CHAPTER 12

Performance Monitor Administration

Effective network management requires the fastest possible identification and resolution of events that occur on mission-critical systems.

Performance Monitor administrative options enable you to configure event detection that identifies, displays, and logs events proactively, according to formula-based and user-configurable thresholds.

The following table describes the administrative options that you access from within Performance Monitor.

Table 12-1 Performance Monitor Administrative Options

Option	Description
Notifications	Configure and enable notification for monitored services through SNMP traps, Syslog entries, or email when a performance event or failure occurs. See Working with Notifications, page 12-1.
Events	Configure and enable thresholds to generate performance or failure events of any priority. See Working with Event Thresholds, page 12-7.
System Parameters	Configure and enable polling intervals and truncation intervals for available data types. See Working with System Parameters, page 12-9.
Logs	Display and export debugging log files, or display a summary of disconnected RAS user sessions. See Working with Logs, page 12-10.
My Profile	Select a page that displays by default when you start Performance Monitor. See Selecting a Default Page, page 12-12.

Working with Notifications

Performance Monitor can notify you automatically when important conditions meet or exceed the performance parameters that you define globally or for a specific service. Performance Monitor sends separate notifications for each notification type that you configure.

The following topics explain notifications and how to configure them:

- Understanding Supported SNMP Traps and Syslog Messages, page 12-2
- Configuring Notification Settings, page 12-3
- Understanding Supported Event Types for Notifications, page 12-5

Understanding Supported SNMP Traps and Syslog Messages

Notifications require that Performance Monitor receive essential information from monitored devices, which provide that information by means of SNMP traps, Syslog messages, and device polling. For additional information, see Receiving SNMP Traps, page 2-15.

Performance Monitor can process the following kinds of SNMP traps:

Source Device	Supported SNMP Traps and Syslog Messages
ASA devices	• ASA-4-113019 • ASA-7-713052
CSM service module	• Real server state transition • Interface operation status
VPN service module	• Policy added • Policy deleted • Cryptomap added • Cryptomap deleted • Cryptomap attached • Cryptomap detached • Tunnel start • Tunnel stop • Interface operational status
VPN router	• Policy added • Policy deleted • Cryptomap added • Cryptomap deleted • Cryptomap attached • Cryptomap detached • Tunnel start • Tunnel stop • Interface operational status

Performance Monitor can process the following kinds of Syslog messages:

Source Device	Supported Syslog Message Types
VPN 3000 concentrator	• IKE-5-120 • AUTH-5-28
PIX firewalls	• PIX-1-104001 • PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • PIX-4-113019 • PIX-7-713052
Firewall service modules	• PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • FWSM-4-113019 • FWSM-7-713052

Configuring Notification Settings

Performance Monitor can notify you automatically when important conditions meet or exceed the performance parameters that you define globally or for a specific service. Performance Monitor sends separate notifications for each notification type that you configure.

Three notification levels exist:

- Global—all events for all service types.
- Service—all events for one service type.
- Event—a specific event for a specific service type.

Note If you configure a notification setting globally and duplicate it at either the service level or the event level, you will receive duplicate notifications. You will also receive duplicate notifications if you configure notification settings at the event level that overlap with notification settings you configure at the service level.

Before You Begin

- Make sure that you have configured CiscoWorks Common Services to use an email server. See Setting Common Services to Use Email, page 2-15.
- Make sure that you have the correct privileges to configure notification settings. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select **Admin > Notifications**.

Step 2 Select the type of notification you want to configure in the tree:

- **Global**—To configure Global notifications.
- A service type (**Firewall**, **Load Balancing**, **Remote Access VPN**, **SSL**, **Site-to-Site VPN**)—To configure notifications for all event types for that service.
- An event type within a service type (the lowest nodes in the tree, for example, CPU Usage)—To configure notifications only for that event type. See Understanding Supported Event Types for Notifications, page 12-5.

Tip Your selection in the tree refreshes the screen, but your selection is not retained in the tree. To see what kind of notification you are configuring, you must look at the title in the right pane above the Email Recipients list. This title will say "Global Notifications," "Service Notifications: *Service Type*," or "Event Notifications: *Event Type*."

