CHAPTER 10

Operating and Monitoring the Network

Under the Operate tab, Prime Infrastructure provides tools to help you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.

Monitoring Dashboards

Prime Infrastructure automatically displays monitoring data in dashboards and dashlets. You can choose one of the following dashboards under **Operate > Monitoring Dashboard** to view summary information:

- Overview—Displays overview information about your network such as device counts, and the top 5 devices by CPU and memory utilization. From the overview dashboard, you can click on device or interface alarms counts to view detailed dashboards and alarms and events in order to help troubleshoot and isolate issues.
- Incidents—Displays a summary of alarms and events for your entire network, for a particular site, or for a particular device. By clicking on an item in the dashboard, you can view details about the alarm or event and troubleshoot the problem.
- Performance—Displays CPU and memory utilization information.
- Detail Dashboards—Displays network health summaries for sites, devices, or interfaces. The detailed dashboards allow you to see congestion in your network and gather detailed site, device, and interface information. For example, you can view detailed dashboards for a particular site to determine which devices have the most alarms, device reachability status for the site, etc.

You can change the information displayed in the dashboards as explained in Dashboards and Dashlets.

Table 10-1 describes where to find monitoring information in the Prime Infrastructure dashboards.

Table 10-1 Finding Monitoring Data

To View this Monitoring Data	Choose this Dashboard
Alarm information	**Operate > Monitoring Dashboard > Incidents**
CPU utilization	**Operate > Monitoring Dashboard > Performance**
Detailed device information	**Operate > Monitoring Dashboard > Detail Dashboards**
Detailed interface information	**Operate > Monitoring Dashboard > Detail Dashboards**
Device reachability status	**Operate > Monitoring Dashboard > Overview**

Table 10-1 Finding Monitoring Data

To View this Monitoring Data	Choose this Dashboard
Event information	**Operate > Monitoring Dashboard > Incidents**
Interface status, availability, and utilization information	**Operate > Monitoring Dashboard > Performance**
Licensing information	**Operate > Monitoring Dashboard > Overview**
Memory utilization	**Operate > Monitoring Dashboard > Performance**
Site information	**Operate > Monitoring Dashboard > Detail Dashboards**
Syslog sender information	**Operate > Monitoring Dashboard > Incidents**
Utilization statistics	**Operate > Monitoring Dashboard > Overview**

Configuring Monitoring Settings

You can define how Prime Infrastructure monitors the devices and interfaces in your network.

By enabling the Auto Monitoring option, you can have Prime Infrastructure monitor the availability, CPU, memory and temperature of all your network devices automatically. By default, Prime NCS (WAN) polls all devices in your network every 15 minutes for device-health data. Most users will want to enable Auto Monitoring.

You may want to avoid enabling Auto Monitoring if you have a very large network or Prime Infrastructure deployment, to avoid excessive polling traffic. In this case, you can leave Auto Monitoring disabled, and create one or more device groups containing your business-critical devices only. You may also want to create a version of the default device health monitoring template with a polling frequency appropriate for these devices. When you deploy the default or custom device health monitoring template, you can select to apply it to your business-critical device group only.

You can also enable deduplication, if applicable, for Cisco IOS Netflow and Cisco Prime Assurance. If you have multiple routers and switches that send netflow to the Cisco Prime Assurance server and multiple NAMs that Cisco Prime Assurance retrieves data from, Cisco Prime Assurance could receive the same traffic statistic more than once. You can enable deduplication so that Cisco Prime Assurance doesn't count the same metrics more than once.

Step 1 Choose **Administration > System Settings**, then select **Monitoring Settings**.

Step 2 Check the following options:

- **Auto monitoring** to have Prime Infrastructure monitor all devices and interfaces automatically.
- **Enable deduplication** to have Prime Infrastructure eliminate redundant data.

Device Work Center

From **Operate > Device Work Center**, you can view the device inventory and device configuration information. The Device Work Center contains general administrative functions at the top and configuration functions at the bottom as described in Table 10-2.

