure that time and date information are consistent across your network. The following topics provide guidelines on how to do this.

Table 2-1 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
Catalyst 3750-X / 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP and UDP traffic	See the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure User Guide*.
Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure User Guide*. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**
Catalyst 4500	15.0(1)XO and 15.0(2)	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure User Guide*. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**
Catalyst 6500	SG15.1(1)SY	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure User Guide*. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**

Table 2-1 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions (continued)

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice & Video	To configure TCP, UDP, and ART, see the "Configuring NetFlow on ISR Devices" section in *Cisco Prime Infrastructure User Guide*. To configure Voice & Video, use this CLI template: **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon**
ISR G2	15.2(4) M2 or later, 15.3(1)T or later	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see the "Configuring Application Visibility" section in the *Cisco Prime Infrastructure User Guide*.
ASR	15.3(1)S1 or later	TCP and UDP traffic, application response time, Voice & Video, HTTP URL visibility	
ISR G3	15.3(2)S or later		

Enabling Medianet NetFlow

To ensure that Cisco Prime Infrastructure can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in Prime Infrastructure.
- Export the Medianet NetfFlow data to the Prime Infrastructure server and port.

Use a configuration like the following example to ensure that Prime Infrastructure gets the Medianet data it needs:

flow record type performance-monitor PerfMonRecord

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
collect application media bytes counter
```

```
  collect application media bytes rate
  collect application media packets counter
  collect application media packets rate
  collect application media event
  collect interface input
  collect interface output
  collect counter bytes
  collect counter packets
  collect routing forwarding-status
  collect transport packets expected counter
  collect transport packets lost counter
  collect transport packets lost rate
  collect transport round-trip-time
  collect transport event packet-loss counter
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect timestamp interval
  collect ipv4 dscp
  collect ipv4 ttl
  collect ipv4 source mask
  collect ipv4 destination mask
  collect monitor event
flow monitor type performance-monitor PerfMon
  record PerfMonRecord
  exporter PerfMonExporter
flow exporter PerfMonExporter
  destination PrInIP
  source Loopback0
  transport udp PiInPort
policy-map type performance-monitor PerfMonPolicy
  class class-default
! Enter flow monitor configuration mode.
  flow monitor PerfMon
! Enter RTP monitor metric configuration mode.
  monitor metric rtp
!Specifies the minimum number of sequential packets required to identify a stream as being
an RTP flow.
  min-sequential 2
! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring
metrics.
  max-dropout 2
! Specifies the maximum number of reorders allowed when sampling RTP video-monitoring
metrics.
  max-reorder 4
! Enter IP-CBR monitor metric configuration mode
```

```
  monitor metric ip-cbr
! Rate for monitoring the metrics (1 packet per sec)
  rate layer3 packet 1
interface interfacename
  service-policy type performance-monitor input PerfMonPolicy
  service-policy type performance-monitor output PerfMonPolicy
```

In this example configuration:

- *PrInIP* is the IP address of the Prime Infrastructure server.
- *PiInPort* is the UDP port on which the Prime Infrastructure server is listening for Medianet data (the default is 9991).
- *interfacename* is the name of the interface (such as GigabitEthernet0/0 or fastethernet 0/1) sending Medianet NetFlow data to the specified *PrInIP*.

For more information on Medianet configuration, see the *Medianet Reference Guide*.

Enabling NetFlow and Flexible NetFlow

To ensure that Prime Infrastructure can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces that you want to monitor.
- Export the NetFlow data to the Prime Infrastructure server and port.

As of version 2.1, Prime Infrastructure supports Flexible NetFlow versions 5 and 9. Note that you must enable NetFlow on each *physical* interface for which you want Prime Infrastructure to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to enable NetFlow on Cisco IOS devices:

```
Device(config)# interface interfaceName
Device(config)# ip route-cache flow
```

where *interfaceName* is the name of the interface (such as fastethernet or fastethernet0/1) on which you want to enable NetFlow.

Once NetFlow is enabled on your devices, you must configure exporters to export NetFlow data to Prime Infrastructure. You can configure an exporter using these commands:

```
Device(config)# ip flow-export version 5
Device(config)# ip flow-export destination PrInIP PiInPort
Device(config)# ip flow-export source interfaceName
```

where:

- *PrInIP* is the IP address of the Prime Infrastructure server.
- *PiInPort* is the UDP port on which the Prime Infrastructure server is listening for NetFlow data. (The default is 9991.)
- *interfaceName* is the name of the interface sending NetFlow data to the specified *PrInIP*. This will cause the source interface's IP address to be sent to Prime Infrastructure as part of NetFlow export datagrams.

If you configure multiple NetFlow exporters on the same router, make sure that only one of them exports to the Prime Infrastructure server. If you have more than one exporter on the same router exporting to the same destination, you risk data corruption.

Use the following commands to verify that NetFlow is working on a device:

```
Device# show ip flow export
Device# show ip cache flow
Device# show ip cache verbose flow
```

For more information on NetFlow configuration, see:

- *Cisco IOS Switching Services Configuration Guide, Release 12.1*
- *Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T*
- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*
- *Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting*

Deploying Network Analysis Modules (NAMs)

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- *Cisco Network Analysis Module Software 5.1 User Guide*—Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- *Cisco Network Analysis Module Deployment Guide*—See the section “Places in the Network Where NAMs Are Deployed”.

If your NAMs are deployed properly, then no other pre installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

Prime Infrastructure uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to Prime Infrastructure, not via a NAM. Exporting NetFlow data from any NAM to Cisco Prime Infrastructure will result in data duplication.

Enabling Performance Agent

To ensure that Prime Infrastructure can collect application performance data, use the Cisco IOS ***mace*** (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office and data center routers.

For example, use the following commands in Cisco IOS global configuration mode to configure a PA flow exporter on a router:

```
Router (config)# flow exporter mace-export
Router (config)# destination 172.30.104.128
Router (config)# transport udp 9991
```

Use commands like the following to configure flow records for applications with flows across the router:

```
Router (config)# flow record type mace mace-record
Router (config)# collect application name
```

```
Router (config)# collect art all
```

where *application name* is the name of the application whose flow data you want to collect.

To configure the PA flow monitor type:

```
Router (config)# flow monitor type mace mace-monitor
Router (config)# record mace-record
Router (config)# exporter mace-export
```

To collect traffic of interest, use commands like the following:

```
Router (config)# access-list 100 permit tcp any host 10.0.0.1 eq 80
Router (config)# class-map match-any mace-traffic
Router (config)# match access-group 100
```

To configure a PA policy map and forward the PA traffic to the correct monitor:

```
Router (config)# policy-map type mace mace_global
Router (config)# class mace-traffic
Router (config)# flow monitor mace-monitor
```

Finally, enable PA on the WAN interface:

```
Router (config)# interface Serial0/0/0
Router (config)# mace enable
```

For more information on configuring Performance Agent, see the *Cisco Performance Agent Deployment Guide*.

Installing Prime Infrastructure Patches

You may need to install patches to get your version of Prime Infrastructure to the level at which upgrade is supported.You can check the Prime Infrastructure version and patch version you are running by using the CLI commands **show version** and **show application**.

Different patch files are provided for each version of Prime Infrastructure and its predecessor products. Download and install only the patch files that match the version of your existing system and that are required before you upgrade to a later version. You can find the appropriate patches by pointing your browser to the Cisco Download Software navigator.

Before installing a patch, you will need to copy the patch file to your Prime Infrastructure server's default repository. Many users find it easy to do this by first downloading the patch file to a local FTP server, then copying it to the repository. You can also copy the patch file to the default repository using any of the following methods:

- cdrom—Local CD-ROM drive (read only)
- disk—Local hard disk storage
- ftp—URL using an FTP server
- http—URL using an HTTP server (read only)
- https—URL using an HTTPS server (read only)
- nfs—URL using an NFS server
- sftp—URL using an SFTP server
- tftp—URL using a TFTP server

Step 1 Download the appropriate point patch to a local resource in your environment:

a. With the Cisco Download Software navigator displayed in your browser, choose **Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Cisco Prime Infrastructure**.

b. Select the version of Cisco Prime Infrastructure that most closely matches the one you are currently using (for example, **Cisco Prime Infrastructure 3.0**).

c. Click **Prime Infrastructure Patches** to see the list of available patches for that version of the product.

d. Next to each patch that is required, click **Download**, then follow the prompts to download the file.

Step 2 Open a command-line interface session with the Prime Infrastructure server (see Connecting Via CLI in the *Cisco Prime Infrastructure Administrator Guide*).

Step 3 Copy the downloaded patch file to the default local repository. For example:

```
admin# copy source path/defaultRepo
```

Where:

- ***source*** is the downloaded patch file's location and name (for example: ftp://MyFTPServer/pi_9.3.1.0_update.tar.gz).
- ***path*** is the complete path to the default local backup repository, defaultRepo (for example: `/localdisk`)

Step 4 Install the patch:

```
admin# patch install patchFile Repositoryname
```

Where:

- ***patchFile*** is the name of the patch file you copied to /localdisk/defaultRepo
- ***Repositoryname*** is the name of the repository.

For example: `admin# patch install test.tar.gz defaultRepo`