Step 3 Perform any of the tasks explained in Table 12-2.

Notification Configuration Procedures

Table 12-2 Notification Configuration Procedures

Task	Procedure
Add an email recipient.	1. In the Email Recipients area, click **Add**. 2. In the Edit Email Recipients window, enter one email address in the Email Address text box. 3. Define the severity range of events for which to send email messages: Select options in the From Priority list and the To Priority list, where P1 is a problem of high severity, P5 is a problem of low severity, and OK is a resolved problem. The severity level selection in the From area must be lower than the level selection in the To area. 4. Click **Apply**. The Edit Email Recipients window closes. The Notifications page is refreshed and the recipient that you define appears in the Email Recipients list.

Table 12-2 Notification Configuration Procedures (continued)

Task	Procedure
Add an SNMP trap recipient.	1. In the Trap Recipients area, click **Add**. 2. In the Edit Trap Recipients window, enter the monitored device IP address or DNS hostname in the Host text box. 3. Enter the device SNMP port number in the Port text box. 4. Enter the device read community string in the Community text box. 5. Click **Apply**. The Edit Trap Recipients window closes. The Notifications page is refreshed and the recipient that you define appears in the Trap Recipients list.
Add a Syslog recipient.	1. In the Syslog Recipients area, click **Add**. 2. In the Edit Syslog Recipients window, enter one Syslog hostname or IP address in the Host text box. 3. Enter the device port number in the Port text box. 4. Click **Apply**. The Edit Syslog Recipients window closes. The Notifications page is refreshed and the recipient that you define appears in the Syslog Recipients list.
Edit a recipient.	1. Select the recipient to edit and click the Edit button for that area. 2. Change settings as appropriate, then click **Apply**.
Delete a recipient (disable notification).	Select the recipient to delete and click the Delete button for that area. **Note** Deletions take effect immediately. There is no undo function.
Configure thresholds for an event type	If you select a specific event type, you can configure the threshold settings for that event notifications by clicking the Threshold button below the recipients lists. For more information on configuring thresholds, see Working with Event Thresholds, page 12-7.

Understanding Supported Event Types for Notifications

Notifications support more than 40 different event types, categorized by service type (see Table 12-3).

Table 12-3 Notification Event Types

Monitored Service	Supported Event Types
Firewall	CPU Usage
	Command Replication
	Device Accessible via Https
	Device Accessible via Snmp
	Failover
	Failover Cable
	Fragment Size
	HA Other
	Interface State
	Memory Usage
	New Connections
	Regular Translation
	Translation Slot
Load Balancing	Connection Failure
	Created Connection Rate
	Dropped Connection
	Interface Status
	Real Server Status
Remote Access VPN	Bandwidth Usage
	CPU Usage
	Device Accessible via Snmp
	Device Load
	Inbound Connection Failures
	Interface Status
	Packet Drop
	SEP Module Packet Drop
	SEP Module Status
SSL	CPU Usage
	Device Accessible via Https
	Memory Usage
	SSL Errors

Table 12-3 Notification Event Types

Monitored Service	Supported Event Types
Site-to-Site VPN	CPU Usage Connection Failures Crypto Map Binding Crypto Map Change Crypto Packet Drops Device Accessible via Https Device Accessible via Snmp ISAKMP Policy Change Interface Status Memory Usage Packet Drop Tunnel Status You might receive a flood of email messages about your DMVPN spoke-to-spoke tunnels if you do *all* of the following: • Configure DMVPN to use a full mesh topology that supports spoke-to-spoke sessions. • Configure a threshold for site-to-site VPN tunnel down events. • Schedule automatic email notification for those events. Site-to-site tunnels are dynamic and have short lives by design, which include many tunnel down events. If this email flood problem affects you, we recommend that you either disable email notification or configure Performance Monitor to monitor hubs only.