Table 10-2 Device Work Center Tasks

Task	Description	Location in Operate > Device Work Center
Manage devices	Add, edit, bulk import, and delete devices, and force data collection from devices.	Buttons located at the top of the Device Work Center.
View basic device information and collection status	View basic device information such as reachability status, IP address, device type, and collection status information.	Displayed in the top portion of the Device Work Center. Rest your cursor on the Collection Status cell and click on the icon to view errors related to the inventory collection.
Manage device groups	By default, Prime Infrastructure creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.	Displayed on the left pane of the Device Work Center. See Managing Device Groups for more information about creating and using device groups.
Add devices to sites	After you set up a site profile, you can add devices to the site. **Note** A device can belong to one site only.	**Add to Site** button located at the top of the Device Work Center. See Creating Site Profiles for more information about adding devices to sites.
View device details	View device details such as memory, port, environment, and interface information.	Choose a device in the Device Work Center, then click the **Device Details** tab at the bottom of the screen.
	View device information, status, and associated modules, alarms, neighbors, and interfaces. See Getting Device Details Using the 360° View for more information.	Rest your cursor on a device IP address and click the icon that appears.
Create and deploy configuration templates	You can create and deploy configuration templates for the selected device. You can also preview the CLI that will be deployed to the device.	Click the **Configuration** tab at the bottom of the Device Work Center.\ See Configuring Features on a Device for more information about configuring features on a device.
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click the **Configuration Archive** tab at the bottom of the Device Work Center.
View software images	View details about the image on the selected device, the recommended software image for the device, and the latest software image operations for a device.	Click the **Image** tab at the bottom of the Device Work Center.

Monitoring Jobs

Choose **Administration > Jobs Dashboard** to view the status of jobs and to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs for which you are interested

- View details of the most recently submitted job
- View job execution results
- Modify jobs including deleting, editing, running, canceling, pausing, and resuming jobs

Note Internally scheduled jobs are not displayed in the Jobs Dashboard.

If a job fails, you can get troubleshooting information from the Jobs Dashboard. When you expand a job to view its details, click the History tab, and rest your cursor over the Status field. The results window displays troubleshooting information that can help you determine why the job failed.

Monitoring Using Reports

Prime Infrastructure reporting helps you monitor the system and network health as well as troubleshoot problems. Reports can be run immediately or scheduled to run at a time you specify. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on Prime Infrastructure for later download or e-mailed to a specific e-mail address.

Choose **Report > Report Launch Pad** to view the list of available reports.

Tip Rest your cursor on the information icon next to the report type to view report details.

Creating Reports

Step 1 Choose **Report > Report Launch Pad**.

Step 2 Click **New** next to the report you want to create.

Step 3 Enter report details, then click a save option.

Using Packet Capture for Monitoring and Troubleshooting

Prime Infrastructure allows you to run capture traffic in your network to help monitor network usage, gather network statistics, and analyze network problems.

Step 1 Choose **Operate > Packet Capture**, then click **Create**.

Step 2 Specify the required capture session parameters, then click **Create**.

Diagnosing Site Connectivity Issues and Comparing Configurations

You can use the Prime Infrastructure dashboards to monitor your network and locate problematic devices in your network, and then use the Device Workcenter to change the device configuration.

Step 1 Choose **Operate > Detailed Dashboards**, choose the site for which you are experiencing connectivity issues, then click **Go**.

Step 2 Check the data reported under Device Reachability Status and Top *N* Devices with Most Alarms to determine the source of the issue.

Step 3 Click on the name of the device for which you see the most alarms.

Step 4 From the 360-degree view of the device, click the Alarm Browser icon to view the alarms for that device. Expand the alarm to view details for the alarm.

Step 5 To compare the configuration on the device to a previously known good configuration, choose **Operate > Device Work Center**, then select the device whose configuration you want to change.

Step 6 Click the Configuration Archive tab, expand the arrow to view additional options, then select the configuration type and a configuration against which to compare.

Step 7 Change or rollback the configuration. See Rolling Back Device Configuration Versions for more information.