Working with Event Thresholds

When you create a threshold, you:

- Define the boundaries of operational states (such as OK, Degraded, and Overloaded) for a performance metric or failure metric in a specific service.
- Specify the number of consecutive polling cycles during which an operational state must recur before records are updated.
- Associate a priority level with each possible operational state for a specific metric (for display and user notification purposes).

Although the thresholds that you define use different services, metrics, and states, every threshold definition follows the same basic workflow.

Tip When conditions exceed or fall below the thresholds that you define, Performance Monitor records an alarm that you can display and interpret in the relevant Event Browser. If applicable, you can also display critical problems in the Critical Problems summary. See Working in an Event Browser, page 3-12 and Working in the Critical Problems Summary, page 4-2.

Before You Begin

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select **Admin > Events**.

Step 2 Select a service from the TOC.

Note Although IOS routers are displayed in the Firewall Devices page if they are configured with inspection policies, you must set event thresholds for routers by selecting the site-to-site VPN service from Admin > Events. Setting event thresholds for the firewall service from the Threshold Configuration page does not apply to routers.

Step 3 Scan the entries in the Events list until you locate the performance metric or failure metric for which you plan to configure thresholds, then select the radio button in the relevant row.

Step 4 Click **Threshold**.

Tip You can also configure thresholds for an event if you select **Admin > Notifications**, then select an event and click **Threshold**.

A Threshold Configuration page appears.

- If you select a failure metric, two opposite State Name values (such as Up and Down) appear in the Threshold Configuration page. Or, one extreme state value (such as OK) precedes multiple intermediate state values.
- If you select a performance metric, a range of State Name values (such as OK, Medium, and High) appears in the Threshold Configuration page; each value is associated with an upper and lower percentage in a range.

Step 5 Select the Enable check box.

You must select the Enable check box, or you cannot define values in a Threshold Configuration page.

Step 6 Do one of the following:

- If you see two opposite values (such as the benign *Up* and the problematic *Down*) in the State Name area, specify:
  - The event priority level for the problematic state.
  - The number of polling cycle failures that trigger, and the number of successes that clear, the event associated with the problematic state in the **Repetitions before State Change** field.

- If you see a range of three values in the State Name area, specify the upper and lower threshold percentages, polling cycle repetitions, and priority levels for each of the three values in the range. For example, you could select 10% as the lower threshold boundary for the intermediate state. (Your selection would, in such a case, be applied automatically as the upper threshold percentage for the benign state.)

Note When you configure thresholds for a performance metric, the lower threshold percentage for a benign state is always zero (0%), and the priority is always *OK*. The upper threshold percentage for a problematic state is always 100%. You cannot change these values.

Step 7 Do one of the following:

- To discard your selections and return to the Events page, click **Cancel**.
- To save and implement your selections, click **Apply**.
- To reset all values to their default settings and remain in the Threshold Configuration page, click **Default**.

Working with System Parameters

You can configure polling intervals, truncation intervals, and user session data storage settings.

Before You Begin

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select **Admin > System Parameters**.

Step 2 Configure the desired settings as explained in Table 12-4. The table shows the minimum and maximum values allowed for each setting, and the default for the setting. To return all values to their defaults, click the **Default** button.

System Parameters

Table 12-4 System Parameter Settings

Row Name	Optional Task	Procedure
Polling Interval (min)	Configure polling intervals.	Select an option from the list to specify the number of minutes between polls, then click **Apply**.
Hourly aggregated data is kept for (days)	Configure the truncation interval for hourly data.	Select an option from the list to specify the number of days for which hourly data is retained, then click **Apply**.

Table 12-4 System Parameter Settings (continued)

Row Name	Optional Task	Procedure
Daily aggregated data is kept for (days)	Configure the truncation interval for daily data.	Select an option from the list to specify the number of days for which daily data is retained, then click **Apply**.
Weekly aggregated data is kept for (days)	Configure the truncation interval for weekly data.	Select an option from the list to specify the number of days for which weekly data is retained, then click **Apply**.
Monthly aggregated data is kept for (days)	Configure the truncation interval for monthly data.	Select an option from the list to specify the number of days for which monthly data is retained, then click **Apply**.
Event data is kept for (days)	Configure the truncation interval for event history data.	Select an option from the list to specify the number of days after which the event history truncates, then click **Apply**.
Task data is kept for (days)	Configure the truncation interval for task history data.	Select an option from the list to specify the number of days after which the task history truncates, then click **Apply**.
User Session Polling Interval (hours)	Configure the user session polling interval.	Select an option from the list to specify the number of hours between polls, then click **Apply**.
User Session Report data is kept for (days)	Configure the truncation interval for user session data.	Select an option from the list to specify the number of days after which the user session report truncates, then click **Apply**.
Logout User Audit Trail data is kept for (months)	Configure the truncation interval for user audit trail data.	Select an option from the list to specify the number of months after which the user audit trail truncates, then click **Apply**.

Working with Logs

In the unlikely event that you have problems with Performance Monitor itself, you can display or download Performance Monitor debugging log files to assist TAC in resolving the problems.

You can also display an audit trail that describes the VPN sessions of every RAS user whom you (or your colleagues) have logged out.

Before You Begin

Make sure that you have the correct privileges to use this option. You must be either a System Administrator or a Network Administrator to terminate a user session. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select **Admin > Logs**.

Step 2 Select an option from the TOC:

- Click **Debugging Log Files** to display a list of the logs used in troubleshooting Performance Monitor, including their location on the server and current size. The following debugging logs are available:
  - faults.log—The *Faults Log* describes historical fault data.
  - job.log—The *Job Log* describes historical Performance Monitor jobs.
  - polling.log—The *Polling Log* displays historical device polling data.
  - validation.log—The *Validation Log* displays historical device validation data.
  - mcpui.log—The *Monitoring Center for Performance User Interface Log* describes recent user interface operations.
- Click **Logout User Audit Trail** to display statistics about the RAS VPN users whom you (or your colleagues) have logged out. Table 12-5 describes terminated user sessions.

Note The user logout feature is described in Chapter 5, "Monitoring Remote Access VPN Services."

Step 3 (**Optional**) If you selected Debugging Log Files from the TOC, click a radio button to select a log, then do one of the following:

- To view an HTML version of the log, click **View** .
- To save a local copy of the log, click **Download** and then in the window that appears, select **File > Save As** to save the log as a text file or an HTML file.

  You can click **Refresh** while displaying a log to display information from the most recent polling cycle.

Reference

Table 12-5 Logout User Audit Trail

Element	Description
Administrator Name column	Displays the CiscoWorks username of the user who ended (or tried to end) the described VPN session. **Note** You must be either a System Administrator or a Network Administrator to terminate a user session. See Understanding User Permissions, page 3-2.
Status column	States either that the forced logout succeeded or failed.
Error Message column	In cases of failure, displays the relevant error message. **Note** Some failures might occur as a result of unknown errors. In those cases, Performance Monitor displays no text in this column.
Time column	Displays a timestamp that indicates when the described VPN session ended.
Logged Out User column	Displays the username for the terminated VPN session.

Table 12-5 Logout User Audit Trail (continued)

Element	Description
User Group column	States the name of the VPN 3000 user group associated with the RAS user whose session was terminated.
Client IP Addr column	Displays the IP address from which the described RAS user connected to the VPN.
Protocol column	Identifies the protocol of the described VPN session.
VPN3K Device column	Displays the DNS name or IP address of the VPN 3000 concentrator from which the RAS user was disconnected.
Traffic In column	Displays the number of inbound bytes.
Traffic Out column	Displays the number of outbound bytes.
Connection Duration column	Displays the total duration (in seconds) of the VPN tunnel, before its disconnection.
Throughput (kbps) column	Displays the averaged throughput speed in the VPN tunnel, before its disconnection.

Selecting a Default Page

You can select a page to display by default when you start Performance Monitor. The default is Summary > Critical Problems.

Procedure

Step 1 Select **Admin > My Profile**.

Step 2 Click the name of a page in the selection tree to select that page, then click **Apply**.

The page that you select is displayed first the next time you start Performance Monitor.